Open Source Intelligence Methods and Tools

Практическое руководство по онлайн-разведке

Nihad A. Hassan Rami Hijazi

Apress®

Open Source Intelligence Methods and Tools

A Practical Guide to Online Intelligence

Nihad A. Hassan
Rami Hijazi

Apress®

Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence

Nihad A. Hassan
New York, USA

Rami Hijazi
Mississauga, Ontario, Canada

ISBN-13 (pbk): 978-1-4842-3212-5 ISBN-13 (electronic): 978-1-4842-3213-2
https://doi.org/10.1007/978-1-4842-3213-2 Library of Congress Control Number: 2018948821

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Rita Fernando

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springersbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com/ rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484232125. For more detailed information, please visit www.apress.com/source-code.

Printed on acid-free paper

To my mom, Samiha, thank you for everything.

Without you, I'm nothing.

—Nihad A. Hassan

Содержание

Об авторах

Нихад А. Хасан является независимым консультантом по информационной безопасности, экспертом по цифровой криминалистике и кибербезопасности, онлайн-блогером и автором книг. Он уже более десяти лет активно проводит исследования в различных областях информационной безопасности и разработал многочисленные образовательные курсы по кибербезопасности и технические руководства. Он выполнил несколько технических консультаций по вопросам безопасности, связанных с архитектурой безопасности, тестированием на проникновение, расследованием компьютерных преступлений и киберразведкой с открытым исходным кодом (OSINT). Нихад является автором четырех книг и десятков статей по информационной безопасности для различных глобальных изданий. Он также любит участвовать в подготовке кадров по вопросам безопасности, образовании и мотивации. Его текущая работа сосредоточена на цифровой судебной экспертизе, антикриминалистических методах, цифровой конфиденциальности, и кибер OSINT. Он освещает различные темы информационной безопасности и связанные с этим вопросы в своем блоге по безопасности на www.DarknessGate.com а недавно запустил специальный сайт для ресурсов разведки с открытым исходным кодом на www.OSINT. ссылка. Нихад имеет степень бакалавра наук в области компьютерных наук в Университете Гринвича в Соединенном Королевстве.
Дополнительную информацию вы можете посмотреть в Twitter (@DarknessGate), а так же в LinkedIn по адресу https://www.linkedin.com/in/darknessgate.

Рами Хиджази имеет степень магистра в области информационных технологий (информационная безопасность) в Университете Ливерпуля. В настоящее время он работает в MERICLER Inc., образовательной и корпоративной учебной фирме в Торонто, Канада. Рами является опытным ИТ-специалистом, который читает лекции по широкому кругу вопросов, включая объектно-ориентированное программирование, Java, электронную коммерцию, гибкую разработку, проектирование баз данных и анализ обработки данных. Рами также работает в качестве консультанта по информационной безопасности, где он участвует в проектировании систем шифрования и беспроводных сетей, обнаружении вторжений и отслеживании нарушений данных, а также предоставлении рекомендаций по планированию и развитию ИТ-отделов, касающихся планирования на случай непредвиденных обстоятельств.

О техническом рецензенте

Реем Наддар имеет степень бакалавра наук в области математики в Университете Далхаузи и работает в индустрии анализа данных с 2006 года. Она имеет значительный опыт в разработке и реализации решений, которые решают сложные бизнес-проблемы, связанные с крупномасштабным хранением данных, аналитикой в реальном времени, архитектурой программного обеспечения и решениями для отчетности. Она использует передовые инструменты и методы при внедрении быстрого и эффективного сбора данных, включая обработку больших данных, используемую глобальными практиками.

Reem работал в крупных корпорациях и зафрахтованных банках в Канаде как в качестве подрядчика, так и в качестве постоянного сотрудника. Она любит проекты с открытым исходным кодом (OSINT), где она принимает различные рамки и процессы для захвата, преобразования, анализа и хранения терабайт структурированных и неструктурированных данных, собранных из общедоступных источников.

Благодарность

Я начинаю с благодарности Богу за предоставленную мне дар писать и конвертировать мои идеи во что-то полезное. Без Божьего благословения я бы ничего не смог.

Я хочу поблагодарить дам из Apress: Сьюзен, Риту и Лору. Я был рад работать с вами и очень ценю ваши ценные отзывы и поощрение.

Специально, редактора отдела закупок Сюзан Макдермотт, Благодарим Вас за веру в идею моей книги и за вашу честную поддержку до и во время процесса написания. А также редактора проекта Риту Фернандо, вы очень помогли мне во время написания книги. Вы сделали авторство этой книги радостным путешествием. Еще редактора разработки Лору Берендсон, Большое спасибо за вашу прилежную и профессиональную работу в производстве этой книги.

Я также хочу поблагодарить всех сотрудников Apress, которые работали за кулисами, чтобы сделать эту книгу возможной и готовой к запуску. Я надеюсь, что вы будете продолжать свою отличную работу в создании высокоценных книг компьютерной тематики. Ваша работа высоко ценится.

—НихадА. Хасан

Введение

Open Source Intelligence Methods and Tools основное внимание уделяется созданию глубокого понимания того, как использовать методы, методы и инструменты разведки с открытым исходным кодом (OSINT) для получения информации из общедоступных онлайн-источников для поддержки анализа разведки. Собранные данные могут быть использованы в различных сценариях, таких как финансовые, криминальные и террористические расследования, а также в более регулярных задачах, таких как анализ бизнес-конкурентов, проведение фоновых проверок и получение разведданных о физических и юридических лицах. Эта книга также улучшит ваши навыки в получении информации в интернете из surface web, deep web и darknet.

Многие оценки показывают, что 90 процентов полезной информации, получаемой разведывательными службами, поступает из открытых источников (другими словами, из источников OSINT). Сайты социальных сетей открывают многочисленные возможности для проведения расследований из-за огромного количества полезной информации, размещенной в одном месте. Например, вы можете получить очень много Open Source Intelligence Methods and Tools это незаменимое руководство для тех, кто несет ответственность за сбор онлайн-контента из общедоступных данных, и это обязательная ссылка для любого случайного пользователя Интернета, который хочет углубиться в Интернет, чтобы увидеть, какую информацию он содержит.

Целевая аудитория

Следующие типы людей извлекут выгоду из этой книги:

- Пентесторы
- Криминалисты
- Разведывательные службы
- Военнослужащие
- Правоохранительные органы
- Учреждения ООН и некоммерческие организации
- Коммерческие предприятия
- Специалисты по управления рисками
- Журналисты
- Академические исследователи
- Студенты Университетов
- И пользователи кто хочет использовать ресурсы интернета более эффективно.

Чем книга не является

Эта книга не посвящена истории разведки с открытым исходным кодом, и в ней подробно не обсуждаются правовые вопросы личной разведки в Интернете. Мы не будем говорить о политике и правилах, регулирующих разные страны или организации бизнеса. Хотя некоторые из этих вопросов кратко обсуждаются в главе 1, главная цель этой книги - создать руководство для поддержки всех типов исследований. Вы можете читать главы в любом порядке, потому что каждая

глава считается изолированным блоком, в котором подробно обсуждается тема главы.

Краткое содержание

Вот краткое описание содержания каждой главы:

- Глава 1, “Эволюция разведки с открытым исходным кодом”: В этой главе мы познакомим вас с термином OSINT и объясним, как он развивался с течением времени. Мы представляем различные стороны, заинтересованные в использовании общедоступных данных и выгоды, полученные от этого. Мы включаем некоторую техническую информацию о методах онлайн-сбора и связанных с этим проблемах, а также юридические аспекты при сборе данных из общедоступных источников.

- Глава 2, “Введение в онлайн-угрозы и контрмеры”: В этой главе мы научим вас всему, что вам нужно знать, чтобы оставаться в безопасности во время работы в Интернете.Эти знания необходимы при проведении расширенных поисков в Интернете, чтобы избежать отслеживания, так как с помощью передовых поисковых операторов и других методов поиска OSINT которые могут привлечь внимание в Интернете и могут быть перехвачены другой стороной .

- Глава 3, “Скрытый интернет”: Эта глава посвящена раскрытию секретов невидимой паутины, которая содержит как темную сеть, так и глубокую паутину. Эти знания имеют важное значение, поскольку скрытый интернет содержит огромное количество ценной информации, к которой должен иметь доступ любой специалист по кибербезопасности.

- Глава 4, “Методы поиска”: В этой главе мы покажем вам, как использовать передовые методы поиска с помощью типичных поисковых систем, таких как Google и Bing, чтобы найти что-нибудь в Интернете. Мы также освещаем другие специализированные поисковые системы для изображений, видео, новостей, веб-каталогов, файлов и FTP.

- Глава 5, “Социальная медиа разведка": В этой главе мы покажем вам, как использовать широкий спектр инструментов и методов для сбора информации о конкретном человеке или организации из социальных медиа сайтов. Например, с помощью Facebook вы можете собирать информацию

о людях по всему миру. Другие крупные технологические компании, такие как Google и Microsoft, владеют огромными базами данных информации о своих пользователях. Большое количество информации публикуется публично на этих сайтах, и эта глава научит вас, как искать людей, в том числе их отношения, имена, адреса и связи (и взаимодействия) с другими людьми на социальных сайтах, чтобы сформулировать полный профиль о вашей цели.

- Глава 6, “Поисковые машины и публичные записи”: Здесь мы перечислим конкретные поисковые системы и другие общественные ресурсы для поиска имен людей и получения подробной информации о них. Вы научитесь использовать различные критерии обратного поиска, чтобы найти людей в Интернете, таких как записи о рождении, адреса почты, резюме, сайты знакомств, электронная почта, телефонные номера, предыдущие измененые имена пользователей, и многое другое. Мы также покрываем государственные ресурсы, такие как жизненно важные записи, налоговые отчеты, криминальная информация и другие публичные источники, которые можно использовать для получения информации о людях и организациях.
- Глава 7, “Онлайн Карты”: В этой главе рассказывается о том, как использовать Google Maps и другие бесплатные службы геолокации для исследования геолокации информации, полученной о целевых людей.
- Глава 8, “Технический Footprinting”: В этой главе рассказывается о том, как собирать техническую информацию о целевом веб-сайте и сетевой системе в пассивном режиме для поддержки вашей OSINT разведки.
- Глава 9, “Что дальше?”: В этой главе рассматривается процесс OSINT и его будущие тенденции.

Вебсайт ссылок книги

В этой книге мы перечислим сотни онлайн-сервисов, которые помогают собирателям OSINT собирать и анализировать информацию. Мы все знаем о постоянно меняющейся природе Web, хотя; новые сайты запуска и другие закрываются ежедневно, так что некоторые ссылки не смогут работать к тому времени, когда вы будете читаете это. Чтобы предотвратить это и избежать принятия части этой книги бесполезной после публикации, мы создали

специальный веб-сайт, где мы предлагаем цифровой список всех ссылок, упомянутых в этой книге в дополнение к многим другим ресурсам, которые просто не вписываются в печатных версиях. Мы сделаем все возможное, чтобы сохранить этот сайт обновляется и постоянно работать, чтобы добавить новый полезный контент OSINT, который отражает улучшения в этой области. Мертвые ссылки будут удалены или обновлены, так что содержание этой книги будет оставаться актуальным в течение многих лет в будущем. Смотри www.OSINT.link.

Комментарии и вопросы

Чтобы прокомментировать или задать технические вопросы об этой книге, отправьте по электронной почте nihad@protonmail.com. Для получения дополнительных ссылок на эту тему, инструментов компьютерной безопасности, учебников и других связанных с этим вопросов, проверить блог автора на www.DarknessGate.com.

Глава 1

Эволюция OSINT

После окончания "холодной войны" глобальные общества стали более открытыми, а революция в области Интернета и его широкое использование превратили мир в маленькую деревню. Раскрытие сети Интернет для миллиардов людей во всем мире для общения и обмена цифровыми данными сместило весь мир в то, что в настоящее время является информационным веком. Эта трансформация в цифровую эпоху принесла огромные выгоды нашему обществу; однако скорость и масштабы преобразований также вызвали различные виды рисков. Например, киберпреступники, террористические группы, репрессивные режимы и всевозможные злонамеренные субъекты эффективно используют Интернет для совершения своих преступлений. Исследование компании Juniper Research предсказывает, что киберпреступность будет стоить предприятиям более $2 трлн к 2019 году, поэтому эти риски побуждают правительства инвестировать в разработку инструментов и методов разведки с открытым исходным кодом (OSINT) для противодействия текущим и будущим проблемы кибербезопасности.

OSINT относится ко всей информации, которая находится в открытом доступе. Конкретной даты, когда термин OSINT был впервые предложен, не имеется; однако, относительный термин, вероятно, использовался в течение сотен лет для описания акта сбора разведданных путем использования общедоступных ресурсов.

Соединенные Штаты по-прежнему лидируют в мире в области разведки, с огромными ресурсами, выделенными правительством США на свои разведывательные службы, которые позволяют ему создавать сложные программы наблюдения для сбора и анализа большого объема данных, охватывающих все основные разговорные языки. Это делает наше обсуждение истории OSINT в значительной степени зависит от истории США, хотя во время холодной войны многие страны также разработали возможности OSINT для получения разведданных. Тем не менее, ни одна другая страна не достигла уровня программ США.

N. A. Hassan and R. Hijazi, *Open Source Intelligence Methods and Tools*, https://doi.org/10.1007/978-1-4842-3213-2_1

Министерство обороны США (МО) определяет OSINT следующим образом:

"Разведка с открытым исходным кодом (OSINT) — это разведка, которая производится на основе общедоступной информации и собирается, эксплуатируется и распространяется своевременно для соответствующей аудитории с целью решения конкретной задачи ".

В наше время, OSINT был введен во время Второй мировой войны в качестве разведывательного инструмента, когда Соединенные Штаты создали Foreign Broadcast Information Service (FBIS) для мониторинга общедоступной информации, связанной с поддержкой его войск в то время. Все это произошло еще до того, как разведывательное сообщество США начало существовать.

После окончания Второй мировой войны, ФБР продолжает свою работу по эксплуатации источников OSINT во всем мире, до 11 сентября 2001 года, террористические нападения на Соединенные Штаты. Это привлекло внимание к важности создания независимого агентства OSINT для активизации использования этих ресурсов для защиты национальной безопасности. Это то, что было предложено комиссии 9/11, который призвал к созданию специализированного агентства по сбору OSINT. В 2005, комиссия по WMD, который был сформирован для измерения эффективности разведывательного сообщества в ответ на угрозы, вызванные оружием массового уничтожения (WMD) и другие связанные с этим угрозы 21-го века, предложил создание директората с открытым исходным кодом в Центральном разведывательном управлении (ЦРУ).

Следуя этим рекомендациям и другим спорам, директор национальной разведки (DNI) объявил о создании Национального центра разведки с открытым исходным кодом (OSC). Основные задачи OSC собирать информацию, доступную как из онлайновых, так и офлайн-источников, что ранее было сделано FBIS. Позже, Закон о реформе разведки и предупреждении терроризма, которая была предложена для реформирования разведывательной деятельности правительства США, объединила ФБР и другие связанные с ними исследовательские организации в один орган. Эта организация теперь называется Open Source Enterprise и управляется ЦРУ.

Источники OSINT отличаются от других форм разведки, поскольку они должны быть юридически доступны для общественности, не нарушая никаких законов об авторском праве или неприкосновенности частной жизни. Вот почему они считаются "общедоступными". Это различие делает возможность собирать OSINT источники, применимые не только к службам

безопасности. Например, предприятия могут извлечь выгоду из использования этих ресурсов для получения информации о конкурентах.

Примичание! Во время поиска источников oSint может появиться секретная информация, которая не защищена должным образом. это включает в себя утечку документов, таких, как те, опубликованные Wikileaks. этот тип информации называется noSint, в отличие от oSint. разведка обычно учитывает все источники, независимо от их правовой доступности.

В дополнение к его значительному значению для разведывательного сообщества, сбор OSINT является менее дорогостоящим и менее рискованным, чем традиционные шпионские активы. В отличие от других источников разведки, которые могут потребовать использования спутниковых изображений шпиона или секретных агентов для сбора информации, все, что вам нужно для сбора OSINT онлайн-ресурсов является компьютер и подключение к Интернету. И, конечно, вам нужны необходимые навыки поиска.

По мере распространения технологий и увеличения объема имеющихся данных правительственные ведомства, неправительственные организации (НПО) и коммерческие корпорации начинают в значительной степени полагаться на OSINT, а не на частную классифицированную информацию. Эта книга научит вас, как использовать источники OSINT для поиска и сбора информации в Интернете. В этой главе мы оговорим термин OSINT, обсудим типы OSIN и поговорим о преимуществах различных сторон от использования OSINT и их мотивации, а также о тенденциях и вызовах на будущее. В более поздних главах мы рассмотрим, как использовать множество инструментов и методов для получения данных из доступных источников.

Категории информации с открытым исходным кодом

Существуют различные виды информации, с которыми вы можете столкнуться при проведении анализа OSINT. Согласно справочнику НАТО по *открытым источникам V1.2,* опубликованному в 2001 году, существуют четыре категории открытой информации и разведки.

- *Open source data (OSD)*: Это общие данные, поступающие из первоисточника. Примеры включают спутниковые снимки, данные телефонных звонков и метаданные, наборы данных, данные опроса, фотографии и аудио- или видеозаписи, которые записали событие.
- *Open source information (OSINF)*: Это общие данные, которые прошли некоторую фильтрацию сначала для удовлетворения конкретного критерия или необходимости; эти данные также можно назвать вторичным источником. Примеры включают книги по конкретной теме, статьи, диссертации, произведения искусства и интервью.

Примечание! набор источников, юридически доступных для общественности по конкретным каналам, называется *серой литературой.* изображения, и любая информация, которая контролируется его производителем. серая литература является одним из основных элементов oSinf и может быть получена на законных основаниях, получив разрешение ее правообладателя или заплатив за него (например, через подписные агентства, коммерческие книжные магазины и так далее).

- *Open source intelligence (OSINT)*: Это включает в себя всю информацию, которая была обнаружена, отфильтрована и назначена для удовлетворения конкретных потребностей или целей. Эта информация может быть использована непосредственно в любом контексте разведки. OSINT можно определить в двух словах как выход обработки материалов с открытым исходным кодом.
- *Validated OSINT (OSINT-V)*: Это OSINT с высокой степенью уверенности; данные должны быть подтверждены (проверены) с использованием источника, не относящегося к OSINT, или из хорошо авторитетного источника OSINT. Это необходимо, так как некоторые внешние противники могут распространять неточную информацию OSINT с намерением ввести в заблуждение OSINT анализа. Хорошим примером этого является, когда

телевизионная станция вещает в прямом эфире прибытия президента в другую страну; такая информация является OSINT, но она имеет большую степень правдивости.

Как вы видели, OSD и OSINF являются основными источниками (первичными и вторичными) информации, для OSINT.

Еще одна проблема, которая необходимо понять в контексте OSINT, это разница между данными, информацией и знаниями. Эти три термина обычно используются взаимозаменяемо; однако, каждый из них имеет различное значение, хотя три взаимодействуют друг с другом.

- *Данные*: это набор фактов, описывающих что-то без дальнейших объяснений или анализа. Например, "Цена золота за унцию составляет $1,212."
- *Информация*: это своего рода данные, которые были интерпретированы должным образом, чтобы дать полезное значение в определенном контексте. Например, "цена на золото за унцию упала с $1,212 до $1,196 в течение одной недели".
- *Знание*: это сочетание информации, опыта и понимания, которые были изучены или выведены после некоторых экспериментов. Знания описывает то, что ваш мозг записал в прошлом, и эти записи могут помочь вам принимать лучшие решения о будущем, когда сталкиваются с аналогичными контекстами. Например, "когда цена на золото падает более чем на 5 процентов, это означает, что цена на нефть тоже упадет".

Типы OSINT

OSINT включает в себя все общедоступные источники информации. Эту информацию можно найти как в Интернете, так и в автономном режиме, в том числе в следующих местах:

- Интернет, который включает в себя следующие и другие: форумы, блоги, сайты социальных сетей, видео-сайты обмена, как YouTube.com, Wiki, Whois записи зарегистрированных доменных имен, метаданных и цифровых файлов, темных веб-ресурсов, геолокационных данных, IP-адресов, людей поисковых систем, и все, что можно найти в Интернете
- Традиционные средства массовой информации (например, телевидение, радио, газеты, книги, журналы)

- Специализированные журналы, научные публикации, диссертации, конференции, профили компаний, годовые отчеты, новости компании, профили сотрудников и резюме
- Фотографии и видео, включая метаданные
- Геопространственная информация (например, карты и продукты коммерческих изображений)

Объем цифровых данных

Как вы уже видели, OSINT охватывает не только онлайн-источники. Бумажные издания из открытых источников должны также тщательно расследоваться в рамках любого процесса сбора OSINT; однако онлайн-источники составляют самый большой сегмент OSINT

Сегодня мы живем в век информации, и издатели, а также корпорации, университеты и другие поставщики источников OSINT переходят свои бизнес-процессы на цифровые форматы. Число пользователей на сайтах социальных сетей также будет продолжать расти, а количество устройств Интернета вещей (IoT) будет увеличиваться в будущем, что приведет к значительному увеличению объема цифровых данных, поступающих от миллиардов датчиков и машин по всему миру. Другими словами, большинство источников OSINT в будущем будут онлайн-источниками.

Примечание! По оценкам компании gartner, к 2020 году будет использоваться 20,4 миллиарда устройств. [v]

Объем цифровых данных стремительно взрывается. По данным IDC Research,[к] 2020 году общий объем цифровых данных, созданных по всему миру, достигнет 44 зеттабайт, а в течение пяти лет их число увеличится быстрее и достигнет 180 зеттабайт в 2025 году.
К 2020 году, по оценкам исследовательской группы Gartner, средний человек будет тратить время на взаимодействие с автоматизированными ботами больше, чем со своим супругом, и, конечно, все эти взаимодействия будут цифровыми. По другой оценке, в 2021 году 20 процентов всех видов деятельности, которые делает человек, будут связаны с использованием сервиса, по крайней мере, одной из гигантских IT-компаний (Google, Apple, Facebook, Amazon). Не говоря уже о том, что большинство людей предпочитают использовать голосовые команды для взаимодействия со своими вычислительными устройствами по типу. Эти цифры должны дать вам представление о том, как будет выглядеть ближайшее будущее в цифровую эпоху. Объем цифровых данных наряду с увеличением числа людей, использующих Интернет для работы, сделает онлайн-источники OSINT основным источником OSINT как для правительств, так и для бизнес-корпораций в будущем.

OSINT Организаций

Некоторые специализированные организации предоставляют услуги OSINT. Некоторые из них основаны на правительстве, а другие являются частными компаниями, которые предлагают свои услуги различным сторонам, таким как государственные учреждения и

бизнес-корпорации на основе подписки. В этом разделе мы упомянем основные организации OSINT по всему миру.

Правительственные организации

Правительственные организации, работающие в области анализа OSINT, по-прежнему считаются лучшими из-за ресурсов, имеющихся у их правительств для работы. Двумя самыми известными правительственными учреждениями, которые делают OSINT во всем мире, являются Центр открытого исходного кода в США и BBC Monitoring в Великобритании.

Центр с открытым исходным кодом

Мы уже говорили о Центре открытого исходного кода (OSC); это крупнейшая организация OSINT и имеет огромные ресурсы для выполнения своей работы. OSC тесно сотрудничает с другими местными разведывательными службами в Соединенных Штатах и предлагает свои услуги разведывательным службам правительства США.

BBC Monitoring

BBC Monitoring (https://monitoring.bbc.co.uk/login) — департамент Британской вещательной корпорации (Би-би-си), который следит за иностранными СМИ по всему миру. Он имеет аналогичную роль, как Центр открытого исходного кода в Соединенных Штатах, с главным отличием в том, что он не принадлежит к британской разведке. Bbc Monitoring финансируется из своих заинтересованных сторон в дополнение ко многим коммерческим и правительственным организациям по всему миру. Он был основан в 1939 году и имеет офисы в разных странах по всему миру. Она активно следит за телевидением, радиовещанием, печатными средствами массовой информации, Интернетом и возникающими тенденциями из 150 стран на более чем 70 языках. BBC Monitoring управляется BBC и предлагает свои услуги на основе подписки заинтересованным сторонам, таким как коммерческие организации и официальные органы Великобритании.

Частный сектор

Вы не должны недооценивать частный сектор, глядя на то, кто поставляет информацию OSINT; многие частные корпорации разработали передовые программы и методы сбора данных из открытых источников для получения коммерческой выгоды. Действительно, большинство частных корпораций OSINT сотрудничают с государственными учреждениями,

чтобы предоставить им такую информацию. В этом разделе мы упомянем основные из них по всему миру.

Jane’s Information Group

Jane’s Information Group (http://www.janes.com) — британская компания, основанная в 1898 году. Jane's является ведущим поставщиком, который специализируется на военной, терроризм, государственная стабильность, серьезная и организованная преступность, распространение и закупки разведки, аэрокосмической и транспортной тематики. В дополнение к источникам OSINT она издает множество журналов и книг, связанных с вопросами безопасности, которые отслеживают и предсказывают вопросы безопасности в 190 штатах и 30 территориях.

Economist Intelligence Unit

The Economist Intelligence Unit (https://www.eiu.com/home.aspx) является отделом бизнес-аналитики, исследований и анализа Британской Economist Group. Основной областью Economist Intelligence Unit является его бизнес и финансовые прогнозы; он предлагает ежемесячный доклад в дополнение к экономическому прогнозу страны на ближайшие пять лет с всеобъемлющим взглядом на текущие тенденции по экономическим и политическим вопросам.

Oxford Analytica

Oxford Analytica (http://www.oxan.com) является относительно небольшой фирмой OSINT по сравнению с предыдущими двумя. Oxford Analytica специализируется на вопросах геополитики и макроэкономики. Она имеет глобальную сеть макроэкспертов для консультирования своих клиентов по лучшим методам стратегии и производительности при доступе к сложным рынкам. Его экспертные сети содержат более 1400 экспертов. Большинство из них являются учеными по своему предмету, старшими преподавателями ведущих университетов и высокопоставленными специалистами в своем секторе.

Поставщики серой литературы

Мы уже говорили о серой литературе как о части данных OSINF. Тем не менее, этот тип данных заслуживает того, чтобы иметь свою собственную ссылку, когда речь идет об основных источниках информации, используемой в сборе OSINT из-за его большой ценности разведки.Серая литература в основном производится мировыми издательствами. Она включает в себя книги, журналы, газеты и все, что публикуется публично. Однако существует еще один тип серой литературы, называемый *серой информацией,* которая имеет различные требования к приобретению. Обычно термин *gray literature* и *gray information* используются взаимозаменяемо. Однако, в разведке, они немного отличаются. Gray literature относится ко всем публикациям, которые могут быть получены из традиционных каналов книжных магазинов, в то время как серая информация относитсяк другим публикациям, которые не могут быть получены из традиционных маршрутов. Таким образом, серая информация имеет свои каналы, и её может быть трудно определить и приобрести. Серый информация включает в себя следующие и другие: академические статьи, препринты, разбирательства, конференции и дискуссионные документы, отчеты о исследованиях, маркетинговые отчеты, технические характеристики и стандарты, диссертации, диссертации, торговые публикации, меморандумы, правительственные отчеты и документы, не опубликованные на коммерческой публике, переводы, информационные бюллетени, обзоры рынка, отчеты о поездках и программы фестиваля. Серую литературу можно разделить на три основных вида.

- *Белый*: это включает в себя все, опубликованные публично для продажи через традиционные каналы книжный магазин. Публикация должна иметь ISBN или ISSN и может быть получена непосредственно от продавца. Книги, журналы и газеты относятся к этой категории.
- *Эфемерный*: Этот тип недолговечен. Примеры включают расписание полетов, черновые версии, копии счетов-фактур, рекламы, плакатов, билетов, визитных карточек и всего, что публикуется самостоятельно.
- *Серый*: это содержит сочетание ранее упомянутых двух типов.

Как правило, серую литературу можно получить, оплатив абонентскую плату за такой контент или покупая книги, журналы, журналы и другие издания непосредственно из книжных магазинов. Чтобы получить более скрытую серую информацию, вам придется воспользоваться другими специализированными услугами. Ниже приведены некоторые из них.

Factiva

Factiva (http://new.dowjones.com/products/factiva) — глобальная новостная база данных с лицензированным контентом. Он собирает данные из более чем 33 000 премиальных источников, и многие из этих источников (74 процента) лицензированы и не могут быть найдены свободно в Интернете. Factiva собирает источники на 28 языках в дополнение к своей уникальной службе, чтобы быть в состоянии обеспечить доступ к ресурсам, которые еще не были опубликованы их создателями.

LexisNexis

LexisNexis (https://www.lexisnexis.com/en-us/gateway.page) в настоящее время принадлежит RELX Group (ранее Reed Elsevier). Первоначально она была сосредоточена на предоставлении высококачественных юридических и журналистских документов, но она расширила свое освещение, включив в него больше услуг, таких как инструменты мониторинга средств массовой информации, инструменты управления поставками, решения для разведки продаж, инструменты рыночной разведки и риск-решения, которые анализируют общественный и отраслевой контент для прогнозирования рисков и улучшения процесса принятия решений.

Ниже приведены другие компании, которые специализируются на сборе онлайн-информации из государственных и частных источников:

- InsideView (https://www.insideview.com)
- NewsEdge (www.newsedge.com)
- Semantic Visions (www.semantic-visions.com)
- DigitalGlobe (www.digitalglobe.com)

Заинтересованные стороны в OSINT информации

OSINT может быть полезным для различных субъектов. В этом разделе мы перечислим их и объясним, что мотивирует каждого из них на поиск ресурсов OSINT.

Правительство

Государственные органы, особенно военные ведомства, считаются крупнейшим потребителем источников ОСИНТ.Огромные технологические разработки и широкое использование Интернета во всем мире сделали правительства огромным потребителем для разведки OSINT. Правительства нуждаются в источниках OSINT для различных целей, таких как национальная безопасность, борьба с терроризмом, киберотслеживание террористов, понимание мнений внутренней и внешней общественности по различным вопросам, предоставление директивным органам необходимой информации для влияния на их внутреннюю и внешнюю политику, а также использование иностранных средств массовой информации, таких как телевидение, для мгновенного перевода различных событий происходит снаружи. Разведывательные органы объединяют юридически доступную информацию с их тайно приобретенными разведданными (например, с помощью спутниковых снимков-шпионов, электронных станций прослушивания и шпионов), чтобы ответить на конкретный вопрос или предсказать будущее. Эти люди имеют необходимые ресурсы (деньги и оборудование) для сбора и анализа огромных объемов данных в Интернете. Акт добычи данных OSINT правительствами, как ожидается, будет усиливаться, как мы неуклонно двигаться к тому, что в настоящее время цифровой век.

Международные организации

Международные организации, такие как ООН, используют источники OSINT для поддержки операций по поддержанию мира по всему миру. ООН уравновешивает проблемы сверхдержав и развивающихся государств при создании своей политики, которая требует, чтобы она была максимально прозрачной. Для достижения этой цели ООН пришла к выводу, что более удобно использовать источники OSINT (включая коммерческие спутниковые снимки) для нужд разведки, а не в зависимости от сообщений от государств-членов, которые могут иметь противоречивую политику.Гуманитарные организации, такие как Международный Красный Крест, используют источники OSINT для оказания им помощи в их усилиях по оказанию чрезвычайной помощи в период кризиса или катастрофы. Они используют разведданные OSINT для защиты своей цепочки поставок от террористических групп, анализируя сайты социальных сетей и приложения для обмена сообщениями в Интернете для прогнозирования будущих террористических действий.НАТО в значительной степени зависит от источников OSINT для целей разведки и для составления планов операций по поддержанию мира. Она также выигрывает от коммерческих спутниковых снимков для планирования операций, поскольку не все государства-члены НАТО имеют

такие объекты. НАТО опубликовала три стандартных ссылки о том, как использовать OSINT для общественности. Первый — *Справочник НАТО по разведке с открытым исходным кодом*(https://archive.org/ details/NATOOSINTHandbookV1.2). Во-вторых,*NATO Open Source Intelligence Reader* (http://www.au.af.mil/au/awc/awcgate/nato/osint_reader.pdf). Третий из них *NATO Intelligence Exploitation of the Internet* (http://nsarchive2.gwu.edu//NSAEBB/ NSAEBB436/docs/EBB-005.pdf).

Правоохранительные органы

Полиция использует источники OSINT для защиты граждан от жестокого обращения, сексуального насилия, кражи личных данных и других преступлений. Это может быть сделано путем мониторинга социальных каналов средств массовой информации для интересных ключевых слов и фотографий, чтобы помочь предотвратить преступления, прежде чем они обостряются.Правоохранительные органы используют OSINT для мониторинга и отслеживания преступных сетей в разных странах. Например, они используют тактику OSINT для сбора информации о людях, представляющих интерес, чтобы создать полный профиль для каждого из них. Они также используют источники OSINT для онлайн-подделок и нарушений авторских прав.

Бизнес-корпорации

Информация является властью, и корпорации используют источники OSINT для исследования новых рынков, мониторинга деятельности конкурентов, планирования маркетинговой деятельности, и предсказать все, что может повлиять на их текущую деятельность и будущий рост. В прошлом использование источников OSINT ограничивалось крупным и крупным бизнесом с хорошими бюджетами разведки. В настоящее время, с широким использованием Интернета, небольшие компании с ограниченным бюджетом могут эффективно использовать источники OSINT и включить полученную информацию в свои бизнес-план.

Предприятия также используют разведку OSINT для других нефинансовых целей, таких как:

- Для борьбы с утечкой данных, зная, что бизнес-разоблачение конфиденциальной информации и уязвимости безопасности их сетей является причиной будущих киберугроз
- Создать свои стратегии инвенции угроз путем анализа источников OSINT как извне, так и внутри организации, а затем объединения этой информации с другой информацией для достижения эффективной

политики управления киберрисками, которая помогает им защитить свои финансовые интересы, репутацию и клиентскую базу

OSINT особенно полезно для компаний, работающих в оборонной промышленности, так как такие компании должны быть в полной мере осведомлены об окружающих обстоятельствах своих клиентов, чтобы разработать и нацелить их с соответствующим оборудованием.

Пентесторы и хакеры / Преступные организации

OSINT широко используется хакерами и пентесторами для сбора разведданных о конкретной цели в Интернете. Он также считается ценным инструментом для оказания помощи в проведении социальной инженерии. Первая фаза любой методологии тестирования на проникновение начинается разведки (другими словами, с OSINT). Рисунок 1-1 подробные основные фазы тестирования на проникновение.

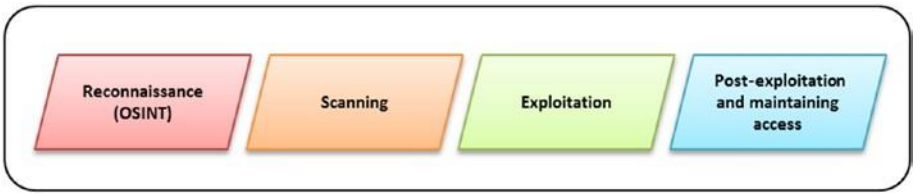

Рисунок 1-1. *Методология тестирования на проникновение (источник:http://www.DarknessGate.com)*

Пинтестерам платят компании, для аудита безопасности с указанием слабых мест и защите от внешних угроз. Это отличается от хакеров, которые используют эти уязвимости для получения несанкционированного доступа к конфиденциальным данным; однако для достижения своей работы используются одни и те же методы и инструменты разведки.

Конфиденциальность сознательных людей

Это обычные люди, которые, возможно, захотите проверить, как посторонние могут ворваться в свои вычислительные устройства и что известно о них в интернете. Они также должны знать свои онлайн уровень, чтобы закрыть любой пробел в безопасности и удалить любые личные данные, которые могут быть опубликованы непреднамеренно. OSINT

является отличным инструментом, чтобы увидеть, как ваша цифровая идентичность появляется во внешнем мире, что позволяет сохранить вашу конфиденциальность.

Физические лица могут также использовать OSINT для борьбы с кражей личных данных, например, в случае если кто-то выдает себя за вас. Во время этой книги мы научим вас различным методам поиска текста, изображений и видео, а также цифровых метаданных файлов.

Действительно, все пользователи Интернета используют методы OSINT в той или иной форме, например, при поиске чего-то в Интернете. Будь то компания, школа, университет или человек, который вы ищете, вы собираете ту или иную форму разведки OSINT.

Террористические организации

Террористы используют источники OSINT для планирования атак, сбора информации о целях, прежде чем атаковать их (например, при использовании спутниковых изображений, таких как Google Maps для расследования целевого местоположения), закупать больше боевиков, анализируя сайты социальных сетей, приобретайте военная информация, случайно выявленная правительствами (например, как строить бомбы), и распространять свою пропаганду по всему миру, используя различные каналы средств массовой информации.

Типы сбора информации

Источники OSINT могут быть собраны с помощью трех основных методов: пассивного, полупассивного и активного. Использование одного в пользу другого зависит от сценария, в котором процесс сбора работает в дополнение к типу данных, которые вас интересуют. Три метода сбора обычно используются для описания способов работы следа, другими словами, получения технической информации о целевой ИТ-инфраструктуре (типы ОС, топология сети, имена серверов и так далее). Однако, имейте в виду, что эта книга научит вас различные методы для сбора разведки OSINT, и технический след считается своего рода сбор информации.

Пассивный метод

Это наиболее часто используемый тип при сборе OSINT разведке. Действительно, все методы разведки OSINT должны использовать пассивный сбор, поскольку основная цель сбора OSINT заключается в сборе информации о цели только через общедоступные ресурсы. В этом типе ваша цель ничего не знает о вашей деятельности по сбору разведданных. Этот вид поиска является весьма анонимным и должно быть сделано тайно. С технической точки зрения, этот тип сбора показывает ограниченную информацию о цели, потому что вы не отправляете трафик (пакеты) на целевой сервер, прямо или косвенно, и основные ресурсы, которые вы можете собрать, ограничены архивом информация (в основном устаревшая информация), незащищенные файлы, оставленные на целевых серверах, и содержимое, присутствующее на целевом веб-сайте.

Полупассивный метод

С технического зрения этот тип сбора отправляет ограниченный трафик на целевые серверы для получения общей информации о них. Этот трафик маскируется под типичный интернет-трафик, чтобы не привлечь внимание к вашей разведывательной деятельности. Таким образом, вы не осуществляете углубленное исследование онлайн-ресурсов цели, а только легко исследуете, не запустив сигнализацию со стороны цели. Хотя этот тип сбора считается как-бы анонимным, цель может знать, что производиться разведка т, если они расследуют проблему (путем проверки сервера или сетевых устройств журналы). Тем не менее, они не должны понять откуда идет разведка.

Активный метод

В этом типе вы взаимодействуете непосредственно с системой для сбора информации об этом. Цель может стать известной о процессе разведки, так как лицо/организация, собирающая информацию, будет использовать передовые методы сбора технических данных о целевой ИТ-инфраструктуре, таких как доступ к открытым портам, сканирование уязвимостей (не обновлённые системы Windows), сканирование веб-серверных приложений и многое другое. Этот трафик будет выглядеть подозрительно или злонамеренное поведение и оставит следы на системе обнаружения вторжений цели (IDS) или системе предотвращения вторжений (IPS). Проведение атак социальной инженерии на цель также считается одним из видов активного сбора информации.Как мы уже говорили ранее, активный сбор и полуактивный сбор являются типами сбора информации, но вы обычно не используете их в сборе OSINT. Пассивный сбор является предпочтительным, потому что он может собирать информацию из открытых источников тайно, и это суть OSINT.

Преимущества OSINT

В современную информационную эпоху никто не может недооценивать жизненно важную роль, которую OSINT играет в различных областях разведки. Преимущества OSINT охватывают многие области в современном мире. Ниже приведены основные из них:

- *Менее рискованно*: Использование общедоступной информации для сбора разведданных не имеет никакого риска по сравнению с другими формами разведки, такими как использование спутников-шпионов или использование человеческих источников на местах для сбора информации, особенно в враждебных странах.

- *Экономично:* Сбор OSINT, как правило, дешевле по сравнению с другими источниками разведки. Например, использование человеческих источников или спутника-шпиона для сбора данных является дорогостоящим делом. Малые предприятия с ограниченными бюджетами разведки могут использовать источники OSINT с минимальными затратами.

- *Простота доступности*: источники OSINT всегда доступны, независимо от того, где вы находитесь, и всегда актуальны. Источники OSINT могут использоваться различными сторонами в любом контексте разведки; все, что вам нужно, это необходимые навыки / инструменты для сбора данных и анализа OSINT должным образом. Например, военные ведомства могут

прогнозировать будущие атаки, анализируя действия на сайтах социальных сетей, в то время как корпорации могут использовать их для построения своих новых стратегий расширения рынка.

- *Правовые вопросы*: ресурсы OSINT могут быть совместно распределены между различными сторонами, не беспокоясь о нарушении какой-либо лицензии на авторские права, поскольку эти ресурсы уже опубликованы публично. Конечно, некоторые ограничения применяются при совместном использовании серой литературы; мы уже рассмотрели это в предыдущем разделе.

- *Помощь финансовых следователей*: OSINT позволяет специализированных государственных учреждений для выявления уклоняющихся от уплаты налогов, например. Многие известные знаменитости и некоторые гигантские компании участвуют в уклонении от уплаты налогов, и мониторинг их учетных записей в социальных сетях, отпуск, и образ жизни имеет большое значение для государственного инспектора, который может преследовать их за незадекларированный доход.

- *Борьба с онлайн-подделкой:* методы OSINT могут быть использованы для поиска фальшивых продуктов/услуг и направления правоохранительных органов на закрытие таких сайтов или отправку предупреждений пользователям о прекращении их работы. Это большое преимущество OSINT, особенно при борьбе с контрафактной фармацевтической и натуральной продукцией для здоровья.

- *Поддержание национальной безопасности и политической стабильности*: Это может быть наиболее важной ролью OSINT; это помогает правительствам понять отношение своего народа и действовать быстро, чтобы избежать любых будущих столкновений. Мудрые правительства используют OSINT в своих будущих стратегиях, особенно для своей внутренней политики.

Проблемы разведки с открытым исходным кодом

Все методологии сбора разведданных имеют некоторые ограничения, и OSINT не освобождается от этого правила. В этом разделе мы упомянем некоторые из проблем, с которыми сталкивается OSINT.

- *Огромный объем данных*: Сбор OSINT будет производить огромный объем данных, которые должны быть проанализированы, увеличивает стоимость. Конечно, для этой цели существует много автоматизированных инструментов, и многие правительства и гигантские компании разработали свой собственный набор инструментов и методов искусственного интеллекта для фильтрации полученных данных. Тем не менее, огромный объем данных будет оставаться проблемой для собирателя OSINT.
- *Надежность источников*: Имейте в виду, что источники OSINT, особенно при использовании в контексте разведки, должны быть тщательно проверены секретными источниками, прежде чем им можно доверять. Многие правительства передают неточную информацию, чтобы ввести в заблуждение при сборе данных из OSINT.
- *Человеческие усилия*: как мы уже упоминали, сам объем данных считается самой большой проблемой для сбора OSINT. Людям необходимо просмотреть результаты автоматизированных инструментов, чтобы узнать, являются ли собранные данные надежными и надежными; им также необходимо сопоставить его с некоторыми секретными данными (это применимо к некоторой военной и коммерческой информации), чтобы обеспечить ее надежность и актуальность. Это позволит эффективно использовать время и драгоценные человеческие ресурсы.

Правовые и этические ограничения

Несмотря на большое значение OSINT, он имеет правовые проблемы при анализе или захватили во многих случаях. Например, если кто-то приобретает источники OSINT незаконным путем, чтобы оправдать честный случай, как должна решать правовая система? Другая дилемма заключается в том, когда образец OSINT сведен к минимуму или выбран в соответствии с потребностями собирающего информацию. Они могли бы эффективно отказаться от важных источников намеренно в пользу обеспечения

конкретного результата. Еще одна проблема заключается в том, когда некоторые формы скрытой общественной информации собираются и широко пропагандируются в рамках скандала. Как вы собираетесь видеть в этой книге, много общественной информации не может быть просмотрено регулярным пользователем Интернета и нуждается в конкретные методы / методов для приобретения. Что такое следствие для таких вещей? Каковы будут последствия для некоторых групп или отдельных лиц при раскрытии такой информации о них? Каковы моральные последствия? За последние пять лет многие разоблачители украли секретную информацию из хорошо охраняемых учреждений и учреждений и опубликовали ее в Интернете (Эдвард Сноуден является наглядным примером). Должны ли мы учитывать эту информацию, принадлежащую общественному источнику? Конечно, военные ведомства во всем мире будут жаждать такой информации, но мы должны использовать ее как отдельные лица или компании, как публичный источник нашей разведки? Многие корпорации (Facebook и Google являются примерами) собирают большой объем данных онлайн-пользователей для коммерческой разведки; большая часть этих данных относится к действиям и поведению пользователя в Интернете и не может быть использована для распознавания реальной личности пользователя. Например, существует два типа данных, которые могут быть собраны в Интернете:

- Конфиденциальная личная информация (SPI), такая как имя, номер социального страхования, место рождения, имена родителей, паспорт или идентификационный номер
- Анонимная информация, такая как техническая информация, такая как тип и версия ОС, версия браузера, IP-адрес, местоположение подключенного устройства и все, что передается между более чем одним подключенным пользователем

Чтобы оправдать сбор, эти корпорации говорят, что они приобретают только анонимные данные, но что, если эта анонимная информация была объединена с другими источниками, чтобы стать SPI? Каким образом такая информация должна обрабатываться аналитиком OSINT? Окончательная юридическая проблема, которую мы собираемся охватить, это опора на автоматизированные машины для сбора и анализа информации OSINT. Можем ли мы доверять результату автоматизированных машин и относиться к ним так же, как к данным, собранным людьми? Что делать, если есть недостаток программного обеспечения в инструменте, который производит неточный выход, который приводит к вредным последствиям? Как мы можем найти баланс между использованием автоматизированных машин, которые необходимы в процессе сбора OSINT, и оставаясь этичными?

Ограничения OSINT в дополнение к его правовым ограничения должны поощрять

его следовать индивидуальному и индивидуальному подходу при его использовании.

Итоги

В этой главе вы обнаружили сущность OSINT, его типы и пользователей, и как он может быть использован в различных контекстах различными сторонами для разведки. Мы различали различные способы сбора информации в Интернете (в основном технические) и кратко рассказало о методах. В заключение мы говорили о преимуществах и ограничениях сбора OSINT. Никакая методология сбора информации не считается 100-процентной завершенной; однако при правильном планировании и достаточных ресурсах и экспертных знаниях эксплуатация OSINT даст точные результаты в больших масштабах.OSINT является прекрасным местом для получения информации о будущих событиях, но проведения OSINT само по себе недостаточно, для получения точных результатов. Например, для достижения наилучших результатов из источников OSINT на этапе анализа необходимо учитывать некоторые задачи с добавленной стоимостью, такие как использование эксперта-аналитика, слияние информации OSINT с секретной информацией при обработке военной информации и принятие правильных методов для проведения непредвзятой разведки OSINT.Эта глава была введением к теме. В следующих главах мы подробно рассмотрим множество методов и инструментов для сбора и анализа информации OSINT. Прежде чем мы начнем погружение в мир OSINT, однако, важно, чтобы узнать, как сохранить нашу цифровую конфиденциальность и скрывать нашу деятельность в Интернете при проведении сбора OSINT, и это будет предметом следующей главы.

Примечание

i. Juniperresearch, “CYBERCRIME WILL COST BUSINESSES OVER $2 TRILLION BY 2019” August 25, 2017. https://www. juniperresearch.com/press/press- releases/cybercrimecost-businesses-over-2trillion

ii. Gpo, “Public Law 109-163 109th Congress” August 25, 2017.https://www.gpo.gov/fdsys/pkg/PLAW-109publ163/html/ PLAW-109publ163.htm iii. CIA, “Intelligence in Public Literature “August 25, 2017.https:// www.cia.gov/library/center-for-the-study-ofintelligence/csi-publications/csi- studies/studies/vol.56-no.-1/no-more-secrets-open-source-information-andthe-reshaping-of-u.s.-intelligence.html

iv. Fas, “Final Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction” August 25, 2017. https://fas.org/irp/offdocs/ wmdcomm.html

v. Gartner, “Gartner Says 8.4 Billion Connected ‘Things’ Will Be in Use in 2017, Up 31 Percent From 2016” August 25, 2017. https://www.gartner.com/newsroom/id/3598917

vi. Comsoc, “IDC Directions 2016: IoT (Internet of Things) Outlook vs Current Market Assessment” August 25, 2017. http://techblog. comsoc.org/2016/03/09/idc-directions-2016-iot-internetof-things-outlook-vs-current-market-assessment

Глава 2

Введение в Онлайн-угрозы и контрмеры

Когда вы делаете разведку из открытых источников, вы, безусловно, оставить цифровые следы, которые могут быть использованы для отслеживания вас. Например, рассмотрим следователя, выполняющего онлайн-поиск наркоторговцев в Мексике. Что делать, если люди, которых следователь искал обнаруживает его поиск? Что делать, если они могут узнать источник поиска (организация или лицо, стоящее за поиском) и местоположение поискового? Если вы считаете, что преступные организации технически не подкованы, мы боимся, что вы ошибаетесь. Террористы и преступные организации имеют специализированные группы, работающие в области ИТ для сбора разведданных в Интернете, и даже небольшие преступные организации с ограниченным бюджетом используют аутсорсинг для таких задач в специализированных организациях за плату. Как вы видели в главе 1, OSINT является полезным для многих групп пользователей. Мы уже привели пример для следователя, разыскивав наркодилера; однако то же самое относится ко всем, кто проводит сбор данных используя OSINT, такие как физические лица, государственные учреждения, коммерческие корпорации и даже НПО и глобальные организации, такие как НАТО. Выявление личности поисковика при проведении поисков OSINT может иметь опасные и даже юридические последствия для некоторых пользовательских сегментов. В этой главе мы научим вас, как скрыть свою цифровую личность и стать анонимным в Интернете. Вы узнаете, как обмениваться данными тайно через враждебные среды, как Интернет и как общаться со своими коллегами в частном порядке и анонимно. Вы также узнаете, как проверить свой цифровой след и узнать, какие цифровые следы вы оставляете позади. Но прежде, чем мы начнем, мы будем охватывать онлайн угрозы и как внешние противники могут использовать вычислительные устройства и сети для кражи конфиденциальной информации. Контрмеры и рекомендации по поддержанию вашей конфиденциальности в Интернете будут тщательно охвачены. Это самая длинная глава в этой книге; Вы можете рассматривать его как мини-книгу, которая учит вас, как работать в Интернете в частном порядке. Эти знания обязательны, так как вы не можете проводить поиск OSINT с вашей реальной личностью.

Примечание! Мы не можем научить вас, как стать на 100 процентов анонимным в одной главе. Однако, чтобы начать проводить поиск OSINT, этой главы достаточно, чтобы помочь вам избежать привлечения внешних наблюдателей к вашей деятельности по сбору OSINT.

Чтобы понять все понятия в глубину и узнать, как различные субъекты могут вторгнуться в вашу частную жизнь, вы должны прочитать нашу книгу *Цифровой конфиденциальности и безопасности с помощью Windows* (https://www.apress.com/gp/book/9781484227985),который считается идеальным спутником этой книги. Если у вас уже есть эта книга, вы можете пропустить эту главу.

Онлайн-угрозы

Несмотря на свои огромные блага для человечества, Интернет по-прежнему является враждебной средой. Плохие парни всегда там, чтобы нарушить вашу жизнь. В этом разделе мы перечислим основные риски, с которыми сталкиваются пользователи Интернета при выходе в Интернет, и дадим краткие рекомендации/контрмеры для каждого из них.

ВРЕДОНОСНЫХ ПРОГРАММ

Вредоносное ПО является сокращением от "вредоносного программного обеспечения". Это термин, используемый для любого вредоносного программного обеспечения / кода, которые могут повредить ваше вычислительное устройство или украсть конфиденциальную информацию без вашего согласия. Существуют различные виды вредоносных программ, таких как вирусы, программы-шпионы, руткиты, черви, вымогателей, условно бесплатное ПО, и рекламное.

Примечание! Есть много веб-сайтов, которые предлагают бесплатные образцы живого вредоносного кода (вредоносного ПО) для исследователей безопасности, реагирования на инциденты, судебных аналитиков и любой заинтересованной стороны. Некоторые из этих сайтов являются следующими:

https://virusshare.com https://www.virustotal.com

http://malc0de.com/database https://virusscan.jotti.org

Хакеры/ Киберпреступники

Хакеры / Киберпреступники люди со хорошими вычислительными навыками. Они стремятся вторгнуться в частные сети и ЭВМ других людей, чтобы украсть личную информацию или для проведения других вредоносных действий. Обычно они используют уязвимости в ОС, в программах приложений или в сетевых устройствах для получения несанкционированного доступа. После получения доступа, они могут установить кейлоггер или троянский конь, чтобы сохранить свой доступ, украсть информацию, или шпионить за деятельностью пользователя.

ФАРМИНГ

Pharming — это кибератака, предназначенная для перенаправления пользователей с легального веб-сайта на мошеннический сайт без их ведома. Фарминг может быть проведен либо путем изменения файла хостов на компьютере жертвы или путем отравления серверных записей Domain Name System (DNS) с ложной информацией, чтобы привести пользователей к нежелательным направлениям. Пользователи Windows могут предотвратить такого тип атаки на свои локальные машины, предотвращая модификации файлов хостов с помощью следующих шагов:

- Перейдите к%SYSTEMDRIVE%\Windows\Ssystem32\drivers\etc folder (SYSTEMDRIVE is where you installed Windows, usually at C:\).
- Нажмите правой кнопкой мыши файл хоста, выберите Свойства и выберите атрибут Readonly; наконец, нажмите OK (см. Рисунок 2-1).

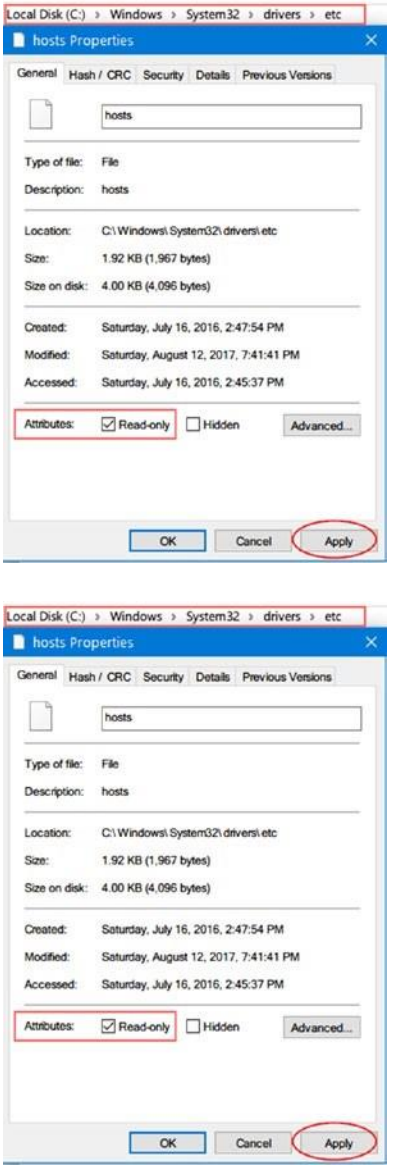

Рисунок 2-1. *Изменение атрибутов файлов хоста на только для чтения, чтобы избежать фарминговых атак на компьютерах Windows*

Примечание! Вы можете редактировать файл hosts в Windows с помощью разных инструментов. Такие инструменты позволяют добавлять записи, чтобы блокировать вредоносные сайты и включить или отключить файл хостов. Просмотреть мануал на файл hosts можно по ссылке (www.abelhadigital.com/hostsman) и Sysmate - Hosts File Walker (https://sourceforge.net/projects/sysmate-hosts- file-walker/).

ФИШИНГ

Фишинг является своего рода социальной инженерии атаки, где злоумышленник использует психологические трюки (социальные трюки) по телефону или использует вычислительное устройство (электронные письма, чат), чтобы убедить людей передать конфиденциальную информацию о себе или организации и ее компьютерах.Фишинговые письма отображаются так, как если бы они были отправлены законной компанией или кем-то из ваших знакомых (например, человеком из списка контактов). Эти письма обычно содержат ссылку, которую пользователь должен нажать, чтобы получить доступ/ обновить онлайн-аккаунт (например, банковский или социальный аккаунт сайта). При нажатии на такие ссылки, пользователь будет направлен на мошеннический веб-сайт, который, кажется, правильным. Когда пользователь предоставляет свои учетные данные, злоумышленник будет хранить их для последующего использования и перенаправит пользователя на исходный веб-сайт.Фишинговые письма имеют некоторые характеристики, которые каждый может обнаружить. Вот список основных из них:

- Они используют угрожающие или срочные слова в строке темы, чтобы побудить пользователя действовать быстро. Они обычно просят вас обновить свой онлайн-аккаунт или отправить свои личные данные, ответив на электронную почту.
- Некоторые фишинговые письма предлагают призы, вакансии на дому с большими зарплатами и отсутствием необходимой квалификации, или

бизнес-инвестиции с высокой прибылью. Затем они просят ваши контактные данные для дальнейших переговоров.

- Фишинговые письма выглядят непрофессионально и содержат много грамматических ошибок; они также происходят из другой области, чем компания, которую они претендуют представлять. Например, письмо от PayPal должно поступать из PayPal.com домена, а не из xyz. PayPal.com.

Всякий раз, когда вы подозреваете, что письмо является фишинговым письмом, не отвечайте на него. Чтобы проверить, является ли это фишинговое письмо, поищите мышью (но не щелкните) по ссылкам в электронной почте, чтобы узнать, соответствует ли адрес ссылке, которая была напечатана в сообщении, или доменному имени отправителя. Кроме того, не предоставляйте никакой личной информации, если фишинг-письмо просит вас заполнить какие-либо формы (см. рисунок 2-2).

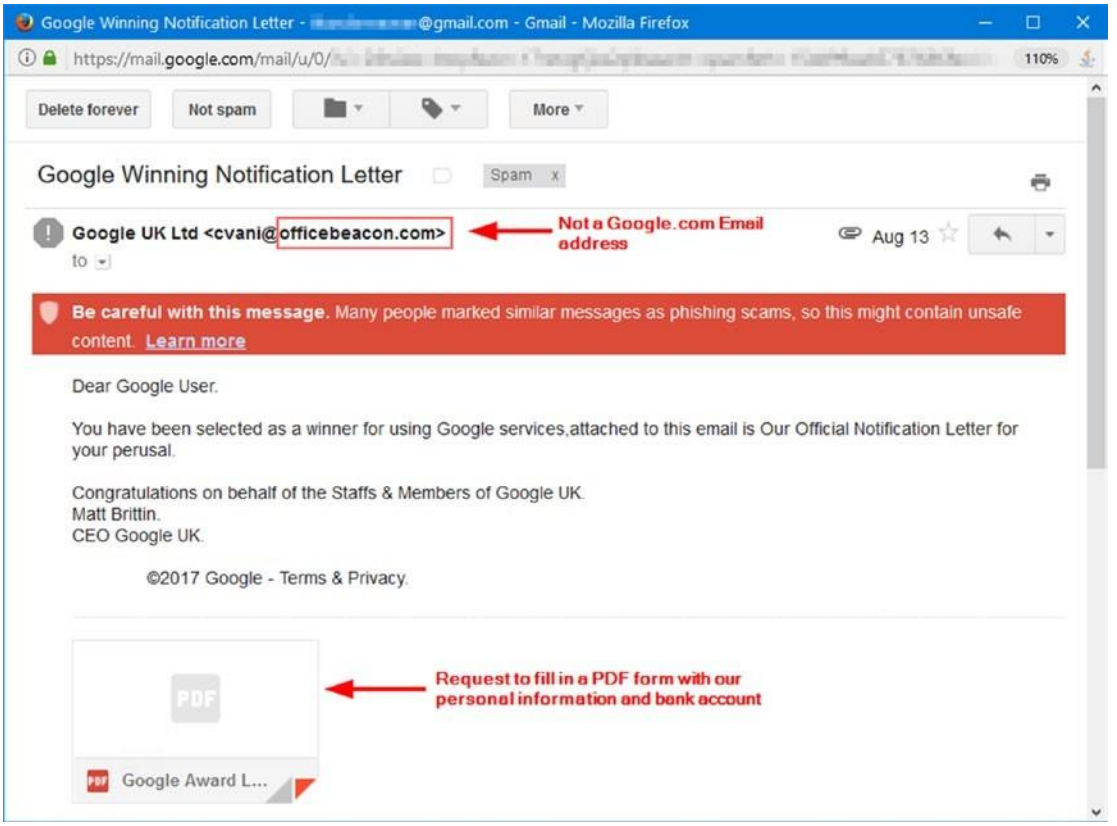

Рисунок 2-2. *Пример фишинговой электронной почты, притворяющейся от Google*

Некоторые злоумышленники используют службы сокращения URL-адресов для маскировки реального фишингового URL-адреса, отправленного пользователю. Если вы подозреваете, что короткий URL может быть афера, вы можете расширить его с помощью этих бесплатных онлайн-сервисов, чтобы увидеть его назначения:

- http://checkshorturl.com
- www.getlinkinfo.com
- http://wheredoesthislinkgo.com
- https://linkexpander.com

Примечание! lehigh university предоставляет различные типы фишинговых писем с кратким описанием каждого из них (https://lts.lehigh.edu/phishing/examples).Сайт по адресу www.phishing.org/phishing-examples тоже предлагает образец фишинговых писем.

Если вы подозреваете, что стали жертвой фишинговой атаки, https://www.ftc.gov/complaint и подать жалобу. Вы можете сообщить о краже личных данных на той же странице, если вы подозреваете, что кто-то или компания злоупотребляет вашими личными данными. Вы также можете подать жалобу на веб-сайте ФБР по адресу https://www.ic3.gov/complaint/default.aspx.

КИБЕРВЫМОГАТЕЛЬСТВО

Кибервымогательство является вредоносным кодом, который устанавливается бесшумно на компьютере пользователя или мобильное устройство; он работает, блокируя доступ пользователя к его файлам или экрану, шифруя все пользовательские данные на устройстве в дополнение ко всем данным на прикрепленных устройствах хранения(USB флешках, внешних HDD, и SSD) а потом появляется баннер с уведомлением об оплате для разблокировки данных . Некоторые типы кибервымогателей угрожают жертвам публиковать свои данные публично, если они отказываются платить выкуп. Выкуп обычно выплачивается с помощью анонимных способов онлайн-платежей, таких как Bitcoin, который является своего рода цифровой валютой, чтобы получить ключ расшифровки.

Заражение кибервымогателями приходит через различные методы. Например, может быть прикреплен к спам-письмам, установлен при посещении вредоносных веб-сайтов, или установлен как часть законной программы, которая была изменена злоумышленником, чтобы скрыть вымогателей в нем. Он также может быть получен через другие вредоносные программы, такие как троянский конь или комплексы эксплойтов.Есть два основных типа кибервымогателей.

- Первый тип, также известный как *локер который* блокирует экран системы таким образом, что легко для опытного пользователя компьютера, чтобы разблокировать ограничение.
- Второй тип, также известный как *крипто-вымогатель*- шифрует весь диск или некоторые типы файлов, включая все прикрепленные съемные хранилища, и просит выкуп, чтобы удалить ограничение.

Специальный вариант вымогателей атакует мастер загрузки записи (MBR) уязвимой системы, тем самым предотвращая ОС от загрузки, если жертва платит выкуп. Чтобы противодействовать атакам вымогателей, выполните эти шаги:

- Резервное копирование всех необходимых файлов регулярно. Все типы операционных систем имеют специальную функцию резервного копирования. В Windows 10 вы можете получить доступ к функции резервного копирования через настройки Windows (Windows - I) - Обновление и безопасность.
- Регулярно устанавливайте все патчи безопасности для операционной системы и всех установленных приложений и держите их в актуальном состоянии.
- Установка антивирусных и антивредоносных решений, если это возможно, и поддерживать их в актуальном состоянии.
- Не запускайте макросы в файлах Microsoft Office при получении таких файлов от неизвестного пользователя или при их загрузке из Интернета.

Если атака с целью выкупа успешно компрометирует вашу систему, выполните следующие действия:

- Отключите компьютер от сети/Интернета.

- Выполнить полное сканирование всех подключенных устройств/носителей хранения.
- Обратитесь за советом к специалисту, чтобы узнать тип вымогателей, какие инструменты удаления доступны для конкретных версий вымогателей.
- Формат затронутых устройств при необходимости и выполнение переустановки ОС.
- Восстановление данных из предыдущей резервной копии.
- Информировать правоохранительные органы о факте заражения и не платить выкуп.

Подсказка Crypto Sheriff (https://www.nomoreransom.org/crypto-sheriff.php?lang=en) помогает пользователям оправиться от атак вымогателей, предлагая бесплатный сервис, чтобы проверить тип вымогателей, влияющих на ваше устройство, а затем помочь вам скачать решение расшифровки, если доступно.

Рекламное и шпионское ПО

Adware является своего рода рекламным программным обеспечением, которое отслеживает деятельность пользователей в Интернете для отображения соответствующей рекламы, тем самым принося доход для его автора. Он обычно устанавливается как часть бесплатных интернет-программ, таких как системные утилиты, игры или панели инструментов браузера. Вы не можете рассматривать все рекламное программное обеспечение как вредоносное, потому что многие из них установлены как часть законного программного обеспечения, которое заявляет о существовании рекламного программного обеспечения в рамках своего соглашения о лицензии конечного пользователя (EULA). Тем не менее, большинство пользователей просто нажмите кнопку "Я согласен", не зная, что они устанавливают рекламное на своей машине.

Шпионские программы является еще одним видом отслеживания программного обеспечения; однако, это только для злонамеренных целей. Шпионские программы отслеживают все, что вы вводите на клавиатуре, и отправляет его своему оператору. Некоторые типы устанавливают другие вредоносные программы (например, программы-вымогатели) на вашей машине, чтобы облегчить выполнение других вредоносных действий.

Троян

Это своего рода вредоносная компьютерная программа, которая устанавливается бесшумно на машину жертвы. Это позволяет своему оператору иметь полный контроль над машиной жертвы, включая камеру и микрофон. Большинство популярных банковских угроз исходит от троянской семьи, как Zeus и SpyEye.

Вирус

Это то, что большинство не-компьютер подкованных пользователей означает, когда речь идет о вредоносные компьютерные программы. Вирусы считаются одним из старейших традиционных рисков с первых дней персональных компьютеров. Основная цель вируса состоит в том, чтобы сделать операционную систему жертвы неработоспособной, тем самым заставив пользователя отформатировать ее, чтобы вернуться в исходное состояние.

Черви

Моррис червь, или интернет-червь, был одним из первых, чтобы увидеть в дикой природе. В ноябре 1988 года она была распространена через Интернет и нанесла значительный ущерб зараженным системам. Это теперь другой тип нападения старой школы который все еще широко использован. Основное намерение червя состоит в том, чтобы распространяться от одной машины к другой через внутренние сети или Интернет для распространения вредоносного кода. Реплицируя себя, черви потребляют большое количество пропускной способности сети, например, отправка файлов по электронной почте, что наносит большой ущерб корпоративным сетям. Черви также могут устанавливать бэкдоры на компьютерах.

Scareware

Scareware является своего рода вредоносное программное обеспечение, также известный как *обман программного обеспечения,* изгоев *сканер программного обеспечения*, или fraud ware - *это* трюки жертвы в покупке программного обеспечения безопасности (таких как антивирус и анти-вредоносных программ) удалить инфекцию с пк. Например, пользователь может видеть всплывающее сообщение на своем компьютере о том, что он заражен вредоносными программами и должен действовать быстро, приобретая специальное решение по борьбе с вредоносными программами, которое является поддельным! -для очистки ПК. Идея здесь заключается в том, чтобы обмануть пользователя в покупке ПО у злоумышленников, чтобы взять деньги пользователя.Заражение червем может быть смягчены путем установки программного обеспечения безопасности и поддержания Вашей ОС и антивирусное решение в актуальном состоянии.

РАСПРЕДЕЛЕННЫЙ ОТКАЗ В ОБСЛУЖИВАНИИ

Распределенная атака типа «отказ в обслуживании» (DDoS) происходит, когда многие скомпрометированные вычислительные устройства наводняют целевой компьютер, например, сервер, а также одновременное множество поддельных запросов, что делает его безответным для обслуживания законных пользователей. Эта атака нацелена на большое количество организаций, таких как банки, торговые сайты и информационные агентства. В отличие от других атак, которые направлены на кражу конфиденциальных данных, основная цель DDoS-атаки - сделать ваш веб-сайт и серверы недоступными для законных пользователей.

РУТКИТ

Руткит является опасным типом вредоносных программ; потенциально он может получить административный доступ к системе и может помешать нормальной программе обнаружения (антивирусные и анти-руткитные программы) замечать ее присутствие. Некоторые опасные руткиты атакуют на аппаратном уровне (микропрограммное rootkit), и удаление может потребовать замены оборудования или специализированного вмешательства.

Обнаружение Rootkit затруднено, поскольку не существует единого решения безопасности, которое может удалить все известные и неизвестные руткиты. Тем не менее, есть много ценных программ, которые могут удалить большое количество типов руткитов, как вы увидите позже в главе.

Juice Jacking

Это тип кибератаки, когда злоумышленник копирует данные или устанавливает вредоносное ПО на смартфон/планшет жертвы, когда жертва подключает устройство через USB-кабель к публичной зарядной станции, которая была изменена, чтобы играть вредоносную роль. Общественные зарядные станции можно найти в аэропортах, гостиницах, торговых центрах и конференциях.

Wi-Fi подслушивание

Бесплатные точки доступа Wi-Fi распространяются практически везде. Злоумышленник может использовать уязвимости в таких устройствах для перехвата всех сообщений, с помощью телефонных звонков, мгновенных сообщений и видеоконференций, которые прошли через них. Настоятельно рекомендуется не пользоваться бесплатным Wi-Fi в общественных местах, если только для защиты связи не используется сильная виртуальная частная сеть (VPN).

Программное обеспечение безопасности

Важно установить антивирусное решение на вашем компьютере, прежде чем вредоносная часть программного обеспечения компрометирует его. Наличие антивирусной программы считается первой линией защиты от кибератак. Новые вирусы создаются почти каждую минуту. Это работа антивирусного программного обеспечения, чтобы идти в ногу с последними угрозами.

Имейте в виду, что наличие антивирусной программы, установленной на вашем компьютере, не дает вам 100-процентной защиты. Благодаря изощренности современных кибератак необходимо более чем одну меру для защиты ваших вычислительных устройств и сети. Например, установка решения для брандмауэра не менее важна, чем антивирусная программа. Многие антивирусные решения оснащены встроенным брандмауэром. В этой книге мы упомянем только бесплатные продукты.

Антивирус

Коммерческие антивирусные решения всегда лучше, чем их свободные аналоги (см. таблицу 2-1), поэтому мы начнем с разговора о рекомендуемых функций, которые должны существовать в любом антивирусном решении, чтобы считаться полезными.

- Он должен быть оснащен встроенным брандмауэром.

- Он должен быть в состоянии сканировать почтовые клиенты, такие как Thunderbird и Outlook, и обнаруживать фишинговые атаки.
- Он должен обновить себя автоматически и обнаружить нулевой день вредоносных программ, прежде чем он попадает в вашу машину.
- Он должен быть в состоянии обнаружить передовые вредоносные программы, как rootkits и вымогателей и все виды вредоносного программного обеспечения, как рекламное и шпионское программное обеспечение.
- Он должен защитить ваш браузер от уязвимостей браузера и иметь защиту DNS.
- Он не должен потреблять высокие вычислительные ресурсы для работы.

Таблица 2-1. *Бесплатное антивирусное программное обеспечение (Коммерческие версии этих продуктов также доступны с расширенными функциями защиты)*

Tool	Main Features	URL
avast Free antivirus	обнаруживать и блокировать вирусы, вредоносные программы, программы-шпионы, программы-вымогатели и фишинг. защитить ваш браузер от кибератак, защитить домашнее подключение Wi-Fi, имеет встроенный менеджерпаролей.	https://www.avast.com/ free-antivirus- download
Comodo Internet Security	многие функции, включая личный брандмауэр и расширенную защиту от вредоносных программ нулевого дня.	https://www.comodo.com/ home/internet- security/ free-internet- security. php
Avira	защита от червей, вирусов, троянов, шпионских программ. Имеет защиту облака, сканирует неизвестные файлы анонимно в облако в режиме реального времени для максимального обнаружения.	https://www.avira.com/ en/free- antivirus- win

Windows 10 поставляется с бесплатным антивирусным решением, Windows Defender. Эта программа помогает защитить ваш компьютер от вирусов и других передовых угроз, таких как руткиты и буткиты; однако его главным недостатком является отсутствие личного брандмауэра. Это не должно позволить вам недооценивать Windows Defender, потому что вы можете установить бесплатный специальный брандмауэр, как мы покажем следующий.

Брандмауэра

Брандмауэр отслеживает и контролирует входящий и исходящий сетевой трафик и помогает отсеивать хакеров, вирусов и червей, которые пытаются добраться до компьютера через Интернет. Как мы уже говорили, не все бесплатные антивирусные решения оснащены персональным брандмауэром, но есть много бесплатных выделенных персональных брандмауэров, которые могут выполнять эту работу. См Таблица 2-2 для самых известных из них.

Таблица 2-2. *Бесплатные брандмауэры*

Брандмауэр	**URL**
Comodo	https://personalfirewall.comodo.com
Zonealarm Free Firewall	https://www.zonealarm.com/software/free- firewall/

Антивредоносные программы

Кибератаки развиваются постоянно. Каждый день сложные вредоносные скрипты и программы создаются киберпреступниками, а антивредоносные решения помогают обнаруживать угрозы, которые ранее не были обнаружены обычными антивирусными решениями. Для достижения максимальной защиты необходимо иметь антивредоносное решение в дополнение к установленной антивирусной программе.

Бесплатное издание Spybot (https://www.safer-networking.org/dl/) имеет анти-вредоносных программ и анти-шпионских функций, которые могут быть установлены вместе с вашим антивирусным решением.Еще одна известная программа для обнаружения вредоносных программ malwarebytes (https://www.malwarebytes.com). Бесплатная версия имеет основные анти-вредоносных программы и шпионские защиты в дополнение к его способности удалять rootkits и ремонтировать файлы, которые повреждены. Он также может работать с любой антивирусной программой, уже установленной.

Обеспечение операционной системы

Независимо от того, какие виды программного обеспечения безопасности вы уже установили на ОС, обеспечение самой ОС по-прежнему является первой задачей, которую вы должны сделать перед установкой каких-либо программ или доступа к локальной сети или Интернету.

Существует два типа рисков, которые угрожаютOS.

- Логические угрозы, исходят от вредоносных программ и других вредоносных программ.

- Физические угрозы. Это происходит, когда злоумышленник получает физический доступ к вашей машине (например, через USB или другие порты) для выполнения созданных вредоносных действий.

Мы уже рассмотрели, как обеспечить первую часть логической стороны ОС путем установки программного обеспечения безопасности. В этом разделе мы будем продолжать охватывать другие части логической безопасности ОС, которая связана с конфигурацией ОС, в дополнение к физической безопасности.

Мы не будем углубляться в безопасность ОС, так как это требует написание другой отдельной книги. Для этой книги мы рассмотрим основную конфигурацию безопасности, которую вы должны сделать для повышения безопасности и конфиденциальности ОС. Основное внимание будет уделено ОС Windows, потому что это наиболее широко используемая ОС на земле.

Усиление настроек Windows OS

ОС Windows не предназначена для безопасной, анонимной ОС. При проведении поисков OSINT, вы должны избегать раскрытия вашей реальной личности в Интернете. Windows может быть настроена, чтобы быть более конфиденциальной после простых шагов. Кроме того, программное обеспечение и методы, которые мы собираемся продемонстрировать позже позволит вам проводить поиск OSINT анонимно в дополнение к сокрытию / маскировки цифрового отпечатка.

Примечание! Есть много различных операционных систем, как macOS, linux, и Windows в дополнение к мобильным ОС, как ioOS от яблока и андроида от Google. Независимо от ОС вы используете, он не был создан, чтобы быть полностью анонимным и частным. Есть специальные дистрибутивы, как правило, на основе linux, которые обеспечивают максимальную безопасность и анонимность при переходе в Интернете, как Tails OS, об этом позже в этой главе.

Предупреждение! Создайте новую точку восстановления системы перед реализацией настроек в этой главе, чтобы вы могли безопасно вернуть свои изменения в случае, если что-то пойдет не так.

На данный момент, давайте начнем наш список рекомендаций, чтобы укрепить вашу Windows.

ОБНОВЛЕНИЕ WINDOWS

Функция автоматического обновления для ОС Windows всегда должна быть включена. Обновление Windows 10 настроено на автоматическое по умолчанию.

ОБНОВЛЕНИЕ ВСЕХ УСТАНОВЛЕННЫХ ПРОГРАММ

Windows обычно обновляет программы Майкрософт, такие как пакет Microsoft Office и браузер Edge (IE) как часть обновления Windows, но вы должны убедиться, что другие программы (Adobe Reader, VPN клиенты, Firefox и Opera) также регулярно обновляются.

БЛОКИРОВКА КОМПЬЮТЕРА С ПОМОЩЬЮ USB-ДИСКА

Проверка подлинности входа в Windows по умолчанию не гарантирует необходимую безопасность для пользователей. Многие хакеры успешно скомпрометировали эту функциональность, чтобы получить несанкционированный доступ к Windows. Чтобы добавить дополнительный уровень безопасности, можно заблокировать компьютер USB-накопителем в дополнение к входу по умолчанию. Эта процедура необходима для старых версий Windows (7, XP), которые не могут быть защищены с помощью расширенных функций Windows 10.

USB Raptor позволяет заблокировать компьютер с помощью ФЛЭш-карты USB. Это бесплатная программа со многими расширенными функциями. Вы можете найти его на https://sourceforge.net/projects/ usbraptor/?source=typ_redirect.

ИСПОЛЬЗОВАНИЕ УЧЕТНОЙ ЗАПИСИ С МЕНЕЕ ПРИВИЛЕГИРОВАННЫМ ПОЛЬЗОВАТЕЛЕМ

При проведении поиска OSINT нет необходимости использовать учетную запись администратора; всегда желательно, чтобы вы использовали ограниченную учетную запись пользователя для ваших ежедневных задач. Это позволит эффективно защитить ваш компьютер от вредоносных программ, установленных непреднамеренно и предотвратить внешних хакеров от вторжения в вашу систему и установки вредоносного программного обеспечения. Вы можете настроить учетные записи Windows (все версии), перейдя в панель управления и учетные записи пользователей.

ИСПОЛЬЗОВАНИЕ СИЛЬНОГО ПАРОЛЯ ДЛЯ WINDOWS

Используйте надежный пароль для защиты входа в Windows и убедитесь, что изменить его один раз в три месяца. Позже в этой главе мы дадим советы о том, как создать надежные пароли и хранить их в менеджере паролей.

Для обеспечения соблюдения политики паролей в Windows 10 (все издания) выполните следующие действия:

- Перейдите в панель управления (Административные инструменты, Политика местной безопасности, Настройки безопасности, Политика учетных записей - Политика пароля.
- Справа нажмите дважды на кнопку "Максимальный возраст паролей".
- Установите количество дней, когда пароль может быть использован до Windows 10, необходимо, чтобы пользователи изменили его до 90 дней.

ВЕДЕНИЕ УПРАВЛЕНИЯ УЧЕТНОЙ ЗАПИСЬЮ ПОЛЬЗОВАТЕЛЯ ВКЛЮЧЕНО

Контроль учетной записи пользователя (UAC) отслеживает, какие изменения будут внесены в ваш компьютер, показывая всплывающее окно, когда вы пытаетесь выполнить действия, которые требуют административного доступа, как установка / установка программы. Включение UAC поможет вам удержать вредоносные программы от внесения изменений в ваш компьютер. Вы можете настроить UAC для каждой учетной записи пользователя через панель управления и учетные записи пользователей; затем нажмите кнопку "Изменить настройки управления учетными записями пользователей" (см. рисунок 2-3).

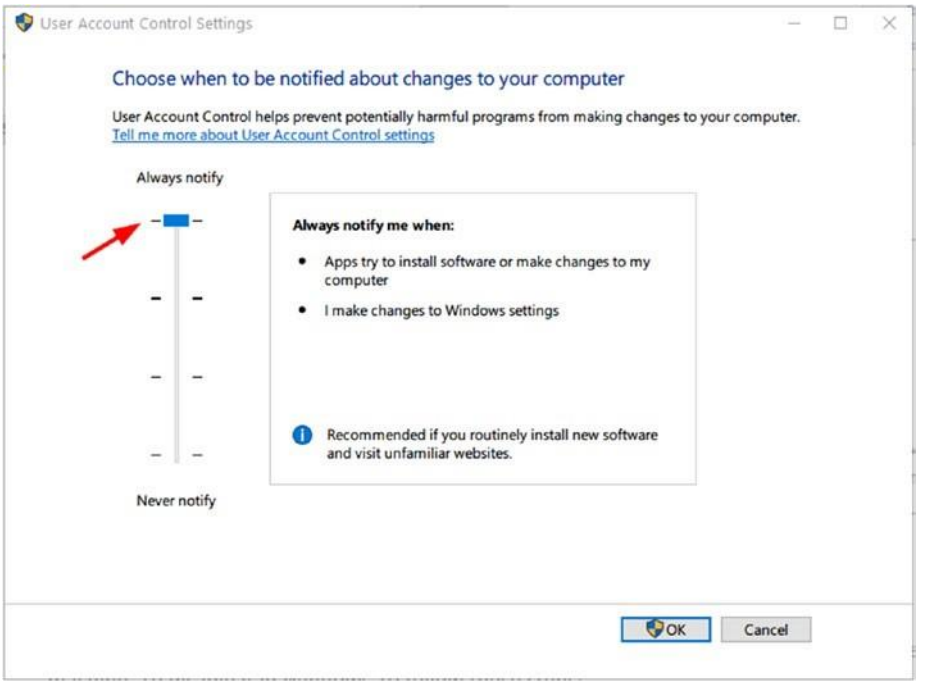

Рисунок 2-3. *Отрегулируйте настройки UAC под Windows 10, чтобы уведомить пользователя о любых изменениях в Windows и других приложениях*

ОТКЛЮЧЕНИЕ УДАЛЕННОЙ ПОМОЩИ

Эта функция позволяет удаленному пользователю получить доступ к вашей машине через сетевое соединение. Если вы не используете эту функцию, вы можете отключить ее, чтобы предотвратить хакеров от использования его, чтобы получить несанкционированный доступ к вашей машине. Чтобы отключить его в Windows 10, следуйте этим шагам (см. рисунок 2-4):

1. Введите **удаленные настройки** в поле поиска Cortana и выберите "Разрешить удаленный доступ к компьютеру".

1. Убедитесь, что выбрана опция "Не разрешайте удаленное подключение к этому компьютеру".

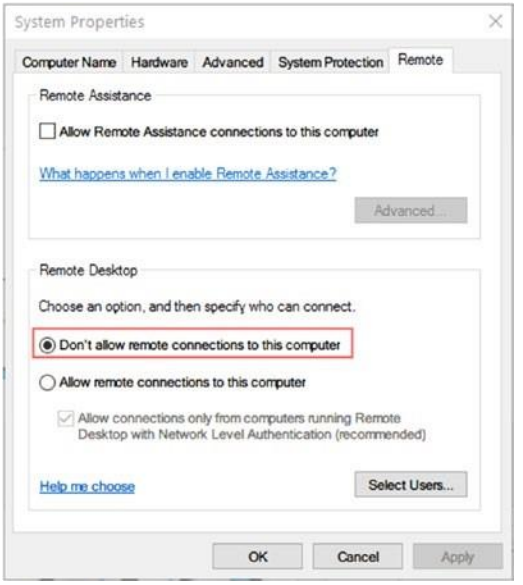

Рисунок 2-4. *Отключение удаленных соединений в Windows 10*

СОЗДАНИЕ СКРЫТЫХ ФАЙЛОВ ВИДИМЫМ

Некоторые вредоносные программы и другие вредоносные программы скрыты с помощью того же атрибута, что

Windows использует, чтобы скрыть свои системные файлы. Для отображения скрытых файлов и папок под Windows 10 выберите панель управления и параметры Файлового Исследователя, а затем перейдите на вкладку View и выберите опцию "Показать скрытые файлы, папки и диски". Кроме того, убедитесь, что отменить опцию "Скрыть защищенные файлы операционных систем". Рекомендуется просматривать расширения файлов, отменяя опцию "Скрыть расширения для известных типов файлов".

ЗАМОРАЖИВАНИЕ ЖЕСТКОГО ДИСКА

Замораживание программного обеспечения позволяет пользователю Windows восстановить свою ОС в предыдущем стабильном состоянии в течение нескольких секунд каждый раз, когда компьютер перезапускается. Например, рассмотрим ситуацию, когда

часть вредоносных программ попадает в вашу ОС, если у вас уже есть программа замораживания, и она активирована. Все, что вам нужно сделать, это перезапустить вашу машину, и все вернется в прежнее состояние.

RollBack Rx Home Edition (бесплатно для личного пользования) — это программа для замораживания компьютеров Windows. Вы можете найти её на http://horizondatasys.com/rollback-rx-time-machine/ rollback-rx-home/.

Многие кибератаки против операционных систем и программного обеспечения шифрования (полное шифрование диска) полагаются на загрузку машины жертвы с помощью USB или CD/DVD, чтобы взломать ключи шифрования или найти способ украсть конфиденциальные данные жертвы. Установив пароль для BIOS/UEFI, каждый раз, когда пользователь загружает машину, он должен предоставить своего рода учетные данные, следовательно, пароль, прежде чем компьютер загружает ОС. Этот трюк также предотвратит злоумышленника от изменения настроек BIOS или повреждения компьютера, стирания жесткого диска. Каждый производитель материнской платы имеет свое собственное меню, чтобы установить этот пароль, как правило, в разделе безопасности. Вы должны сначала загрузиться в BOIS/ UEFI, а затем активировать эту опцию.

ОТКЛЮЧЕНИЕ НЕНУЖНЫХ ПОРТОВ/ПРОТОКОЛОВ И УСЛУГ

Каждый открытый порт считается угрозой безопасности. Хакеры обычно сканируют открытые порты, чтобы попытаться получить доступ к машине жертвы. Мониторинг трафика, проходящих через порты, является задачей брандмауэра; при правильной настройке личного брандмауэра злоумышленники предотвращают использование открытых портов в злонамеренных целях. Наилучшей безопасной конфигурацией является "интерактивный режим" (в брандмауэре Comodo это правило называется Custom Ruleset), где брандмауэр просит вас предоставить или отказать в доступе к любому подключению, проходящее через порты ОС (см. рисунок 2-5).

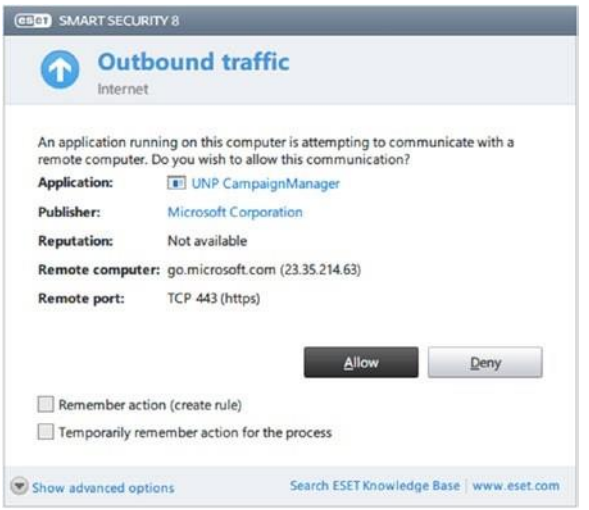

Рисунок 2-5. *Пример диалог предупреждения, выданный брандмауэром ESET, когда служба или приложение пытается установить постоянное соединение с удаленным узлам*

Как и порты, ненужные службы должны быть отключены. Windows загружает основные службы при запуске, но другие неиспользуемые службы должны быть отключены. Чтобы отключить службу в Windows, сделайте следующее:

1. Перейти к панели управления➤ Администрирование ➤ Службы.
2. Найдите неиспользуемые службы.
3. Дважды щелкните его, чтобы открыть диалоговое окно Свойств.
1. Выберите тип запуска Disabled .

Стать приватным в Windows 10

По сравнению с предыдущими версиями Windows, Windows 10 оснащена расширенными функциями безопасности для шифрования и аутентификации. Windows 10 также является более надежным против загрузки и руткит атак. Для использования современных функций безопасности, предлагаемых Windows 10, ваш компьютер должен иметь определенные аппаратные компоненты.

- *Trusted Platform Module (TPM) version 2.0*: Это используется для хранения криптографических ключей BitLocker. Это полная функция шифрования диска,

предлагаемая некоторыми изданиями Windows 10 (Windows 10 поддерживает BitLocker на Pro, Enterprise и Education изданиях).

- *Unified Extensible Firmware Interface (UEFI)*: Это замена BIOS, используемая в современных сертифицированных компьютерах Windows.
- *Fingerprint scanner*: Это улучшает традиционную схему проверки подлинности Windows.

Высоко рекомендуется биометрический сканер и 3D-камера для распознавания лиц, чтобы вы могли активировать расширенную схему биометрической аутентификации функции Windows 10 Hello. Тем не менее, их существование в современных компьютерах по-прежнему ограничено, потому что они увеличивают цену компьютера значительно.

Как мы уже говорили, Windows 10 улучшает регулярную аутентификацию Windows, внедряя современный механизм аутентификации под названием Hello. Это приложение позволяет пользователю войти в машину с помощью отпечатков пальцев, лица или даже радужной оболочки глаза. Биометрические данные пользователя не будут храниться где-либо в Интернете, для работы этой функции.

Настоятельно рекомендуется не использовать функцию Hello на компьютере, где вы собираетесь проводить поиск OSINT. Всегда желательно использовать локальную учетную запись Windows при входе в Windows, так как никто не может гарантировать, что может произойти при отправке ваших учетных данных или другой конфиденциальной информации через незащищенную среду, например в Интернете.

Windows 10 оснащена множеством новых функций для персонализации пользовательского интерфейса при его использовании. Например, Cortana — это цифровая помощь Windows, которая позволяет пользователю перемещаться по Windows с помощью голосовых команд; он также отслеживает действия пользователей на Windows, например, то, что пользователь вводит и ищет, и персонализирует будущие события в соответствии с этим. Чтобы контролировать сбор и использование данных Cortana, проверьте https://privacy.microsoft.com/en-us/windows-10-cortana-and-privacy, который содержит инструкции о том, как отключить его на различных устройствах Windows.

Несколько конфигураций конфиденциальности Windows 10 хранятся в одном месте. Windows 10 создала панель мониторинга конфиденциальности, доступ к которым можно получить, Зайдя в настройки Windows, чтобы получить доступ к странице "Настройки", а затем выбрать конфиденциальность (см. рисунок 2-6).

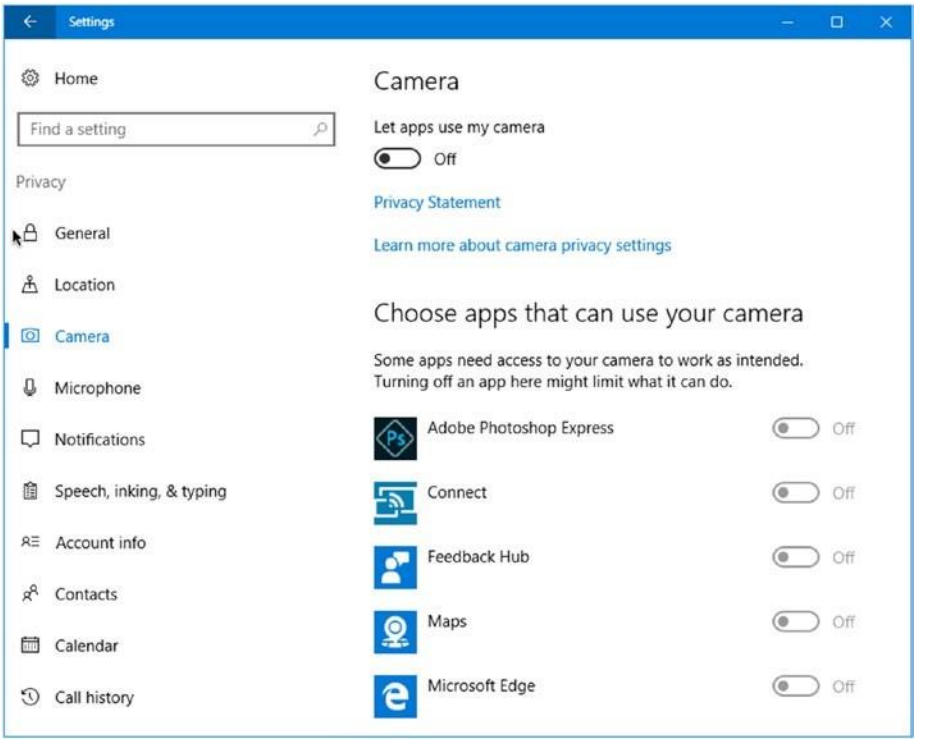

Рисунок 2-6. *Настройки конфиденциальности в Windows 10 объединены в одном месте*

Все в панели мониторинга конфиденциальности самоочевидно; желательно отключить все, что вам не нужно, и не использовать браузер Microsoft Edge для проведения онлайн-поиска. Skype, Dropbox и Microsoft OneDrive также не рекомендуются для обмена важными файлами. Безопасные альтернативы этим программам будут даны позже в главе.

Уничтожение цифровых следов

Уничтожение данных является важным шагом в освещении ваших цифровых следов при проведении поисков OSINT. Цифровые следы – предыдущее использование – на компьютере остаются даже после форматирования много раз. Есть три способа, в которых данные и остатки его могут быть уничтожены надежно: физическое, размагничивание и логическое разрушение. Мы кратко опишите каждый метод, но давайте сначала поговорим о различных типах жестких дисков, используемых сегодня.

Существует два типа жестких дисков, используемых в настоящее время в вычислительных устройствах.

- *Hard disk drive (HDD):* Это старый тип, который был использован с первых дней персональных компьютеров. Это механическое устройство, которое в основном состоит из металлического диска (может быть более одного) из стекла или алюминия, покрытого магнитным материалом для хранения данных. HDD обычно используются для массового хранения и стоят меньше, чем SSD.
- *Solid-state drive (SSD)*: Это более продвинутая версия диска. Он не содержит движущихся частей и не имеет дисков. Вместо этого он хранит данные о небольших микрочипах (например, USB-флэш-накопителях). SSD быстрее и меньше, чем HDD, но имеет ограниченный срок службы по сравнению с HDD.

Современные компьютеры и все смартфоны и планшеты используют SSD как единственный тип единицы памяти; однако, это не означает, что HDD будет исчезать. HDD является зрелой технологией, и она будет оставаться в использовании в течение длительного времени в соответствии со многими исследованиями.

Для этой книги давайте посмотрим разницу между SSD и HDD с точки зрения восстановления данных.

Восстановление данных из HDD относительно легко и может быть проведено любым пользователем с соответствующими инструментами. При удалении файла в HDD файл не удаляется напрямую; вместо этого удаляется только указатель на этот файл на диске. Эта операция помогает ускорить процесс удаления, экономя драгоценное время. Восстановление данных с SSD-диска во многих случаях довольно сложно и невозможно. Например, SSD использует другой механизм при обработке удаленных файлов. Все современные SSD-диски выполнгяют команду TRIM при включении. Эта команда будет удалять удаленные блоки данных файла мгновенно, что позволяет другому файлу занять это место. Это ускоряет процесс записи при следующем письме ОС на диск. Существует множество подходов к внедрению TRIM на SSD-устройствах, в зависимости от использования ОС. Некоторые операционные системы будут выполнять TRIM мгновенно после каждого удаления файла, в то время как другие будут выполнять TRIM через регулярные промежутки времени.

Теперь давайте посмотрим, как данные могут быть полностью уничтожены при использовании обоих типов жесткого диска. Для достижения этой цели используются следующие методы:

- *Physical destruction*: Это наиболее безопасный и обычно предпочтительный метод, используемый разведывательными службами и гигантскими корпорациями для уничтожения секретных и высококлассных активов данных. Этот метод работает, физически разрушая среду хранения, будь то HDD, SSD, CD/DVD, или флэш-накопитель, так что он больше не может быть использован.

1. *Размагничивание*: Это еще один безопасный метод для предотвращения антивосстановления методов восстановления данных из среды хранения; он работает, подвергая среде хранения мощного магнитного поля размагничивание уничтожить хранящиеся данные на магнитных носителях. Этот метод хорошо работает с HDD. SSD-устройства лучше уничтожаются физически, чтобы избежать возможности восстановления сверхсекретных данных.

1. *Логическое разрушение*: Это наиболее широко используемый метод уничтожения данных при сохранении среды хранения для использования в будущем. Этот метод работает с помощью специализированного программного обеспечения для покрытия старых данных и остатков данных со случайными символами, написанными инструментом вытирания. Есть много алгоритмов вытирания уже используется для уничтожения данных в цифровом виде таким образом; некоторые из них являются более безопасными, чем другие. Однако, что вы должны знать при использовании такой техники для уничтожения данных является то, что он не может гарантировать 100-процентное удаление всех данных на диске. Некоторые передовые методы восстановления, основанные на оборудовании, по-прежнему способны захватить ваши старые данные, или, по крайней мере, их части (но это дорого и отнимает много времени). Логические методы уничтожения данных имеют некоторые недостатки тоже; им нужно время, чтобы закончить, потому что они должны писать случайные данные несколько раз (несколько проходов) по всем доступным секторам на жестком диске. Кроме того, этот метод предполагает, что ваш жесткий диск работает и записывается, чтобы написать случайные данные в него. Еще одна проблема с вытирая программное обеспечение возникает при использовании его для уничтожения данных, хранящихся с помощью технологии RAID. Эта технология обеспечивает отказоустойчивость путем зеркального

отражения данных на нескольких дисках в различных физических местах. В такой ситуации инструмент вытирания должен отслеживать все зеркальные данные на всех корпоративных серверах хранения данных.

Разработаны различные стандарты для уничтожения данных (логическое уничтожение данных) на жестких дисках. Таблица2-3показывает самые популярные из них.

Таблица 2-3. *Алгоритмы обработки данных*

Техника стирания	Уровень безопасности	Количество перезаписей
HmG Infosec Standard 5	High	3
dod 5220.22-m	High	3
Bruce Schneier's algorithm	High	7
German standard BSI/VSITr	High	7

Существуют различные программы для уничтожения жестких дисков, и большинство поддерживает более одного стандарта стирания. В таблице 2-4 перечислены самые популярные из них (только бесплатные инструменты).

Table 2-4. *Data Destruction Tools*

Program	URL	Comments
dBaN	https://dban.org	Бесплатная версия поддерживает только HDD.
eraser	www.heidi.ie/eraser/	Опенсорс; поддерживает SSD.
CCleaner	www.piriform.com/ccleaner	Программа под Windows.
Sdelete	https://technet.microsoft.com/en-us/sysinternals/sdelete.aspx	стирает данные в соответствии cDoD 5220.22-m.

Для SSD-дисков большинство производителей SSD предлагают утилиты для безопасного удаления данных из своих дисков. Вы можете проверить веб-сайт производителя SSD-диска для таких утилит. Таблица 2-5 дает прямые ссылки на некоторые из них.

Таблица 2-5. *Инструменты для стирания данных SSD*

Tool	URL

Intel Solid State drive Toolbox	https://downloadcenter.intel.com/download/26574?v=t
Corsair SSd Toolbox	www.corsair.com/en-eu/support/downloads
Samsung magician	www.samsung.com/semiconductor/minisite/ssd/download/tools.html
Sandisk SSd	https://kb.sandisk.com/app/answers/detail/ a_id/16678/~/secure-erase-and-sanitize

Уничтожение цифровых следов важно при проведении поисков OSINT. Имейте в виду, что браузеры, программное обеспечение для просмотра изображений, программы Microsoft Office и все, что вы делаете на вашем компьютере, оставят цифровые следы. Используя советы в этом разделе, вы сделаете отслеживание ваших следов трудным и даже невозможным.

Предупреждение! Для людей (правоохранительных и военных должностных лиц), проводящих сверхсекретные поиски OSINT, которые нуждаются в максимальной анонимности возможно, очень желательно использовать анонимные ОС, как Tails OS, охватываемых позже в главе.

Общие настройки конфиденциальности

В этом разделе мы перечислим некоторые рекомендации по поддержанию конфиденциальности при переходе в Интернет. Некоторые из этих советов можно считать тривиальными на первый взгляд; однако, важно реализовать их, потому что не делать этого может нанести серьезный ущерб вашей частной жизни, если используется внешними противниками.

Изоляция камеры ноутбука

Хакеры и спецслужбы гоняетесь за компьютерными камерами и микрофонами при нападении на конкретных людей. Таким образом, желательно, заклеить ваши веб-камеры с лентой для обеспечения безопасности.

Как избежать пиратского программного обеспечения

Пиратское программное обеспечение может включать вредоносную полезную нагрузку, например, троян или кейлоггер, которые могут вторгаться в частную жизнь пользователей и шпионить за вычислительным устройством. Настоятельно рекомендуется не получать контент с пиратских сайтов.

Если вы предпочитаете использовать бесплатные программы, загруженные из Интернета, очень желательно использовать антивирусное решение для их сканирования перед их выполнением. Чтобы стать более уверенным, вы можете сканировать загруженную программу с помощью бесплатных сервисов сканирования, что пригодится, когда вы хотите сканировать определенный файл/программу с помощью нескольких антивирусных движков.

VirusTotal (https://www.virustotal.com) это бесплатная служба, которая анализирует подозрительные файлы и URL-адреса и облегчает быстрое обнаружение вирусов, червей, троянов и всех видов вредоносных программ. Все, что вам нужно сделать, это ввести URL-адрес веб-сайта вы хотите проверить или загрузить файл / программы, чтобы увидеть, является ли это ясно из вредоносных угроз.

Обработка цифровых файлов Метаданные

Метаданные — это данные о данных; он содержит описательную, как правило, скрытую информацию о файле, к которому он принадлежит. Метаданные цифрового файла включают имя автора, размер файла, местоположение, дату создания/время и комментарии.

Концептуально все типы цифровых файлов могут включать метаданные. С точки зрения конфиденциальности, пользователи в основном обеспокоены метаданными, которые существуют в цифровых изображениях, аудиофайлах и видеофайлах. Microsoft Office и другое программное обеспечение для создания цифровых текстовых документов также содержит множество метаданных. Метаданные обычно хранятся в цифровом файле; однако, некоторые типы файлов хранят его в отдельном файле.

Одним типом метаданных, существующим в файлах изображений, является EXIF. Это стандарт, который определяет формат изображений, звуковых и вспомогательных тегов, используемых цифровыми камерами (включая смартфоны), сканерами и другими системами обработки изображений и звуковых файлов, записанных цифровыми камерами. Данные EXIF встраиваются в файл изображения и работают только с изображениями JPEG. Метаданные EXIF могут содержать метаданные геолокации в дополнение к широкому спектру технической информации.

Другие типы включают в себя расширяемую платформу метаданных (XMP), которая поддерживает различные типы цифровых файлов и не ограничивается изображениями, и Международный совет по телекоммуникациям прессы (IPTC), который считается старым форматом метаинформации.

Рекомендуется проверить метаданные всех цифровых файлов, прежде чем загружать их в Интернет или делиться ими с коллегами, чтобы избежать утечки личной информации о себе и устройстве. Есть много бесплатных инструментов, которые могут просматривать и отсылать метаданные цифрового файла; Начнем с цифровых изображений.

Exif Pilot (www.colorpilot.com/exif.html) — это бесплатный редактор EXIF, который позволяет просматривать, отсчитывать и удалять данные EXIF, EXIF GPS, IPTC и XMP в дополнение к добавлению новых тегов и импорту и экспорту EXIF и IPTC в/из текстовых и файлов Microsoft Excel. Другие бесплатные инструменты, которые могут быть использованы для просмотра метаданных изображений, являются GIMP (https://www.gimp.org) и XnView (www.xnview.com/en/), который поставляется бесплатно для частного и образовательного использования (см. Рисунок 2-7).

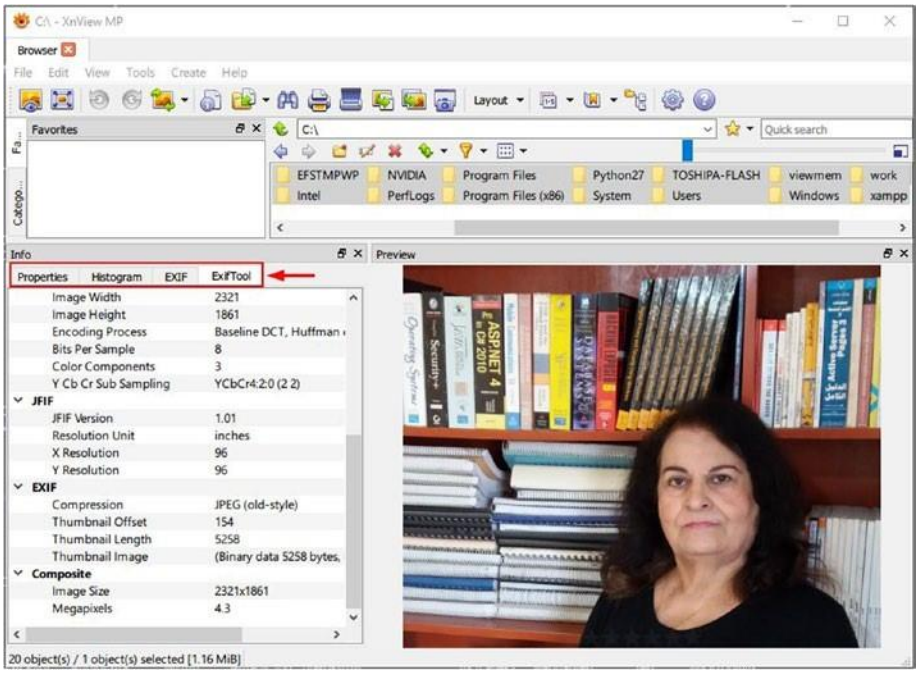

Рисунок 2-7. *Using the XnView tool to view EXIF tags*

Windows поставляется со встроенной функцией, которая позволяет просматривать и удалять некоторые метаданные, связанные с документами и цифровыми изображениями.

Однако имейте в виду, что Windows может быть не в состоянии удалить все теги EXIF, поэтому, если вы собираетесь совместно использовать важные файлы, всегда используйте уже упомянутые сторонние инструменты.

Чтобы удалить EXIF с помощью Windows, нажмите правой кнопкой мыши изображения, выберите Свойства и перейдите на вкладку «Подробности». В нижней части, нажмите удалить свойства и личную информацию, чтобы открыть инструмент удаления EXIF. Инструмент позволяет либо создать копию изображения со всеми удаленными метаданными, либо выбрать свойства для удаления из выбранного файла (см. рисунок 2-8).

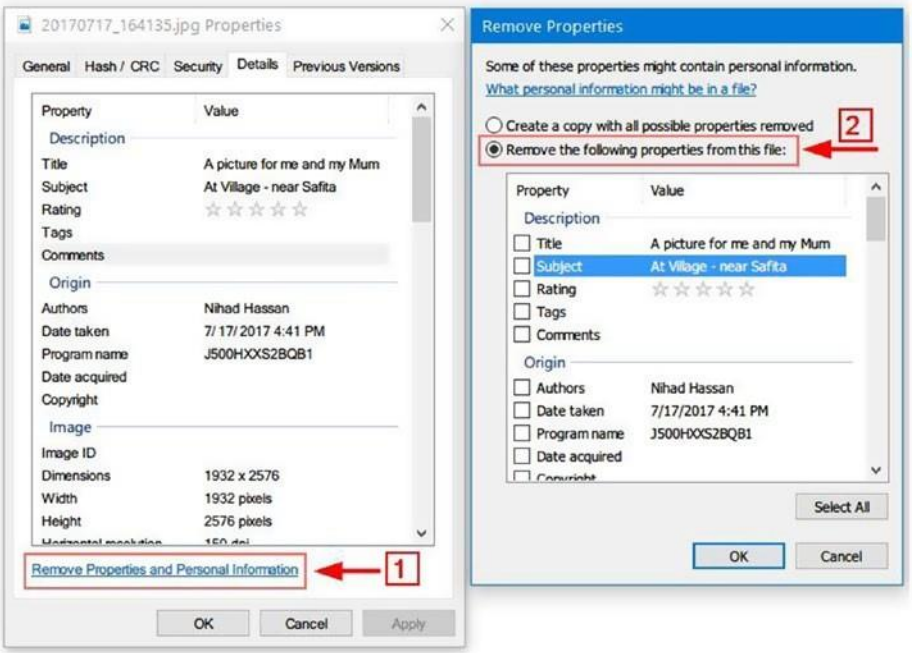

Рисунок 2-8. *Удаление метаданных EXIF с помощью встроенной функции Windows*

Как мы уже говорили, метаданные также существуют в PDF-файлах, файлах Microsoft Office, а также в аудио- и видеофайлах. В этом разделе мы кратко рассмотрим некоторые полезные инструменты для очистки метаданных от таких типов файлов.

Чтобы очистить метаданные из файлов PDF, Adobe имеет функцию под названием Sanitize Document. После нажатия на него можно удалить все скрытые метаданные из предназначенного файла PDF(см. Рисунок 2-9).

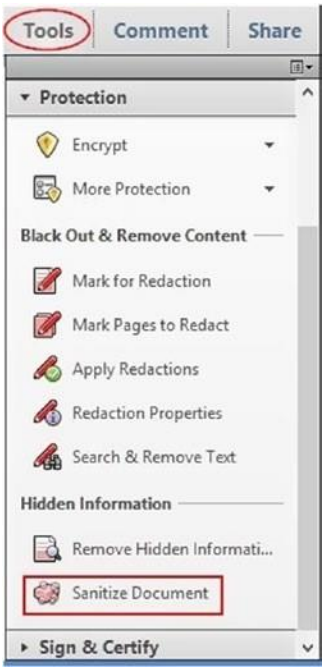

Рисунок 2-9. *Очистка метаданных файлов PDF*

Примечание! Не все версии считывателя adobe поддерживают функцию отчистки. Если текущая версия не имеет этой функции, вы можете использовать сторонние инструменты для удаления метаданных из файлов pdF, таких как BeCypdFmetaedit(www.becyhome.de/becypdfmetaedit/description_eng.htm) or pdF metadata editor (http://broken-by.me/pdf-metadata-editor).

Для просмотра/редактирования и удаления метаданных аудиофайлов используйте Mp3tag (www.mp3tag.de/en). Для метаданных видеофайла используйте MediaInfo (https://mediaarea.net/en/MediaInfo).

Чтобы удалить метаданные из документов Microsoft Office 2010, 2013 и 2016, можно проверить метаданные документа, выбрав файл, а затем перейти на вкладку Info. Панель Свойств будет на правой стороне; отсюда вы можете удалить метаданные документа, нажав кнопку Свойства и выбрав Расширенные свойства (см. Рисунок 2-10).

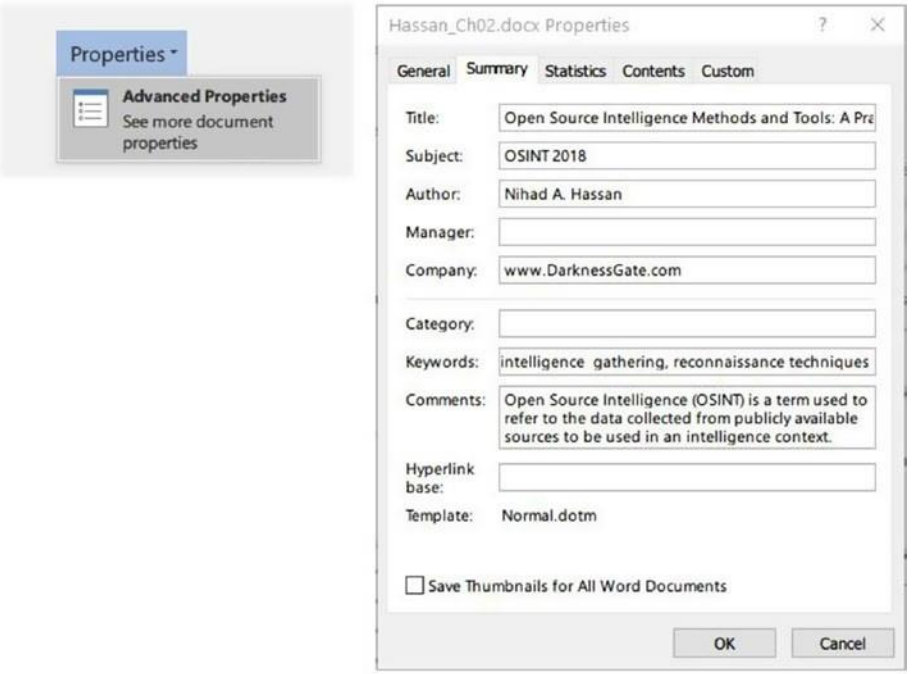

Рисунок 2-10. *Удаление метаданных документа Microsoft Office*

В Microsoft Office 2007 необходимо нажать кнопку Microsoft Office, а затем выбрать Prepare➤ Свойства для редактирования метаданных документа.

Еще одна проблема, необходимость рассмотрения при отправке документов Microsoft Office сторонним сторонам, заключается в удалении других скрытых метаданных. К счастью, Microsoft Office предоставляет функциональность для удаления скрытых метаданных. Вы можете получить доступ к этой функции в Microsoft Word 2010, 2013 и 2016, выбрав файл➤ Информация ➤ Проверка на наличие проблем➤ Проверка документа. В Microsoft Word 2007 вы можете получить доступ к этой функции, нажав кнопку Office и выбрав Подготовить ➤ Осмотр Документа.

Физическое обеспечение безопасности ПК

Мы уже рассмотрели различные меры предосторожности для поддержания вашей конфиденциальности, но все бесполезно, если ваше вычислительное устройство или оборудование (или портативные единицы хранения) будут украдены или получать несанкционированный физический доступ находясь без присмотра. Люди, работающие для сбора информации OSINT для расследования преступлений и других официальных

вопросов, должны проявлять особую осторожность, чтобы избежать раскрытия любой информации о случаях, над которыми они работают, и исключить потерю своего оборудование, содержащее конфиденциальную информацию.

Корпорации и правительственные учреждения проводят специальную политику количественной оценки рисков для ИТ-инфраструктуры и возможных последствий, а также меры защиты, которые должны быть приняты для смягчения таких рисков. Пользователи должны следовать этим руководящим принципам, когда это применимо.

Лица также страдают от физических угроз. Кража и аппаратные дефекты могут помешать им получить доступ к данным, хранящимся на вычислительных устройствах, в дополнение к раскрытию этих данных неавторизованным пользователям. Например, ноутбуки, которые остаются без присмотра без блокировки кабеля, могут быть быстро украдены. Для защиты мобильных устройств используйте эти советы:

- При использовании ноутбука в общественных местах, закрепите его с помощью кабельного замка, прикрепленного к тяжелому объекту (например, стол, стол, колонка в саду).
- Не выходите из офиса, не запирая его, когда в нем есть портативные устройства.
- Не храните конфиденциальные файлы вашей работы на вашем вычислительном устройстве без соответствующего разрешения, и убедитесь, что для шифрования все, если вы храните такие данные на вашем устройстве.
- Не храните конфиденциальные/личные данные на мобильных устройствах без надлежащего шифрования.
- Используйте пароль для защиты мобильного устройства от несанкционированного доступа.
- Не включайте Bluetooth-соединение в общественных местах и при необходимости запускайте его в течение короткого периода времени для получения или отправки срочных файлов.
- Выключите Wi-Fi, когда вы его не используете. Будьте осторожны при использовании общедоступных точек доступа и шифруйте свое соединение с помощью VPN при использовании небезопасных подключений к Интернету.

- Храните письменный отчет о модели, серийном номере, MAC-адресе и другой соответствующей информации о вашем портативном устройстве в случае его кражи.

Методы онлайн-слежения

Веб-отслеживание используется для записи поведения пользователей при просмотре веб-страниц при выходе в Интернет. Эта деятельность проводится различными сторонами для различных целей. Например, социальные сайты могут отслеживать своих пользователей на многих веб-сайтах. Эта информация может быть позже связана с каждой учетной записью пользователя, например, с учетной записью Facebook, чтобы показывать персонализированную рекламу и услуги.

В этом разделе мы познакомим вас с тем, как работают технологии онлайн-отслеживания. Эти знания имеют важное значение для понимания того, как вы должны скрыть свою личность позже, чтобы избежать отслеживания при проведении поисков OSINT.

Отслеживание по IP-адресу

Первое техническое, что вам нужно понять, это концепция Интернет-протокола (IP). Важно понять эту концепцию и как устройства подключены к Интернету, потому что большинство методов анонимизации работают, заслоняя ваш реальный IP-адрес, чтобы избежать отслеживания. Кроме того, вы не можете защитить свою цифровую конфиденциальность, не зная, как подключены интернет-устройства в современном цифровом мире.

Что такое IP-адрес?

IP-адрес — это уникальный адрес, который вычислительные устройства используют для подключения к Интернету, идентификации себя и связи с другими устройствами в сети IP. Этот адрес уникален для каждого устройства в сети IP; следовательно, ни одно из двух устройств не может иметь одинаковый адрес в каждой сети.

Уже используются два стандарта IP-адресов. Стандарт IPv4 является наиболее широко используемым; он может вместить до 4,3 миллиарда адресов. По-видимому, этого числа недостаточно, особенно при взрыве использования устройств Интернета вещей (IoT). Этот факт привел к тому, что другой стандарт под названием IPv6, который может вместить более чем в 7,9-1028 раз больше адресов, чем IPv4.

При подключении к Интернету вы либо используете один и тот же IP-адрес каждый раз (известный как статический IP), либо каждый раз — по-разному —так же (известный как динамический IP).).

Статический IP-адрес — это адрес, который назначается вашим поставщиком услуг Интернета (ISP) и не изменяется с течением времени. Этот вид адреса обычно используется бизнес-корпорациями, государственным сектором и другими ИТ-провайдерами, такими как поставщики услуг электронной почты.

Динамический IP-адрес, с другой стороны, назначается динамически вашим ISP каждый раз, когда вы подключаетесь к Интернету. Он использует протокол под названием Dynamic Host Configuration Protocol (DHCP) для присвоения новых IP-адресов всякий раз, когда вы подключаетесь к Интернету или, ваш маршрутизатор перезагружается.

Примечание! Чтобы определить, назначен ли вам динамический или статический IP-адрес, откройте запрос командной строки. В Windows 10 нажмите Windows и X, а затем нажмите запрос команды (админ). Введите ***ipconfig /all,*** а затем нажмите клавишу ввода. Если DHCP включен установлен на Да (см. Рисунок 2-11),то у вас , скорее всего, динамический внутренний ip-адрес.

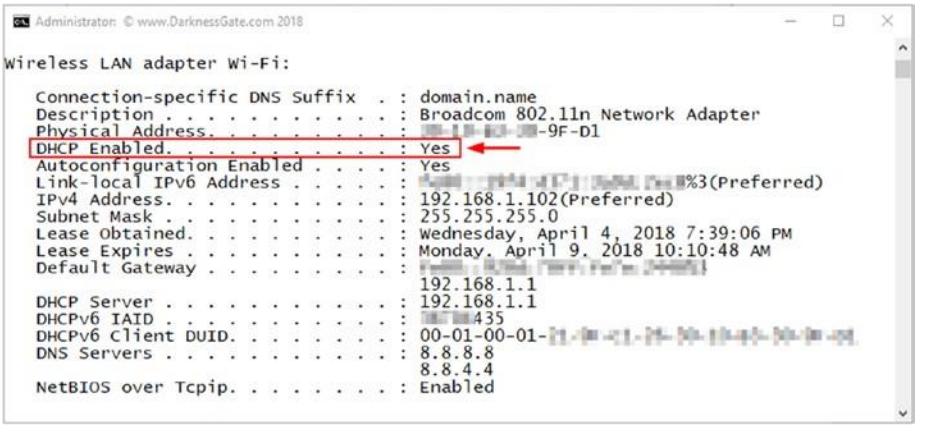

Рисунок 2-11. *Определите, использует ли ваш компьютер динамический или статический IP-адрес.В этом случае мы используем динамический IP-адрес.*

IP-адреса бывают двух типов: общедоступные и частные IP-адреса. Публичный IP-адрес обеспечивает прямой доступ в Интернет. Частный IP-адрес является IP-адресом, не находящимся в Интернете во внутренней сети, и используется для присвоения личного номера вашим вычислительным устройствам в вашей домашней или офисной сети, чтобы избежать их непосредственного воздействия в Интернете. Например, вы можете иметь один публичный IP-адрес, назначенный вашим маршрутизатор в вашей офисной сети, и каждый из компьютеров, планшетов, смартфонов и периферийных устройств, подключенных к маршрутизатору (через проводное соединение или Wi-Fi) получить частный IP-адрес от вашего маршрутизатора через DHCP.

Примечание! DHCP — это сетевой протокол, используемый в ip-сетях. Он работает, динамически распределяя ip-адреса на набор подключенных узлов на основе предварительно настроенного пула адресов.

Как используеться IP-адрес для отслеживания вас в Интернете?

Всякий раз, когда вы посещаете веб-сайт, проводите поиск в Интернете или получаете доступ к учетной записи вашего социального сайта, ваш IP-адрес соединения будет доступен для подключенного сайта. Почти все веб-сайты записывают IP-адреса своих посетителей среди других деталей, таких как дата/время посещения, посещенных страниц и продолжительность, действия пользователей на веб-сайте и многое другое. Зная IP-адрес также почти-достаточно, чтобы выяснить примерно ваше текущее географическое положение.

Ваш интернет-президент также запишет ваш IP-адрес. Интернет-провайдеры обычно записывают историю просмотра своих пользователей и связывают ее с реальной личностью каждого пользователя (провайдеры обычно запрашивают действительный правительственный идентификатор для предоставления интернет-соединений для своих клиентов).

Социальные сайты, такие как Facebook и Twitter, отслеживают историю просмотра своих пользователей на многих веб-сайтах. Например, кнопки «Нравится и Добавить» facebook и кнопки твита Twitter используются для отслеживания действий пользователя в Интернете,

даже если пользователь не нажимает на них. Вся эта информация хранится в отдельном журнале, прилагаемом с идентификатором учетной записи социальной учетной записи каждого пользователя — Facebook, Instagram или Twitter, чтобы лучше настроить пользователя на заказную рекламу. Хранение таких журналов опасно, потому что все ваши веб-поиска и веб-истории подключиться к вашему реальному имени. Во многих разоблачениях WikiLeaks говорится о том, что спецслужбы имеют различные возможности для доступа к пользователю гигантских ИТ-провайдеров. Гигантские корпорации также заинтересованы в таких данных, чтобы использовать их для получения коммерческой выгоды. Это означает, что все ваши конфиденциальные данные будут выставлены в той или иной форме.

Хотя отслеживание онлайн-пользователей через их IP-адреса по-прежнему является наиболее распространенным методом, используемым различными субъектами, существуют и другие передовые технические методы, которые позволяют стороннему наблюдателю отслеживать действия пользователя в Интернете, даже не зная пользователя IP-адрес, и это то, что мы будем говорить о в предстоящем разделе.

Cookie

Cookie представляют собой небольшие текстовые файлы, обычно хранящиеся в браузере клиентского компьютера. Файл cookie содержит информацию, специфичную для компьютера клиента в дополнение к названию веб-сайта, сроку годности и идентификационному номеру пользователя, чтобы отличить пользователя от других посетителей. Cookie позволяют владельцу веб-сайта, чтобы иметь возможность распознавать браузер посетителя в следующий раз, для эффективной работы веб-сайта.

В основном уже используются два типа файлов cookie: сессионные cookie и постоянные cookie.

Файлы сессии хранятся во временном месте в клиентском браузере и удаляются, когда пользователь закрывает веб-браузер или выбивает журналы из текущего сеанса. Такие файлы cookie обычно используются для запоминания информации о корзине пользователей или для хранения данных между несколькими страницами.

Примечание! большинство веб-сайтов завод HTTP cookie для отслеживания посетителей сайта или запоминания учетных данных пользователя. Этот вид менее рискованно, чем постоянные файлы

cookie, и может быть безопасно удален с помощью стандартной функции браузера удалить cookie-файлы.

Постоянные cookies бывают двух основных типов: flash cookies и ever cookies. Постоянные cookies более настойчивы, чем файлы cookie HTTP, и содержат информацию с других веб-сайтов, которая используется для отслеживания деятельности пользователя в Интернете на нескольких веб-сайтах. С flash cookies, файлы cookie хранятся в определенной папке на жестком диске клиента (не в клиентском браузере, например HTTP cookie). Другими словами, такие файлы cookie не будут удалены при использовании стандартной функции браузера Удалить cookie. По соображениям безопасности настоятельно рекомендуется отключить этот вид cookie и удалить установленный в настоящее время. Вы можете достичь этого, перейдя к панели управления➤ Flash Player и выбор опции "Блокировать все сайты от хранения информации на этом компьютере" (рисунок2-12).

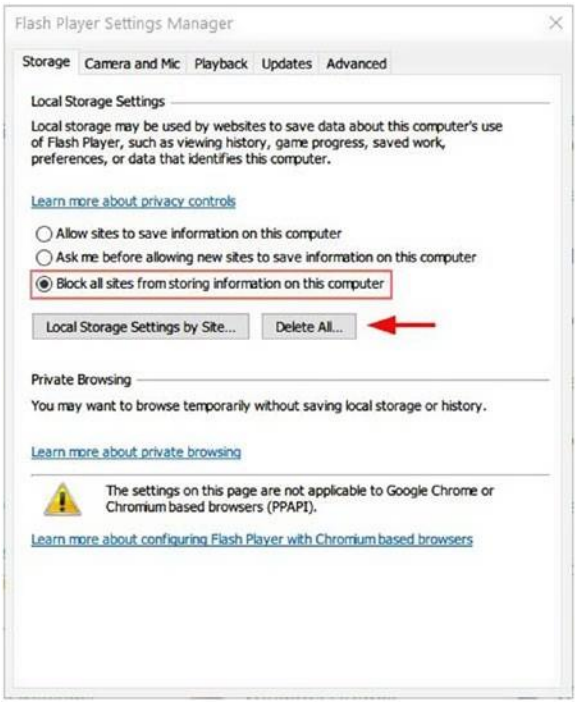

Рисунок 2-12. *Отключение Flash – cookies через Flash Player в Настройки менеджера*

Примечание! FlashCookiesView (www.nirsoft.net/utils/flash_cookies_view.html) это небольшая утилита, созданная NirSoft что позволяет отображать список Flash cookies которые существуют в вашей системе и удалить их.

Постсоянные cookie является еще одним типом стойких cookies. Этот тип cookie — это файл cookie на основе JavaScript, который может выжить даже после того, как пользователь удаляет файлы cookie HTTP и Flash из своего аппарата. К счастью, браузеры и анти-вредоносные программы, которые существуют сегодня, теперь могут обнаруживать и блокировать когда-либо cookie .

Примечание! Следует отключить плагины Java или, по крайней мере, установить настройки безопасности на высоком уровне. Для этого выберите

панель управления➤ Java; затем перейдите на вкладку безопасности и выберите опцию "Очень высокая".

Цифровые отпечатки

Отпечатки браузера — это набор технической информации о клиентской ОС и браузере, который можно использовать для различения клиентской машины в Интернете. Такая техническая информация включает тип браузера, установленное дополнение, пользовательский агент, установленные шрифты, настройки языка, часовой пояс, размер экрана, операционная система (ОС) версия, и глубина цвета, среди прочего.

Отпечатки позволяют трекерам отслеживать компьютер пользователя, даже если файлы cookie и JavaScript отключены, и это позволяет им различать клиентскую машину между миллионами подключенных устройств. Вы можете думать, что такая техническая информация является универсальной и не может быть использована для распознавания конкретного вычислительного устройства. Мы боимся, что вы ошибаетесь, потому что, когда такая информация объединена, вы можете нарисовать всеобъемлющую уникальную картину о каждой машине пользователя, а позже, эта информация может быть связана с реальной личностью, в сочетании с другими конфиденциальной личной информации (SPI), таких как имя, номер социального страхования или номер телефона. Это должно эффективно позволять различным сторонам легко профилировать людей без использования традиционных методов отслеживания, таких как IP-адреса компьютера и файлы cookie.

Существует два основных типа дактилоскопии устройств: методы на основе сценариев и активного окна.

ОТПЕЧАТОК НА ОСНОВЕ СЦЕНАРИЕВ

Этот тип работает, загружая сценарий, обычно используется JavaScript (Flash, Silverlight и Java applets) — в браузер пользователя. Этот скрипт будет выполнять и собирать техническую информацию о браузерах пользователей и технических спецификациях машины, таких как разрешение экрана, тип процессора и другие сведения о целевой системе. Затем хэш производится на основе собранной информации, которая впоследствии используется для идентификации и отслеживания вашего компьютера, как IP-адрес.

Основная защита от этого метода заключается в том, чтобы отключить JavaScript в вашем браузере. Однако такой подход нецелесообразен и может привести к взлому многих веб-сайтов

(большинство инфраструктур веб-дизайна основаны на JavaScript для предоставления функциональности).

ОТПЕЧАТОК АКТИВНОГО ОКНА

Отпечаток активного окна далее(canvas) — это html-элемент, используемый для рисования графики (линии, формы, текст, изображения) и анимации на веб-страницах с помощью API JavaScript. Этот метод используется различными субъектами, особенно рекламодателями, для браузеров отпечатков пальцев для профилирования людей и отслеживания их в Интернете.

Canvas отпечаток работает, рисуя невидимое изображение в клиентском браузере пользователя. После того, как обращается на клиентском браузере, изображение будет собирать различные технические сведения о браузере пользователя и ОС. Затем на основе собранной информации создается хэш. Это позволяет онлайн-трекерам отслеживать действия пользователей на различных веб-сайтах на основе этого хэша, который является уникальным для клиентской машины каждого пользователя.

Отпечаток браузера является мощным инструментом для отслеживания пользователей на многих веб-сайтах. Этот тип отслеживания (также известный как *stateless tracking*) вызывает серьезные проблемы конфиденциальности, поскольку трудно обнаружить и неподкованным пользователям может быть трудно противостоять таким методам.

HTML5

HTML5 является последней версией HTML. Он поставляется с новыми функциями, которые могут быть использованы для отслеживания пользователей в Интернете. Например, HTML5 Web Storage feature—который используется для хранения содержимого в автономном режиме на пользовательских машинах, может быть использован для хранения кода отслеживания, как файлы cookie.

Проверка цифрового следа

Отпечатки в настоящее время считается наибольшим риском, с которым сталкиваются пользователи при серфинге в Интернете. Мы не можем проводить безопасные поиски OSINT, не полностью понимая этот риск и не работая над его предотвращением. В следующем разделе мы покажем, что показывает ваш текущий цифровой отпечаток с помощью двух бесплатных услуг.

BROWSERLEAKS

Browserleaks (https://browserleaks.com) это инструмент тестирования веб-безопасности, который показывает вам, какие личные данные могут быть утечки без вашего разрешения, когда вы просматриваете в Интернете.

PANOPTICLICK

Panopticlick (https://panopticlick.eff.org) является исследовательским проектом, созданным Electronic Frontier Foundation (https://www.eff.org/). Он будет анализировать, насколько хорошо ваш браузер и дополнения защищают вас от методов отслеживания в Интернете.

Безопасный просмотр в Интернете

Ранее вы узнали, как браузеры могут утечки личной идентифицирующей информации о вас и вашей машине. В этом разделе мы рассмотрим, как настроить ваш браузер, чтобы стать более частным в дополнение и предложить советы и инструменты, чтобы скрыть ваш реальный цифровой отпечаток.

Есть много настольных браузеров; доля рынка в основном делится между Microsoft Internet Explorer (IE), Mozilla Firefox, Safari, Opera и Google Chrome. IE и его преемник Edge предустановлены на ОС Windows; однако мы всегда рекомендуем пользователям использовать программное обеспечение с открытым исходным кодом для обеспечения максимальной безопасности при работе в Интернете. Mozilla Firefox по-прежнему считается единственным истинным браузером с открытым исходным кодом из основных браузеров, упомянутых, так что в этой книге, мы рассмотрим, как сделать этот браузер более приватным.

Примечание! Эпический браузер разработан группой под названием Hidden reflex и способствует конфиденциальности во всем мире; этот браузер основан на Хромиуме (форке Chrome от Google) и поставляется с расширенными функциями безопасности для устранения онлайн отслеживания. Он также поставляется со свободным встроенным VPN для сокрытия вашего ip-адреса и защиты ваших онлайн-коммуникаций. Вы можете попробовать его скачав по ссылке https://epicbrowser.com/index.html.

Настройка Firefox, с максимальной приватностью

В этом разделе мы дадим основные советы для обеспечения вашего просмотра в Интернете при использовании Firefox.

ВКЛЮЧЕНИЕ ПРИВАТНОГО ПРОСМОТРА

Когда вы включаете приватный просмотр в Firefox, браузер не будет записывать ваши посещаемые страницы, файлы cookie, временные файлы и поиск. Firefox также активирует защиту отслеживания, которая будет блокировать онлайн трекеры от мониторинга истории

просмотра через несколько веб-сайтов. Для обеспечения приватного режима в Firefox откройте браузер Firefox и нажмите Ctrl+Shift+ P. Появится новое приватное окно просмотра (увидеть рисунок2-13).

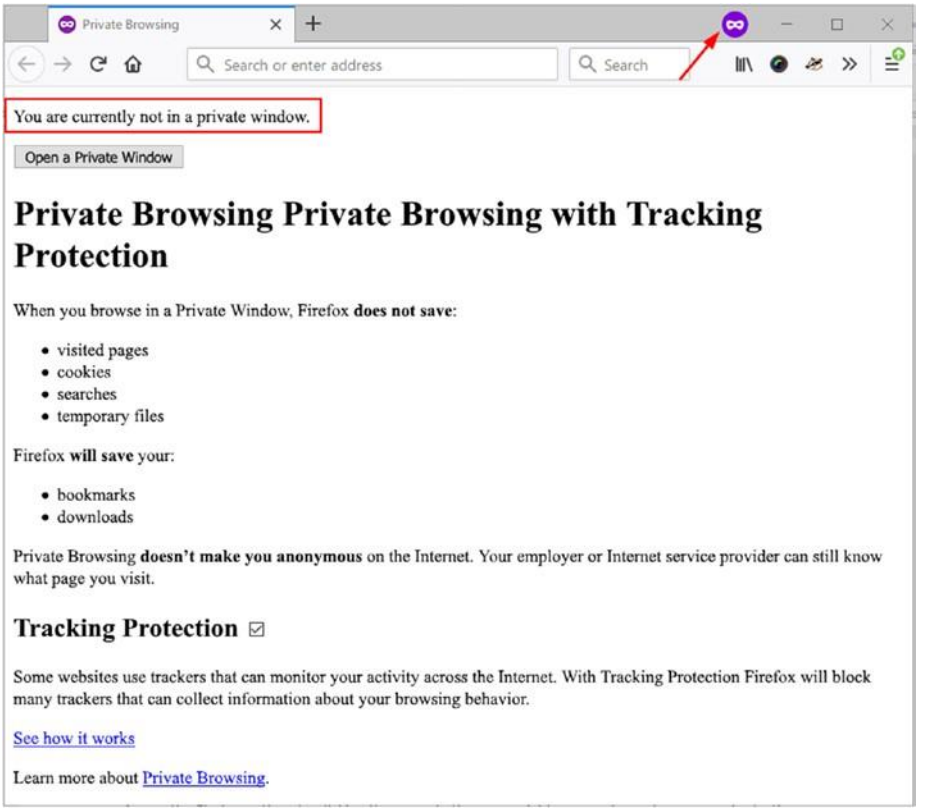

Рисунок 2-13. *В браузере Firefox открылось новое окно приватной сессии*

ИЗМЕНЕНИЕ НАСТРОЙКИ FIREFOX, ЧТОБЫ СТАТЬ ПРИВАТНЫМ

Есть много настроек, чтобы сделать ваш браузер Firefox более приватным. В этом разделе мы рассмотрим основной.

Доступ к опциям Firefox, нажав на меню в правом верхнем углу браузера и выбрав параметры (рисунок2-14).

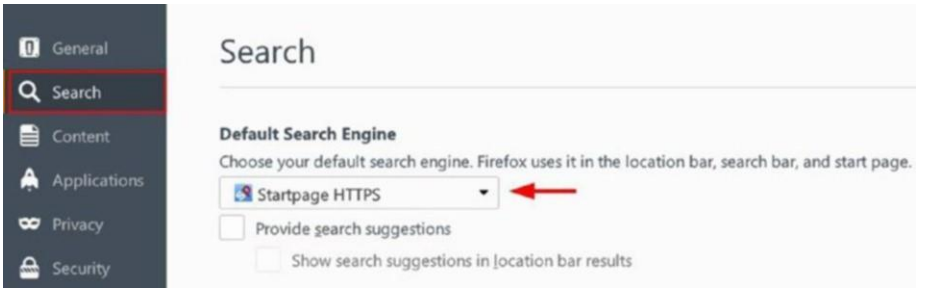

Рисунок 2-14. *Используйте анонимную безопасную поисковую систему, которая не отслеживает вашу деятельность в Интернете*

Перейдите на вкладку Конфиденциальность. Вам нужно включить опцию Защита от отслеживания использования в приватные окна. Теперь перейдите в раздел История на той же странице и выберите вариант "Никогда не запоминать историю", так что Firefox будет удалять всю историю каждый раз, когда вы закрываете его. Наконец, перейдите в раздел «Место бар» и удалите все предложения в панели поиска, поскольку там возможна утечка данных о вас. Вкладка Конфиденциальность должна выглядеть как рисунок2-15.

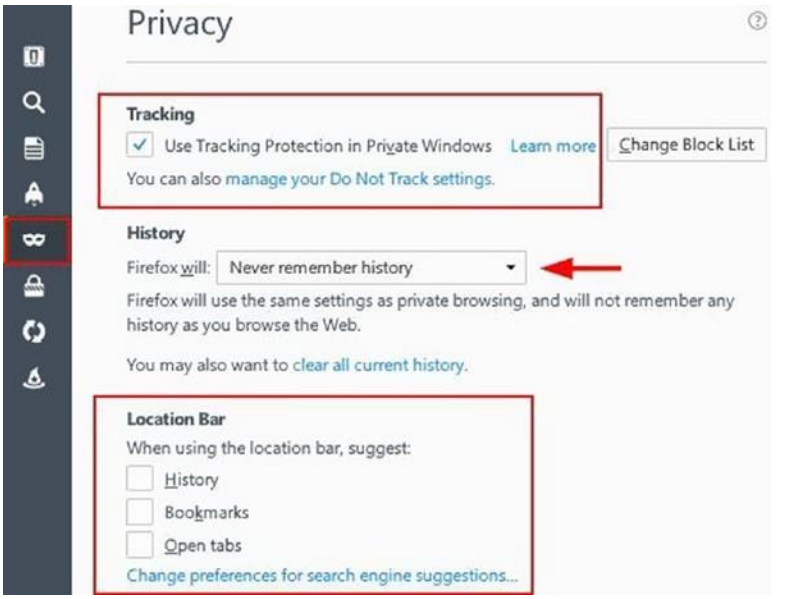

Рисунок 2-15. *Настройка вкладки Конфиденциальность в браузере Firefox для лучшей конфиденциальности*

Перейдите на вкладку безопасности и настройте ее, как на рисунке2-16.

Рисунок 2-16. *Настройка вкладки безопасности, чтобы остановить фишинг и опасные веб-сайты*

Go to “Privacy & Security” tab ➤ "Firefox сбора данных и использования" панели и отключить следующие варианты: Разрешить Firefox для отправки технических и взаимодействия данных Mozilla и Разрешить Firefox для отправки отстающих отчетов о аварии от вашего имени. Мы используем для этого шага Firefox Quantum edition - 61 версию. Отчеты о сбоях могут содержать ценные данные о состоянии компьютера, которые могут сделать вас уязвимыми, если он попадает в чужие руки, поэтому лучше отключить их.

Пока вы все еще находитесь на Расширенная вкладка, перейдите в вкладку Сети и убедитесь, что опция “Скажите мне, когда веб-сайт просит хранить данные для автономного использования” выбрана. Это предотвращает действия tracking на вашем компьютере.

Теперь, когда вы закончили настройку основных настроек Firefox, чтобы сделать его более удобным для конфиденциальности, вам нужно перейти к расширенным настройкам, чтобы продолжить работу. Введите **about:config** для доступа к расширенной странице настроек Firefox, в строке адреса URL вашего браузера. Появится предупреждающее сообщение; нажмите кнопку "Я принимаю риск!" для доступа к расширенной панели настроек.

Чтобы получить доступ к определенному параметру, необходимо ввести его имя в поле поиска, которое отображается в верхней части страницы. Для начала давайте изменим первую настройку под названием browser.formfill. выставив false (двойной клик, чтобы изменить значение настроек). Это заставляет Firefox забыть информацию о форме (см. Рисунок 2-17).

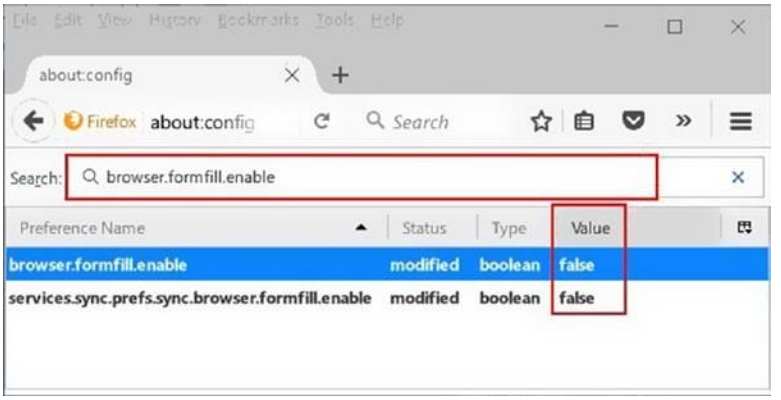

Рисунок 2-17. *Доступ к расширенной странице настроек в Firefox и отключение истории в Firefox*

Теперь, таким же образом, вам нужно изменить следующие настройки:

- Изменить browser.cache.disk.enable на false.
- Изменить browser.cache.disk_cache_ssl на false.
- Изменить browser.cache.offline.enable на false.
- Изменить dom.event.clipboardevents.enabled на false.
- Изменить geo.enabled на false.
- Изменить network.cookie.lifetimePolicys value на 2.
- Изменить plugin.scan.plid.all на false.

Эти главные конфигурации будут "Усиливать" Firefox и сделать его более трудным для другой стороны, в отслеживании вашей деятельностьи. В следующем разделе мы рассмотрим дополнения конфиденциальности, которые могут еще больше защитить Firefox и бороться с онлайн-отслеживанием и профилированием пользователей.

РАСШИРЕНАЯ КОНФИДЕНЦИАЛЬНОСТИ FIREFOX

Выбор лучших расширений Firefox (см. таблицу 2-6),которые помогут вам сохранить вашу конфиденциальность в Интернете будут упомянуты здесь. Пожалуйста, обратите внимание, что некоторые поставщики дополнений могут обманывать пользователей и собирать личные данные о привычках просмотра и даже личную информацию без их согласия, поэтому желательно избегать установки каких-либо дополнений, за исключением тех, которые упоминаются в этом разделе. Кроме того,если новое надежное дополнение

появится позже (скажем, после публикации этой книги), убедитесь, что она исходит от авторитетного доверенного разработчика и установить его только из https://addons.mozilla.org исключительно.

Таблица2-6. *Firefox Добавление конфидициальности*

Add-on	Work	URL
HTTpS everywhere	шифрует ваши сообщения со многими крупными веб-сайтами, делая ваш просмотр более безопасным.	https://www.eff.org/HTTPS-EVERYWHERE
privacy Badger	Блокировка шпионаж объявлений и невидимые трекеры.	https://www.eff.org/ privacybadger
uBlock Origin	Блокировщик общего поль-зования	https://addons.mozilla.org/ en-US/firefox/addon/ublockorigin/
random agent Spoofer	Изменяет профиль рандомно (из Реальных браузеров /устройств) С интервалами времени.	https://addons.mozilla.org/ nn-no/firefox/addon/random-agent-spoofer/

БОРЬБА С ЦИФРОВЫМИ ОТПЕЧАТКАМИ И УТЕЧКАМИ БРАУЗЕРА

Мы уже рассмотрели большое количество информации о том, как сделать ваш веб-браузер более устойчивым к атакам на вашу цифровую личностью. Несмотря на все эти методы, мы не можем гарантировать 100-процентное техническое решение, чтобы остановить это вторжение в частную жизнь. Наилучшим решением является доступ в Интернет с помощью свежеустановленного браузера Firefox. Это позволит сделать ваш браузер таким же как отпечатки большинства браузеров! Чтобы сделать вещи более скрытыми, установите веб-браузер в виртуальной машине. Это также будет скрывать текущую машину - аппаратное и программное обеспечение-конфигурации. Конечно, вам все еще нужно использовать VPN для шифрования подключения и скрыть свой IP-адрес.

Безопасная онлайн-коммуникация

В этом разделе мы покажем вам, как использовать различные методы, чтобы скрыть ваш реальный IP-адрес и сделать ваше соединение зашифрованным, так что его трудно было

перехватить. Обратите внимание, что термин *«конфиденциальность»* отличается от анонимности, хотя и во многом связан между собой. Таким образом, в этом контексте, VPN и прокси-серверы помогут замаскировать ваш трафик; внешние наблюдатели увидят, что есть трафик, происходящий с вашего компьютера, но они не могут видеть, что проходит (например, провайдеры и правительства не могут видеть, какие веб-сайты вы посещаете). Кроме того, все веб-сайты, которые вы посещаете, и приложения, которые вы используете, не будут видеть ваш реальный IP-адрес. На условиях анонимности внешний наблюдатель не должен быть в состоянии знать источник соединения; следовательно, они не могут приписать ваши действия в Интернете к вам. Конфиденциальность и анонимность важны для любого аналитика OSINT и должны быть полностью поняты, прежде чем начать работу с OSINT в остальной части книги.

VPN

VPN позволяет пользователю установить безопасное соединение с одного сайта на другой через Интернет (см. рисунок 2-18). Он широко используется корпорациями для доступа к удаленным сайтам, обеспечивая при этом конфиденциальность конфиденциальных данных. VPN также предоставляет пользователям анонимные IP-адреса, позволяя изменять данные о местоположении, чтобы они могли избежать цензуры, обмениваться файлами с другими людьми в частном порядке, и многое другое. В настоящее время VPN является необходимостью для тех, кто заботится о своей конфиденциальности при работе в Интернете.

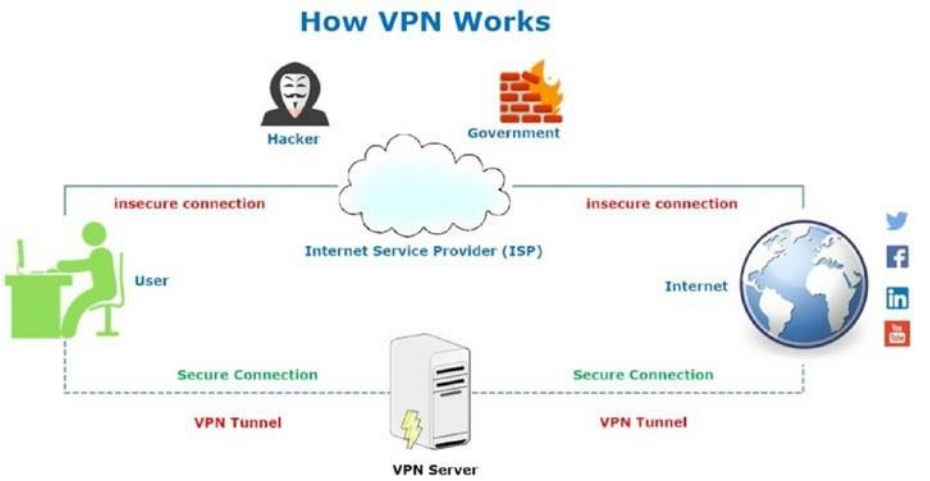

Рисунок 2-18. *Как работает VPN(Источник: www.DarknessGate.com)*

VPN вендоры предлагают различные функции. Вы должны заботиться о следующих функциях при выборе поставщика VPN:

- Не подписывайтесь на VPN-провайдеров, которые базируются в одной из следующих стран: США, Великобритания, Австралия, Новая Зеландия, Канада, Дания, Франция, Нидерланды, Норвегия, Бельгия, Германия, Италия, Испания, Израиль, Швеция, и, конечно, таких странах, как Россия, Китай, Иран и все арабские государства. Лучшие поставщики базируются в Швейцарии и следуют ее юрисдикции.
- Поставщик VPN должен иметь свой собственный DNS-сервер; он должен также поддерживать dNS защиты от утечки (подробнее об этом следующем).
- Предпочтительно, чтобы программное обеспечение VPN поддерживало программное обеспечение OpenVPN. Это программа с открытым исходным кодом, которая может быть проверена кем-либо, чтобы гарантировать, что она пуста от любых бэкдоров.
- Он должен принимать анонимные платежи, такие как биткойн, подарочные карты, дебетовые карты и наличные.
- Лучше поддерживать несколько устройств одновременно, чтобы вы могли защитить данные планшета и смартфона в дополнение к ноутбуку или ПК.
- Это не должно требовать много деталей для настройки; имя пользователя и пароль должно быть достаточно.

Примечание! Если вашей конечной целью является анонимность и, используйте Tor Browser вместо VPN.

Прокси

Прокси-сервер — это промежуточный компьютер, который находится между вычислительным устройством и Интернетом. Корпорации используют прокси для фильтрации контента и обеспечения уровня безопасности путем отделения корпоративной локальной сети от Интернета. Существуют различные виды прокси; основным типом является веб-прокси, что большинство пользователей Интернета означает при

использовании термина *прокси*. Его основная функция заключается в том, чтобы получить онлайн-ресурсы, будь то страница или файл- из Интернета, а затем отправить их на ваш компьютер. Они также обеспечивают анонимность, изменяя реальный IP-адрес компьютера пользователя в IP-адрес прокси-сервера (см. рисунок 2-19).

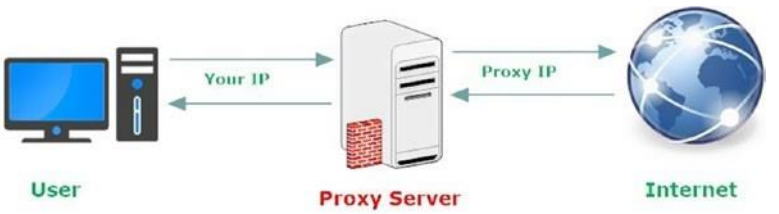

Рисунок 2-19. *Как работает прокси-сервер (Источник: www.GarknessGate.com)*

Многочисленные бесплатные прокси-серверы доступны в Интернете. Тем не менее, мы настоятельно рекомендуем, чтобы такие услуги не используются. Бесплатный прокси обычно показывает рекламу в вашем браузере, которая может ввести вредоносное программное обеспечение или другие скрипты отслеживания, которые могут заразить или скомпрометировать вашу машину, если вы нажмете вредоносную ссылку. Кроме того, большинство бесплатных прокси не являются достаточно безопасными чтобы им доверять обработку и общение критически важных данных, таких как данные кредитной карты и пароли учетных записей.

Тест утечки DNS

Использование VPN и других сервисов анонимности не гарантирует, что история просмотра веб-страниц не будет раскрыта. Иногда, даже если вы защищаете свое соединение с помощью VPN, может произойти утечка соединения и выявить реальный IP-адрес и вы не будете знать что произошла утечка . Такая утечка происходит, когда часть трафика вычислительных устройств (DNS- трафик) не передается через защищенный канал службы анонимности, который вы используете, и, следовательно, VPN. Вместо этого, он получает направлены на интернет-серверы вашего интернет-провайдера (см. Рисунок 2-20),что позволяет им потенциально контролировать и регистрировать полную историю просмотра веб-страниц, даже если вы используете VPN.

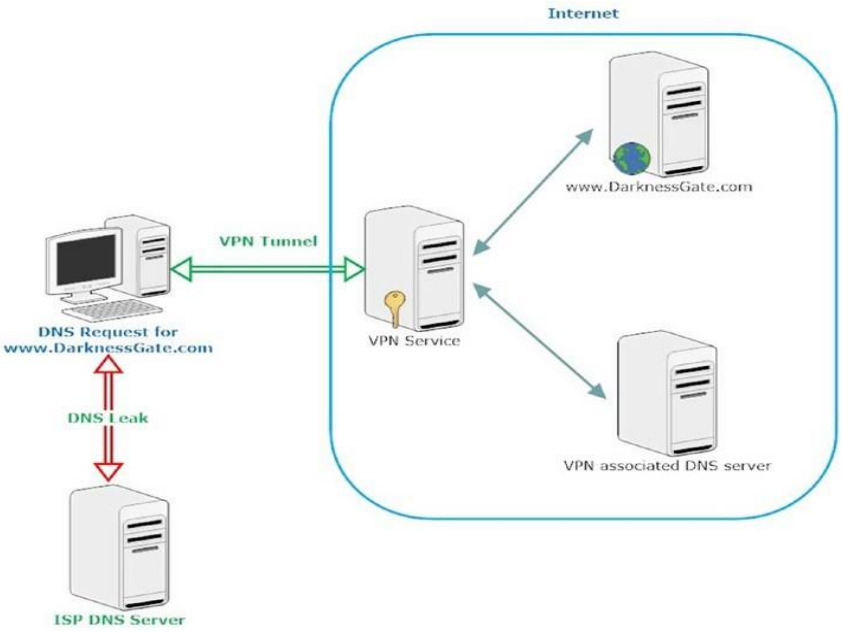

Рисунок 2-20. *Как происходит утечка DNS (источник: www.darknessgate.com)*

Чтобы убедиться, что ваш VPN-провайдер не уязвим к этому риску, настоятельно рекомендуется протестировать подключение непосредственно после подключения к поставщику VPN, следующим образом:

1. Перейти к https://www.dnsleaktest.com.
2. Вы увидите две кнопки вместе с текущим IP-адресом. Первая кнопка помечена как "Стандартный тест", а вторая - "Расширенный тест". Нажмите вторую кнопку для получения подробных результатов.
3. На странице подробных результатов будет показан список всех DNS-серверов (наряду с их местоположением), которые используются для решения URL-адресов набранного веб-сайта на IP-адреса. Если какой-либо из этих серверов не связан с вашим VPN, это означает, что ваше соединение является утечкой информации о вас.

Авторитетные VPN-провайдеры имеют механизм предотвращения утечки соединения. Тем не менее, вы должны убедиться, что ваш VPN-провайдер имеет эту функцию и она включена автоматически для вашего соединения.

Предупреждение! всегда делать DNS тестирования утечки, чтобы гарантировать, что ваш трафик DNS туннелируется через Ваш VPN-зашифрованный туннель, а не через ISP.

Анонимность в Интернете

При работе в Интернете для сбора источников OSINT, крайне важно оставаться полностью анонимным. VPN позволяет замаскировать ваш IP-адрес и передовать шифрованное содержимое на ваш компьютер и с вашего компьютера. Тем не менее, VPN-провайдер может перехватить все ваши сообщения на выходе .Для выполнения критически важных задач настоятельно рекомендуется использовать анонимные сети (e.g., Tor, I2P, and Freenet). Это позволяет скрыть свою личность при серфинге или публикации информации в Интернете. В следующем разделе мы рассмотрим сеть Tor, которая сегодня считается наиболее часто используемой анонимной сетью.

ИспользованиеTOR Network

Tor является самой популярной анонимной сетью, используемой в настоящее время в Интернете; она в основном состоит из этих двух частей:

1. Часть программного обеспечения, которую вы запустите на вашей машине для анонимного доступа в Интернет
1. Сеть добровольных компьютеров Tor, которые направляют ваш интернет-трафик

Tor позволяет пользователям достичь высокого уровня анонимности в Интернете, шифруя как данные, так и IP-адреса назначения до отправки их через виртуальную схему, которая состоит из множества узлов (не менее трех узлов в любой момент времени). Затем каждый узел расшифровывает часть данных, чтобы выявить только следующий узел в цепи, чтобы направить оставшиеся зашифрованные данные к нему. Следующий узел выполняет ту же функцию до тех пор, пока сообщение не достигнет финального узла, называемого *ретранслятором выхода.* Выходная ретранслятор расшифровывает данные, не раскрывая IP-адрес источника, отправляя его к месту назначения (см. рисунок 2-21).

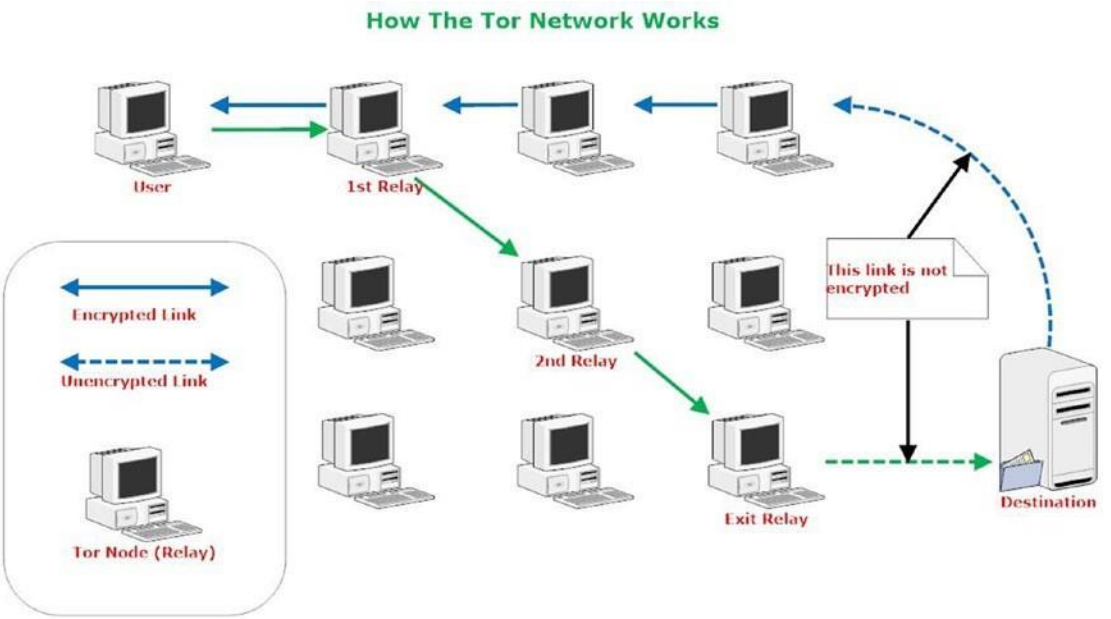

Рисунок 2-21. *Как работает сеть Tor*

Примечание! Термин *узла* используется для описания любого сервера, работающего как часть сети ретрансляторов Tor. Иногда люди используют различные термины для узла, такие как сервер, *реле*или *маршрутизатор*.

При использовании Tor для анонимизации вашего местоположения он будет использовать IP-адрес ретрансляции выхода вместо вашего реального IP-адреса в качестве исходного IP-адреса. Это позволит эффективно скрыть вашу личность в Интернете.

Чтобы использовать сеть Tor для начала поиска OSINT, все, что вам нужно сделать, это загрузить и использовать браузер Tor.

TOR БРАУЗЕР

Чтобы получить доступ к сети Tor, загрузите браузер Tor из| https://www.torproject.org/projects/torbrowser.html.en. Браузер Tor является форком Firefox не требует установки на клиентской машине; Вы можете безопасно запустить его с USB-накопителя. Он поставляется

с программным обеспечением Tor, которое позволяет получить доступ к сети Tor прозрачно при запуске этого браузера без какой-либо дополнительной конфигурации(рисунок2- 22)

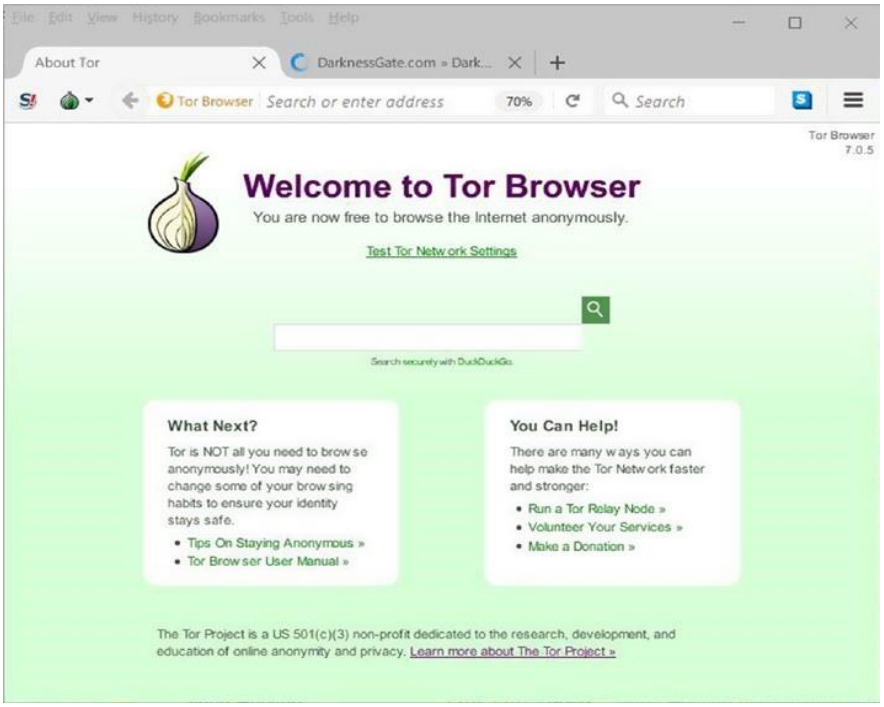

Рисунок 2-22. *Успешный запуск браузера Tor*

Пожалуйста, обратите внимание, что только веб-сайты, посещаемые через tor Browser, будут анонимно направляться через сеть Tor; другие браузеры и приложения, уже установленные на вашем устройстве, не будут использовать сеть Tor.

СКРЫТИЕ ИСПОЛЬЗОВАНИЯ TOR

Важным моментом, который следует тщательно рассмотреть, является сокрытие использования браузера Tor от вашего интернет-сайта. Этот шаг имеет важное значение, поскольку использование Tor Browser может считаться подозрительным и даже незаконным в некоторых странах. Другие страны и интернет-провайдеры могут запретить доступ к сети Tor. Это сделает использование Tor Browser более трудным для начинающих пользователей.

Обнаружение использования Tor возможно с использованием различных технических методов. Однако в этом разделе мы представим некоторые методы, чтобы скрыть ваше использование Tor в значительной степени, что затрудняет его обнаружение.

Использование VPN

Вы можете скрыть использование Tor от вашего интернет-приложения с помощью виртуального частного сетевого сервиса. VPN создаст зашифрованный туннель между вашей машиной и VPN-сервером. Как только это будет начато, вы можете запустить tor Browser, который будет в значительной степени скрыт от вашего ISP.

Использование мостов Tor

Ретрансляторы моста (или *мосты* для краткости) являются релеи Tor, которые не перечислены в главном каталоге Tor. Мосты считаются точками входа в сеть Tor. Поскольку нет полного публичного списка из них, даже если ваш интернет фильтрует соединений ко всем известным ретрансляторам Tor, он, вероятно, не сможет заблокировать все мосты.

Пожалуйста, помните, что этот метод не может полностью гарантировать, что ваш интернет-президент не будет обнаруживать использование Tor, но это сделает открытие этого факта трудным и потребует сложных методов, чтобы раскрыть. Чтобы получить мосты Tor, сделайте один из следующих:

- Перейти кhttps://bridges.torproject.org/bridges и получить ваши мосты.
- Отправить электронное письмо bridges@torproject.org с текстом“get bridges” в теле сообщения. Вы должны отправить это письмо от одного из следующих поставщиков электронной почты: Riseup, Gmail, или Yahoo.

Теперь вам нужно настроить браузер Tor, чтобы использовать эти мосты. Чтобы сделать это, выполните эти шаги:

1. Чтобы войти в мосты в браузер Tor, запустите браузер Tor и перед подключением Tor Browser нажмите кнопку «Открытые настройки» (Рисунок 2-23).

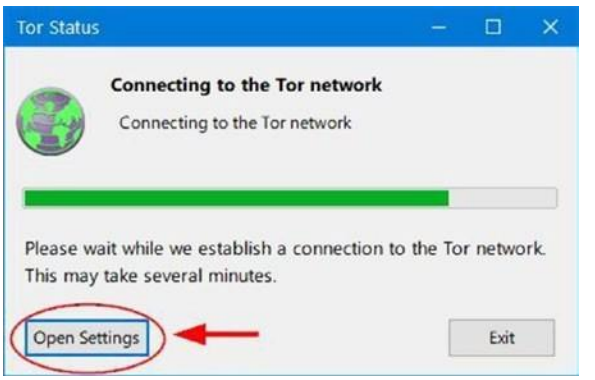

Рисунок 2-23. *Доступ к настройкам сети Tor перед запуском браузера Tor*

2. Появляется окно настроек сети Tor; нажмите кнопку «Настройка».
3. Tor спрашивает вас, блокирует ли ваш интернет-провайдер или иным образом цензуру подключений к сети Tor; нажмите Да и нажмите Далее, чтобы продолжить.
4. В следующем окне мастера выберите опцию "Введите пользовательские мосты" (см. рисунок 2-24). Копировать мосты у вас есть от шага 1 или шаг 2 и вставьте их в поле; нажмите Далее, чтобы продолжить.

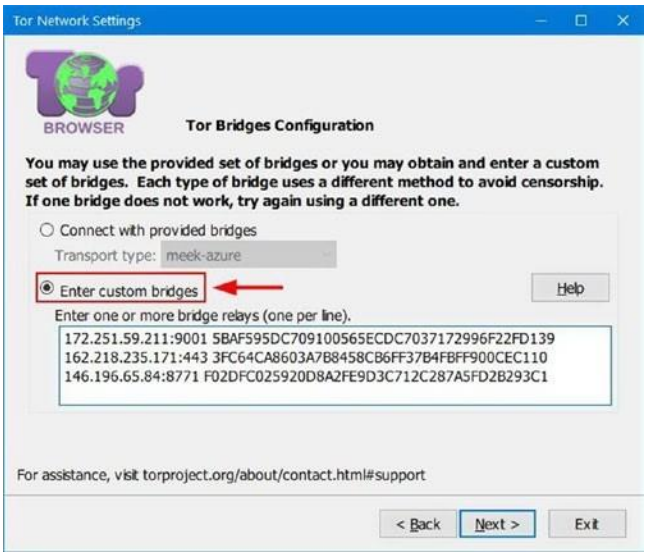

Рисунок 2-24. *Ввод пользовательских мостов в браузер Tor*
Рисунок 2-24. *Ввод пользовательских мостов в браузер Tor*

5. Следующий мастер спрашивает вас, находится ли ваш компьютер за прокси-сервером; в нашем случае, вам не нужен один (который является наиболее распространенным). Выберите Нет и нажмите кнопку Connect для продолжения. Если вы сидите за прокси-сервером, выберите Да, затем введите настройки прокси и, наконец, нажмите Connect.

Если все будет работать как ожидалось, Tor Browser откроется с помощью индивидуальных мостов.

Как мы уже представили, использование индивидуальных мостов Tor не может полностью замаскировать ваш вход в сеть Tor. Некоторые страны используют метод глубокой проверки пакетов (DPI) для анализа потоков интернет-трафика по протоколу,

чтобы проверить, содержат ли они трафик Tor. Тем не менее, использование индивидуальных мостов по-прежнему является хорошим способом обойти цензуру Tor и скрыть ее использование во многих странах.

Использывание Pluggable Transports

Для работы вокруг техники цензуры DPI, Tor ввел плагинный транспорт (PT). Этот метод преобразует трафик между компьютером и мостом в типичный интернет-трафик, тем самым скрывая использование Tor от вашего интернет-президента. Для использования pluggable transport, сделать следующее:

1. Запустите браузер Tor и нажмите кнопку "Открытые настройки" перед запуском Tor.
2. Нажмите кнопку «Настройка», выберите опцию «Да», когда его спросили, блокирует ли ваш интернет-пользователь или цензорирует подключение к сети Tor, и нажмите далее, чтобы продолжить.
3. Выберите опцию "Связь с предоставленными мостами" и выберите мост из меню выпадения типа транспорта (Рисунок 2-25).

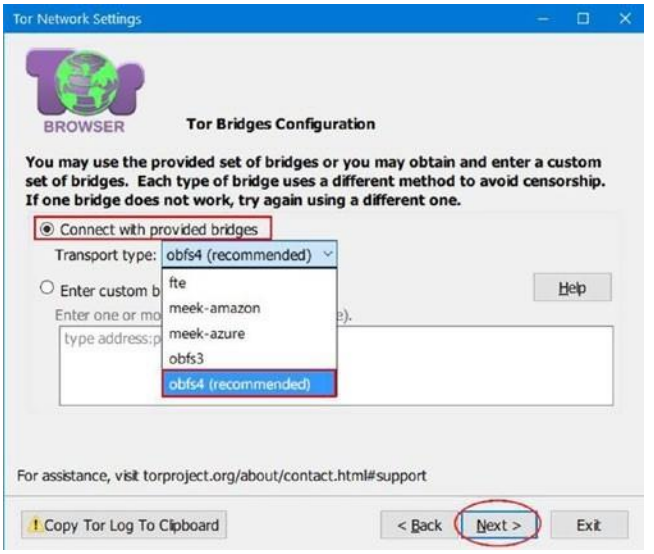

Рисунок 2-25. *Подключение к сети Tor с помощью pluggable transport чтобы скрыть использование Tor*

4. Окончательное окно мастера спросит вас, находится ли этот компьютер за прокси-сервером. В нашем случае этого нет, поэтому вы можете выбрать опцию No и нажать кнопку Connect. Если вы сидите за прокси-сервером, выберите да, введите настройки прокси и нажмите кнопку Connect.

Если все пойдет хорошо, Tor Browser теперь должен успешно загрузиться.

Предупреждение! Что следует сделать, чтобы оставаться анонимным при использовании браузера Tor?

1. Не устанавливайте дополнения в браузер tor, такие как Flash-плеер, adobe reader и проигрыватель quickTime. Такие расширения, как правило, открывают независимые соединения за пределами цепи Tor, и это будет утечка вашего реального Ip-адреса.
2. не открывайте файлы PDF или воспроизводить флэш-видео в вашем браузере Tor.
3. Если вы обмениваетесь конфиденциальными данными через сеть Tor, убедитесь, что сначала зашифруйте их. Ретранслятор выхода Tor, который используется для установления связи с пунктом назначения, не зашифрован. Если злоумышленник сидит в этом месте, он может перехватить ваше соединение.
4. Убедитесь, что при использовании Tor Browser не использовать вашу истинную личность для регистрации или размещения комментариев на веб-сайтах. Конечно, как анализатор OSINT, сохранение вашей личности в тайне является основной причиной для использования сети Tor.

Использование Tails OS и другие Security OSs

Иногда вы можете достичь максимальной анонимности, возможной с помощью специализированной ОС, которая направляет весь интернет-трафик через сеть Tor. Tor Browser более чем достаточно для сокрытия вашей личности при проведении регулярных

поисков OSINT; однако при работе над конфиденциальными делами или обмена информацией с другими сторонами необходимо использовать анонимную ОС.

Tails — это безопасная ОС, на основе Linux, которая использует Tor в качестве сетевого приложения по умолчанию. Он считается лучшим анонимным ОС в настоящее время. Вы можете использовать Tails для общения в частном порядке с уверенностью в крайне враждебной среде.

Tails портативный. Таким образом, вы можете выполнить его из USB-накопителя, и он полностью не зависит от принимающей машины. Tails работает с помощью оперативной памяти хоста и не копирует файлы на жесткий диск машины-резидента.

Tails достигает своей анонимности, заставляя все сетевые соединения пройти через сеть Tor. Если приложение пытается подключиться к Интернету напрямую, подключение автоматически блокируется. Tails не оставляет следов на жестком диске хоста. После остановки, Tails будет удалять все файлы пользователей, если явно не просили не (постоянное хранение). Tails поставляется со многими криптографическими инструментами, которые позволяют отправлять зашифрованные электронные письма и работать в безопасных чатах.

Мы рассмотрим установку и использование Tails в главе3.

Безопасное совместное использование файлов

Иногда вы можете поделиться файлами в частном порядке с другими сторонами, расположенными в другом месте. Это особенно важно для любого аналитика OSINT, которому может потребоваться запросить и поделиться информацией с коллегами, чтобы поддержать дело. Существует множество сервисов обмена файлами, но большинство из них не построены, чтобы быть полностью анонимным. Они обычно требуют, чтобы учетная запись обменивалась файлами и хранила некоторую информацию (также называемую *метаданными транзакций,* которая включает в себя IP-адреса загрузчика и загрузчика) о каждой транзакции, происходящей через них. Такая вещь не подходит для следователей, работающих над деликатными судебными делами. В этом разделе мы представим безопасную службу обмена файлами через сеть Tor; он считается наиболее анонимным решением для обмена личными файлами в Интернете.

ONIONSHARE

OnionShare — это инструмент с открытым исходным кодом, который использует сеть Tor для анонимного обмена файлами.

Вы можете поделиться любым типом и размером файлов. Ваши общие файлы не будут загружены в Интернет. Вместо этого они останутся на вашем компьютере, который

играет роль хостинг-сервиса. Все, что вам нужно сделать, чтобы поделиться файлами, это поделиться URL,данный инструментом, с человеком, с которым вы переписываетесь, который должен получить к нему доступ с помощью tor Browser. Для использования OnionShare, следовать этим шагам:

1. Скачать и установить программу из https://onionshare.org.
2. Запустите инструмент и выберите файлы/ папки, которыми вы хотите поделиться. Убедитесь, что ваш браузер Tor запущен и подключен к сети Tor.
3. После выбора файлов/папок, которыми вы хотите поделиться, нажмите кнопку «Начало доступа». OnionShare создаст скрытый сервис Tor для ваших общих файлов, размещенных в сети Tor, и даст вам URL для отправки вашему корреспонденту. Вы можете получить этот URL, нажав кнопку Копировать URL (Рисунок 2-26).

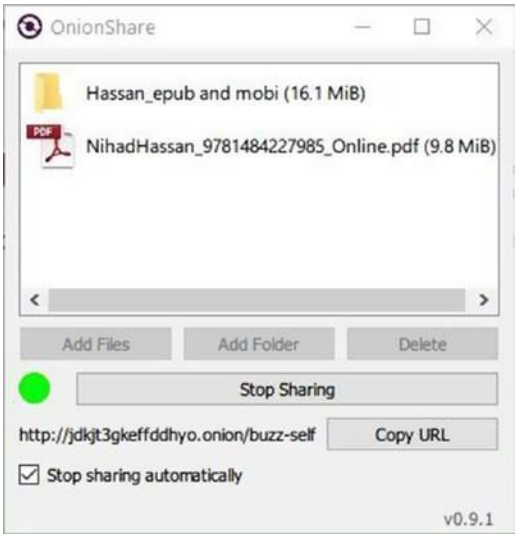

Рисунок 2-26. *OnionShare предоставляет URL-адрес для общих файлов, отправляет его получателю и сохраняет его закрытым*

4. Ваш корреспондент должен получить доступ к общему URL через браузер Tor.
5. Ваш OnionShare программа и браузер Tor должны оставаться открытыми до тех пор, пока ваш корреспондент не закончит загрузку ваших общих файлов. Когда получатель успешно получает ваш файл, OnionShare остановит процесс совместного использования автоматически. (Чтобы автоматически прекратить совместное использование файла после получения файла, необходимо включить опциюЧтобы автоматически прекратить совместное использование файла после получения файла, необходимо включить опцию“Stop sharing automatically” в OnionShare программе перед обменом файлами.)

Примечание! Для людей, заботящихся о безопасности, которые хотят поделиться конфиденциальными файлами, мы советуем вам Tails OS при совместном использовании файлов через программу OnionShare.

Making Anonymous Payments

Как анализатор OSINT, во время поиска источников OSINT, вы можете столкнуться с веб-сайтами, которые просят вас заплатить плату, чтобы увидеть некоторые ресурсы (в основном серая литература). Это часто происходит при запросе научных работ или внутренних документов корпорации. То же самое относится и при покупке услуг анонимности онлайн (например, оплатить VPN-провайдера анонимно). Как вы знаете, вы можете быть частью юридического расследования и не хотите раскрывать свою истинную личность при расследовании некоторых видов ресурсов.

В таких случаях необходимо оплачивать такие услуги анонимно.

В обычных случаях, когда вы покупаете что-то в Интернете, ваше имя, информация о кредитной карте, и другие данные о транзакциях будут доступны для интернет-торговли. Эмитент вашей кредитной карты и банк также будут знать о ваших данных транзакции, и никто не может гарантировать, как долго эти данные будут храниться и может ли какая-либо третья сторона (например, рекламное агентство) иметь к ней доступ. Для покупки цифровых товаров и услуг онлайн анонимно, вы можете использовать подарочные кредитные карты или оплатить с помощью криптовалюты.

ПРЕДОПЛАЧЕННАЯ ПОДАРОЧНАЯ КАРТА

Крупные поставщики кредитных карт предлагают предоплаченные карты для своих клиентов. Такие карты не требуют какой-либо личной информации для настройки; они также не требуют наличия банковского счета для работы. Такие карты доступны в аптеках и супермаркетах и используются специально для покупки цифровых товаров, таких как VPN и другие услуги анонимности (хотя, пожалуйста, обратите внимание, что не все веб-сайты принимают такие карты).

Существуют различные типы предоплаченных карт. То, что мы заботимся о этой книге является анонимным типом, который является "незагружаемой" карты. Эта карта поставляется с предустановленной с определенной суммой наличных денег, как правило, меньше, чем $ 500. Вы можете приобрести их наличными (что невозможно отследить) без раскрытия какой-либо личной информации; даже ваш адрес электронной почты не требуется.

Предупреждение! не покупайте предоплаченные кредитные карты онлайн. Если вы покупаете предоплаченную кредитную карту онлайн, вам нужно заплатить за нее, используя некоторую форму неанонимных платежей, как обычная кредитная карта, банковский чек, или PayPal. Кроме того, для получения карты необходимо предоставить свой почтовый адрес

(если это физическая пластиковая карта). Это свяжет купленную кредитную карту с вашей настоящей личностью.

КРИПТОВАЛЮТЫ

Криптовалюта является одним из видов цифровой валюты, которая предназначена для работы в качестве средства обмена с использованием криптографии для обеспечения транзакции и контроля за созданием дополнительных единиц валюты. Существуют сотни типов криптовалют, которые уже используются; самой известной по-прежнему остается система биткоинов. Вы можете найти список доступных криптовалют в настоящее время на https://coinmarketcap.com.

Bitcoin (https://bitcoin.org) является децентрализованной и нерегулируемой одноранговой платежной сети (например, сеть Torrent), которая питается от своих пользователей без центрального органа или посредника. Биткойн - это цифровая система; он не печатается как обычная валюта (доллары и евро) и создается людьми и компаниями, использующими специализированную программу с открытым исходным кодом под названием биткоин-кошелек (кошелек может быть онлайн-сервисом; следовательно, он называется *электронным кошельком).* Биткойн не взимает плату за транзакции, и это не возврат (как только вы отправляете биткойн получателю, он исчезнет навсегда, если получатель не вернет вам биткойн).

Мы не будем углубляться в техническую сторону цифровой валюты Bitcoin и как создать счет, чтобы купить продукты, используя его, потому что это вне сферы книги. Что вы должны знать о Bitcoin является то, что вы можете сделать анонимные покупки, используя эту валюту, которые почти невозможно раскрыть. В следующем списке, мы дадим вам некоторые авторитетные онлайн-источники, чтобы понять, как эта валюта работает.

- *Начало работы с Bitcoin*: https://bitcoin.org/en/getting- started
- *Биткоин-кошельки*: https://blockchain.info/wallet
- *Биткоин-кошельки программы*: https://en.bitcoin.it/wiki/Clients
- *Купить биткоин анонимно с помощью банкоматов*: https://coinatmradar.com

Платежи в биткоинах крайне анонимны; однако, есть немного моментов для покупки и обмена биткойном.

Прежде чем двигаться дальше, рассмотрим следующее при проведении анонимных покупок в Интернете:

- Шифрование онлайн-соединения перед анонимным платежом. При анонимной оплате в Интернете, убедитесь, что анонимизировать

подключение с помощью анонимной сети, как Tor или I2P. Оплата анонимно, не маскируя свой IP-адрес, предоставит информацию о вашем техническом подключении различным сторонам, и это может привести к раскрытию вашей личности.

- Регистрация на услуги анонимности, таких как VPN, и даже проведение некоторых онлайн-покупок с использованием анонимного способа оплаты могут потребовать от пользователей предоставить свой адрес электронной почты в рамках транзакции. Убедитесь в том, чтобы не использовать ваш основной адрес электронной почты; вместо этого используйте временный адрес электронной почты для таких задач.

Методы шифрования

Шифрование обеспечивает надежный набор методов для обеспечения безопасных транзакционных потоков конфиденциальных данных в Интернете, тем самым предотвращая хакеров и киберпреступников от доступа к конфиденциальному контенту, даже если им удастся захватить передаваемые зашифрованные данные. Математических формул, участвующих в современных криптографических стандартах, достаточно для предотвращения расшифровки украденных данных большинством злоумышленников. В этом разделе мы представим некоторые инструменты и рекомендации, которые помогут вам сохранить ваши конфиденциальные данные конфиденциальными, шифруя их.

Защита паролей

Убедитесь в том, чтобы обезопасить свои учетные записи в Интернете, используя надежные, сложные пароли. Также настоятельно рекомендуется менять пароль каждые три месяца. Есть много бесплатных инструментов, чтобы помочь вам в процессе генерации паролей. Такие инструменты будут производить высоконадежные пароли, содержащие комбинацию букв, цифр и символов. Вот список некоторых из этих инструментов:

- Free Password Generator (https://www.securesafepro.com/ pasgen.html)
- PWGen (http://pwgen-win.sourceforge.net)

Многие веб-сайты предлагают услуги по генерации паролей в Интернете. Тем не менее, мы предпочитаем не использовать такие услуги, потому что ваш пароль может быть перехвачен во время путешествия на ваш компьютер.

Для хранения паролей необходимо использовать программу безопасности для обеспечения их безопасности; использование программы менеджера паролей необходимо для сохранения всех паролей в безопасном месте.Менеджер паролей шифрует базу

данных, содержащую ваши учетные данные, и защищает ее с помощью главногопароля.Это единственный пароль, который вы должны помнить.

- KeePass Password Safe (http://keepass.info)
- Master Password (https://ssl.masterpasswordapp.com)
- Password Safe (https://www.pwsafe.org)

Шифрование жесткого диска/USB

Шифрование данных становится важным в цифровую эпоху, поскольку считается последней линией защиты, если злоумышленник успешно получает доступ к вашим конфиденциальным данным. Другими словами, шифрование будет вашей последней надеждой предотвратить компрометации, использование или раскрытие вашей конфиденциальной информации общественности или вашим врагам.

Хранение сохраненной информации на жестком диске безопасно легко при использовании программного обеспечения шифрования. Например, Windows предоставляет встроенную утилиту шифрования, которая доступна для большинства ее версий (Windows 7 и за ее пределами) под названием BitLocker. Использовать эту утилиту легко; все, что вам нужно сделать, это право нажать на диск, который вы хотите шифровать и выбрать Включить BitLocker (см. Рисунок 2-27). Появится мастер, который проведет вас через все шаги, чтобы настроить шифрование диска (установка пароля и хранение ключа восстановления).

Figure 2-27. *Activate BitLocker on a Windows box*

Есть много авторитетных приложений программного обеспечения шифрования дисков, которые обеспечивают диск и даже шифрование разделов OS.

VeraCrypt (https://www.veracrypt.fr/en/Home.html) поддерживается на всех основныхОС. Он может шифровать жесткие диски, включая разделы ОС и USB . VeraCrypt также создает зашифрованные хранилища, которые могут быть использованы для хранения данных, а затем передать их в USB-флешку или отправить его через Интернет безопасно. Вы можете проверить раздел документации о том, как использовать этот инструмент в различных сценариях.

DiskCryptor (https://diskcryptor.net/wiki/Main_Page) обеспечивает шифрование всех разделов диска, включая систему разделов. Он поддерживается только на Windows OS.

Безопасность облачных хранилищ

Большинство людей используют облачное хранилище для резервного копирования и хранения конфиденциальных данных (таких как документы, личные фотографии, списки контактов, адресные книги и тому подобное). Многочисленные инциденты, связанные с безопасностью, которые произошли в последнее время с крупными поставщиками облачных услуг, показывают, что одних их мер безопасности может быть недостаточно, чтобы остановить такие компромиссы. Чтобы противостоять таким рискам, не полагайтесь на поставщика облачных услуг для защиты ваших данных. Всегда шифруйте свои данные перед загрузкой в облако и убедитесь, что резервная копия хранится в другом месте при работе с конфиденциальными данными. Вот две программы, которые могут быть использованы для защиты ваших данных перед загрузкой их в облако:

1. Duplicati (https://www.duplicati.com) использует AES-256 или GPG для шифрования данных перед отправкой в облако.
2. Cryptomator (https://cryptomator.org) использует AES-256 для шифрования данных и SCRYPT для защиты от атак грубой силы. Он работает, создавая зашифрованный свод - виртуальный жесткий диск на локальной машине, которая шифрует все внутри него, прежде чем загружать его поставщику облачных технологий.

Обратите внимание, что программы сжатия, такие как7-Zip (www.7-zip.org) И PeaZip (www.peazip.org) также предлагают функции шифрования, так что вы можете сжать и защитить свои файлы с паролем, прежде чем загружать его в облако.

Безопасная электронная почта

Всякий раз, когда электронное письмо отправляется, оно должно быть зашифровано, чтобы гарантировать целостность и конфиденциальность его содержимого. В современную цифровую эпоху электронная почта становится основным средством коммуникации как для частных лиц, так и для государственных/частных организаций, и нарушение этого средства связи будет иметь серьезные последствия.Утечки данных электронной почты происходят ежедневно, чтобы гарантировать, что содержимое ваших писем является безопасным, поэтому вы должны использовать программное обеспечение для шифрования.

Подробная информация о том, как включить шифрование в вашу электронную почту выходит за рамки этой книги. Однако в этом контексте вы должны понимать, что при обмене информацией с коллегами (например, в рамках расследования OSINT) по электронной почте, вы должны позаботиться о ее шифровании в первую очередь. В этом разделе мы предоставим вам ресурсы и инструменты, чтобы узнать, как это сделать. Однако, если вы хотите понять все части и выходы шифрования электронной почты, вы должны проверить нашу книгу*Digital Privacy and Security Using Windows: A Practical Guide* (Apress, 2017).

- Gpg4win (GNU Privacy Guard for Windows) позволяет создавать криптографические ключи (публичные и частные ключи), шифровать файлы и папки, а также подписывать электронную почту перед отправкой (цифровая подпись). Gpg4win является официальным дистрибутором GnuPG для Windows иhttps://www.gpg4win.org.
- Очередную реализацию проекта GnuPG, который будет использоваться на других платформах, можно найти на https://www.gnupg.org/download/index.html.
- Mozilla Thunderbird может быть настроен для использования GnuPG на всех основных платформах путем установки дополнения Enigma, которое добавляет шифрование сообщений OpenPGP и аутентификацию клиенту почты Thunderbird. Он оснащен автоматическим шифрованием, расшифровкой и интегрированной функциональностью управления ключами.

Примечание! Вы можете направлять свои сообщения по электронной почте Thunderbird через сеть Tor, используя расширение для Mozilla Thunderbird под названием TorBirdy. по словам его создателей (он принадлежит к проекту Tor), TorBirdy все еще находится в бета-релизе и не должен использоваться для обеспечения связи в крайне враждебной среде. Вы можете найти информацию о том, как установить и использовать это расширение в https://trac.torproject.org/projects/tor/wiki/torbirdy.

Расширение браузера доступно как для Firefox, так и для Google Chrome под названием Mailvelope, которое можно использовать в большинстве служб электронной почты. Это позволяет своим пользователям обмениваться зашифрованными электронными письмами с помощью схемы шифрования OpenPGP. Вы можете либо создать свою ключевую пару, либо импортировать существующую (например, из Kleopatra). Вы можете использовать это расширение без установки каких-либо инструментов, кроме расширения в вашем браузере. Он является открытым исходным кодом и доступен по адресу https://www.mailvelope.com/en. Тем не менее, мы не рекомендуем шифровать сообщения в веб-браузерах, потому что это сделает их более уязвимыми для кибератак, которые регулярно поражают браузеры.

БЕЗОПАСНЫЕ ПОСТАВЩИКИ ЭЛЕКТРОННОЙ ПОЧТЫ

Если вы предпочитаете использовать веб-почту для некоторых из ваших задач, желательно использовать безопасный поставщик адресной электронной почты, который предлагает расширенные функции безопасности для вашей учетной записи электронной почты. Например, ProtonMail(https://protonmail.com) отличается от других регулярных поставщиков электронной почты во многих отношениях. Он базируется в Швейцарии и следует своей юрисдикции, которая считается лучшей в мире с точки зрения защиты конфиденциальности пользователей. ProtonMail использует два пароля для защиты вашей учетной записи электронной почты. Первый проверяет подлинность учетных данных вашей учетной записи на сервере, а второй расшифровывает ваш почтовый ящик в веб-браузере или приложении, что означает, что он никогда не выходит в интернет на сервер ProtonMail. Если вы обмениваетесь электронной почтой с другим пользователем ProtonMail, вы можете безопасно настроить электронную почту, чтобы уничтожить себя в течение определенного срока в дополнение к отправке зашифрованных сообщений электронной почты другим пользователям ProtonMail. Особенно полезно автоматически уничтожать конфиденциальные сообщения электронной почты по обе стороны
Коммуникаций.

Наконец, если вы хотите использовать электронную почту только один раз (например, для активации некоторых услуг анонимно), вы можете пойти с любой из следующих двух услуг:

- https://hidester.com/temporary-email
- https://www.guerrillamail.com

БЕЗОПАСНЫЕ УСЛУГИ ВЫЗОВА В ИНТЕРНЕТЕ

IM разговоры являются еще одной формой связи, которую может потребоваться для защиты. Никто не может гарантировать, что гигантские ИТ-провайдеры, предлагающие бесплатный чат, озвучку IP и услуги видеоконференций, не регистрируют ваш чат или, по крайней мере, метаданные беседы, такие как дата/время и IP-адрес входа в систему в течение некоторого периода времени. Мы не можем обсуждать особенности безопасности каждого доступного приложения в этой книге. Тем не менее, мы сосредоточимся на функции безопасности, которая делает одно приложение более безопасным, чем остальные. Например, большинство приложений VoIP и чата работают одинаково. Они шифруют сообщения, обмениваемые между людьми, участвующими в разговоре, но они не шифруют метаданные сообщения.

Наилучшим безопасным приложением VoIP/IM является приложение, которое имеет следующие технические характеристики: оно должно быть открытым исходным кодом, чтобы его код мог быть проверен независимыми экспертами по безопасности, он не должен предлагать/показывать рекламу или любой тип коммерческой рекламы, поставщика и следовательно, приложение не должно хранить ключ расшифровки на своем сервере, чтобы никто не мог запросить ключ для расшифровки пользовательских данных, он не должен хранить какие-либо метаданные о подключении пользователя, и список контактов пользователя не должен храниться на сервере приложения и при необходимости он должен быть сохранен d зашифрован. Он должен предложить четкие варианты выбора того, что вы хотите создать резервную базу, прежде чем отправлять его поставщику облачных услуг.

Ниже приведены некоторые популярные безопасные и хорошо поддерживаемые приложения для обмена сообщениями:

- *Tor Messenger* (https://trac.torproject.org/projects/tor/wiki/doc/TorMessenger): Хотя он по-прежнему в бета-версии, это считается лучшим безопасным чат чата. Трафик направляется через сеть Tor для максимальной анонимности.
- *Cryptocat* (https://crypto.cat/security.html): Это защищенное приложение для обмена сообщениями с открытым исходным кодом, оно шифрует все сообщения по умолчанию и позволяет обеспечить безопасный обмен файлами в Интернете.
- *Signal* (https://whispersystems.org): Это безопасное приложение для обмена сообщениями и VoIP; он прост в использовании и предлагает

аналогичные функции, как WhatsApp и Viber Apps. Это приложение работает только на устройствах Android и iPhone.

- *Ghost Call* (https://ghostcall.io): Это сквозная зашифрованная служба вызова.
- *ChatSecure* (https://chatsecure.org): Эта программа im работает только на iOS, когда она настроена на использование OTR над XMPP.

Технология виртуализации

Используйте технологию виртуализации для повышения конфиденциальности и защиты принимающей машины от вредоносных программ и других угроз безопасности. Виртуальная машина позволяет иметь виртуальную операционную систему, которая ведет себя как полный, отдельный компьютер. Вы можете использовать виртуальные машины для выполнения программ, открытых вложений электронной почты, тестовых программ и безопасного посещения опасных веб-сайтов, не боясь вредоносных программ, затрагивающих вашу операционную систему, потому что виртуальная машина будет работать в песочнице изолированы полностью от операционная система его принимающей машины. Онлайн следователи могут использовать виртуальные машины для проведения своих онлайн-исследований безопасно, и они могут использовать недавно установленные браузеры, чтобы замаскировать свои цифровые отпечатки пальцев, что делает его похожим на миллионы подобных браузеров. Наконец, они могут удалить всю виртуальную машину, чтобы очистить любые цифровые следы, которые могут быть оставлены на принимающей машине!

Это самые популярные две виртуальные машины:

- VMware Player (Рисунок 2-28) (www.vmware.com/products/player/playerpro-evaluation.htm)
- Virtual Box (https://www.virtualbox.org)

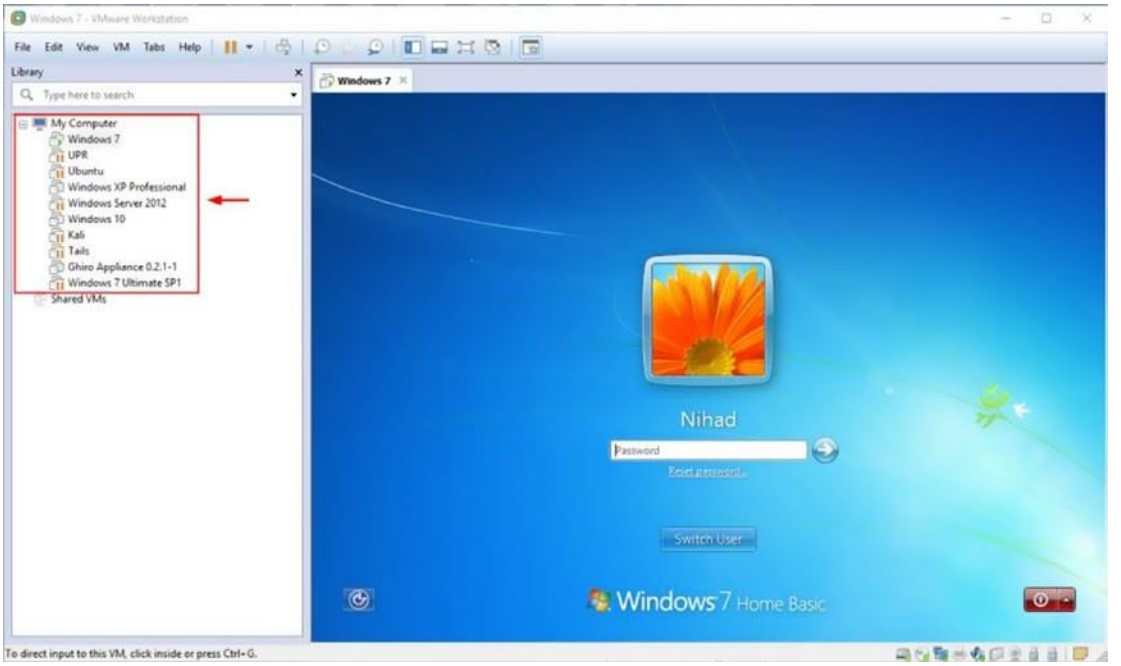

Рисунок ***2-28.*** *Несколько ОС могут быть установлены на каждой виртуальной машине; на этом изображении показано несколько ос, установленных в одном экземпляре VMware*

Вы также можете использовать портативные программы, которые не должны быть установлены для запуска. Такие программы, как правило, оставляют небольшой след на принимающей машине, но он по-прежнему считается способом свести к минимуму ваш цифровой след в Интернете.

Использование загружаемого LiveUSB или живого CD/DVD при работе над конфиденциальными документами также является отличной практикой для сокрытия ваших цифровых следов. Запуск Tails OS(https://tails boum.org)в автономном режиме является большой практикой. Есть много инструментов, которые могут помочь вам создать загружаемый USB / CD диск. Ниже приведены некоторые из них:

- Windows USB/DVD download tool (https://wudt.codeplex.com)
- Rufus (https://rufus.akeo.ie)
- WinBuilder (http://winbuilder.net)

Windows To Go — это новая функция, доступная в Windows10 (Enterprise and Education editions only). Это позволяет запускать полную Windows 10 Live с USB диска без установки

на HDD компьютера. Вы можете получить доступ к этой функции с панели управления ➤ Windows To Go. Эта функция позволяет взять Windows с собой, но имейте в виду, что некоторые функции Windows 10 могут не работать при использовании Windows To Go.

Android и iOS эмулятор

Эмулятор позволяет запускать приложение Android на вашем компьютере, как если бы оно было на вашем смартфоне. Есть множество причин, почему онлайн следователь может хотеть, чтобы это произошло; может быть, он хочет проверить функциональность конкретного приложения или просто хочет собрать некоторую информацию с помощью функции, которая доступна только для приложений смартфонов. Защитные меры, чтобы остаться анонимным могут быть реализованы более легко при запуске таких приложений с помощью эмулятора на вашем компьютере, а не на вашем смартфоне. Например, использование VPN и доступ к ресурсам с помощью Tor анонимно более удобно использовать компьютер с помощью мыши.То же самое можно сделать с приложениями для смартфонов при запуске на компьютере с помощью эмуляторов. Вот список самых популярных эмуляторов для обоих Android и Apple OS:

- Andy (https://www.andyroid.net)
- ARChon (https://github.com/vladikoff/chromeos-apk/blob/ master/archon.md), Google Chrome
- MEmu (www.memuplay.com)
- MOBIONE STUDIO (http://download.cnet.com/MobiOne-Design-Center/3001-2247_4-75910775.html), Apple apps

Основные предпосылки

В этом разделе мы перечислим некоторые из вспомогательного программного обеспечения и методов, которые могут помочь следователю для подготовки собранных данных OSINT в пригодные для использования форматы для дальнейшего анализа.

ПО для рисования и визуализации

По для рисования —включает умственное сопоставление — инструменты визуализации данных помогают онлайн-следователям визуализировать свои выводы, сделать планы поиска,и не забыть что-то во время процесса сбора; они также представляют

окончательные результаты в ясной форме. В этом разделе мы сосредоточимся на лучших бесплатных программах/услугах, доступных для оказания помощи следователям OSINT в завершении их миссии.

ЛОГИЧЕСКИЕ СХЕМЫ И ИНСТРУМЕНТЫ ГЕНЕРАЦИИ ИДЕЙ

При проведении сбора OSINT, лучше использовать некоторые инструменты для организации ваших выводов. Ниже приведены некоторые популярные инструменты для рисования диаграмм и диаграмм, заметок, и логических схем, чтобы визуализировать свои результаты.

FreeMind

FreeMind (http://freemind.sourceforge.net/wiki/index.php/Main_Page) является самым популярным свободным программным обеспечением для составление логических схем. Используя этот инструмент, можно нарисовать различные диаграммы, которые визуально организуют информацию.

Storytelling Tools

Эти инструменты помогут вам создать временную шкалу для сбора OSINT. Вот некоторые популярные бесплатные решения:

- Story Map (https://storymap.knightlab.com)
- Visual Investigative Scenarios (https://vis.occrp.org)

DIAGRAMMING SOFTWARE

Ниже приведены некоторые инструменты для диаграммирования.

Apache OpenOffice Draw

Apache OpenOffice Draw (https://www.openoffice.org/product/draw.html) позволяет рисовать различные диаграммы технических и бизнес-процессов.

Google Drawings

Google Drawings (https://docs.google.com/drawings/create) — это бесплатный облачный инструмент диаграммирования, разработанный Google.

NOTE MANAGEMENT

Вот некоторые инструменты для управления заметками.

TagSpaces

TagSpaces (https://www.tagspaces.org) — это автономный, открытый исходный код, менеджер персональных данных, который помогает вам организовывать файлы на ОС, Windows, Linux, Android или Mac– используя теги и заметки для файлов/папок.

KeepNote

KeepNote (http://keepnote.org) представляет собой кросс-платформную программу с открытым исходным кодом для организации ваших заметок и списка дел. Вы можете прикрепить к вашей заметке различные носители, например, и видео, что делает ее более информативной.

Визуализация данных

Вот некоторые инструменты для визуализации данных.

Microsoft

Excel

Это поможет вам обобщить большие объемы данных и представить их в диаграммах/таблицах и других графических визуализациях. Microsoft Excel является несвободным программным обеспечением корпорации Майкрософт.

Business Intelligence and Reporting Tools

Инструменты бизнес-аналитики и отчетности(https://www.eclipse.org/birt/about) это программное обеспечение с открытым исходным кодом, которое поможет вам визуализировать данные и создавать отчеты на его основе.

Dradis CE

Dradis CE (https://dradisframework.com/ce/) является инструментом отчетности и сотрудничества с открытым исходным кодом для профессионалов InfoSec; это позволяет комбинировать выход различных инструментов, таких как Burp, Nessus, Nmap, и Qualys для создания единого отчета для конкретного случая.

ЗАКЛАДКИ

Работая над сбором источников OSINT, вы столкнетесь с большой суммой полезных интернет-ресурсов. Для обработки этого большого объема данных, вам нужен метод или инструмент для организации ваших любимых веб-страниц. Все веб-браузеры имеют встроенную функцию для организации избранного; мы уже рекомендовали Firefox в качестве предпочтительного веб-браузера для проведения поиска OSINT. Встроенного организатора закладок, связанного с Firefox, достаточно, чтобы организовать вашу работу. Тем не менее, предпочтительнее использовать его эффективно, связывая ваши закладки(Рисунок 2-29) с тегами и группированием связанных закладок в одной папке. Firefox также дает вам возможность экспортировать ваши закладки в HTML файл, так что вы можете импортировать этот HTML-файл в другой браузер позже. Для экспорта закладок в Firefox выберите закладки ➤ Показать все закладки➤ Импорт и резервное копирование➤ Экспортировать закладки в HTML.

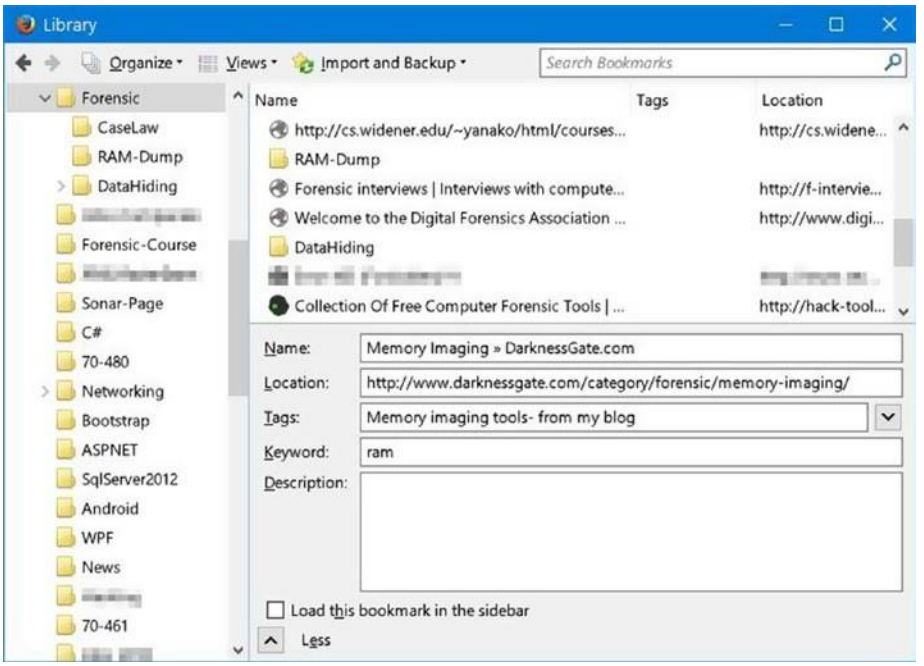

Рисунок 2-29. *Организация избранного в Firefox*

Есть много онлайн закладок менеджеров; однако, мы обнаружили, что хранение закладок с помощью онлайн-сервисов не является хорошей вещью для секретности расследования OSINT.

Переводчики

Во время поиска OSINT вы столкнетесь с полезными ресурсами на других языках, которые вы не понимаете, например, на арабском языке. Онлайн услуги мгновенного перевода предлагают большое помощь, чтобы понять эти иностранные ресурсы, чтобы добавить их в свой случай данных. Ниже приведены некоторые бесплатные сервисы перевода:

- Google Translate (https://translate.google.com)
- Bing Translator (https://www.bing.com/translator)
- Babylon's Free Online Translation (http://translation.babylon- software.com)
- Systranet (www.systranet.com/web)

Заключительные советы

Наконец, мы хотим дать вам несколько советов которым нужно следовать, прежде чем начать онлайн OSINT исследование.

ИСПОЛЬЗУЙТЕ ФАЛЬШИВУЮ ИДЕНТИФИКАЦИЮ ДЛЯ РЕГИСТРАЦИИ НА НЕКОТОРЫХ ВЕБ-САЙТАХ

В то время как вы проводите поиск OSINT, некоторые веб-сайты могут потребовать от вас зарегистрироваться или создать бесплатную учетную запись, чтобы использовать его услугу или получить доступ к некоторым разделам. Убедитесь в том, чтобы не использовать вашу реальную личную информацию; Вы также должны иметь специализированный адрес электронной почты (желательно на Gmail) для этой проблемы с поддельной информацией. То же самое относится и к открытию поддельных аккаунтов в Facebook, Twitter, Instagram и других социальных сетях для проведения поиска OSINT.

Предупреждение! Некоторые социальные сайты запрещают создавать поддельные аккаунты; всегда целесообразно прочитать правила, прежде чем зарегистрироваться. Однако для людей, работающих в разведывательной сфере, маловероятно, что они будут подчиняться таким условиям!

Поддельный генератор идентичности может генерировать все, что вам нужно, чтобы стать новым цифровым гражданином. Это включает в себя телефон, веб-сайт, электронную почту, имя пользователя, пароль, вопросы безопасности учетной записи, поддельные номера кредитной карты и социального страхования, профессия, компания, физические черты, и многое другое. Вот список самых популярных веб-сайтов поколения идентичности:

- www.fakenamegenerator.com
- https://names.igopaygo.com/people/fake-person
- www.elfqrin.com/fakeid.php

БУДЬТЕ АНОНИМНЫМИ

Включите VPN-сервис или просто воспользуйтесь браузером Tor, прежде чем начать поиск OSINT. Если вы не используете Tor, не забудьте использовать виртуальную машину, которая имеет недавно установленный веб-браузер в нем для сбора онлайн-ресурсов. Убедитесь, что подключение VPN включено для всех приложений, установленных на вашей машине, включая экземпляр виртуальной машины.

УНИЧТОЖИТЬ ВАШИ ЦИФРОВЫЕ СЛЕДЫ ПОСЛЕ ОКОНЧАНИЯ .

Используйте виртуальные машины и просматривайте веб-страницы с помощью режима Firefox incognito. Убедитесь в том, чтобы использовать такие инструменты, как BleachBit(https://www.bleachbit.org),чтобы очистить цифровые следы вашего приложения в дополнение к любым остаткам, оставленным на жестком диске.

USE LINUX

Многие мощные инструменты OSINT работают на системах на базе Linux. Эти инструменты доступны на Kali Linux (преемник Backtrack), хотя многие из этих инструментов были импортированы в Windows. Вы можете скачать Кали из https://www.kali.org и установить его на виртуальную машину. Освоение дистрибутива Kali Linux имеет важное значение для любого тестера проникновения и цифрового судебно-медицинского следователя. Kali оснащен множеством готовых инструментов безопасности.

Итоги

В этой главе мы подготовили этап, прежде чем начать поиск OSINT. Мы говорили о различных онлайн-угроз и о том, как можно противостоять им с помощью программного обеспечения безопасности, а также передового опыта при использовании вычислительных устройств. Мы рассмотрели некоторые а том числе Windows, так как он по-прежнему считается иметь самую большую базу пользователей во всем мире. А так же повысили приватность с помощью настроек.

Мы говорили о том, как онлайн отслеживание работает технически, перечисляя его типы и дал контрмеры, чтобы предотвратить отслеживание вашей деятельности в Интернете. Затем мы перешли к разговору о безопасном просмотре в Интернете; мы дали советы по усилению приватности для браузера Firefox, а также полезные дополнения конфиденциальности. Использование VPN для шифрования интернет-трафика важно для любого интернет-пользователя; мы кратко описали концепцию VPN и прокси-сервера, а затем дали важные подсказки о том, как использовать их безопасно, чтобы избежать утечки вашего реального IP-адреса без вашего ведома, даже если вы используете VPN-сервис. Раздел анонимности необходим перед проведением поиска OSINT; Вы не должны делать какой-либо поиск OSINT без активации службы анонимности или VPN. Мы говорили об использовании Tor Browser для анонимного серфинга в Интернете. Для людей, которые живут в крайне враждебной среде, использование Tails OS, которая направляет весь ваш интернет-трафик через сеть анонимности Tor, настоятельно рекомендуется.

Технология виртуализации пригодится, когда вы хотите протестировать другие приложения или просто покрыть цифровые следы на хост-машине. Виртуальные машины также помогут вам снизить цифровой след при проведении исследований в Интернете, как вы можете использовать стандартную ОС и веб-браузер установки, чтобы сделать поиск и, наконец, удалить всю ОС в один клик.

Это была длинная глава, полная советов о том, как бороться с сегодняшними онлайн-угрозами. Понимание онлайн-угроз, контрмер и того, как стать анонимным в Интернете, необходимо перед началом работы по сбору ресурсов OSINT в Интернете. Остальные главы этой книги посвящены методам поиска OSINT. В следующей главе мы будем углубляться под поверхность обычного Интернета, чтобы исследовать скрытый подземный Интернет, известный как глубокая паутина.

Глава3

Глубокий Интернет

Насколько хорошо вы знаете Интернет? Будучи регулярным пользователем Facebook, Twitter и Instagram и зная, как использовать Google, чтобы найти вещи в Интернете не сделает вас суперинтернет-пользователя, потому что вы просто пользуетесь вершиной айсберга под названием Интернет. Большинство веб-контента скрыто и нуждается в специальных методах для доступа к нему.

По данным Internet World Stats, число пользователей Интернета в мире за июнь 30, 2017, достигла 3,885,567,619. (Население мира 7,519,028,970 человек.[i]) Это огромное количество, и, по прогнозам, к 2020 году он увеличится до 4 миллиардов пользователей Интернета.

Большинство пользователей Интернета во всем мире используют поверхностный интернет, также известный как обычный Интернет. Лишь незначительный процент пользователей Интернета используют другие скрытые слои Интернета на ежедневной основе или даже слышали о них!

В августе2017, общее количество живых веб-сайтов, принадлежащих к поверхности веб-было 1,800,566,882,[ii] в то время как предполагаемое количество сайтов Tor в даркнете с марта2016 до марта2017 было около 50,000 - 60,000. Несмотря на огромное количество веб-сайтов в рамках поверхности веб-страницы, их содержимое, которое может быть проиндексировано типичными поисковыми системами, составляет всего 4 процента от всей сети, в то время как остальная часть принадлежит глубокой веб-части (которая включает в себя darknet).

В этой главе мы познакомим вас с терминами *глубокая паутина* и *темная паутина.* Оба термина используются для указать на ту часть Интернета, которая скрыта от обычного пользователя Интернета и не может быть проиндексирована типичными поисковыми системами. Глубокое содержимое веб-страниц можно получить с помощью регулярного протокола HTTP/HTTPS и типичных веб-браузеров; однако, это не то же самое для darknet, которая нуждается в специальном программном обеспечении для доступа к его содержимому. Прежде чем начать наше обсуждение, давайте сначала дифференцировать между тремя терминами-поверхность, глубокий, и темный Интернет.

N. A. Hassan and R. Hijazi, *Open Source Intelligence Methods and Tools*, https://doi.org/10.1007/978-1-4842-3213-2_3

Слои Интернета

Начнем с обычного Интернета или поверхностного интернета. Это часть Интернета, которая включает в себя все содержимое, которое легко доступно для общественности. Веб-сайты на поверхности веб могут быть проиндексированы с помощью регулярных поисковых систем, таких как Google, чтобы пользователь мог легко найти их.

Поисковые системы используют программное обеспечение, известное как *веб-сканеры в дальнейшем (*Crawlers*),* чтобы обнаружить общедоступные веб-страницы. Crawlers работают, собирая гиперссылки внутри страниц, а затем отправляют эти страницы (результаты) на серверы поисковых систем, которые организуют результаты в поисковом индексе. Индекс поиска содержит сотни миллиардов индексированных страниц. Наконец, пользователь отправляет поисковый запрос, а поисковая система отвечает на рейтинговые страницы, которые соответствуют запросу пользователя, и возвращает упорядоченный список (Рисунок 3-1).

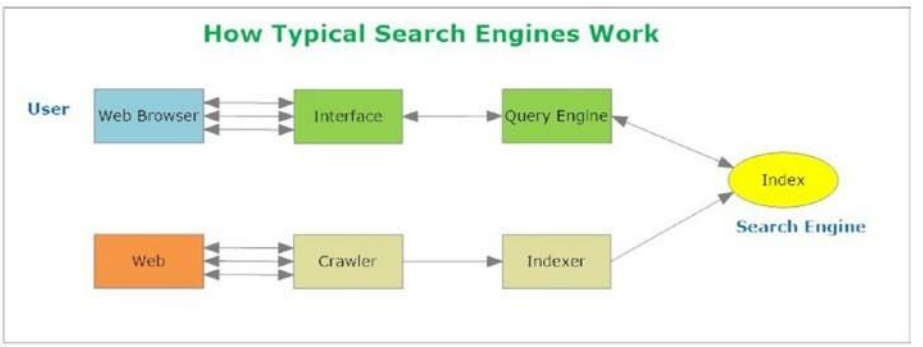

Рисунок 3-1. *Как поисковые системы индексируют веб-сайты (Источник: www.darknessgate.com)*

Примечание! Если вы хотите понять, как поисковые системы индексируют веб-сайты, Google предлагает простой учебник, описывающий эту проблему. Вы можете найти его на https://www.google.com/search/howsearchworks/.

По состоянию на ноябрь 2017, Google известно о 130 триллионов страниц. Цифры постоянно меняются из-за быстро меняющегося характера Интернета.

Как уже упоминалось, поисковые системы веб-сканеры обнаружить новые страницы через гиперссылки. Тем не менее, этот метод не является совершенным, и огромный объем данных останется неиндексированным, как поисковые системы не могут проиндексировать их через crawlers

В качестве примера, скажем, вы хотите знать, канадский курс доллара в 2000 году. Есть много сайтов, которые предлагают обменные курсы валют с течением времени. Итак, для этого примера вы идете в www.xe.com веб-сайт, чтобы увидеть канадский обменный курс в 2000 году. Но подождите, есть проблема здесь. Если вы хотите выступать в качестве обычного crawlers, вы можете перейди по гиперссылки! Но это не даст вам нужного результата. Однако, если вы действуете как человек и пошел к форме поиска на www.xe.com/currencytables и ввел конкретную дату поиска (2000/01/01) и нажал кнопку Отправка, затем веб-сайт будет получать исторический результат из своей базы данных и представить его вам(Рисунок 3-2). Этот результат не может быть получен с помощью обычных поисковых систем, поскольку он требует, чтобы вы использовали окно поиска на веб-сайте и ввести поисковый запрос, чтобы получить его. Полученный результат является наглядным примером глубокого веб-контента

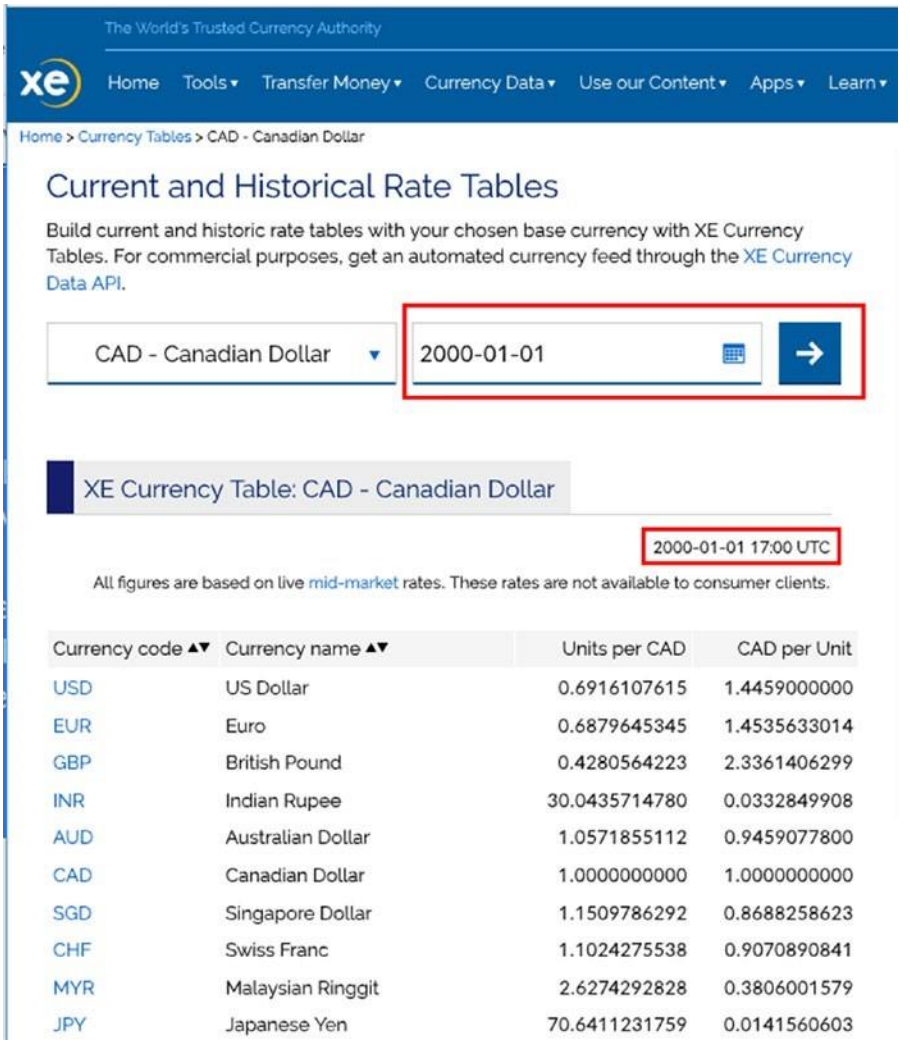

Рисунок 3-2. *Исторические данные, извлеченные из базы данных веб-сайта, является примером глубоких веб-данных*

Многие интернет-пользователи, и даже некоторые эксперты, использовать термины *глубокий веб* и *darknet* синонимом, но есть разница между ними. Термин глубокий *веб* описывает все интернет-ресурсы, которые не индексируются с помощью обычных поисковых систем, таких как Google, Bing, или Yahoo, но глубокий веб-прежнему можно получить доступ, как и любой обычный веб-сайт, используя стандартный http/HTTPS веб-протокол и типичные веб-браузеры без использования какого-либо специального программного обеспечения. Любой пользователь Интернета, безусловно, использовали некоторый тип глубокой веб-

браузера во время просмотра в Интернете; однако, большинство пользователей могут не знать, что такие ресурсы принадлежат к глубокой сети.

Глубокие веб-ресурсы обычно закапываются в базы данных, доступные для общедоступного просмотра в Интернете, но пользователю необходимо ввести запрос (например, в форму поиска в Интернете) или использовать выпадающее меню для установки некоторых значений поиска для получения содержимого этих баз данных. Это то, что делает его содержание скрытым; он не может быть замечен типичными поисковыми системами, потому что он не может быть доступен через гиперссылки. То же самое относится и к веб-сайтам, которые требуют регистрации (имя пользователя и пароль) для доступа к контенту и веб-сайты, которые специально предназначены для сдерживания crawlers. Зашифрованные сети и веб-сайты, требующие оплаты для просмотра контента, также подпадают под категорию глубокой сети. Никто не может знать точный объем глубоких веб-сайтов из-за постоянно меняющегося характера веб-контента, но многие исследования показывают, что это примерно в 500 раз больше, чем поверхности сети. Вот несколько примеров основных глубоких веб-сайтов:

- Библиотека Конгресса(https://www.loc.gov) Это крупнейшая национальная библиотека в мире, она включает в себя огромные коллекции ресурсов, таких как книги, фотографии, архив газет, карты и рукописи - в различных темах.
- Vital Records (www.vitalrec.com) предоставляет доступ к свидетельствам о рождении в США, записям о смерти и свидетельствам о браке.
- Science.gov (https://www.science.gov) дает доступ к более чем 200 миллионам страниц авторитетной федеральной научной информации.
- Alexa (https://www.alexa.com) дает подробную аналитическую информацию о веб-сайтах.
- Directory of Open Access Journals (https://doaj.org) предоставляет доступ к высококачественным, открытым, рецензируемым журналам.
- The Online Books Page (http://onlinebooks.library.upenn.edu) предоставляет бесплатный доступ к более чем двум миллионам книг, которые доступны (и читаемы) в Интернете.

Как вы уже видели, поиск контента в глубокой сети не является простой задачей для обычного пользователя, и большая часть ценного глубокого содержимого веб должны быть извлечены вручную. Однако существует много подходов к упрощению этой задачи:

- *Специализированные поисковые системы*: Это включает в себя любую поисковую систему, которая поможет вам найти глубокий веб-контент в рамках одного предмета или более.Ниже приведены некоторые примеры:

a. https://www.doi.org помогает решить идентификатор цифрового объекта (DOI) любой публикации.

b. https://www.100searchengines.com содержит специализированные поисковые системы для почти любой темы в Интернете. Это позволяет искать несколько поисковых систем в то же время (хотя поиск нескольких поисковых систем в то же время может опустить некоторые результаты, потому что не все поисковые системы используют тот же механизм для получения данных из своего индекса).

c. https://books.google.com/?hl=en является одним из крупнейших глубоких веб-баз данных, который содержит миллионы книг. Google включает результаты этой базы данных при проведении регулярных поисков.

d. www.academicindex.net является научно-академической поисковой системы доступа только выбранный набор веб-сайтов, которые специализируются на академических и научных работ.

e. https://www.truthfinder.com поиск в социальных сетях, фотографиях, полицейских записях, проверках, контактной информации и многом. Результат будет извлечен из базы данных TruthFinder глубоких веб-источников.

- *Веб-каталоги*: Каталог веб-сайт, который показывает список веб-сайтов, организованных по категориям. Пользователь вводит поисковый запрос, и каталог предоставляет пользователю относительные объекты в вводимый запрос. Каждый предмет может содержать сотни и даже тысячи веб-сайтов, которые подпадают под эту категорию. Чтобы просмотреть каталог, пользователь выбирает тему, а затем переходит от самой широкой к самой узкой. Некоторые каталоги оплачиваются, в то время как другие являются бесплатными и поддерживаются сообществом редакторов-добровольцев. Веб-каталоги меньше, чем поисковые системы, поскольку они поддерживаются людьми, в отличие от поисковых систем, которые в основном поддерживаются crawler (веб-сканеры). Ниже приведены некоторые известные веб-каталоги:

a. https://www.hotfrog.com.au является крупнейшим онлайн-каталог бизнеса; в нем перечислены 120 миллионов предприятий в 38 странах.

b. www.akama.com is a U.S. business directory.

c. http://vlib.org является WWW Виртуальная библиотека.

d. http://dmoztools.net закрыт в марте 2017 года. Он по-прежнему считается крупнейшим веб-каталог онлайн.

- *Интернет вещей (IoT) поисковые системы*: Термин Интернет вещей используется для описания любого устройства, которое может подключиться к Интернету и может собирать и обмениваться данными. Список устройств включает в себя маршрутизаторы, серверы, светофоры, сотовые телефоны, кофеварки, стиральные машины, наушники, лампы, носимые устройства, такие как часы, системы безопасности, включая сигнализацию, Wi-Fi камеры, детские мониторы, умные холодильники, смарт-телевизор наборы, интеллектуальные системы кондиционирования воздуха, которые могут регулировать тепло удаленно, и почти все остальное вы можете себе представить, что может быть подключен к Интернету и управляться удаленно. Shodan (https://www.shodan.io) является сложной поисковой системой, которая специализируется на поиске подключенных к Интернету устройств путем поиска, где они находятся и кто использует их. Shodan собирает данные в основном по этим портам: HTTP (80), FTP (21), SSH (22), Telnet (23) и SNMP (161). Shodan позволяет как частным лицам, так и корпорациям обезопасить свои устройства IoT, обнаружив, какой из них уязвим для внешних атак или неправильной настройки (например, по-прежнему использует имя пользователя и пароль производителя по умолчанию). Эта поисковая система может быть эффективно использована для поиска информации об активных устройствах IoT по всему миру.

Теперь мы подошли к третьему уровеньу Интернета. Это самый глубокий и называется *darknet*. Darknet-или темная паутина - это интернет-ресурс, который был разработан специально, чтобы быть скрытым и анонимным. Darknet образует небольшую часть глубокой паутины, но в отличие от глубокой паутины, этот не может быть доступен с помощью типичных веб-браузеров. Он нуждается в специальном программном обеспечении для доступа к нему, таких как Tor (сокращение от лукового маршрутизатора).

Darknet-или анонимность-сети состоят из коллекций компьютеров, разбросанных по всему миру, которые образуют децентрализованную сеть. Эти сети анонимности образуют коллективно то, что известно как darknet. Пользователи могут получить доступ к этим сетям для анонимного серфинга в Интернете или для посещения анонимных скрытых веб-сайтов в этих сетях.

Физические лица попадают в даркнет для различных целей, и значительное их количество незаконно. Хотя нет точной статистики о количестве незаконных сайтов (так называемых *Tor*

услуг или *скрытых услуг* в сети Tor), группа Intelliagg в 2015 году рассмотрела более 1000 образцов скрытых услуг Tor и обнаружила, что 68 процентов содержимого Tor darknet являются незаконными.[iii]Преступники не только посещают даркнет, чтобы искать незаконные продукты, но используют ее в качестве средства для анонимизации их онлайн-корреспонденции и удерживают других от следования за ними при использовании поверхностного WEB. Тем не менее, несмотря на то, что большинство веб-сайтов darknet связаны с незаконной деятельностью, многие люди используют его в законных целях (например, с помощью Tor Browser, чтобы скрыть IP-адрес пользователя и цифровой след машины при серфинге в обычном Интернете).

Существуют различные сети анонимности. Ниже приведены самые популярные:

- Tor Network (https://www.torproject.org/index.html.en)
- I2P network (https://geti2p.net/en/)
- Freenet (https://freenetproject.org/index.html)

Как вы уже видели, глубокие веб-ресурсы можно найти, ища их в рамках целевых веб-сайтов или с помощью специализированных поисковых систем, каталогов и других платных онлайн-сервисов, которые предлагают доступ к несвободному контенту (например, серой литературе). То же самое не относится и к даркнету. Как аналитик OSINT, вы должны понять, с чего начать исследования darknet и как получить доступ и поиск в даркнете. OSINT следователи обычно используют сети darknet, особенно Tor Network,для анонимного просмотра веб-страниц. Это эффективно поможет им скрыть свою деятельность в Интернете от внешних наблюдателей (см. рисунок 3-3). Остальная часть этой главы будет изучать то, что darknet и как получить доступ и использовать свои ресурсы.

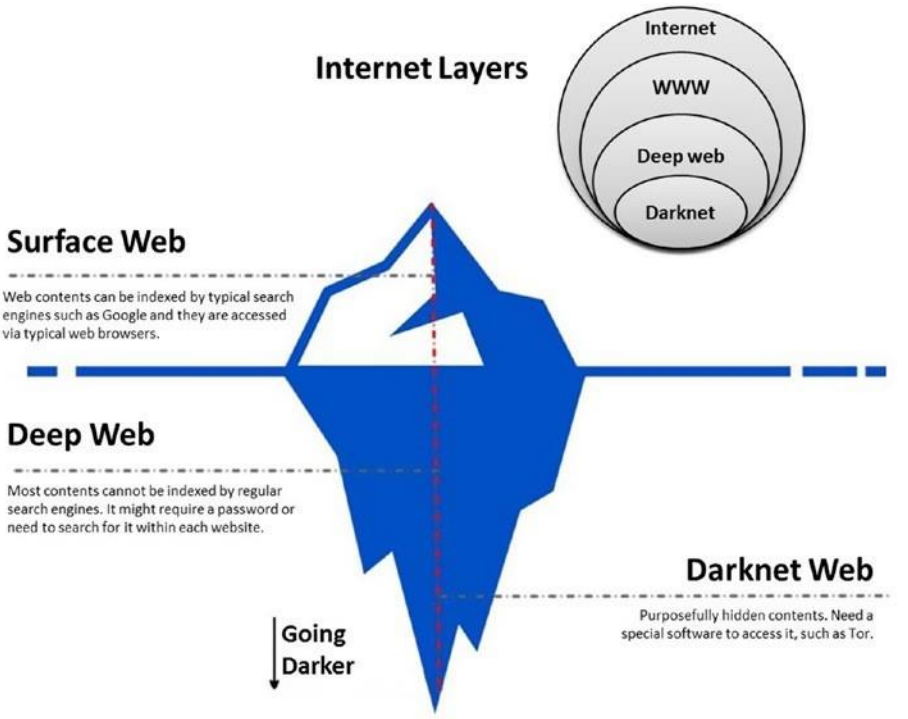

Рисунок 3-3. *Слои Интернета (источник: www.DarknessGate.com)*

Даркнет пользователи

Darknet имеет плохую репутацию за то, что предпочтительное место для злонамеренных субъектов для проведения своей преступной деятельности в Интернете. Ниже приведены некоторые типы пользователей:

- Наркоторговцы используют функцию анонимности даркнета для безопасного осуществления своих незаконных продаж.
- Оружейные дилеры используют даркнет для незаконной покупки и продажи оружия.
- Люди покупают фальшивые государственные документы (например, паспорта и национальные удостоверения).
- Киберпреступники используют его для загрузки и обмена инструментов эксплойта; продаже готовых к запуску распределенных атаки типа «отказ в обслуживании» (DDoS), вымогатели и эксплойтов безопасности; и предлагают шпионские услуги клиентам.
- Террористы используют дарк-нет для обмена информацией и торговли незаконными товарами в дополнение к сокрытию своей деятельности на открытой сети.
- Сайты азартных игр и ставок находятся в даркнете.
- Продавцы украденной информации, такие как корпоративные секреты, номера кредитных карт и личные данные людей, полученные в ходе мошеннических действий, используйте дарк-нет для продажи украденной информации заинтересованным сторонам.

Несмотря на то, что многие сайты даркнета направлены на преступную деятельность, существует множество законных применений для даркнета. Некоторые из них включают в себя следующие:

- Правозащитники, журналисты и разоблачители используют его для раскрытия секретного содержания общественности, не раскрывая их личности.

- Защитники конфиденциальности используют даркнет анонимно вдали от правительств и корпоративного надзора.
- Правоохранительные органы используют даркнет для различных целей (например, отслеживание преступников и сбор информации о них).
- Частные лица, правительства и корпорации используют сети анонимности в качестве надежного средства обмена сверхсекретной информацией.
- Разведывательные службы и военные организации используют дарк-нет для сбора разведывательной информации с открытым исходным кодом и для противодействия террористической деятельности.
- Бизнес-корпорации могут контролировать darknet форумы и блоги, чтобы увидеть свои собственные утечки конфиденциальной информации.

Может быть, вы задаетесь вопросом, как трейдеры делают свой бизнес анонимно на darknet. Ответ прост. Каждый dark-web сайт принимает оплату через биткоины. Мы уже рассмотрели концепцию криптовалюты в главе 2; Bitcoin(https://www.bitcoin.com) является самым популярным и может быть использован для проведения онлайн денежных операций анонимно.

Доступ к Даркнету

Сеть Tor является самой популярной анонимной сетью в мире, поэтому мы сосредоточимся на ней в этой главе, чтобы описать даркнет. Однако, прежде чем мы начнем, помните основные меры предосторожности при доступе к даркнет.

Примечание! Хотя доступ к сети Tor считается законным в большинстве стран, его использование может вызвать подозрение с законом. А некоторые страны рассматривают доступ к сети Tor как незаконную практику, которая может привести к вопросам со стороны властей. Правило Верховного суда США дает разрешение ФБР на поиск и захват любого компьютера по всему миру, который находится с помощью сети Tor или даже службы VPN. [iv] Убедитесь в том, чтобы прочитать раздел о том, как скрыть использование Tor в предыдущей главе.

Проверки безопасности при доступе к Darknet

Глава 2 была полностью посвящена личной кибербезопасности; однако, стоит вспомнить следующие основные моменты, прежде чем получить доступ к даркнету (подробные описания того, как каждая мера предосторожности работает технически доступны в предыдущем глава):

- Сделайте свой вход в сеть Tor скрыты с помощью подключаемых транспортных возможностей, пользовательских мостов или VPN перед запуском вашего Tor Browser.
- Закройте веб-камеру и микрофон.
- Подготовьте свою анонимную электронную почту (например, Protonmail.com) или воспользуйтесь бесплатной услугой электронной почты.
- Создание ложной цифровой идентификации в случае, если вам нужно зарегистрироваться на некоторых веб-сайтах для доступа к некоторым заблокированным содержимому. Убедитесь в том, чтобы не использовать какие-либо личные данные, которые относятся к вам.
- Убедитесь, что ваш Tor Browser обновлен, чтобы избежать утечки вашего реального IP-адреса - Tor Browser предупредит пользователей, чтобы обновить его при запуске в случае, если он станет устаревшим.

1. Убедитесь, что ваша ОС и антивирусное программное обеспечение обновлены. Наличие специального программного обеспечения для борьбы с вредоносным ПО в высокой степени

   Рекомендуется.

   - Отображение JavaScript на вашем браузере Tor путем активации дополнения NoScript, которое поставляется с предустановленным браузером Tor (Рисунок 3-4).

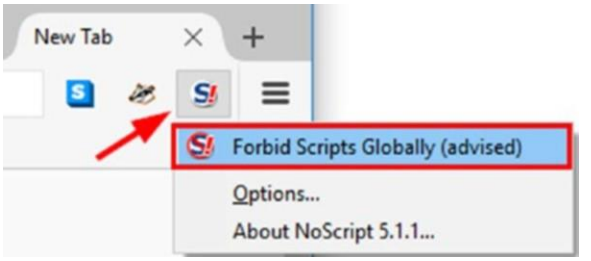

Рисунок 3-4. *Отключение JavaScript на всех веб-сайтах перед доступом к dark web*

- Целесообразно изменить вашу личность он-лайн и следовательно адрес IP для каждого посещенного места на темной паутине, как в рисунке 3-5. Выбор опции New Identity потребует перезагрузки tor Browser и проигрыша текущей сессии.

Рисунок 3-5. *Изменение идентификатора Tor Browser для каждого посещаемого сайта в даркнете*

- Не загружайте ничего из даркнета на компьютер, особенно программное обеспечение и пиратские СМИ, такие как песни и фильмы.
- Будьте подозрительны, прежде чем нажать на любую гиперссылку, потому что вы не знаете, кто работает darknet веб-сайтов и назначения, что такие ссылки будут принимать вас.

Доступ к Даркнету из обычного WEB

Некоторые веб-сайты предлагают функциональность для доступа к скрытым веб-сайтам Tor (скрытые услуги) из поверхности веб-использования обычных браузеров, без

использования программного обеспечения Tor Browser или Tor.В следующем списке показаны некоторые веб-сайты, которые подключают пользователей Интернета к контенту, размещенного в сетиTor.Имейте в виду, что доступ к даркнету таким образом не гарантирует, что вы можете путешествовать по ней, как вы сделали бы с Tor Browser. Этот метод более удобен для случайного пользователя — легко просматривать сеть Tor. Тем не менее, вы потеряете анонимность, что пользователи Интернета стремятся при использовании Tor Браузер в дополнение к тому, чтобы ваша история просмотра может быть перехвачена.

- Not Evil (https://hss3uro2hsxfogfq.onion.to)
- Tor2web (https://tor2web.org)
- Torchtorsearch (www.torchtorsearch.com)

Предупреждение! Если вы хотите получить доступ к darknet (Tor Network) из обычных веб-браузеров с помощью прокси-сайтов, убедитесь, что для шифрования подключения с помощью VPN.

Использование Tor

Мы уже рассмотрели, как работает сеть Tor в главе 2; однако, мы дадим вам краткое описание того, как поток данных работает в этой сети.

Tor отправляет запросы пользователей во многих ретрансляторах (также известных как *сервер* или *маршрутизатор);*обычно используется по крайней мере три ретранслятора. Все соединение в этих ретрансляторах зашифровано. Первый ретранслятор устанавливает подключение пользователя к сети Tor. Этот ретранслятор знает ваше текущее местоположение, поэтому желательно использовать VPN соединение сначала, чтобы замаскировать это или использовать пользовательские мосты / pluggable транспорты, чтобы замаскировать ваш вход в сеть Tor от вашего интернет-президента / правительства или любого другого внешнего противника.

Второй ретранслятор знает, что данные поступают из первого реле, третий реле знает, что данные поступают из второго зависит, и так далее. Последний ретранслятор, также известный как *ретранслятор выхода,*не может знать происхождение данных.

Эстафеты Tor не записывают никаких действий, проходящих через них, и все соединения в этих ретрансляторах полностью зашифрованы. Однако самое слабое звено находится на последнем ретрансляторе – ретрансляторе выхода, так как этот реле может перехватывать данные, протекающие через него, если они еще не зашифрованы. Есть некоторые случаи,

когда этот релей используется злоумышленниками , чтобы разоблачить пользователей Tor и прсмотреть их незашифрованный трафик.

Чтобы уменьшить риск перехвата ваших данных в ретрансляторе выхода, необходимо зашифровать все, прежде чем отправлять их через сеть Tor. Tor Browser поставляется с надстройкой с именемHTTPS Everywhere (https://www.eff.org/https-everywhere) что заставляет ваш браузер прозрачно шифровать вашу связь с основными веб-сайтами, использующими протокол SSL.

Веб-сайты, размещенные в сети Tor, заканчиваются расширением .onion. В отличие от обычных веб-адресов, которые заканчиваются .com или .net, веб-сайты Tor можно получить только через браузер Tor.

Чтобы получить доступ к сети Tor, все, что вам нужно сделать, это скачать и использовать браузер Tor; Вы всегда можете скачать последнюю версию изhttps://www.torproject. org/download/download. Скачать версию, которая соответствует текущей ОС, а затем запустить браузер. Tor Browser — это модернизированная версия Firefox, которая работает вместе с программным обеспечением Tor для обеспечения прозрачного доступа к сети Tor. Браузер Tor также может использоваться для просмотра в Интернете.

Если вы не знаете, с чего начать после запуска Tor Browser, перейдите на скрытые вики(Рисунок 3-6) http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page. Этот сайт предоставляет каталог из самых активных сайтов darknet, организованных в категории. Имейте в виду, что некоторые веб-сайты не могут работать мгновенно; однако это не означает, что даркнет находится в автономном режиме. Многие веб-сайты работают в течение определенное время, так что нужно смотреть когда они работают .

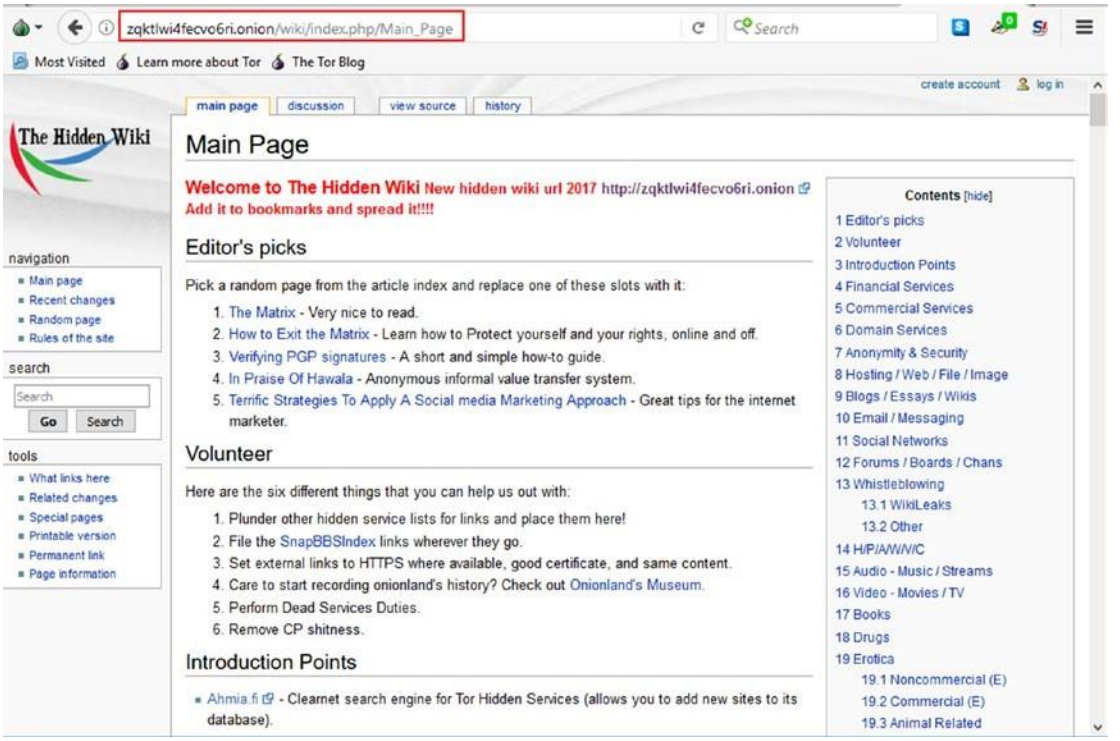

Рисунок 3-6. *Скрытые вики-новичок запись в даркнет*

Tor был создан в первую очередь, чтобы позволить пользователям получить доступ к регулярному (поверхностный) Интернет анонимно. Этот факт считается недостатком для него по сравнению с другими сетями анонимности (например, I2P, которая была создана как автономная сеть в рамках обычного Интернета). Например, способность глобального противника - с хорошими ресурсами - контролировать ретрансляторы выхода Tor (где данные оставляют Tor на поверхность Интернета) может выявить личность пользователей Tor, если их деятельность была успешно коррелирована с их входом в Tor Сеть (первый ретранслятор). Чтобы преодолеть этот ярлык, Tor позволяет своим пользователям иметь свои собственные скрытые веб-сайты, которые никто не может отслеживать. Как уже упоминалось, веб-сайты, размещенные в сети Tor, известны как *службы Tor* или *скрытые службы* и имеют расширение .onion. Эти сайты доступны только в сети Tor. На самом деле, вы можете запустить свой собственный с помощью домашнего компьютера, но вы должны знать, как избежать раскрытия вашей истинной личности. Tor предлагает инструкцию о том, как настроить ваш скрытый веб-сайт в https://www. torproject.org/docs/tor-hidden-service.html.en. Коллекция скрытых веб-сайтов Tor является частью так называемой темной сети; действительно, самые популярные сайты в даркнете принадлежат сети Tor.

Наконец, основным недостатком сети Tor является скорость. Tor, как известно, медленный. Это потому, что трафик должен пройти не менее трех реле до достижения назначения. Tor становиться медленней еще больше, когда большое количество пользователей в сети.

ИспользованиеTails OS

В крайне враждебной среде, где существует высокий риск перехвата сообщений внешними противниками, настоятельно рекомендуется использовать ОС Tails для вашей сверхсекретной связи и автономной работы. В этом разделе мы рассмотрим, как использовать эту ОС в некоторых деталях, показывая вам, как использовать его как в онлайн-режиме, так и в автономном режиме (автономный режим позволяет создавать и читать документы в безопасной среде). Как мы уже говорили в предыдущей главе, Tails — это ОС Debian GNU/Linux, которая направляет все сетевые соединения через сеть Tor. Он оснащен множеством приложений, которые предварительно настроены с учетом безопасности, как Tor Browser, безопасный чат, зашифрованный клиент электронной почты и программное обеспечение для шифрования в дополнение к его производительности приложений, таких как office Suite. Tails является портативная ОС, которая работает из USB или CD / DVD и загружается непосредственно в память о ней памяти машины хозяина; он не оставляет следов на жестком диске хоста. После выключения Tails удалит все пользовательские файлы, если только явно не попросятся этого не делать. Tails могут быть настроены, чтобы позволить пользователю хранить личные документы и настройки программы (постоянное хранение).

Чтобы установить Tails на USB-накопитель, выполните следующие действия:

1. Download Tails from https://tails.boum.org.

Предупреждение! Перед созданием LiveUSB Tails вы должны проверить целостность изображения ISO, загруженное вами, чтобы убедиться, что ваша копия файла Tails является подлинной. Всегда скачать Tails с его официального сайта (https://tails.boum.org/install/index.en.html). не загружайте с других зеркал .

---

2. Скачайте Universal USB Installer из https://www.

pendrivelinux.com/universal-usb-installer-easy-as-1-2-3.

Этот инструмент используется для установки Tails на USB.

3. Настройка Universal USB Installer как показано на рисунке 3-7. Вы должны иметь USB-накопитель с 8 ГБ свободного хранения. Наконец, нажмите кнопку «Create».

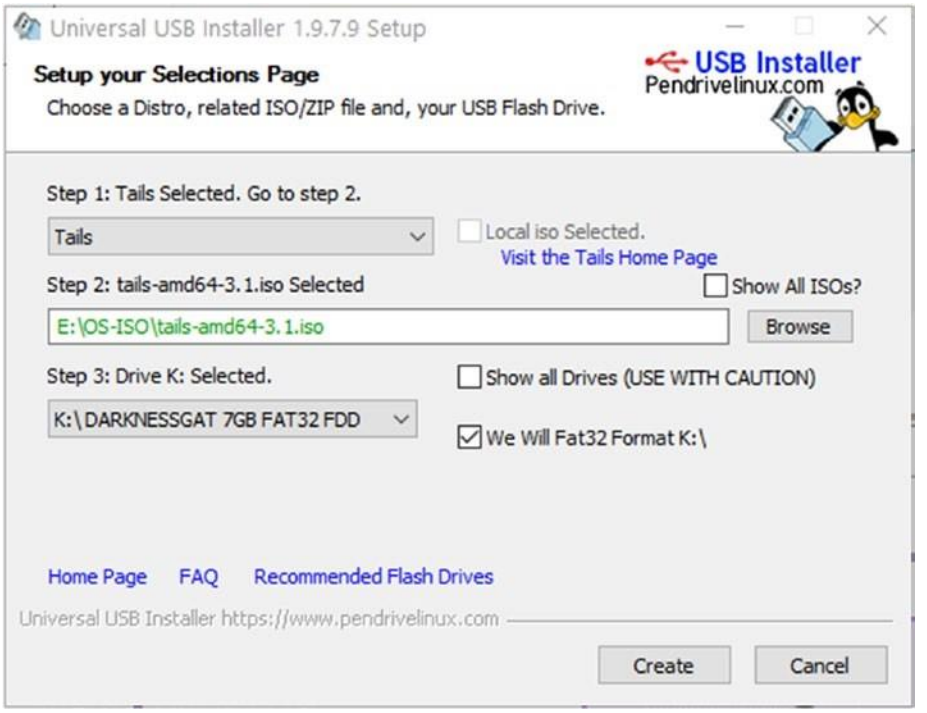

Рисунок 3-7. *Установка Tails на USB-накопителе*

4. Изменените последовательности загрузки компьютера на USB. Каждый производитель компьютеров имеет свой собственный метод доступа к BIOS/UEFI; проконсультируйтесь с веб-сайтом или компьютерным руководством.

5. Подключите USB-флешку Tails и перезапустите хост-машину, чтобы запустить tails. Если Tails загрузиться, то вы увидите экран (Рисунок3-8).

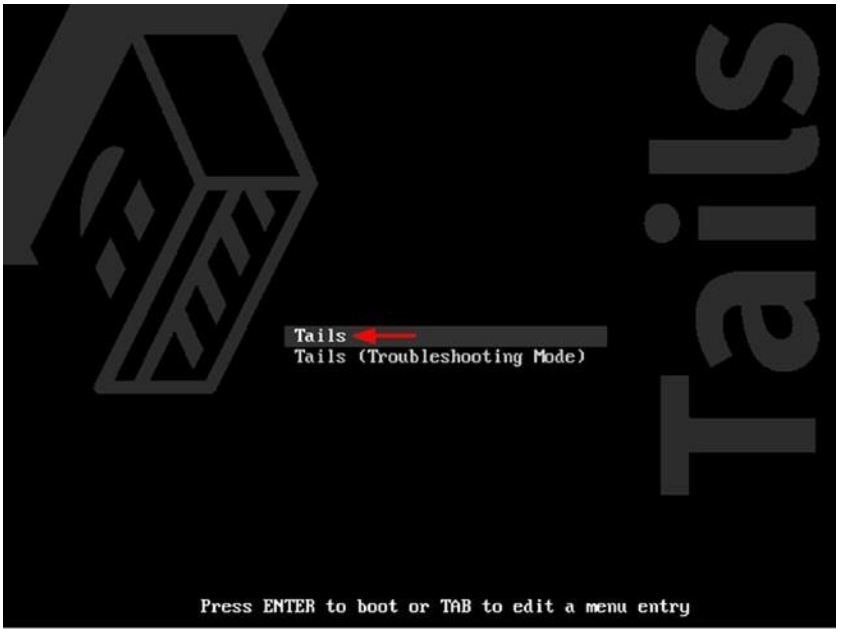

Рисунок3-8. *Tails загрузка экрана*

6. При появляются экраны Tails Greeter (это окно позволяет выбрать настройки языка и компоновку клавиатуры) нажмите кнопку Start Tails, чтобы получить доступ к рабочему столу Tails.

После запуска, Хвосты нуждается в маленьких конфигурациях, потому что все уже настроено на работу через сеть Tor (см. рисунок 3-9). Все, что вам нужно сделать, это настроить Wi-Fi, введя пароль точки доступа; если вы подключаетесь через кабель, конфигурация не требуется.

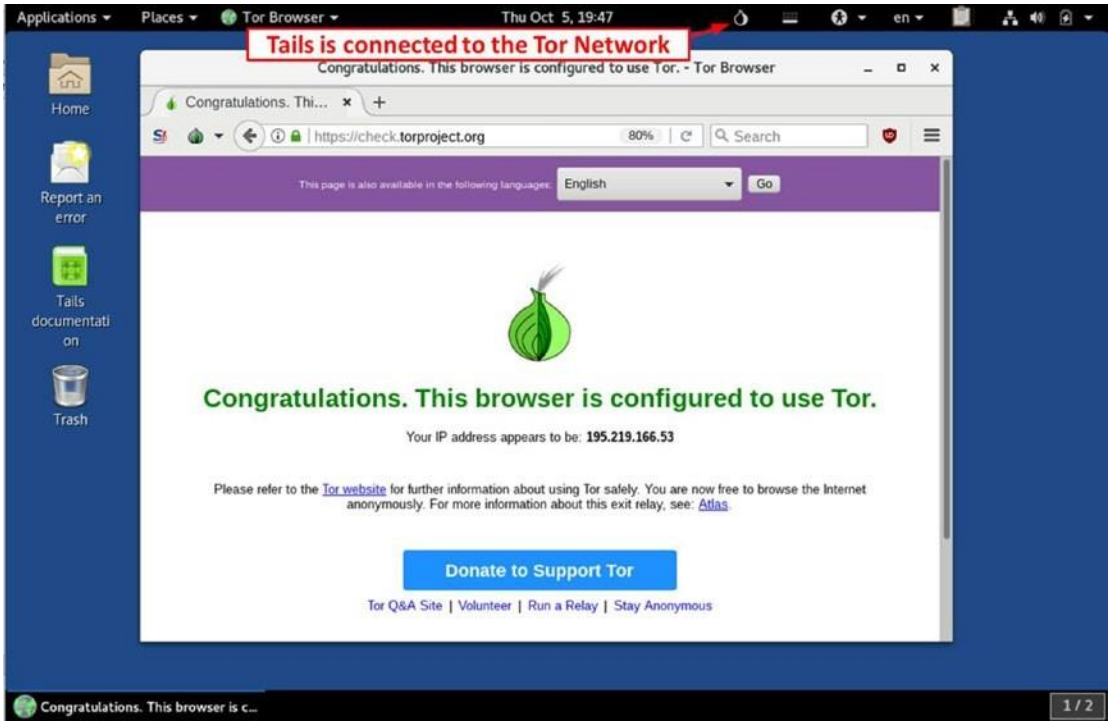

Рисунок 3-9. *Tails рабочий стол, показывающий запуск tor Browser*

Вы только что установилиTails в режиме только для чтения -промежуточного. В этом режиме установки вы не получите выгоду от таких важных функций, как автоматическое обновление безопасности или возможность хранить некоторые из ваших документов и конфигураций в зашифрованном хранилище. В следующем разделе мы покажем вам, как установить Tails в постоянном режиме хранения, чтобы вы могли сохранить настройки программы, закладки, сохраненные документы и заметки при проведении поисковых действий OSINT.

Для установки tails в качестве постоянного хранения, вам понадобится еще один USB на 8 ГБ. Конечно, если вы планируете хранить большие файлы, используйте USB-накопитель повышенной емкости.

1. Подключите второй USB вставить в компьютер в то время как Tails OS is будет запущен.
2. Перейти к приложениям➤ Tails ➤ Tails Installer и запуститие Tails Installer.
3. Когда Tails Installer запушен, выберите“Install by cloning” option.
4. Выберите второй USB диск в списке выпадающих устройств целевого устройства, а затем нажмите УстановитьTails (Картинка 3-10).

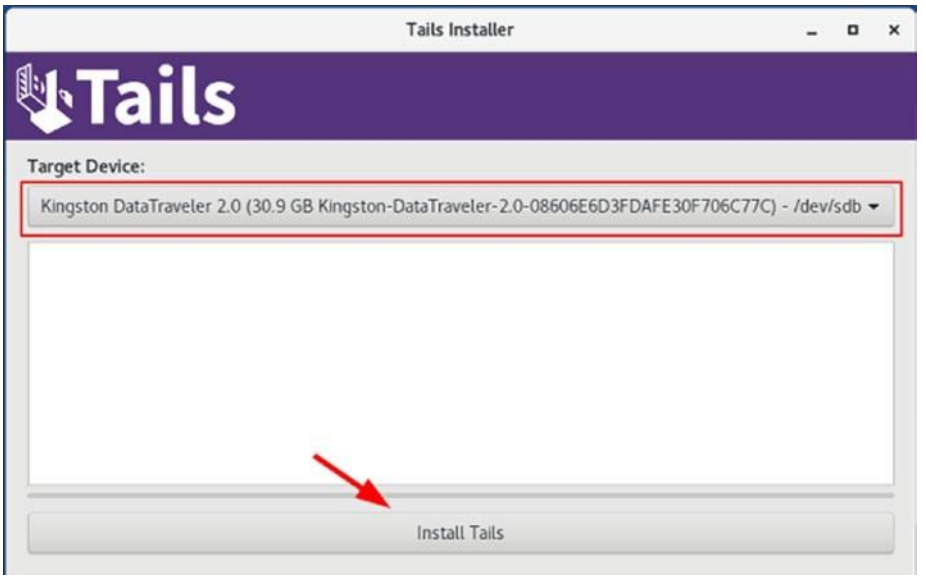

Рисунок 3-10. *Выберите целевую USB-флешку, где вы хотите установить Tails с постоянным хранением*

5. Появляется предупреждающее сообщение, информирующее вас о том, что все данные на выбранном диске будут потеряны. Подтвердите свое действие, и Tails начнет процесс установки, который может длиться около трех минут.

Теперь, чтобы получить доступ к новой Tails, перезапустите машину, оставляя вторую USB-флешку, подключенную к ней, вы должны удалить первую. Запуститиь Tails, как вы делали раньше.

Чтобы сохранить некоторые из ваших документов и конфигураций в зашифрованном хранилище на последней USB-флешке Tails, необходимо создать зашифрованное постоянное хранилище. Выполните следующие действия, чтобы создать такое хранилище. Это хранилище займет оставшееся пространство на диске USB с Tails.

1. Перейти к приложению➤ Tails ➤ Настроить хранилище. Выберите пароль для защиты зашифрованных данных в постоянном хранилище.
2. Нажмите кнопку «Создание», чтобы начать.
1. После окончания, Tail будет спросить, какие файлы вы хотите хранить в хранилище. Мы рекомендуем выбрать Личный
   Данные, сетевое подключение, GnuPG и закладки браузера.

3. Нажмите кнопку Сохранить, и Tails перезагрузится.
4. На этот раз экран Tails Greeter спросит вас, хотите ли вы использовать постоянное хранилище. Нажмите Да, а затем введите пароль.
5. Теперь можно сохранить рабочие документы в папке «Стойкий». Чтобы открыть постоянную папку, перейдите в Места➤ Постоянные.

Предупреждение! помните две точки при работе над постоянным хранением.

- постоянное хранение не скрыто; если кто-то получит физический доступ то данные смогут прочитать с Tails USB.
- Постоянная папка хранения может быть открыта в другом OS; убедитесь, что открыть его на надежном безопасном компьютере, чтобы избежать утечек в безопасности Tails .

Tails может использоваться в автономном режиме без подключения к Интернету, если вы хотите прочитать или создать конфиденциальные документы. Для началаTails в автономном режиме, запуск Tails. Когда вы достигнете стартового экрана Tails, нажмите кнопку yes. Затем нажмите кнопку «Вперед», чтобы войти в расширеный запуск. Отображается расширенное окно запуска. Перейти к нижней части окна и нажмите“Disable all networking”. Затем нажмите кнопку входа.

Предупреждение при использованииTails OS

Tails это отличная аннонимная OS которая использует Tor анонимность сети там по умолчанию, но чтобы оставаться полностью анонимным при использовании этой ОС, Вы должны быть в курсе любых угроз или атак на ОС Tails, которые могут привести к компрометации конфиденциальности при ее использовании.

- *Tails не защищает вас от аппаратных атак*: Оборудование кейлоггеров и других вредоносных программ, которые заражают прошивки компьютера и может делать перехватить ваши сообщения, даже если вы используете Tails.

- *Шифруйте все, прежде чем отправить его через Tor*: Как мы упоминали ранее, Tor Network — это анонимная сеть. Связь между узлами Tor —зашифрована. Однако, как только ваши данные покидают сеть TOR на выходных нода то перестают шифроваться . Tails также не шифрует ваши данные по умолчанию перед отправкой через сеть Tor, но Tails предлагает готовые инструменты для этой задачи, и вы должны рассмотреть возможность их использования.

- *Tails не очищает метаданные цифрового файла по умолчанию*: Как уже упоминалось в главе 2, метаданные существуют в большинстве типов цифровых файлов. Убедитесь в том, чтобы очистить метаданные цифровых файлов-изображений, офисных файлов, видео- перед отправкой их в Интернете, чтобы избежать раскрытия вашей личности.

- *Если вы используете Tails и жить в крайне враждебной среде, вы должны проявлять особую осторожность при работе в Интернете, разделяя вашу личность в Интернете во много цировых личностей*: Например,используйте отдельные цифровые личности когда вы хотите выполнить несколько действийв Интернете, таких как загрузка поста в свойблог, проверка электронной почтыи ответы на комментарии по конкретному блог или веб-сайт. Чтобы остаться анонимным в таких случаях, вы должны перезапустить Tails после выполнения каждой задачи, ранее упомянутой. Это позволит затруднить эффективного отслеживания вас глобальным противником с большими ресурсами.

В время проведения OSINT следователю настоятельно рекомендуется практиковать использование Tails OS и Tor Браузер перед проведением онлайн-исследований.

Поиск в сети Tor

Вы не найдете много полезной информации—Tor network похож на поверхностный Интернет. Эта сеть в основном направлена на незаконную деятельность, и некоторые веб-сайты не всегда могут быть доступны. Тем не менее, он все еще может содержать полезные ресурсы, которые могут помочь вам в вашем онлайн-расследовании. В этом разделе мы упомянем популярные полезные скрытые сервисы, которые помогут вам найти полезные ресурсы вTor Network. Вот некоторые поисковые системы:

- Ahmia (http://msydqstlz2kzerdg.onion/)
- Candle (http://gjobqjj7wyczbqie.onion/)

- Torch (http://xmh57jrzrnw6insl.onion/)
- Grams (http://grams7enufi7jmdl.onion/)
- not Evil (http://hss3uro2hsxfogfq.onion/)
- DuckDuckGo (https://3g2upl4pq6kufc4m.onion/)
- Searx (http://lqdnpadpys4snom2.onion) These sites are bitcoin-related:
- EasyCoin (http://easycoinsayj7p5l.onion/)
- WeBuyBitcoins (http://jzn5w5pac26sqef4.onion/)
- OnionWallet (http://ow24et3tetp6tvmk.onion/) Here are some social networks:
- Atlayo (http://atlayofke5rqhsma.onion/)
- BlackBook (http://blkbook3fxhcsn3u.onion/)
- Daniel's Chat (http://danschatjr7qbwip.onion) Here are some Tor e-mail services:
- Onion Mail (http://p6x47b547s2fkmj3.onion/)
- RetroShare chat server (http://chat7zlxojqcf3nv.onion/)
- TorBox (http://torbox3uiot6wchz.onion/)
- Mail2Tor (http://mail2tor2zyjdctd.onion/)

Другие анонимные сети

Другие сети анонимности выполняют аналогичные роли, что и сеть Tor. Второй по популярности анонимной сетью является I2P, охватываемая следующим.

I2P

I2P выступает за проект «Невидимый Интернет»; он был впервые выпущен в 2003 году. Это сеть анонимности, как Tor, но она отличается от него во многих аспектах. Прежде чем объяснить, как использовать эту сеть для доступа к даркнету, мы кратко объясним техническую сторону этой сети.

I2P является децентрализованной одноранговой (также называемой *клиент, узлом* или *маршрутизатором),* построенной с использованием языка программирования Java. I2P

позволяет размещать веб-сайты и получить доступ к темной сети I2P веб-сайтов (также известный как *deepsites*, которые имеют расширение. I2P). Он предлагает широкий спектр приложений, таких как анонимный веб-хостинг, BitTorrent, электронная почта, обмен файлами, и многое другое. В сети I2P связь между отправителем и пунктом назначения — внутри сети I2P — полностью зашифрована. Трафик обычно проходит через четыре уровня шифрования до достижения пункта назначения.

Использывание I2P

Теперь мы начнем объяснять, как получить доступ к сети I2P.

Примечание! Чтобы запустить I2p на вашем компьютере, вы должны иметь Java уже установлен на вашей машине, потому что I2p написанс с помощью языка программирования Java. Вы можете скачать Java изhttps://www.java.com/en/download/index.jsp.

---

1. Перейти к https://geti2p.net и скачать версию программного обеспечения, которая соответствует текущей ОС.
2. После установки программного обеспечения (маршрутизатор I2P) нажмите“Start I2P (restartable)” значок, который будет настраивать консоли маршрутизатора с помощью браузера по умолчанию, который имеет дополнительные инструкции для настройки этой сети. Если консоль маршрутизатора не всплывает автоматически, перейдите наhttp://127.0.0.1:7657/home для просмотра.
3. Это может занять несколько минут, прежде чем I2P успешно подключается к сети; сообщение с пометкой "Сеть OK"(Рисунок 3-11) должны отображаться на консоли маршрутизатора. Если вместо него появляется другое сообщение об ошибке (например, “Network: Firewalled”), необходимо проверить настройки брандмауэра, чтобы разрешить подключение к портам I2P. Мы не можем описать причины /предлагаемые решения для всех возможных проблем. Вы всегда можете скопировать сообщение об ошибке и Google его, чтобы найти соответствующее решение. Запуск I2P внутри виртуальной машины без установки брандмауэра является еще одним вариантом для нетехнически подкованных пользователей.

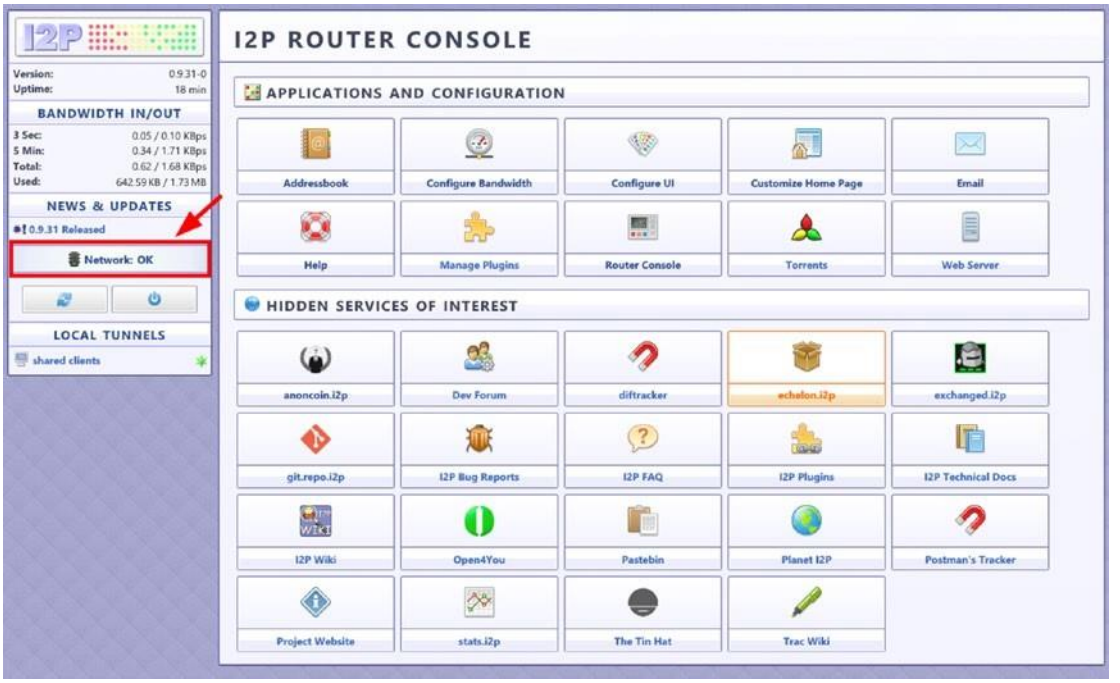

Рисунок 3-11. *I2P вид консоли маршрутизатора-"Сеть ОК"*

4. Теперь вам нужно настроить свой веб-браузер, чтобы использовать сеть I2P. Мы опишите, как это сделать для Firefox; другие браузеры используют аналогичные конфигурации.

5. Открытые варианты Firefox - Общий прокси-сервер (находится в нижней части страницы) и нажмите кнопку "Настройки".

1. В окне настроек подключения щелкните по кругу рядом с "Ручная конфигурация прокси." Затем введите **127.0.0.1** в HTTP

Поле прокси и **4444** в поле порта. Введите **127.0.0.1** в SSL

Поле прокси и **4445** в поле порта. Обязательно введите **localhost, 127.0.0.1** в поле "Нет прокси для". Наконец, нажмите кнопку ОК, чтобы принять новые настройки(Рисунок 3-12).

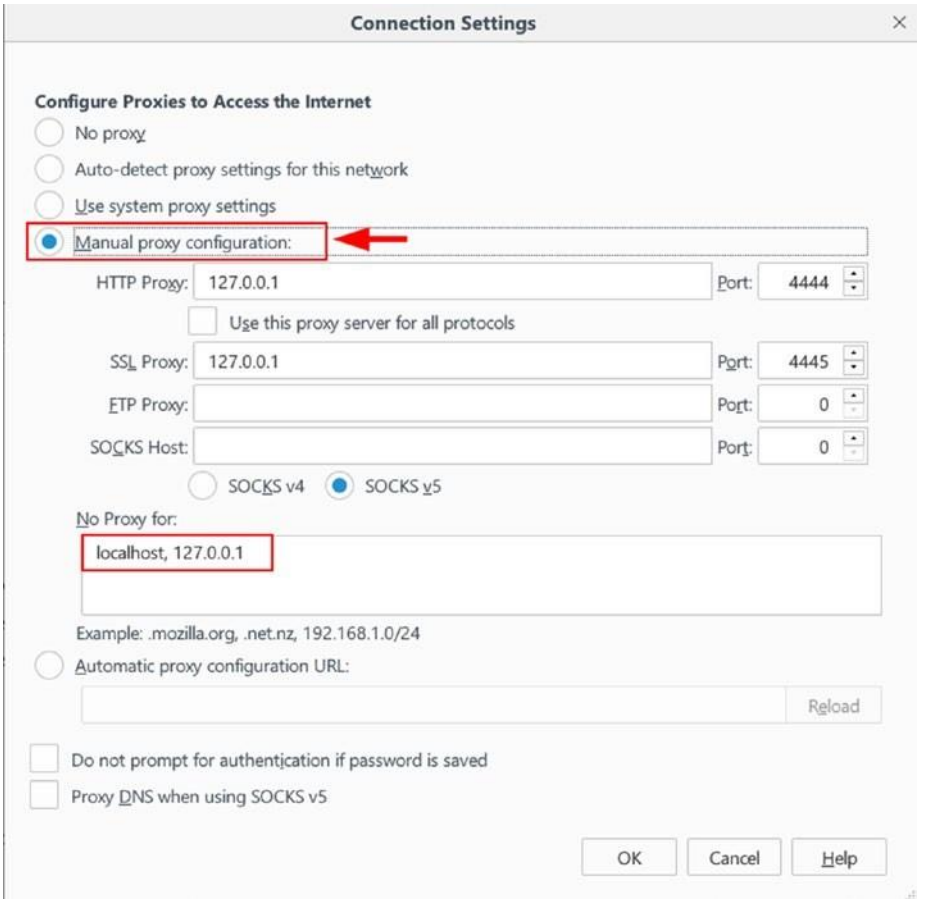

Рисунок 3-12. *Налажить Firefox, чтобы использовать сеть анонимности I2P*

Предупреждение! В отличие от Tor, I2p не предоставляет механизм, чтобы скрыть ваше вхождение в сеть I2p от вашего ISp и правительства. однако, как только соединение будет установлено, все станет полностью зашифрованным и анонимным.

I2p не проходит через Tor.

Предыдущая конфигурация Firefox позволяет использовать обычный Интернет анонимно. Таким же образом, вы можете получить доступ к любому веб-сайту, размещенном в анонимной сети I2P (такие веб-сайты имеют расширение .i2p вместо .com или .org).

После успешного подключения к сети I2P и настройки браузера должным образом использовать его, вы можете начать открывать эту сеть. Если вы застряли и не знаете, с чего начать, направьте браузер на вики I2P наhttp://i2pwiki.i2p.

При первом посещении веб-сайта I2P вы можете получить сообщение об ошибке с указанием "Сайт не найден в адресной книге", потому что у вас нет адресов веб-сайта I2P в адресной книге маршрутизатора. Чтобы решить эту проблему, вам нужно нажать на одну из ссылок службы прыжка в конце страницы (см. рисунок3-13).

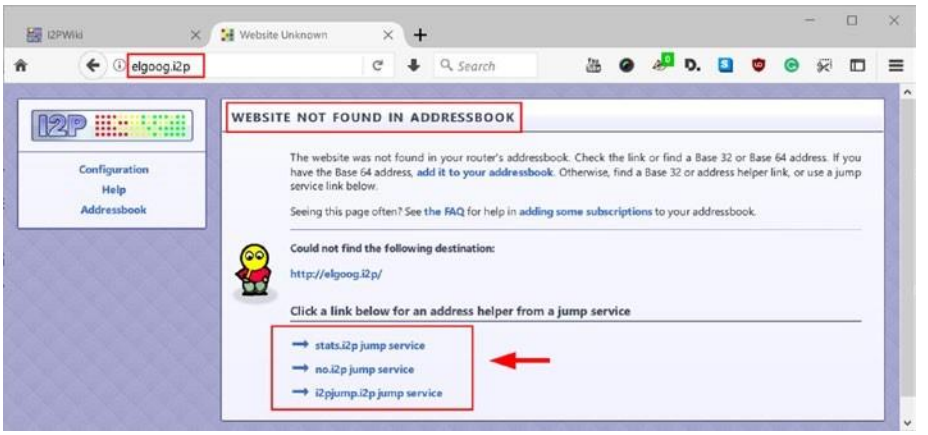

Рисунок 3-13. *Доступ к веб-сайту I2P впервые — посещенный веб-сайт не был найден в адресной книге маршрутизатора*

Попробуйте нажать каждую ссылку службы до тех пор, пока вы найдете тот, который доставит вас на страницу, которая позволяет добавить этот сайт в адресную книгу маршрутизатора I2P (см. Рисунок 3-14).

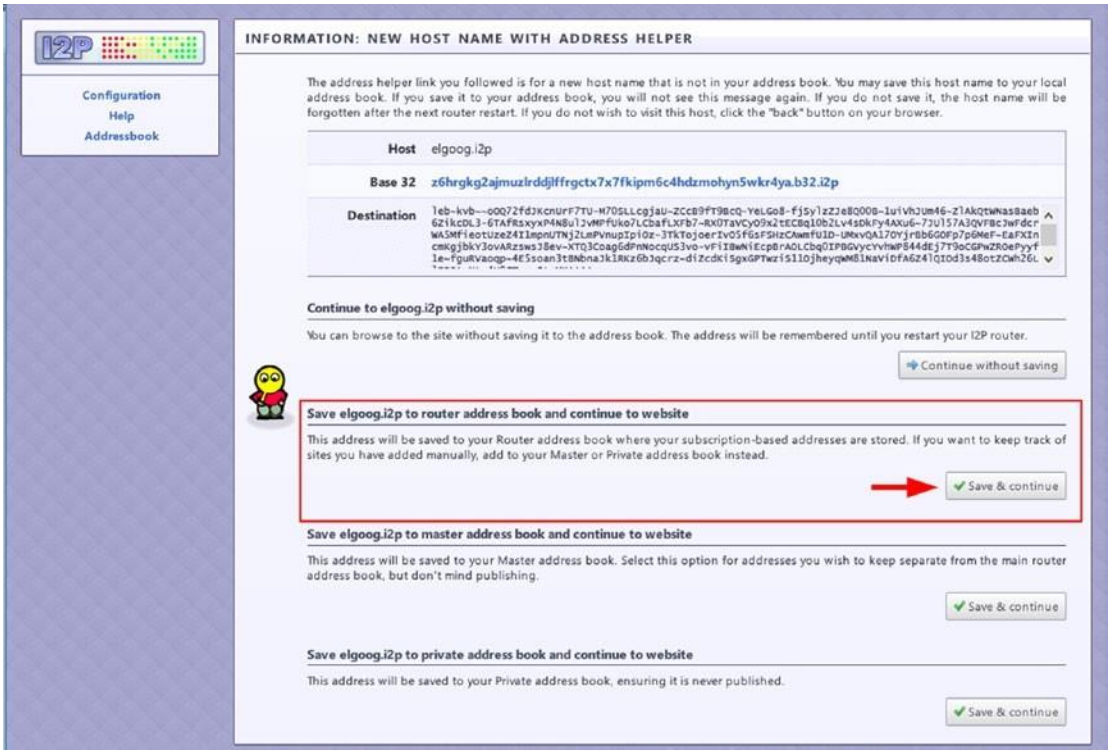

Рисунок 3-14. *Добавление нового веб-сайта I2P, который ранее не посещался, в адресную книгу маршрутизаторов. В следующий раз, когда вы посетите этот сайт, вы не увидите это сообщение.*

После нажатия кнопки "Сохранить и продолжить" в разделе "Сохранить "Имя веб-сайта" на маршрутизатор адресной книги и продолжить на веб-сайте ", страница, показанная на рисунке 3-15 перенаправит вас на предполагаемый веб-сайт (ELGOOG. I2P в этом примере).

Рисунок 3-15. *Перенаправление автоматически на запрашиваемый веб-сайт после добавления имени хоста веб-сайта в адресную книгу маршрутизатора*

I2P VS. TOP

Основное различие между Tor и I2P заключается в том, как их дизайнеры восприняли модель угроз. Например, Tor был создан в первую очередь, чтобы позволить пользователям

путешествовать по поверхности веб анонимно. I2P был создан как автономная сеть анонимности, которая позволяет полностью анонимное общение между двумя сторонами в рамках своей сети.

Tor использует метод переключения цепи для управления данными через сеть Tor, в то время как I2P использует модель переключения пакетов. Переключение цепи изначально было изобретено для голосовой связи, и оно было менее подходящим для передачи данных. Tor использует единый путь для передачи данных, в то время как I2P использует коммутацию пакетов, что заставляет всех узлов участвовать в переадресовке пакетов по сети. В отличие от Tor, I2P использует два маршрута (туннель) для направления входящего и исходящего трафика. Это позволит эффективно улучшить общую анонимность системы и сделает доставку данных более гибкой, так как каждый пакет будет принимать различные маршруты, чтобы добраться до пункта назначения, в отличие от пакетов Tor, которые должны путешествовать с помощью одного пути в обоих направлениях (срок службы каждой трассы Tor составляет десять минут). I2P быстрее при перемещении больших файлов в сети, чем сеть Tor, которая страдает от перегрузки сети и перебоев в обслуживании, так как она использует только один маршрут для доставки данных.

Tor использует структуру каталога для просмотра общей производительности всей сети, а также для сбора и представления статистики. Каталоги Tor ведут список всех узлов Tor и размещают скрытые услуги в сети Tor и размещаются в США и Европе. Подход I2P заключается в использовании децентрализованной одноранговой сети, где нет единой точки для просмотра всей сети, и каждый одноранговый (маршрутизатор) локально поддерживает список всех известных маршрутизаторов (реле).

I2P использует чесночное шифрование—который является вариантом шифрования луковица— где несколько сообщений для разных получателей в комплекте вместе. Это затрудняет для внешних противников анализ потока трафика через сеть, а также ускорить передачу данных и сделать его более надежным.

Tor имеет больше выходрелов по сравнению с I2P. I2P использует термин *outproxy,* чтобы назвать свой собственный маршрутизаторы ретранслятора выхода. Количество пользователей I2P меньше, чем у Tor. Это делает число I2P outproxies значительно меньше, чем Tor выхода реле. Это позволит сделать I2P более восприимчивым к внешнему анализу трафика по сравнению с Tor Network, которая владеет большим количеством выходных ретрансляторов.

Tor действует как прокси-сервер с помощью SOCKS, поэтому любое приложение (например, веб-браузер, чат для чата или клиент электронной почты), способное использовать SOCKS, может быть настроено на использование программного обеспечения Tor напрямую. I2P использует свой собственный API, который должен быть реализован любыми приложениями, желающими общаться через сеть I2P. Это делает I2P более безопасным и анонимным, чем Tor, так как его API разработан специально для анонимности. Тем не менее, приложения должны

быть скорректированы, чтобы использовать его, и это как-то дорого и ограничивает количество приложений, которые готовы использовать сеть I2P.

Наконец, Tor хорошо финансируется. Он имеет большую базу пользователей и больше сторонников из академических и хакерских сообществ по сравнению с i2P сети. Это ясно видно из его веб-сайта, документации и других проектов, осуществляемых в настоящее время. Tor также имеет преимущество в написании на языке C, что делает его быстрее при работе на клиентских машинах, чем I2P, который написан с помощью Java и потребляет больше памяти оперативной памяти.

В заключение, как I2P и Tor являются отличными анонимными сетями, но контекст, в котором они используются определяет, какой из них является лучшим с точки зрения производительности и анонимности. Например, I2P предпочтительнее Tor для размещения анонимных сайтов и для создания сообщений в I2P darknet, поскольку это быстрее и дает более сильную анонимность. Tor предпочитает анонимизировать трафик при доступе к поверхности Интернета, в отличие от I2P, который практически непригоден для этой задачи.

Freenet

Freenet является еще одной анонимной сети. Это полностью распределенная, одноранговая анонимная издательская сеть. Мы не будем охватывать, как использовать эту сеть, как мы это делали с предыдущими. Тем не менее, вы можете проверить http://freesocial.draketo.de для полного учебника о том, как использовать эту анонимную сеть. Tor, I2P и Freenet являются самыми популярными анонимными сетями, доступными в настоящее время. Tor превосходит два других в том, более широко используется и более зрелым. Мы рекомендуем использовать сеть Tor для всей вашей работы в Интернете, которая требует анонимности.

Двигаемся дальше

Как вы видели в этой главе, поиск глубоких и темных ресурсов не является простым. Современные поисковые системы оптимизированы для поиска в веб-сети поверхности и не могут искать и индексировать содержимое под ним, даже несмотря на то, что некоторые коммерческие компании, которые разработали некоторые передовые поисковые инструменты, пытаются собрать данные из глубокой паутины (включая темную паутину). Эффективность таких инструментов по-прежнему ограничена с точки зрения получения точных, связанных и полных результатов.

Теперь, с продвижением вычислительных технологий и широким использованием интернет-услуг по всему миру, все больше преступников перекладывают свою деятельность в Интернете. Киберпреступники, террористические организации и страны, контролируемые репрессивными режимами, также используют Интернет, особенно «даркнет», для осуществления незаконной деятельности. Правительства и правоохранительные органы во всем мире должны использовать все возможные ресурсы для захвата и предотвращения использования асоциальными субъектами Интернет-технологий для содействия совершению своих преступлений. Чтобы помочь преодолеть эти проблемы, Агентство перспективных оборонных исследовательских проектов (DARPA) в Соединенных Штатах создало программу Memex, чтобы помочь в борьбе с торговлей людьми деятельности по всему миру. Memex — это поисковая система нового поколения, которая фокусируется на оказании помощи следователям правоохранительных органов в поиске онлайн-преступников, занимающихся торговлей людьми в киберпространстве. Memex имеет возможность поиска в даркнет и глубоком интернете в дополнение к поверхностному Интернету, чтобы найти связанную информацию, распространенную повсюду в Интернете для поддержки иследователей в их миссии.

Хотя ключевой миссией Memex является борьба с глобальной торговлей людьми, она может быть использована разведывательными службами и другими военными организациями для сбора и сопоставления полезной информации OSINT из глубокой/темной паутины о том, что они хотят.

Итоги

Глубокая сеть и darknet привлекают все большее внимание исследователей, правоохранительных органов и государственных органов. Тем не менее, оба термина до сих пор неясны для большинства пользователей Интернета. Кроме того, природа и техническая архитектура сетей даркнета по-прежнему не имеют ясности для многих людей.

В этой главе мы прольем свет на концепцию слоев Интернета и продемонстрировали на примере содержимое каждого слоя и то, как к ним можно получить доступ для получения информации из них.

Были представлены и сравнена две сети даркнетов. В то время как Tor является зрелой анонимной сетью с широкой базой пользователей и в основном используется для анонимного просмотра веб-страниц из-за его многочисленных узлов выхода, I2P начинает получать больше внимания в качестве предпочтительного решения для размещения скрытых веб-сайтов внутри сети I2P darknet из-за его скорости и более сильной анонимности как для пользователей, так и для операторов веб-сайтов.

Как мы уже говорили, многие сайты даркнетпосвящены в незаконную деятельность; это не цель этой главы, чтобы познакомить вас с такими незаконными услугами и научить вас, как получить к ним доступ. Мы настоятельно рекомендуем типичному пользователю Интернета вообще не посещать даркнет. Главное здесь заключается в том, чтобы познакомить вас, особенно следователей OSINT, как использовать онлайн-инструменты анонимности, такие как Tor Browser и Tails OS для проведения онлайн-расследований безопасно и анонимно. Информация, представленная в этой главе, также принесет пользу онлайн-следователям при доступе к темным областям Интернета и поиске.

Эта глава была посвящена самым глубоким слоям Интернета. В следующей главе мы вернемся на поверхность, чтобы научить вас, как использовать передовые методы с использованием типичных поисковых систем, таких как Google и Bing для поиска ресурсов OSINT онлайн.

Примечания

i. Internet World Stats, “World Internet Users and 2017 Population Stats,” November 5, 2017, www.internetworldstats.com/stats.htm.

ii. Netcraft, “October 2017 Web Server Survey,” November 1, 2017, https://news.netcraft.com/archives/category/web-serversurvey/.

iii. Aclweb, “Classifying Illegal Activities on Tor Network Based on Web Textual Contents,” November 2, 2017, https://www.aclweb. org/anthology/E/E17/E17-1004.pdf.

iv. Techworm, “Tor and VPN users labeled as criminals will be hacked and spied by FBI under new law,” November 5, 2017, https://www.techworm.net/2016/05/tor-vpn-users-labeled criminals-hacked-spied-fbi-new-law.html.

Глава 4

Методы поиска

Число пользователей Интернета неуклонно растет, как и количество активных веб-сайтов. По данным опроса Netcraft за январь 2017 года, веб-серверов Netcraft насчитывается 1 800 047 111 миллиардов веб-сайтов.[i] Количество страниц на этих сайтах постоянно меняется в зависимости от многих факторов. По оценкам Google Inside Search, по состоянию на октябрь 2017 года google обнаружил более 130 триллионов веб-страниц; около 50 миллиардов из них были включены в поисковый индекс Google.[ii] Не забывайте, что Google-и аналогичные поисковые системы-неможет индексировать весь веб, как страницы, которые принадлежат к глубокой/темной сети не могут быть обнаружены типичными поисковыми системами.

Как вы можете видеть, количество веб-страниц, которые существуют огромен, и найти свой путь в этом средствах массовой информации будет очень трудно без поисковых систем. Поисковая система работает, отправляя *сканер*- автоматизированное программное обеспечение, чтобы постоянно сканировать активные веб-сайты, чтобы добавить обнаруженный контент в свой индекс, который хранится в массивных базах данных. Затем пользователь запрашивает индекс поисковой системы, который возвращает результаты, которые могут содержать сочетание веб-страниц, изображений, видео и других типов файлов, как список соответствующих сайтов, ранжированных по актуальности.

Без поисковой системы, пользователь должен будет получить доступ и проверить каждый веб-сайт вручную при поиске конкретной информации. Это было бы сложной задачей и потреблять значительное количество времени для каждого поиска. Поисковые системы также помогают пользователям просматривать только релевантные результаты. Например, программное обеспечение поисковой системы сканирует каждую индексируемую страницу и выбирает список ключевых слов из нее, чтобы классифицировать ее. Когда пользователь, например, ищет *cheap flight to Hawaii*, все страницы, предлагающие перелеты на Гавайи, будут отображаться в списке результатов поиска.

Тем не менее, высший ранг будет для страниц / веб-сайтов, строго связанных с критериями поиска пользователя. Пожалуйста, обратите внимание, что алгоритм ранжирования веб-

сайтов в результатах поиска является секретным для каждого поставщика поисковых систем, и ранг для каждого веб-сайта, даже для одного и того же запроса, может изменяться ежечасно. Тем не менее, наивысший ранг будет для веб-сайтов, которые удовлетворяют критериям алгоритма ранжирования с точки зрения популярности и релевантности поискового запроса пользователя.

N. A. Hassan and R. Hijazi, *Open Source Intelligence Methods and Tools*, https://doi.org/10.1007/978-1-4842-3213-2_4

Типичные поисковые системы, такие как Bing и Google, предлагают свои услуги бесплатно. Они также предлагают расширенные функции поиска, которые могут быть использованы пользователями для проведения расширенного поиска. Например, Google предлагает мощный Расширенный поиск(https://www.google.com/advanced_search),который дает более конкретные результаты поиска (см. рисунок 4-1).

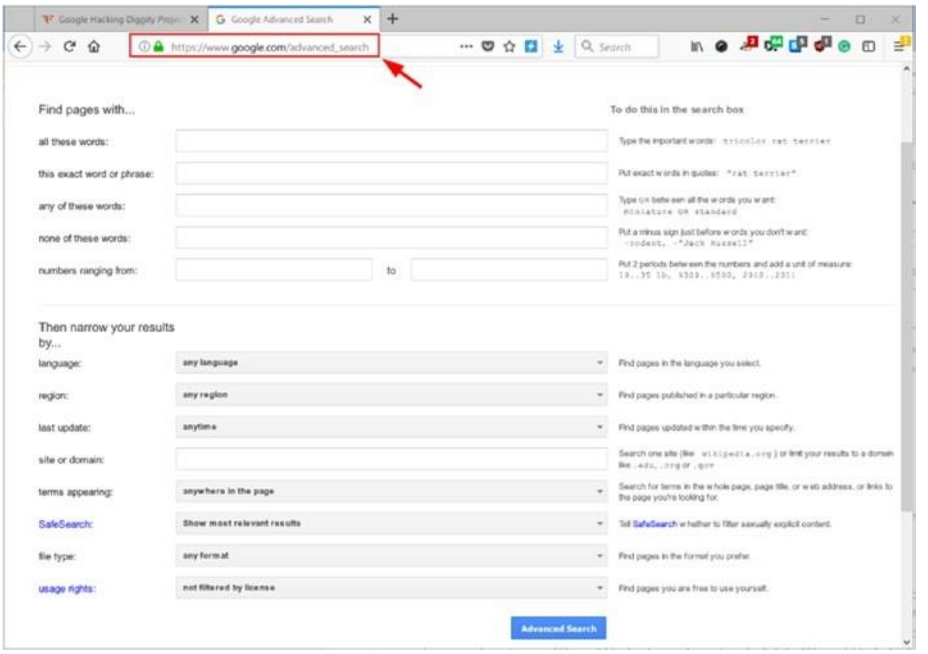

Рисунок 4-1. *Функциональность Google Расширенный поиск возвращает более конкретные результаты поиска*

Внутренний механизм поисковых систем не так прост, как их интерфейс. Чем сложнее поисковая система, тем сложнее алгоритм, который она использует для поиска и индексирования содержимого из Интернета. В этой главе мы рассмотрим, как использовать

различные типы поисковых систем эффективно, чтобы найти информацию в Интернете.Мы начнем с фокусировки на Google, потому что он считается крупнейшим и имеет много специализированных операторов для проведения расширенных поисков (также известный как Google *dorks*). Мы также рассмотрим, как искать конкретные типы цифровых файлов, таких как изображения и видео в дополнение к использованию многих бесплатных онлайн-сервисов для проверки ваших выводов. Прежде чем мы начнем, давайте рассмотрим, как выбрать ключевые слова поиска, чтобы вернуть наиболее релевантные результаты из поисковых систем.

Ключевые слова для обнаружения и исследования

Как иследователь OSINT, вы должны овладеть искусством онлайн-поиска, который требует от вас использовать правильные ключевые слова поиска. Типичные поисковые системы обнаруживают и индексируют веб-страницы, используя различные критерии. По-видимому, наиболее важным из них является набор ключевых слов, доступных в рамках целевой страницы.

Открытие ключевых слов поможет поисковикам расширить широту поиска, включив в них различные вариации одного и того же ключевого слова и раскрыть синонимы и семантически связанные термины и фразы, чтобы они могли лучше найти контент, который может быть редко доступен типичным пользователям проведение аналогичных поисков.

Ключевые слова открытие широко используется интернет-маркетингу в поисковой оптимизации (SEO), чтобы увидеть, какие ключевые слова используются разными людьми, используя различные поисковые системы для поиска аналогичной темы. Онлайн следователи могут использовать тот же метод для поиска вариаций фразы / ключевого слова в дополнение к приобретению интеллекта о текущих тенденциях поиска.

Ниже приведены самые популярные инструменты исследования ключевых слов:

- Google Keyword Suggest Tool (http://tools.seochat.com/tools/ suggest-tool): Это дает ключевые слова предложения для Google, Bing, Amazon и YouTube.
- Google AdWords (https://adwords.google.com/home/tools/ keyword-planner/) и Google Trends (https://www.google.com/ trends): Они покажут объем поиска и матрицы поиска Google для любого географического региона во всем мире.
- One Look (www.onelook.com/reverse-dictionary.shtml): Введите слово, фразу, предложение или шаблон для поиска связанных слов.

Использование поисковых систем для поиска информации

В этом разделе мы покажем, как использовать поисковые системы, чтобы получить точные результаты, начиная с гиганта, Google.

Google

Поисковая система Google является лидером среди своих коллег и имеет наибольшую долю рынка с более чем 77 процентов глобального поискового трафика с его помощью.

Количество ежедневных поисков, проводимых веб-пользователей по всему миру на поисковых системах огромен. Таблица 4-1 показывает количество ежедневных поисков в поисковой системе.[iii]

Таблица 4-1.*Количество ежедневных поисков в основных поисковых системах*

Поисковые системы	**Поиски в день**
Google	4,464,000,000
Bing	873,964,000
Baidu	583,520,803
Yahoo	536,101,505
Other (aOL, ask, etc.)	128,427,264

Большинство веб-пользователей использовали веб-поиск Google, чтобы найти что-то в Интернете. Основной поиск Google — это то, что вы видите при посещении домашней страницы Google (www.google.com). Вы вводите запрос поиска в поле поиска Google и нажмете кнопку поиска Google. Кроме того, вы можете использовать свой голос для входа в поисковый запрос, нажав значок микрофона. Домашняя страница Google предлагает другие полезные услуги, такие как поиск изображений, видео, групп новостей и карт в дополнение к службе Google Translate. Давайте посмотрим, как вы можете использовать некоторые слова Google для уточнения основного поиска для лучших результатов.

Предупреждение! При использовании следующих слов поиска Google(symbols), убедитесь, что не оставляете пробелы между символом и термином поиска (query).

1. Для поиска в социальных сетях используйте символ @ затем имя в социальных сетях; затем введите двоеточие (:) в ваш поисковый запрос. Например, введите **@facebook:nihad hassan** для поиска имени *Нихад Хассан* в Facebook).
2. Для поиска хэштегов поместите # хештег перед запросом. Например, введите **#USAelection**.
3. Поиск точного совпадения, возмите ваш поиск термин / фразу в кавычки. Например, введите**"data hiding"**.
4. Тильда (~) оператор поиска которое стоит после него и для его синонимов . Например, ввод **Excel ~guide** вернет Excel учебники, советы, помощник, видео тренинги, и все, слова являющиеся синонимом *слова guide*.
5. Оператор OR пишеться только большими буквами—так же вместо оператора используеться пайп (|)— используется для поиска страниц, содержащих поисковые термины. Например, ввод **Apress OR springer** (или ввод**Apress|Springer**) будет получать страницы, которые содержат либо термин *Apress* или термин *Springer*.
6. Чтобы исключить слова из поиска, поставте минус (-) символ перед словом (Фразой) что бы это слово или фраза не обрабатывалось. Например, введите **lacoste -animal**.
7. Для поиска неизвестных слов используйте звездочку, чтобы заменить ее одним или несколько словами. Например, введите **data hiding in ***.
8. Используйте двойные точки (..) без пробелов для предоставления диапазона номеров, таких как дата, число или ценовой диапазон. Например, введите **USA earthquake 1980..2000**.
9. Для поиска подобных веб-страниц, поместите *слово, связанное:* в передней части веб-адреса, что вы хотите увидеть аналогичные страницы. Например, введите **related:springer.com**.

10. Используйте слово *info:* чтобы вернуть информацию, которая есть у Google о определенном домене.Например, введите**info:springer.com**.

1. Используйте слово *define,* чтобы найти определение поставляемого ключевого слова.Например, введите**define:information**.

11. Используйте слово *кэш:* чтобы вернуть Кэш-версию веб-страницы, кэшированной Google.Например, введите**cache:apress.com**.

12. Для поиска информации о конкретной песне или фильме введите **Music:** или **Movie:** затем песня или название фильма.

13. Чтобы проверить текущую погоду в любом месте по всему миру, используйте ключевое слово*погоды.*Например, введите **weather:London**.

14. Чтобы показать цену акций любой компании, используйте *акции* по ключевым словам*:*

    затем символ компании тикер. Например, ввод **stocks:MSFT** будет показывать информацию о запасах для корпорации Майкрософт. Вы можете посмотреть тикет компании, перейдя по сслыке https://www.marketwatch.com/tools/quotes/lookup.asp.

15. Используйте ключевое слово *map:* затем имя местоположения и Google покажет вам карту на основе результатов. Например, введите **map:New York**.

16. Введите **time keyword** чтобы проверить текущую дату/время вашего текущего местоположения. Чтобы найти время другого местоположения, предшествуем ключевому слову *времени* с именем местоположения (например, введите**time New York**).

Примечание! http://localtimes.info показывает интерактивную карту времени по всему миру прямо сейчас. www.thetimenow.com показывает дату, время и календарь в дополнение к прогнозам погоды и более подробную информацию о текущем местоположении. (Текущее местоположение обнаруживается с помощью IP-адреса подключения, поэтому не забудьте обновить свое местоположение, если вы используете сервис Vpn, который маскирует ваш реальный IP-адрес.)

---

17. Google также может быть использован в качестве конвертера между валютами и мерами. Например, введите **(190 cm in feet)** или **(1000 dollars in yen)**.

1. Вы даже можете проверить информацию о рейсе с помощью Google. Введите название авиакомпании и номер рейса в поле поиска Google, и он покажет вам информацию о статусе рейса графически (см. рисунок 4-2).

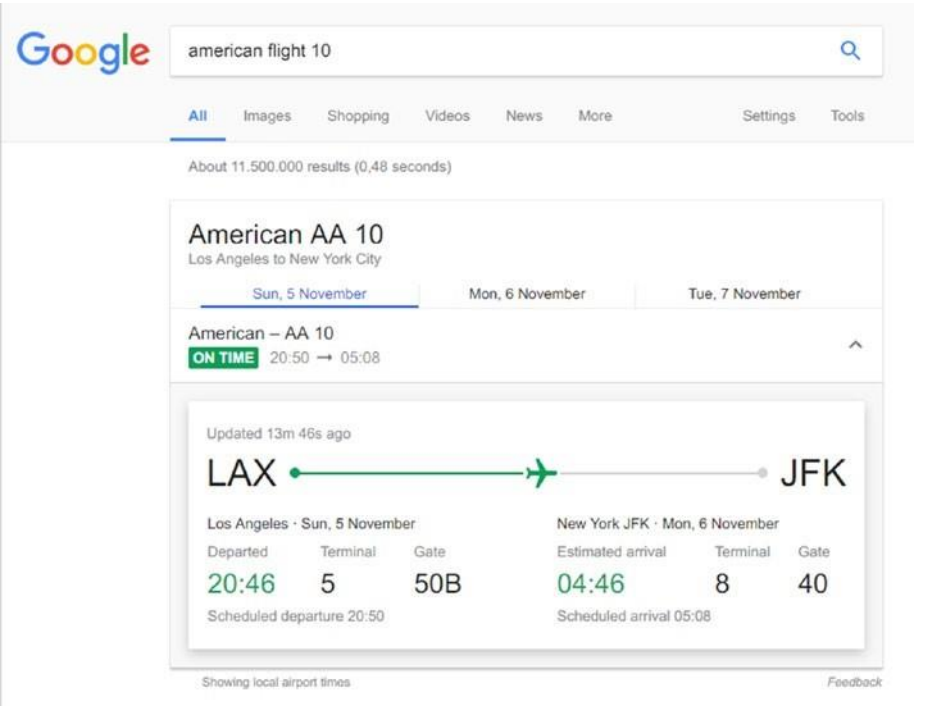

Рисунок 4-2. *Отображение информации для американской авиакомпании, рейс 10*

Google также известен своим поиском изображений. Например, для поиска определенного изображения можно использовать поиск изображений Google Advanced https://www.google.com/ advanced_image_search, что позволяет установить различные критерии поиска изображений (например, размер, цвет, тип и т.д.), чтобы найти целевое изображение.

Базовый поиск подходит для начинающих, и вам не нужно беспокоиться о написании или капитализации ваших поисковых ключевых слов, потому что Google исправит это для вас. Однако, когда дело доходит до получения соответствующей информации, связанной с конкретной темой, необходимо использовать специальных операторов Google для возврата информации, которую трудно найти с помощью простых поисковых запросов.

GOOGLE РАСШИРЕННЫЕ ОПЕРАТОРЫ

Расширенные варианты также известны как *Google hack*ing или *Google dorks*. Google hacking происходит, когда пользователь объединяет ключевые слова поиска с продвинутыми операторами поиска Google, чтобы найти скрытую информацию, которую трудно найти с помощью базового поиска Google. Например, взлом Google может быть использован для поиска уязвимых веб-серверов или списков лично идентифицирующих информацию (PII)

файлов для сотрудников/клиентов в конкретной компании, которые могли быть оставлены на сервере компании без защиты. Киберпреступники, и даже террористы используют этот метод для сбора конфиденциальных данных в Интернете для облегчения дальнейших атак против цели.

В следующем списке мы показываем примеры продвинутых поисковых операторов Google, начиная с простейших. Общий формат заключается в следующем: **operator:search_term**. (оператор , колон (:), и поиск ключевых слов пишуться слитно).

- Оператор *site* оператор просит Google искать в пределах одного веб-сайта или домена. Например, если вы введете**hide site:darknessgate.com**, Google будет искать слово *hide* только в приделах сайта *darknessgate.com*. Используя одного и того жеоператора, можно ограничить поиск в одном домене. Например, введите **computer forensics site:gov** для поиска термина *computer forensics* на всех веб-сайтах с доменом .gov.

- Вставьте термин поиска запроса после *allintext* оператор и Google ограничат свой поиск всеми страницами, содержащими указанные термины. Например, введите **allintext:free SMicrosoft service** и Google будет возвращать только страницы, которые имеют три термина *free* , *SMS* и *service* в своем тексте.

- Начав поиск с оператора *allintitle* и задав ему с условиями поиска. Google будет возвращать только страницы, содержащие ваш поисковый запрос в своих заголовках. Например, введите**allintitle:Nihad hassan** чтобы Google вернуть все страницы, которые *Нихад Хассан* в их названии (название страницы появляется в верхней части окна браузера), как показано на рисунке 4-3.

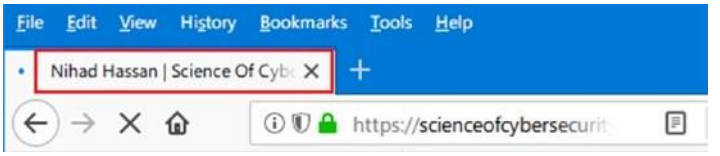

Рисунок 4-3. *Поиск в заголовках страниц для определенного термина*

- Если вы используете оператора *allintitle* в поиске изображений, он будет возвращать изображения в файлах, имена которых содержат указанный поисковый запрос.

- Начните поиск с оператора *allinurl,* за которым следует ваш поисковый термин, и Google ограничит его результаты всеми страницами, которые содержат ваши поисковые термины в их URL-. Например, введите**allinurl:OSINT intelligence** и

Google будет возвращать страницы с терминами *OSINT разведки* в своих URL-адресов (см. Рисунок 4-4). Вы не сможете включить других поисковых операторов с оператором *allinurl*.

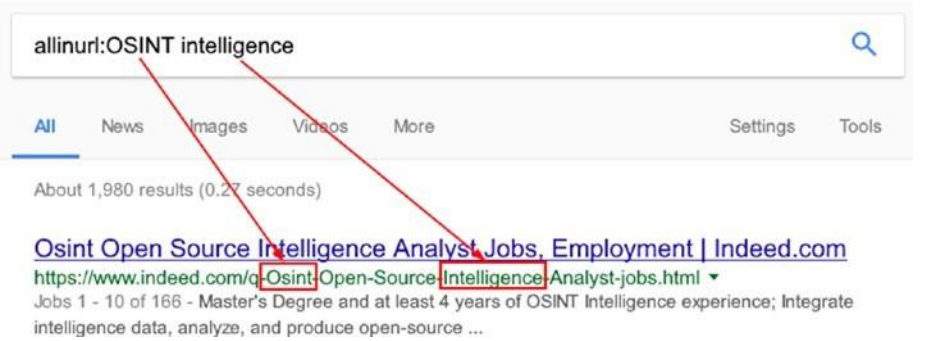

Рисунок 4-4. *Использование оператора Google allintitle*

- При использовании *filetype* суффикса с вашими условиями поиска, Google будет ограничивать результаты веб-страниц, которые заканчиваются с этим расширением. Например, введите **osint intelligence filetype:PDF** и Google вернет PDF-файлы, которые соответствуют указанному поисковому запросу.
- Для поиска более одного типа файла добавьте их расширения в поисковый запрос следующим образом: **osint intelligence filetype:pdf OR filetype:doc**. Google поддерживает поиск различных типов файлов; список индексируемых форматов файлов доступен по адресу (https://www.google.com/support/enterprise/static/gsa/docs/admin/74/gsa_doc_set/file_formats/file_formats.html).

Все эти примеры являются простыми демонстрациями того, как можно использовать продвинутых поисковых операторов Google для возврата точных соответствующих результатов. Онлайн иследователи должны быть творческими и работать, чтобы развивать свои навыки поиска, используя различные поисковые операторы в одном запросе, чтобы вернуть лучшие результаты.

Примечание! Google расширенный поиск(https://www.google.com/advanced_ search) позволяет пользователям использовать передовые поисковые операторы, не вводя их вручную в поле поиска, хотя он по-прежнему имеет ограничения на проведение более творческих поисков. однако, он по-прежнему считается отличным инструментом для случайных пользователей для поиска Google профессионально.

GOOGLE HACKING DATABASE

Google Hacking Database (см. Рисунок 4-5), созданный Джонни Лонг содержит сотни готовых к использованию расширенных поисковых терминов Google, которые могут быть использованы для разведки в Интернете. Это может помочь вам найти следующее и более:

- Уязвимые веб-серверы
- Файлы, содержащие конфиденциальную информацию, такую как имена пользователей/пароли в дополнение к файлам конфигурации, которые содержат настройки и другую важную информацию с интернет-устройств
- Чувствительные каталоги, оставшиеся без защиты
- Сообщения об ошибках, генерируемые серверами, базами данных и другим программным обеспечением, которое может быть использовано для вторжения в информационные системы
- Информация о сетевых устройствах, таких как брандмауэры, журналы IDS и конфигурации
- Различные устройства IoT и панели управления незащищенных устройств
- Скрытые страницы, такие как интрасети, VPN-сервисы и другие

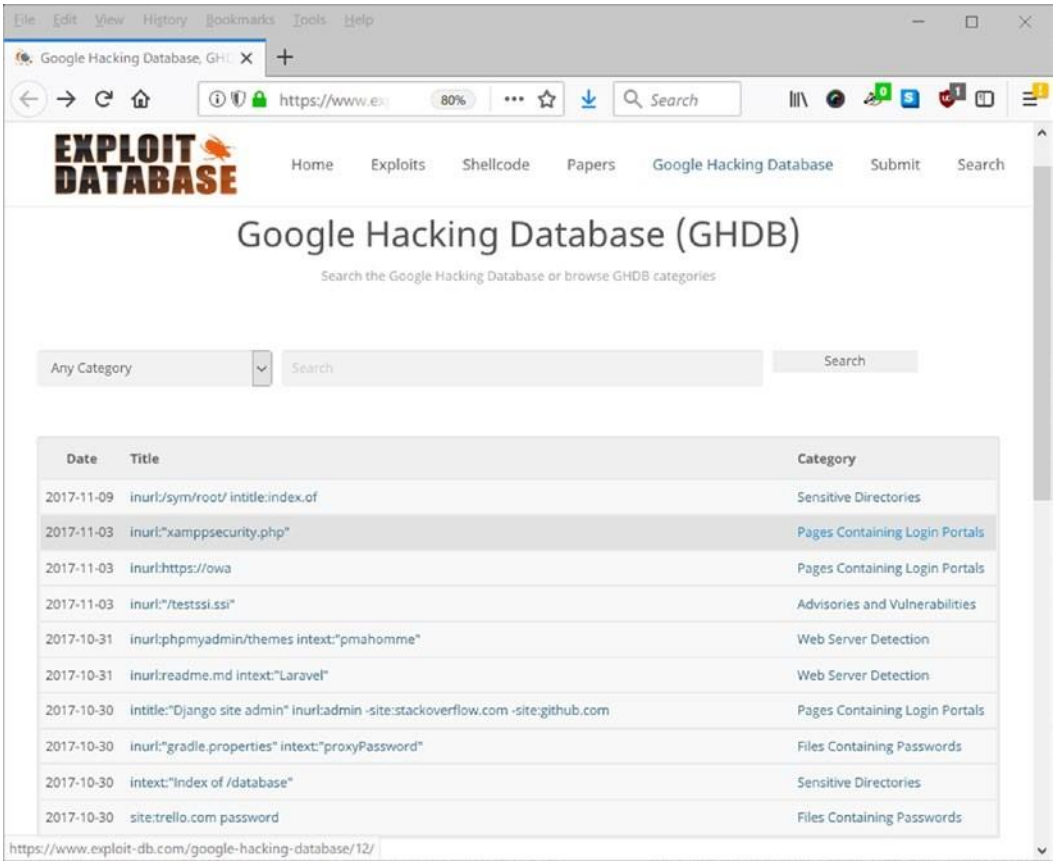

Рисунок 4-5. *Google Hacking Database (www.exploit-db.com/google-dorks)*

Вот несколько примеров поиска терминов, которые можно использовать на Google, чтобы найти конфиденциальную информацию в Интернете:

- *"Index of /backup"*: Это вернет список незащищенных серверов, содержащих данные резервного копирования. Такие файлы могут содержать конфиденциальную информацию.
- *"robots.txt" "Disallow:" filetype:txt*: Файл robots.txt обычно находится в корневом каталоге веб-сервера и инструктирует сканеры поисковых систем на участках вашего веб-сайта, на которые вы не хотите смотреть (другими словами, что вы хотите игнорировать процесс индексации). Хакеры проверяют файлы robots.txt, чтобы увидеть неиндексированные файлы, чтобы получить интеллект или получить доступ к конфиденциальным местам.

- *budget site:gov filetype:xls*: Этот запрос вернет все общедоступные таблицы Microsoft Excel с *термином бюджета* всех веб-сайтов, которые имеют доменное имя .gov.

Примечание! найти обновленные списки Google dorks, запустить следующие поиски с помощью Google:

allintext:Google Dorks filetype:pdf

allintitle:Google hacking

SEARCH ENGINES POWERED BY GOOGLE

Google и другие гигантские ИТ-провайдеры в некоторой степени следят за онлайн-деятельностью своих пользователей, чтобы понять их привычки просмотра, и таким образом нацеливаются на них с помощью индивидуальной рекламы. Другим недостатком использования поиска Google является тот факт, что Google записывает ваши предыдущие поиски и может опустить некоторые результаты будущих поисков, если он считает их неимеющими в ваших привычках просмотра. Это опасно для онлайн-расследований, поскольку это может ограничить набор результатов, возвращенных Google, в соответствии с предыдущей историей просмотра поисковика.

Алгоритм поиска Google считается лучшим соотношением запрос результат. Тем не менее, конфиденциальности данных людей там минимальная, есть много поисковых систем, которые получают свои результаты поиска от Google без вторжения в конфиденциальности, собирая информацию поиска. Это самые популярные:

- StartPage (https://www.startpage.com)
- Lukol (https://www.lukol.com)
- Mozbot (https://www.mozbot.com)

Bing

Bing является второй по популярности поисковой системой после Google; он был разработан корпорацией Майкрософт и является поисковой системой по умолчанию в браузерах Internet Explorer и Edge. Bing имеет много общего с google основных поисковых операторов. В таблице 4-2 перечислены основные поисковые операторы, которые могут быть использованы для уточнения поиска на Bing (не используйте пробел после колона (:) в примерах).

Таблица 4-2. *Операторы поиска Bing*

Оператор	Примере	Описание
“”	**“French food”**	Поиск точной фразы
NOT or minus sign	**Virus -computer**	исключает веб-страницы, содержащие термин или фразу.
Or	**Nokia OR Apple**	Поиск любого из этих слов *Nokia* или *Apple*
define:	**define:computer**	получает определение для указанного слова
Site:	**Windows site:darknessgate.com**	Ограничивает результаты поиска одним сайтом (поиск по одному сайту для определенного слова или фразы)
Filetype:	**Bing search operator filetype:pdf**	Поиск результатов с определенным типом файла (PDF в этом примере)
inbody:	**inbody:digital privacy**	возвращает веб-страницы, содержащие указанный термин в теле страницы
Ip	**ip:193.70.110.132**	Находит все веб-сайты, размещенные по указанному IP-адресу
Language:	**unicef language:ar**	возвращает веб-страницы для определенного языка; в этом примере мы искали слово *UNICEF* только на арабских страницах (обратите внимание: чтобы увидеть список стран, регионов и языковых кодов, поддерживаемых Bing, перейдите на

http://help.bingads.
microsoft.com/apex/index/18/en-US/10004.)

Feed:	**feed:computer security**	Находит RSS каналы на веб-сайтах, которые соответствуют вашим критериям поиска
prefer:	**computer hacking prefer:tutorials**	добавляет акцент на термин поиска или на другого поискового оператора, чтобы сосредоточить результаты поиска на нем; в этом примере, мы ищем термины *взлома компьютера,* но с акцентом на учебники

Вы можете сравнить результаты, полученные Google и Bing для одного и того же поискового запроса, перейдя к по http://bvsg.org/index.html.

Еще одна полезная услуга, которая позволяет создавать сложные поисковые запросы для Google и Bing визуально Advangle (http://advangle.com), как показано на рисунке 4-6.Вы также можете сохранить свои запросы в учетной записи Advangle (регистрация бесплатна), чтобы вернуться к ним позже.

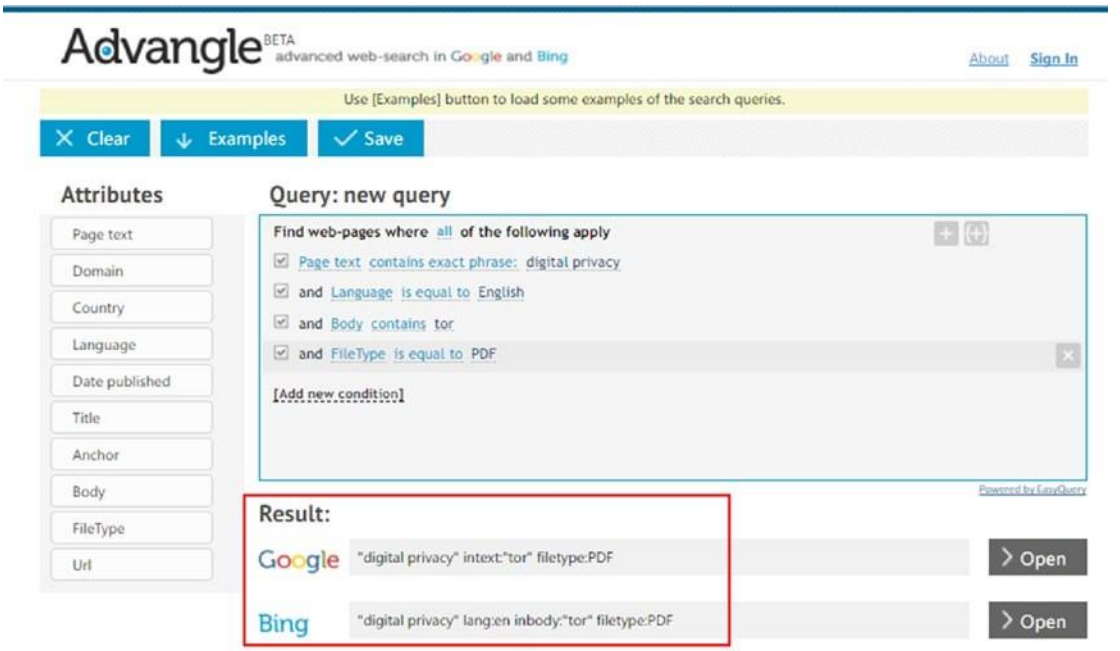

Рисунок 4-6. *Использование сервиса Advangle для создания расширенного запроса Google и Bing*

Поисковые системы, ориентированные на конфиденциальность

Это самые популярные поисковые системы, которые не отслеживают действия пользователей:

- *DuckDuckGo* (https://duckduckgo.com/): Интернет иследователи обычно используют её для поиска читого веб при использовании Tor Browser. • *Qwant* (https://www.qwant.combased): Это базируется во Франции.
- *Oscobo* (https://oscobo.co.uk): Это базируется в Соединенном Королевстве.
- *Swisscows* (https://swisscows.com): Это конфиденциальность безопасного веб-поиска, базирующегося в Швейцарии.
- *Privatelee* (https://privatelee.com): Поиск веб-сайтов и изображений в частном порядке.
- *Gigablast* (https://www.gigablast.com): Это поисковая система с открытым исходным кодом.
- *Gibiru* (www.gibiru.com): Это неподцензурная и анонимная поисковая система.

Другие поисковые системы

Много OSINT иследователи предпочитают использовать более чем одну поисковую систему для получения результатов. Действительно, вы будете удивлены разнообразием результатов при использовании различных поисковых систем для поиска одного и того же запроса. Таблица 4-3 списки других популярных поисковых систем, которые могут быть использованы для поиска информации в Интернете, по популярности. Имейте в виду, что вы должны анонимизировать подключение перед проведением любого поиска, или вы можете просто использовать Tor Browser для проведения поиска.

Таблица 4-3. *Другие поисковые системы*

Номер	название	URL
1	Yahoo! advanced web search	https://search.yahoo.com/web/advanced
2	Yandex	https://www.yandex.com
3	aOL	http://search.aol.com
4	Dothop	http://dothop.com/home
5	excite	www.excite.com
6	goodsearch	https://www.goodsearch.com
7	Factbites	www.factbites.com
8	infospace	http://infospace.com
9	Lycos	www.lycos.com/
10	exalead	www.exalead.com/search/web/
11	Search	https://www.search.com/
12	Search engine Colossus	http://searchenginecolossus.com (содержит каталог поисковых систем из 317 стран и территорий по всему миру, охватывающий все разговорные языки мира)
13	Search engines Directory	www.searchengineguide.com/searchengines.html
14	the ultimate Search engine Links page	www.searchenginelinks.co.uk/

Существуют также национальные поисковые системы, которые могут быть использованы для поиска информации в конкретных странах. Таблица 4-4 перечисляет основные из них по популярности.

Таблица 4-4. *Популярные национальные поисковые системы*

Номер	Название	URL	Страна
1	Yandex	https://www.yandex.com	russia
2	Search	https://www.search.ch/	Switzerland
3	alleba	www.alleba.com/	Philippines
4	Baidu	https://www.baidu.com	China
5	eniro	https://www.eniro.se	Sweden
6	Daum	https://www.daum.net (www.naver.com)	South Korea
7	goo	www.goo.ne.jp	Japan
8	Onet	https://www.onet.pl	poland
9	parseek	www.parseek.com	iran
10	SapO	https://www.sapo.pt	portugal
11	aOnDe	www.aonde.com	Brazil
12	Lableb	https://www.lableb.com	arabic-based search engine

Сайты бизнес-поиска

Хотя термин OSINT происходит от военных, его значение не ограничивается только этим контекстом. В настоящее время предприятия в значительной степени полагаются на OSINT, чтобы расширить возможности своих процессов принятия решений в дополнение к прогнозированию будущих событий.

Поиск информации о корпорациях имеет важное значение для любого онлайн-расследования. Например, бизнес-информация, собранная из источников OSINT, может раскрывать важную информацию, такую как прибыль бизнеса, текущие и будущие проекты, бизнес-иерархия и даты компании (например, ежегодные встречи, корпоративные праздники или встречи с инвесторами). Такая информация полезна во многих случаях (например,

выяснить, была ли конкретная компания или лицо частью дела об уклонении от уплаты налогов).

В этом разделе мы перечислим сайты, которые могут быть использованы для получения важной информации о компаниях по всему миру.

НАЙТИ ЕЖЕГОДНЫЕ БИЗНЕС ОТЧЕТЫ

Годовой отчет – это документ, выдаваемый компанией ее акционерам один раз в год. Он содержит ценную информацию о финансовом состоянии корпорации, такую как ее бюджет, финансовое положение, прибыль, отчеты о убытках, управлении и аудиторе, а также денежные потоки. Вы также можете найти общее описание отрасли, в которой принадлежит компания, предназначенная.

Следующие сайты дают свободный доступ к тысячам ежегодных отчетов, опубликованных в различных отраслях:

- www.annualreports.com перечисляет тысячи годовых записей от 5333 компаний по всему миру.
- https://www.reportlinker.com содержит более 60 миллионов поисковых таблиц, цифр и наборов данных.
- https://www.gov.uk/government/publications/overseas- registries/overseas-registries перечисляет все реестры компаний, расположенные по всему миру, предлагаемые правительством Великобритании.

1. https://www.sec.gov/edgar/searchedgar/companysearch.html является Комиссией по ценным бумагам и биржам США (см. рисунок 4-7).

Рисунок 4-7. *Поиск заявок компании на*www.sec.gov

- www.sedar.com предоставляет доступ к документам и информации, поданных всеми канадскими администраторами ценных бумаг.
- https://www.commercial-register.sg.ch/home/worldwide.html дает список государственных и коммерческих регистров по всему миру.

Ежегодные отчеты также можно найти на веб-сайте корпорации; просто перейдите на страницу About Us или провести поиск *годового отчета* с помощью корпоративного средства поиска сайта, чтобы найти такие файлы. Они обычно приходят в формате PDF или HTML.

ДЕЛОВАЯ ИНФОРМАЦИЯ(ПРОФИЛИ)

Веб-сайты профиля корпорации и каталога предоставляют ценную информацию о таких компаниях, как их адреса, местоположение, филиалы, контактные данные, имена сотрудников (и могут включать их бизнес-телефоны и электронные письма), типы услуг или промышленности, и многое Больше. Ниже приведены самые популярные сайты бизнес-профиля для получения такой информации:

- *Open Corporates* (https://opencorporates.com): Это крупнейшая открытая база данных компаний в мире.

- *Crunchbase* (https://www.crunchbase.com): Предоставляет информацию о бизнес-компаниях, от стартапов на ранних стадиях до Fortune 1000.
- *Corporationwiki* (https://www.corporationwiki.com): Это позволяет искать любую компанию и визуализировать связь между людьми, работающими в ней. Вы также можете скачать файл Excel, содержащий подробную информацию (включая ссылку на страницу на сайте, содержащую известный адрес человека) о каждом человеке, который работает в компании.
- *Zoom Info* (https://www.zoominfo.com/company-directory/us): На этом сайте перечислены компании в Соединенных Штатах, классифицированные по отраслям, и содержится информация, включая контактные данные, для людей, работающих в этих компаниях. Услуга платная и предлагает пробную версию для тестирования услуги.
- *Kompass* (https://www.kompass.com/selectcountry/): Это глобальный бизнес-портал с информацией о компаниях в более чем 60 странах.
- *Infobel* (www.infobel.com): Вы можете искать компанию или человека в любой точке мира.
- *Orbis directory* (https://orbisdirectory.bvdinfo.com/ version-20171019/OrbisDirectory/Companies): Это дает информацию о частных компаниях по всему миру бесплатно. Платная услуга предлагает более подробные отчеты.
- *Manta* (https://www.manta.com/business): Это бизнес-каталог для американских предприятий.
- *Canadian Company Capabilities* (http://strategis.ic.gc.ca/ eic/site/ccc-rec.nsf/eng/Home): Это веб-сайт поддерживается канадским правительством; она имеет базу данных из 60000 канадских предприятий, классифицированных в соответствии с каждой отрасли. Каждый бизнес-профиль содержит информацию о контактах, продуктах, услугах, опыте торговли и технологиях.
- *Canadian Importers Database* (https://strategis.ic.gc.ca/ eic/site/cid-dic.nsf/eng/home): Это приводит списки компаний, импортирующих товары в Канаду, по продуктам, по городам и по странам происхождения.
- *LittleSis* (https://littlesis.org): Это мощный сайт профилирования, который перечисляет огромное количество информации о 185000 человек и 67000 организаций на различных стадиях завершения. Этот сайт ориентирован на влиятельных людей и

организации в государственном и частном секторах, таких как политики, бизнесмены, лоббисты, бизнес-корпорации и некоммерческие организации, такие как фонды, социальные клубы, художественные группы и политические Организаций.

- *Companies House* (https://beta.companieshouse.gov.uk): Это регистр предприятий Великобритании (также содержит информацию о лицах в различных отраслях промышленности в Соединенном Королевстве).
- *CDREX* (http://cdrex.com): Это дает информацию, втом есть местоположение GPS для бизнеса в Сша (около 7 миллионов компаний, классифицированных в зависимости от местоположения или отрасли).
- *EUROPAGES* (https://www.europages.co.uk): Это европейский бизнес-портал, вмещает 3 миллиона зарегистрированных предприятий на 26 языках.
- *Vault* (www.vault.com): Это информация о американских компаниях (более 5000 компаний в 120 отраслях). Отзывы и рейтинги сотрудников также доступны для каждой компании, включенной в перечень. Платные абоненты имеют доступ к подробной информации.
- *Owler* (https://www.owler.com): Это большое количество информации о более чем 15 миллионах компаний по всему миру.
- *The United Kingdom Limited Liability Company list* (https://www. companiesintheuk.co.uk): Предоставляет бесплатную информацию и официальные документы о любой компании с ограниченной ответственностью в Великобритании.
- *Kvk* (www.kvk.nl): Это Голландская торговая палата, которая является реестром немецких компаний.
- *International White and Yellow Pages* (www.wayp.com): Здесь содержатся имена, адреса, номера телефонов и факсов.

Finally, it is worth mentioning Google Finance (https://finance.google.com/ finance). Это дает подробную актуальную информацию о мировых рынках и новости компании.

Поисковые системы метаданных

При проведении поиска с помощью типичной поисковой системы, такой как Google, ваш запрос будет обрабатываться поисковой системой, которая просматривает ваш поисковый запрос в

своей базе данных индекса и соответственно получает соответствующие результаты. Двигатели Metasearch отличаются; эти двигатели не имеют своих собственных индексов. Вместо этого они отправляют поисковый запрос в другие поисковые системы (например, Google, Bing и Yahoo) в дополнение к другим сторонним источникам данных. Затем они получить результаты, ранжировуют их, и представляют окончательный вывод для вас через их веб-интерфейс.

Движки Metasearch делают запросы к поисковым системам (например, Google и Bing), чтобы позволить им искать и получать содержимое из своих индексов. Некоторые мета поисковые системы используют свои собственные схемы рейтинга представления собранных результатов для конечных пользователей. Тем не менее, они не могут вмешиваться или решать касаемо ранга и релевантности содержимого, поставляемого им их источниками данных. Таким образом, вы должны, как правило, придерживаться лучших результатов от каждого партнера поисковой системы.

Основным преимуществом метапоисковых систем является их способность собирать результаты из многих источников для каждого поискового запроса пользователя. Поиск нескольких источников мгновенно сократит время, необходимое для проведения поиска и вернется более полные результаты, не забывая о расширенной конфиденциальности по сравнению с другими типичными поисковыми системами (например, Google и Bing). В следующем списке мы обсуждаем самые популярные метапоисковые двигатели, доступные в настоящее время:

- www.etools.ch/search.do собирает его результаты из крупных международных поисковых систем, сохраняя конфиденциальность пользователей, не собирая и не обмениваясь личной информацией о своих пользователях. Эта поисковая система быстро и показывает резюме для каждого поискового запроса - на правой стороне,подробно источник его результатов (см. рисунок 4-8).

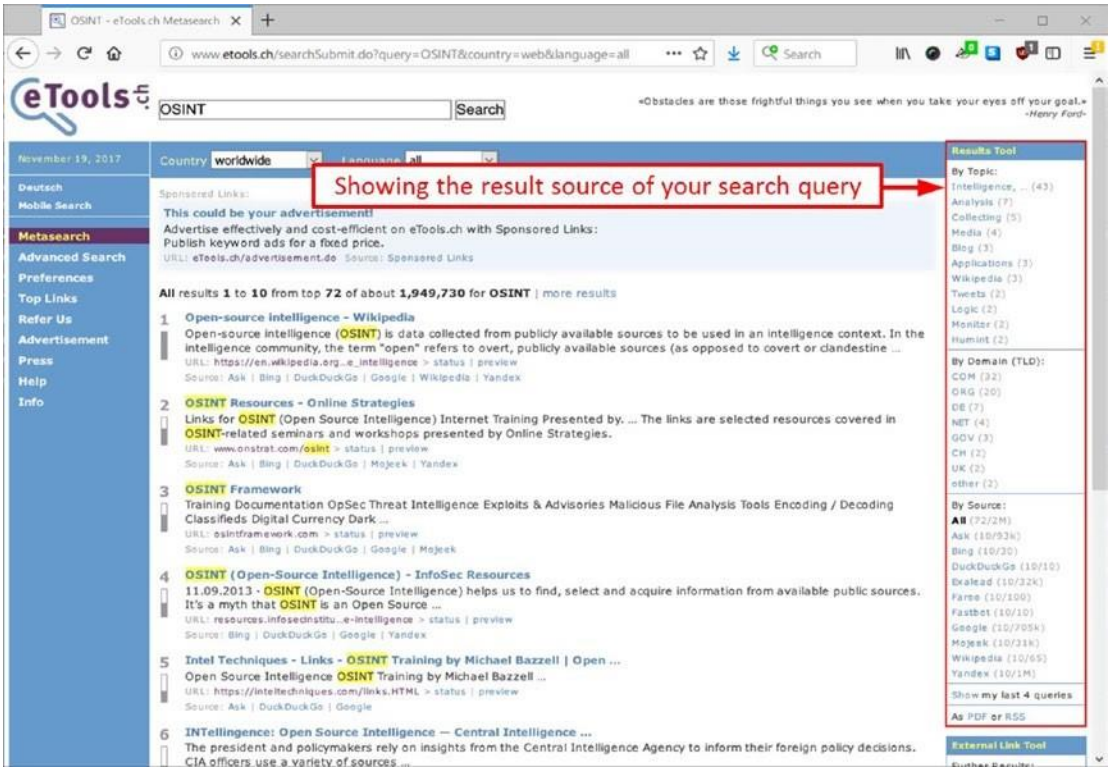

Рисунок 4-8. *Отображение исходного результата поискового запроса при использовании etools.ch*

- All the Internet (https://www.alltheInternet.com) запросы основных поисковых систем, включая торговые сайты, как Amazon и eBay.
- Fagan Finder (www.faganfinder.com/engines) запросы основных поисковых систем, а также ответы двигателей и вопросов и ответов сайтов и блогов.
- www.izito.com агрегирует данные из нескольких источников (Yahoo, Bing, Wikipedia, YouTube и др.) для получения оптимальных результатов, включающие изображения, видео, новости и статьи.
- Metacrawler (www.metacrawler.com) агрегирует результаты от Google и Yahoo.
- My All Search (https://www.myallsearch.com) агрегирует результаты через Bing, DuckDuckGo, AOL Search, Ask, Oscobo, Mojeek, ZapMeta и MetaCrawler.
- Carrot2 (http://search.carrot2.org/) агрегирует результаты от Google API, Bing API, eTools Meta Search, Lucene, SOLR и многое другое. Он организует результаты в тематические

категории (круги и пены деревьев), помогая пользователям сузить их поиск визуально, разделив его на многие темы (см. Рисунок 4-9).

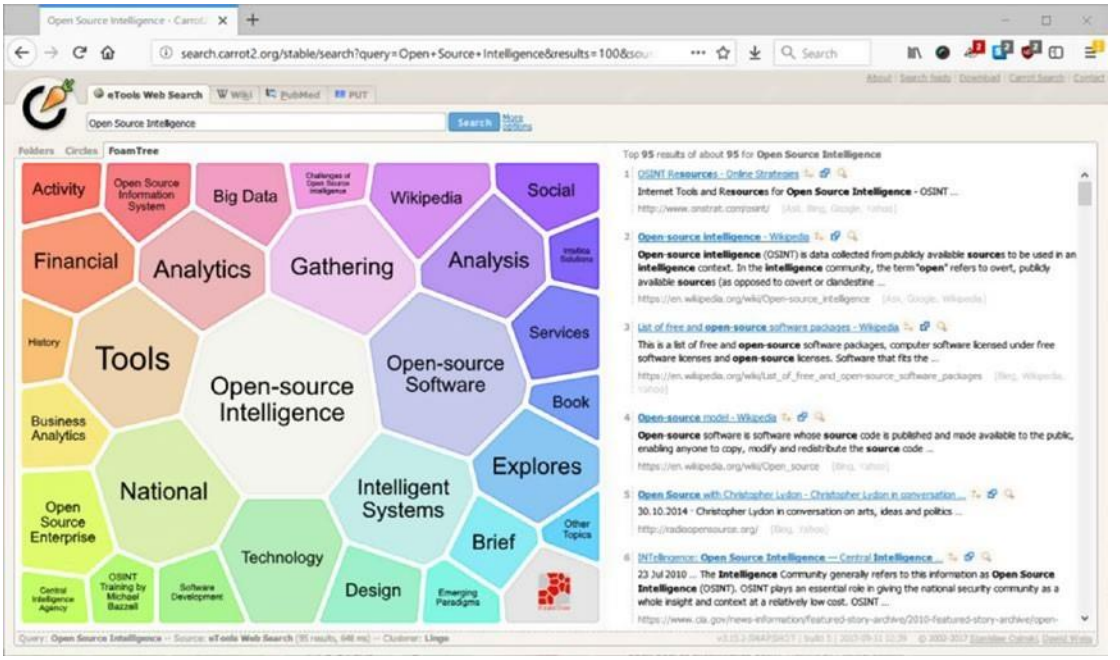

Рисунок 4-9. *Carrot2 разделение результатов поиска на тематические категории*

- elocalfinder (www.elocalfinder.com/HSearch.aspx) получает результаты от Google, Yahoo, Ask, и Bing и отображает их в таблице для сравнения вместе с общим рейтингом.
- Opentext (http://fqs.opentext.com/web.htm) — это метапоисковый движок, основанный на Google, Yahoo!, Ask, Bing, Википедии и Open Directory. Он также предлагает поиск утилиты для поиска в социальных сайтах, как Facebook, Twitter, YouTube и LinkedIn в дополнение к новости поисковых систем (агрегирование результатов от Guardian, Reuters, Washington Post, BBC News, и Лос-Анджелес таймс ") и здоровья поисковые системы.

Code Search

Как онлайн-иследователь, вы можете столкнуться со случаями, когда вам нужно искать фрагмент кода (например, для реконструкции встроенного программного обеспечения). Ниже приведены основные поисковые системы исходного кода:

- Searchcode (https://searchcode.com) поиск по Google code, GitHub, Bitbucket, CodePlex, Sourceforge, Fedora Project, and GitLab.
- Nerdaydata (https://nerdydata.com/search) требует ежемесячную подписку, чтобы разблокировать все функции.
- Krugle (www.krugle.org) это еще один.
- Codase (www.codase.com) поиск по 250 миллионов строк кода.
- The O'Reilly source code search (http://labs.oreilly.com) дает доступ ко всем фрагментам кода в книгах O'Reilly.
- Symbolhound (http://symbolhound.com) поиск поисковых систем кода и не игнорирует специальные символы.
- Merobase (http://merobase.com) — поисковая система кода для компонентов программного обеспечения Java.
- GitHub Dorks (https://github.com/techgaun/github-dorks)
  поиск инструмента Python для поиска конфиденциальных данных, таких как частные ключи, учетные данные и маркеры аутентификации в различных репозиториях.

FTP Поисковые системы

File Transfer Protocol (FTP) старый протокол изобрел в первые дни Интернета и до сих пор используется миллионами веб-сайтов. Как следует из названия, он используется для передачи файлов между компьютерами через сети, такие как Интернет. Веб-хостинг компании обычно дают своим клиентам FTP счет для передачи файлов на хостинг пространстве. Многие компании, университеты, учреждения и проекты сотрудничества размещают большие архивные файлы и другое загружаемое программное обеспечение на серверах FTP, чтобы облегчить обмен информацией между своими сотрудниками. FTP учетные записи могут быть доступны с помощью специального клиента, таких как FileZilla (https://filezilla-проект.Орг), которая поддерживает загрузку,загрузкуи переименованиефайлов.Компании обычно защищают свои серверы FTP с помощью пароля. Тем не менее, вы можете найти много из них оставили незащищенные онлайн (без пароля), и такие публичные серверы FTP можно получить доступ через веб-браузеры непосредственно для просмотра / загрузки их содержимого.

По данным IEEE Computer Society,[iv] Есть более чем 13 миллионов FTP серверов в мире, 1,1 миллиона из которых позволяют "анонимный" (общественный) доступ. Множество полезной информации можно найти на общедоступных серверах FTP, начиная от музыкальных и

видеофайлов и конретизируясь программного обеспечения, налоговых документов и криптографических секретов в дополнение к личным файлам и каталогам.

При поиске содержимого на серверах FTP с помощью специализированных поисковых систем FTP вы ищете только имена файлов и каталоги, так как индексировать весь контент на всех серверах FTP сложно и не легко достичь. Давайте сначала начнем тестирование некоторых методов с Google, чтобы найти контент на серверах FTP; см. Таблицу 4-5.

Таблица 4-5. *Расширенные поисковые запросы Google для поиска серверов FTP*

Google запрос для поиска ftp	значение
inurl:“ftp://www.” “Index of /”	этот поисковый запрос может быть использован для поиска серверов Ftp онлайн.
inurl:ftp -inurl:(http|https) “SEARCH QUERY”	используйте это для поиска всех серверов Ftp, которые имеют указанный поисковый запрос.

Ниже приведены некоторые сайты для поиска FTP-серверов:

- Global file search (http://globalfilesearch.com)
- Filemare (https://filemare.com/en-nl)
- Archie (http://archie.icm.edu.pl/archie_eng.html)
- File watcher (www.filewatcher.com)

Автоматизированные инструменты поиска

Автоматизированные инструменты позволяют автоматизироватьонлайн проверку и процесс поиска с помощью крупных поисковых систем, таких как Google, Bing и Shodan. Автоматизированные инструменты быстрые и позволяют постоянно тестировать большое количество поисковых запросов, тем самым возвращая более полные результаты, поскольку инструмент поиска может создавать сложные поисковые запросы лучше, чем человек. Следующие разделы подчеркивают самые известные автоматизированные поисковые утилиты .

SEARCHDIGGITY

Это самый известный инструмент взлома поисковой системы; это приложение windows GUI, которое соединяет вас с известными базами данных взлома поисковых систем, таких как база

данных Google Hacking. Он работает путем автоматизации процесса поиска на различных платформах поисковых систем, таких как Google, Bing, Shodan, CodeSearch и других, и представляет результаты в основном интерфейсе программы. Просмотреть : https://www.bishopfox.com/ resources/tools/google-hacking-diggity/attack-tools.

SEARCHDOME

Это онлайн-сервис, который позволяет автоматизировать поиск по eBay.com используя широкий спектр критериев поиска (см. рисунок 4-10). Посмотреть :https://www.searchdome.com/ebay.

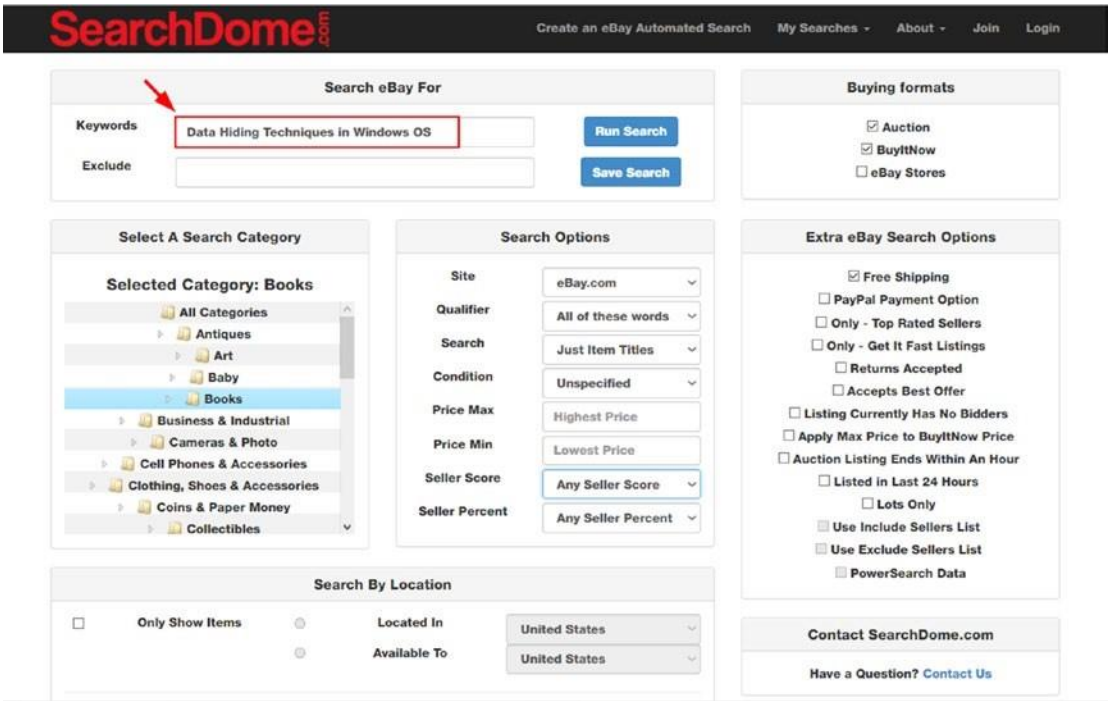

Рисунок 4-10. *Используйте SearchDome для проведения расширенных поисков на eBay.com*

Jeviz

Jeviz поисковая система позволяющая работать с Amazon, передовой поисковой системой. В настоящее время в Соединенных Штатах; сконцентритрованы все крупные поисковые системы в том числе Amazon это позволяет пользователю искать в amazon веб-сайт и найти глубокие

ссылки, которые трудно найти с помощью типичной поисковой системы Amazon. Смотреть https://www.jeviz.com.

Поисковики устройств Интернета вещей (IoT)

Есть много специализированных поисковых систем для подключенных к Интернету устройств (известных как IoT устройств). Ниже приведены некоторые популярные веб-сайты, которые помогут вам обнаружить такие устройства в Интернете:

- *Shodan* (https://www.shodan.io): Shodan является первой в мире поисковой системой для подключенных к Интернету устройств.
- *123Cam* (http://123cam.com List): Это бесплатная веб-камера из разных стран мира.
- *AirportWebcams* (http://airportwebcams.net): Это крупнейшая база данных веб-камер аэропортов (более 1800 веб-камер) из разных стран мира.
- *Insecam* (www.insecam.org): Это каталог онлайн-камер наблюдения безопасности.
- *Lookr* (https://www.lookr.com): Это списки веб-камеры из разных мест по всему миру.
- *Open Street Cam* (https://www.openstreetcam.org/map): В нем перечислены веб-камеры со всего мира.
- *Pictimo* (https://www.pictimo.com): Это поиск для потокового веб-камеры в реальном времени со всего мира.
- *Reolink* (https://reolink.com/unsecured-ip-camera-list): Это список незащищенных IP-камер.
- *Webcam-Network Project* (www.the-webcam-network.com): Это веб-камера каталог.
- *Thingful* (https://www.thingful.net): Это поисковая система для Интернета вещей.

Веб-каталоги

Мы кратко *определили веб-каталог* в предыдущей главе. Веб-каталог, также известный как *каталог объектов*— это веб-сайт, который перечисляет и организует многие сайты по

категориям. Мы можем рассматривать это как телефонную книгу. Каждая буква в этой телефонной книге относится к теме (магазины, новости, информационные технологии, блог), и каждая тема имеет много сайтов, принадлежащих к нему (например, информационная безопасность содержит www.DarknessGate.com).

Тон каталог имеет иерархическую структуру; в нем подчеркивается ссылка на главную страницу сайта вместо ссылки на отдельные страницы, таким образом, уделяя особое внимание общей теме/предмету, к которой принадлежит веб-сайт. Каталоги, как правило, управляются человеческими рецензентами; следовательно, в отличие от поисковых систем, которые используют веб для индексирования веб-содержимого автоматически, веб-каталоги зависят от человеческих усилий, чтобы добавить / обновить их содержание. Чтобы добавить веб-сайт в веб-каталог, веб-мастер должен представить адрес сайта и предоставить некоторые ключевые слова и определить свою нишу. Модератор – этого веб каталога затем проверяет его на пригодность.

Пользователь может использовать в веб-каталоге внутренний поисковик, чтобы найти конкретный вебсайт в каталоге или может просто просматривать все веб-сайты по конкретной теме (см. рисунок 4-11).

Веб-каталоги бывают разных размеров. Yahoo и DMO оба прекращены в настоящее время, но вы можете просмотреть статическую версию DMO на http://dmoztools.net. Существуют огромные каталоги, охватывающие все типы интернет-сайтов. Другие типы являются специализированными веб-каталогами, которые охватывают конкретные предметы и филиалы соответствующих веб-сайтов в них.

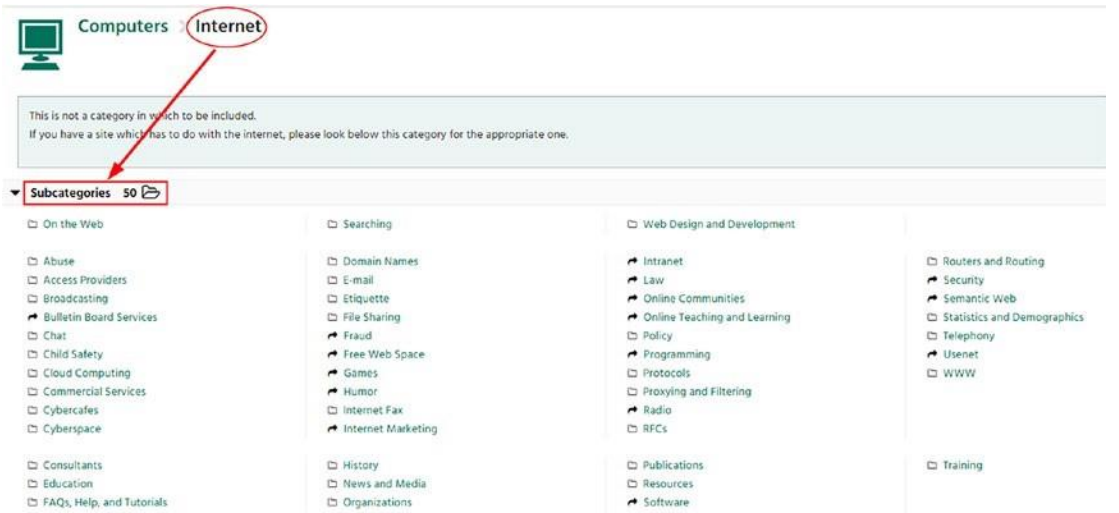

Рисунок 4-11. *Пример веб-каталога(http://dmoztools.net) отображение основных категорий и других подкатегорий*

Веб-каталог может быть как бесплатным, так и платным. Бесплатные сайты не платят за включение вашего сайта в каталоге, в то время как платные из них требуют владелец сайта платить небольшую сумму денег, чтобы включить свой сайт в каталоге. Некоторые веб-каталоги просят взаимной связи. Таким образом, вам нужно поставить ссылку на каталог на главной странице, чтобы включить ваш-свободно-в своем списке.

В то время как веб-сайты используют ключевые слова для поиска и поиска информации в Интернете, веб-каталоги организуют все веб-сайты в соответствии с каждым объектом сайта, что позволяет находить группы соответствующих сайтов в соответствии с предметом, языком и регионом. Затем вы можете использовать методы поиска, например, пользовательский поиск Google для поиска в каждой категории для получения конкретной информации.

Вот самые популярные веб-каталоги:

- The WWW Virtual Library (http://vlib.org)
- DirPopulus (http://dirpopulus.org)
- Best of the Web (https://botw.org)
- GoWorkable (www.goworkable.com)
- 01webdirectory (www.01webdirectory.com)

Сервисы перевода

Во время веб-поиска вы можете столкнуться с полезной информацией на других языках. Такая информация может быть ценной и не может быть опущена во время поиска. Есть много бесплатных онлайн-услуг перевода для перевода документов, текста и даже целых веб-сайтов. Ознакомьтесь со следующим списком:

- Google Translate (https://translate.google.com) является наиболее важным; он может переводить текст и целые веб-страницы на другие языки (см. рисунок 4-12).

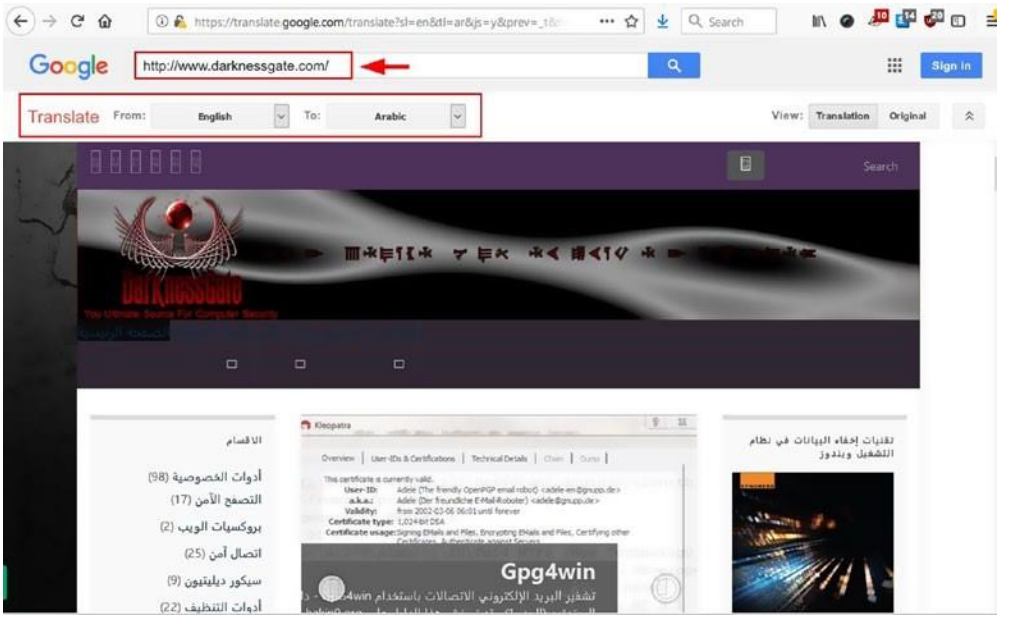

Рисунок 4-12. *Использование сервиса Google Translate для перевода веб-страницы с английского на арабский*

- Google Input Tools (https://www.google.com/inputtools/try) позволяет пользователю вводить текст на любом поддерживаемом языке с помощью своей английской (латинской) клавиатуры, и текст преобразуется в его родной текст. Вы можете скачать оффлайн версию для Windows и Android или просто использовать ее онлайн (см. рисунок 4-13).
- The Yamli Intelligent Arabic Keyboard (https://www.yamli.com/ clavier-arabe) позволяет печатать на арабском языке с помощью латинских символов в фонетический путь, и сайт превратит его в арабские слова.

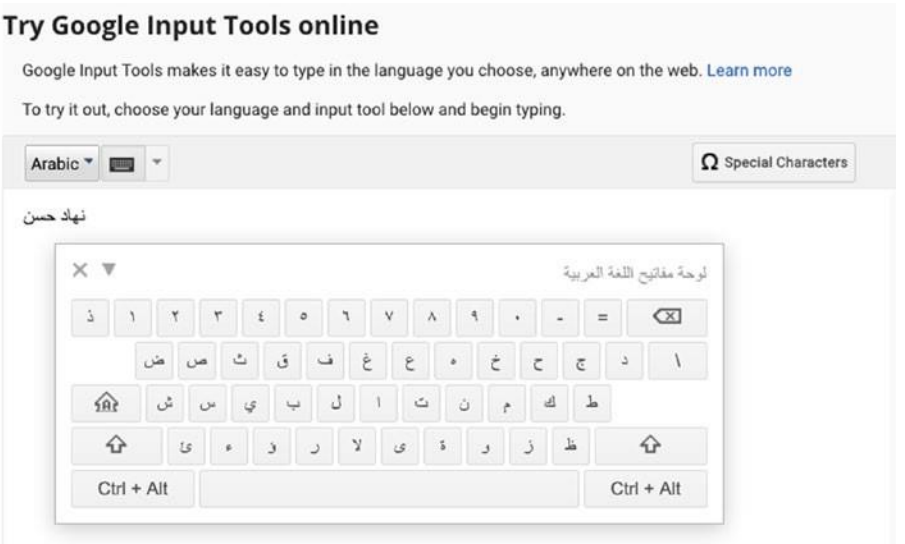

Рисунок 4-13. *Использование ввода Google для преобразования письменного текста на любые языки, поддерживаемые Google*

- Apertium (https://www.apertium.org) является платформой машинного перевода с открытым исходным кодом.
- Babylon (http://translation.babylon-software.com) Это компьютерный словарь и программа перевода, разработанная Компанией Вавилон Программное обеспечение Ltd. Она предлагает перевод в более чем 800 языковых пар.
- Bing Translator (https://www.bing.com/translator) является еще одним сервисом перевода.
- Dictionary (http://translate.reference.com) является еще одним сервисом перевода.
- Wiktionary (https://www.wiktionary.org) еще один сервис перевода.
- Free Translator (www.free-translator.com) еще один сервис перевода.
- No Slang (https://www.noslang.com) переводит сленг, интернет-сленг и аббревиатуры.
- Lexilogos(https://www.lexilogos.com/keyboard/index.htm) поддерживает многоязычную клавиатуру.

История веб-сайта и кэширование веб-сайта

Иногда вы хотите вернуться назад во времени, чтобы исследовать что-то в прошлом. Кэширование веб-сайта полезно для онлайн-исследований, потому что вы можете гарантировать, что снимок данного веб-сайта всегда будет оставаться в сети, даже если оригинальная страница исчезнет. Обратите внимание, что сохраненные страницы обычно хранятся без связанных с ними скриптов, поэтому некоторые функциональные возможности, темы и меню могут работать неправильно.

Есть много интернет-сайтов, которые предлагают такие услуги; следующие являются наиболее популярными из них:

- Internet Archive (the Wayback Machine; https://archive.org/web/ web.php) является самым популярным сайтом архива; он имеет более чем 308 миллиардов веб-страниц, сохраненных с течением времени, и каждый может захватить веб-страницу, чтобы использовать его в будущем в качестве ключа или ссылки. Посмотреть рисунок4-14.

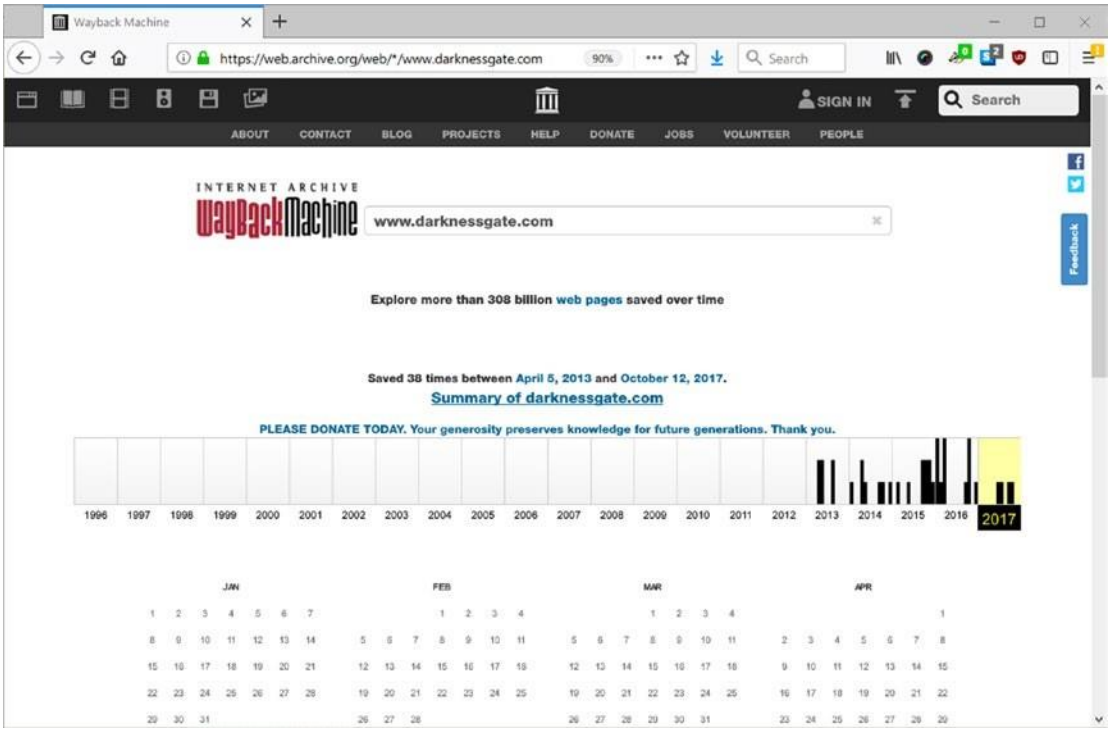

Рисунок 4-14. *Машина wayback показывая исторические данные для www.DarknessGate.com*

- Archive (https://archive.fo/) также доступна.

- Cached pages (www.cachedpages.com/) показывает предыдущие веб-сайты, захваченные на трех различных сайтах архивов (Google кэш, Coral и Archive.org).
- www.screenshots.com показывает историю скриншотов для любого веб-сайта.
- Way Backpack (https://github.com/jsvine/waybackpack) это инструмент, который позволяет загружать весь архив в Wayback Machine для данной веб-страницы.
- Library of Congress (https://loc.gov/websites) это еще один.
- UK Web Archive (www.webarchive.org.uk/ukwa) это еще один.
- Stanford Web Archive Portal (https://swap.stanford.edu) это еще одинэто еще один.
- Oldweb.today (http://oldweb.today) извлекает архивные веб-страницы из различных общедоступных интернет-архивов. Вы также можете отображать архивные веб-сайты с помощью различных веб-браузеров.
- UK Government Web Archive (www.nationalarchives.gov.uk/ webarchive/) содержит веб-архивы правительства Великобритании, опубликованные в Интернете с 1996 года по настоящее время. Архивное содержимое включает видео, твиты и веб-страницы.

Сервисы мониторинга веб-сайта

Иногда вам может понадобиться знать об изменениях на определенном веб-сайте, когда они происходят. Отслеживание изменений на одном веб-сайте может быть достигнуто путем посещения его регулярно. Однако, что вы можете сделать, если вам нужно отслеживать изменения страницы на многих сайтах одновременно?

Есть много онлайн-сервисов, которые позволяют отслеживать неограниченное количество страниц. Это работает, отправив вам оповещение по электронной почте, как только изменение обнаруживается в конкретной странице (выбранной вами). Некоторые платные услуги позволяют получать SMS-оповещения также. Ниже приведены основные бесплатные услуги мониторинга веб-сайта в настоящее время:

- Google Alerts (https://www.google.com/alerts; see Figure 4-15) это обнаружение изменений веб-контента (на основе фразы поиска или ключевых слов) и службы уведомлений, предлагаемых Google. Чтобы установить оповещение, необходимо перейти на страницу Google Alerts (сначала необходимо войти в свой аккаунт Google)

и ввести в поисковую фразу или слово (оно должно быть конкретным, а не общим, чтобы избежать получения слишком большого количества результатов). Google уведомит вас по электронной почте, когда указанная фраза поиска или слово появится в недавно индексированных результатах поиска в любом месте онлайн (он не будет уведомлять вас о текущих результатах, доступных в Интернете).

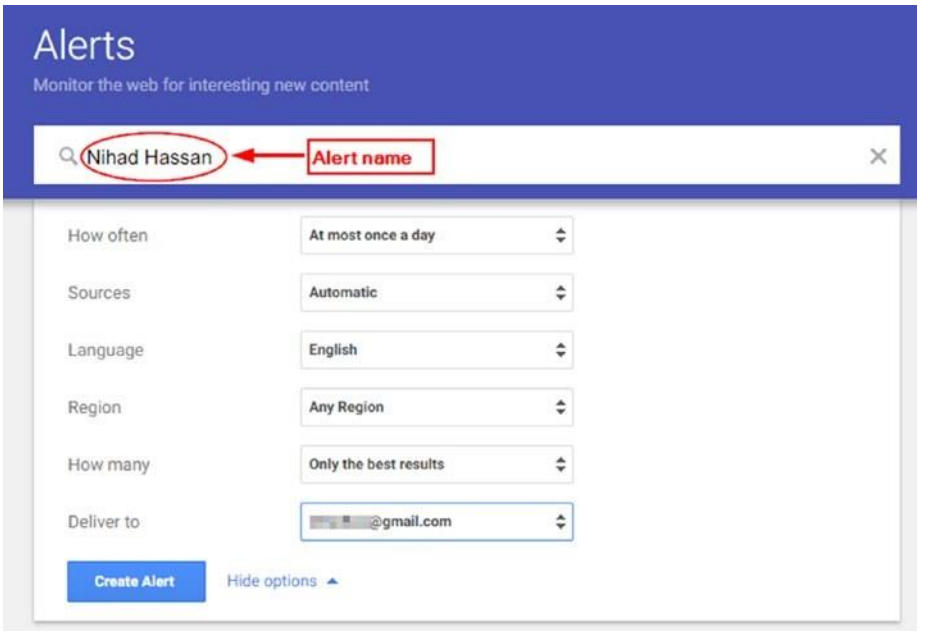

Рисунок 4-15. *Создание нового оповещения Google*

- Talk Walker (www.talkwalker.com/alerts) является альтернативой Google Alert.
- Visual Ping (https://visualping.io) отслеживает веб-страницы для любых обнаруженных изменений; бесплатный счет дает вам 62 проверки в месяц.
- Follow That Page (https://www.followthatpage.com) дает вам две ежедневные проверки с бесплатной учетной записью.
- Watch That Page (www.watchthatpage.com) дает вам 70 еженедельных проверок на всех ваших страницах.
- Update Scanner (https://addons.mozilla.org/en-US/firefox/ addon/update-scanner) — это расширение Firefox, которое отслеживает веб-страницы для обновления.

RSS лента

Другой метод мониторинга изменений веб-сайта заключается в использовании RSS-канала. Итак, что означает RSS?

Really Simple Syndication или Rich Site Summary в XML (текстовом) файл, который позволяет владельцам сайтов информировать подписчиков читателей и других сайтов, о новом контенте, опубликованном на их сайтах. RSS лента оповещает, пользователи Интернета что бы они могли отслеживать обновленный контент в Интернете. Чтобы проверить наличие новых обновлений сайта, пользователю необходимо иметь RSS-ридер. Пользователь подписывается на сайт RSS канал, а затем любой новый контент на этом сайте появится в их ленте читателя автоматически. Каждая запись канала, как правило, содержат название, резюме опубликованного текста, дату публикации и имя автора.

Подписка на веб-сайт RSS сделает пользователя в курсе любых обновлений на своих контролируемых сайтах, тем самым устраняя необходимость посещать предназначенные веб-сайты постоянно, чтобы проверить на наличие недавно опубликованного содержимого.

Основные веб-браузеры предлагают механизм, чтобы подписаться на сайт RSS канал. Mozilla Firefox оснащенв встроенной поддержкой RSS под названием Live Bookmarks. Чтобы подписаться на любой веб-сайт RSS канал через Firefox, выполните следующие шаги:

1. Перейдите на веб-сайт, где вы хотите подписаться на его RSS канал.
2. Из меню закладок выберите Подписку на эту страницу (если браузер не обнаружит RSS-канал на странице, эта опция будет поседена). Затем выберите свой канал. Рисунок 4-16 показывает два канала для этого сайта, потому что это блог, один для комментариев и второй для содержания сайта под названием Feed.

Рисунок 4-16. *Подписаться на RSS-канал с помощью Firefox*

3. Появляется следующая страница. Используйте подписку Firefox поле в верхней части, чтобы подтвердить вашу подписку. Убедитесь в том, чтобы установить опцию, как в рисунке 4-17.

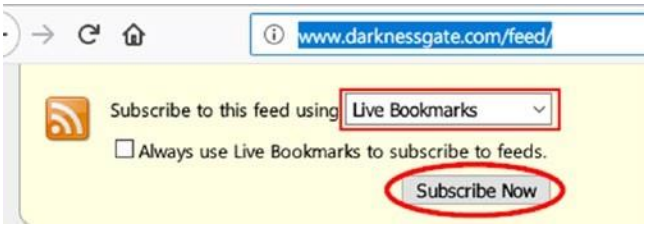

Рисунок 4-17. *Нажмите кнопку Подписка Сейчас, чтобы подписаться на предназначенный канал RSS*

4. После нажатия Подписка Сейчас появится всплывающее сообщение, позволяющее изменить имя и местоположение ленты. Настройки по умолчанию должны быть в порядке. Нажмите кнопку подписки, и вы подпишитесь на ленту !

Встроенный RSS-ридер RSS в браузере имеет ограниченную функциональность по сравнению с некоторыми выделенными настольными RSS-программами для чтения кормов. Например, RSSOwl(www.rssowl.org/) поставляется с мощными функциями, такими как поиск в каналах, сохранение предыдущего поиска каналов и получение уведомлений о новом содержимом. Это бесплатно и поставляется поддерживается на всех основных платформах, как Windows, Linux и macOS.

Есть также расширения браузера-дополнения - для основных веб-браузеров в дополнение к онлайн-сервисам, которые предлагают подписку на каналы. Однако, если вы являетесь частью онлайн-расследования, предпочтительнее использовать только встроенный канал браузера утилиты или программное обеспечение RSSOwl, чтобы избежать утечки информации о вашем сохраненном канале. Многие расширения браузера запрашивать доступ к истории серфинга браузера, и это может привести к нарушению конфиденциальности, если такие записи попадают в чужие руки.

Новостной поиск

Огромное количество полезной информации о чем-либо можно найти в источниках новостей. Например, корпорация может получить глубокое представление о любом конкуренте, как его юридическая история, партнерские соглашения, финансовое положение, и любое негативное упоминание, ища в архивах новостей. Мы привели пример для бизнес-корпораций; однако, то

же самое относится к правительствам, некоммерческим организациям и высокопоставленным лицам.

Поиск в новостях в Интернете проще, чем поиск в архиве медиа-трансляции. В этом разделе мы рассмотрим, как вы можете настроить Новости Google, чтобы узнать о последних обновлениях любого поискового ключевого слова / фразы, появляющейся в глобальных новостных каналах. Мы также упомянем другие источники новостей в Интернете и дадим советы о том, как обнаружить поддельные новости.

Настройка Google News

Google News предлагает современный новостной сервис, агрегированный из различных источников по всему миру. Пользователь может выбрать интересуемую тему, и Google покажет соответствующие результаты по этой теме. Онлайн следователи могут использовать сервис Новостей Google для упрощения поиска конкретных тем или поисковых терминов в новостях. Для этого выполните следующие шаги:

1. Перейти к https://news.google.com.
2. Перейти к левой стороне страницы и нажмите кнопку "Управление разделами" (см. рисунок 4-18).

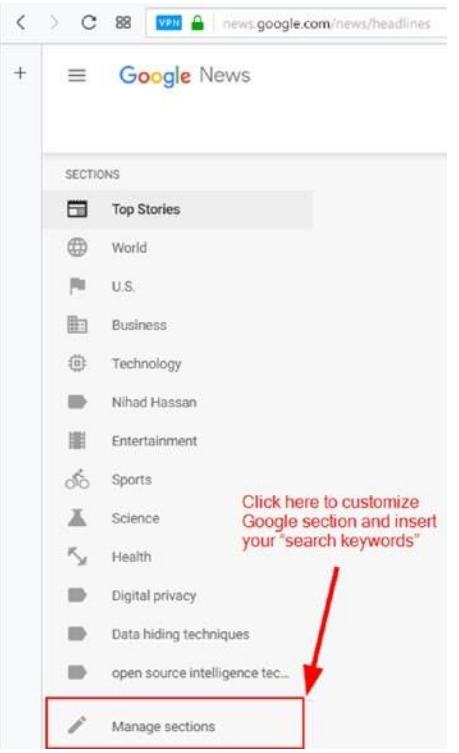

Рисунок 4-18. *Настройка новостей Google*

3. Появляется страница на рисунке 4-19. Введите тему или ключевые слова в текстовом окне "Поиск терминов"; Вы также можете назвать название поиска. Затем нажмите кнопку Добавить раздел.

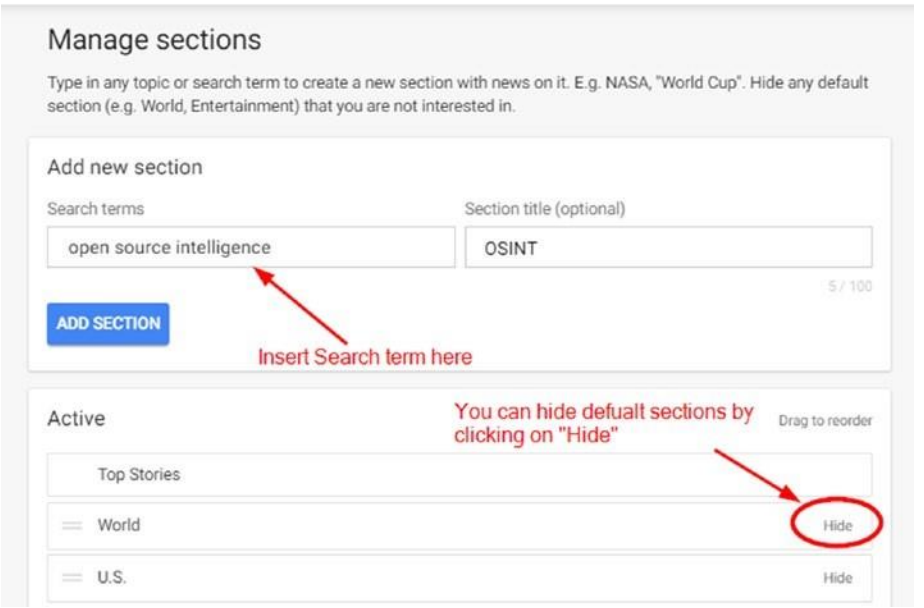

Рисунок 4-19. *Настройка разделов Новостей Google с целью включения ключевых слов*

Теперь в левом вертикальном меню Google News появится новый раздел. Для поиска конкретных ключевых слов, все, что вам нужно сделать, это нажать на имя раздела и Google будет отображать соответствующие результаты поиска новостей.

Примечание! Google хранит архив предыдущих новостей; Вы можете проверить его на https://news.google.com/newspapers.

Новостные сайты

Есть много онлайн-сервисов новостей, которые предлагают актуальную информацию о всех видах тем. Ниже приведены самые популярные из них:

- *1stHeadlines* (https://www.1stheadlines.com): Это списки последних новостей заголовок.
- *News Now* (www.newsnow.co.uk): В этом списке последние новости со всего мира.

- *All You Can Read* (www.allyoucanread.com): Этот веб-сайт перечисляет все основные газеты и средства массовой информации в каждой стране по всему миру (обычно список 30 лучших сайтов).
- *Daily Earth* (http://dailyearth.com/index.html): Это глобальный каталог газет.
- *Chroniclingamerica* (https://chroniclingamerica.loc.gov/ search/titles): Поиск в каталоге газет США.
- *Newspaper Map* (http://newspapermap.com): Это глобальная газетная карта.

1. *World News* (https://wn.com): Сборник мировых новостей, агрегированных из различных источников.

- *The Paperboy* (https://www.thepaperboy.com/index.cfm): Это агрегирует новости от крупных информационных агентств, перечисляет все газеты со всего мира, и показывает, титульная страница крупных газет со всего мира.
- *Site Intel Group* (https://ent.siteintelgroup.com): Этот сайт специализируется на новостях об организации ИГИЛ и других джихадистских группировках.

Обнаружение поддельных новостей

В цифровую эпоху, все подключено в Интернете, и большое количество людей получают свои новости с помощью социальных медиа-сайтов, где каждый может разместить что-нибудь с помощью поддельной личности. Кроме того, есть много ненадежных новостных сайтов, которые публикуют новости без проверки источника. Например, любой источник может распространять вводящие в заблуждение новости для получения коммерческой выгоды, в пропагандистских целях или вводить людей в заблуждение о чем-то. Такие ложные новости могут распространяться мгновенно из-за простоты обмена информацией на различных платформах социальных медиа и, следовательно, через весь Интернет.

Обнаружение фейковых новостей сегодня стало горячей темой и привлекает огромное внимание. Крупные социальные платформы, такие как Twitter и Facebook, пообещали своим пользователям, что найдут решение, чтобы остановить или, по крайней мере, уменьшить вред от фейковых новостей. Исследователи продолжают в этой области с акцентом на разработку решений искусственного интеллекта (таких как машинное обучение и обработка естественного языка) для борьбы с поддельными новостями.

Как следователь OSINT, вы, безусловно, столкнетесь с поддельными новостями во время поиска ресурсов. Любая подозрительная информация не должна быть включена в ваши дела.

Чтобы помочь сортировать достоверную информацию из ложной информации, следует использовать следующий контрольный список для выявления подозрительных новостей:

1. Сначала прочитайте всю статью или часть информации. Не верьте ничему, пока вы не просмотрите его источник.
1. Читайте источник новостей / информации.
2. Если источник исходит от надежного или хорошо известного веб-сайта (например, всемирно известного информационного агентства),:
    a. Перейдите к источнику новостей, чтобы узнать, представлена ли та же информация на его сайте. Например, если новость приписывается Reuters(https://www.reuters.com), проверить свой веб-сайт, чтобы увидеть, существует ли та же информация.
3. Если информация поступает из неизвестного источника, необходимо провести онлайн-поиск, чтобы узнать, кто еще опубликовал ту же новость.
    a. Если достоверный и известный веб-сайт опубликовал одну и ту же историю из того же источника, то, скорее всего, это будет правдивая история.
    b. В противном случае необходимо проверить больше о проблеме или отказаться от использования информации.

Предупреждение! Не доверяйте только информации, опубликованной на социальных сайтах. вместо этого проведите онлайн-поиск, чтобы узнать, были ли опубликованы те же новости в другом месте. если вы обнаружите, что эта новость является ложной, не забудьте сообщить об этом операторам сайта (например, Facebook позволяет своим пользователям сообщать о публикациях для просмотра).

Вы должны читать новости, статьи и другой контент только на авторитетных веб-сайтах. Менее известные сайты должны быть тщательно исследованы, прежде чем рассматривать их как действительные новости.

Есть много сайтов в Интернете, которые помогут вам выяснить, является ли что-то ложные новости / информация. Ниже приведены наиболее важные из них:

- Snopes (https://www.snopes.com) обнаруживает ложные новости, рассказы и городские легенды и исследования / проверяет слухи, чтобы увидеть, являются ли они истинными (см. рисунок4-20).

Рисунок 4-20. *Пример поддельных новостей, обнаруженных Snopes*

- Hoaxy (https://hoaxy.iuni.iu.edu) проверяет распространение ложных утверждений (например, мистификация, слухи, сатира или новостной отчет) через социальные сети. Сайт получает свои результаты от авторитетных организаций по проверке фактов, чтобы вернуть наиболее точные результаты.
- FactCheck (www.factcheck.org/fake-news) сотрудничает с Facebook, чтобы помочь определить и маркировать поддельные новости, о которых сообщают его пользователи. Он также отслеживает различные средства массовой информации для ложной информации, охватывающей широкий спектр тем, как здравоохранение, наука и мистификации распространяется через спам электронной почты.
- https://reporterslab.org/fact-checking дает карту глобальных сайтов по проверке фактов (см. рисунок 4-21).

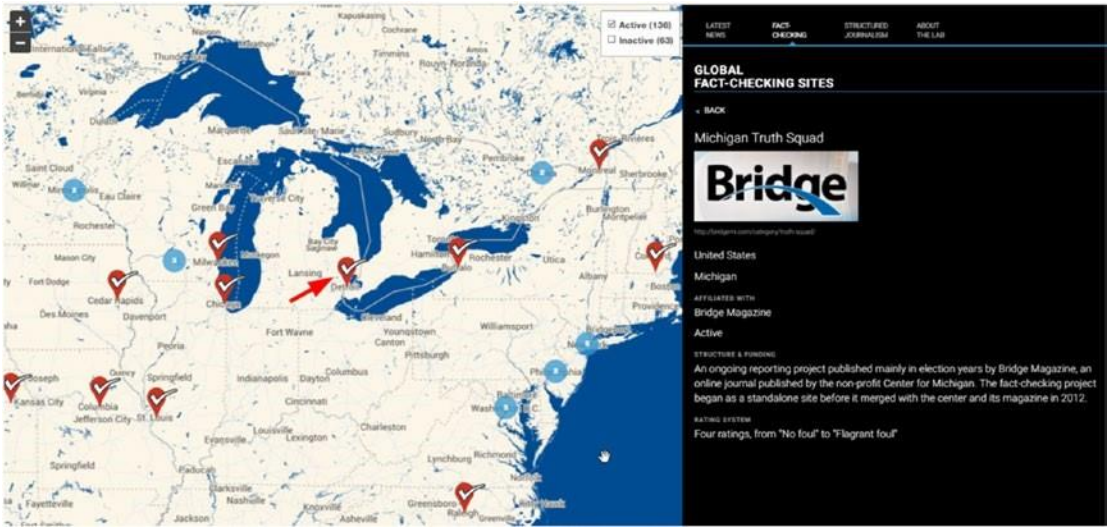

Рисунок 4-21. *reporterslab.org/fact-checking показывает глобальный факт проверки сайтов по всему миру*

- www.truthorfiction.com обнаруживает поддельные новости в различных темах, таких как политика, природа, здоровье, пространство, преступность, полиция и терроризм, и так далее.
- Hoax-Slayer (www.hoax-slayer.com) фокусируется на электронной почте мошенничества и социальных медиа мистификации.
- Verification Handbook (http://verificationhandbook.com) является окончательным руководством по проверке цифрового контента для быстрого освещения на разных языках.
- Verification Junkie (http://verificationjunkie.com) — это каталог инструментов для проверки, проверки фактов и оценки достоверности отчетов очевидцев и самого опубликованного контента в Интернете.
- https://citizenevidence.org есть инструменты и уроки, чтобы научить людей, проверки подлинности пользовательского контента содержимого в Интернете. Он управляется Amnesty International.
- InVID Verification Plugin (www.invid-project.eu/tools-and- services/invid-verification-plugin) поддерживает как Mozilla Firefox, так и Chrome. Это инструмент, созданный европейским проектом InVID, чтобы помочь журналистам проверять контент в социальных сетях.

Поиск цифровых файлов

В предыдущем разделе мы кратко рассказали о том, как использовать передовых поисковых операторов Google и Bing для поиска различных типов цифровых файлов (документы, изображения и видео). В этом разделе мы продолжим наше обсуждение и покажем, как использовать различные методы и специализированные поисковые системы для поиска файлов в различных форматах.

Цифровые файлы составляют важный процент содержимого веб-страниц, расположенных на поверхности сети. Теперь, с наличием бесплатных облачных сервисов обмена файлами (Dropbox, Google Drive) и сайтов обмена видео (YouTube), частные лица и корпорации привыкли использовать такие услуги для онлайн-обмена. Цифровые файлы, найденные в Интернете, могут содержать огромное количество информации не только в их содержании, но и в их метаданных (скрытых атрибутах).

Поиск документов

Этот раздел предназначен для поиска документов в Интернете, но прежде, чем мы начнем, давайте сначала поговорим о наиболее распространенных форматах файлов документов, доступных в Интернете.

DOC И DOCX

DOC и DOCX являются стандартными форматами файлов для документов Microsoft Word. Microsoft Word является частью пакета Microsoft Office, созданного корпорацией Майкрософт. Расширение .doc предназначено для старых версий Microsoft Word, таких как 2003 и старше. Новые издания Microsoft Word (начиная с 2007 года) имеют расширение .docx.

HTML И HTM

Язык разметки Hypertext — это стандартный формат файлов веб-страницы для представления контента в Интернете. Оба расширения (.html и .htm) могут быть использованы взаимозаменяемы. Для редактирования этих файлов можно использовать любой текстовый редактор. Однако для декодирования и отображения содержимого HTML-файлов необходимо открыть HTML-файл с помощью веб-браузера.

ODT

Это формат файла текстового документа (отформатированный с использованием стандарта OASIS OpenDocument XML), например формат файла Microsoft Word; он используется в программе обработки слов с открытым исходным кодом под названием Writer, которая входит в набор Apache OpenOffice. ODT может быть открыт и отредактирован с помощью любой программы, совместимой с OpenOffice, включая NeoOffice (Mac), AbiWord (Mac and Windows), и KWord (Unix). Вы также можете открыть файлы ODT с помощью Microsoft Word и сохранить их в виде файлов DOCX.

XLS И XLSX

XLS и XLSX являются файловыми форматами для Microsoft Excel, используемыми для создания электронных таблиц. Более старые издания имеют расширение .xsl, в то время как современные файлы Microsoft Excel (начиная с 2007 года) имеют расширение. xslx. Excel является частью пакета Microsoft Office, созданного корпорацией Майкрософт.

ODS

ODS означает таблицу OpenDocument; этот формат был создан программой Calc, которая включена в набор Apache OpenOffice. Файлы ODS можно открывать и редактировать с помощью любой совместимой с OpenOffice программы, включая NeoOffice (Mac) и LibreOffice (Mac и Windows). Они также могут быть открыты в Microsoft Excel и сохранены как XLS или XLSX файлы.

PPT И PPTX

PPT и PPTX являются форматом файлов для Microsoft PowerPoint, которые используются для создания мультимедийных презентаций. Так же, как с программами Excel и Word, .ppt используется для старых изданий, в то время как .pptx используется в современных изданиях Microsoft PowerPoint.

ODP

ODP означает OpenDocument Презентация. Он используется в программе Apache OpenOffice Impress, которая входит в набор OpenOffice. Microsoft PowerPoint может быть использован для открытия или сохранения презентации в формате ODP.

TXT

TXT — это базовый формат файла простого текста, который можно открыть с помощью любого текстового редактора на всех операционных системах.

PDF

PDF означает Портативный формат документов, наиболее широко используемый формат файла документов в Интернете, первоначально созданный Adobe Systems. Acrobat Reader, который доступен в качестве бесплатной загрузки с веб-сайта Adobe(https://get.adobe.com/reader), позволяет просматривать и печатать файлыPDF.Формат файлов PDF стал наиболее широко используемым форматом файлов правительствами, корпорациями и учебными заведениями по всему миру.

Примечание! apache OpenOffice можно найти по адресуhttps://www.openoffice.org, и LibreOffice можно найти по адресу https://www.libreoffice.org.

Давайте начнем поиск документов с помощью некоторых операторов Google для поиска файлов на различных поставщиках облачных хранилищ.

Для поиска на сайте Google Doc используйте следующий запрос в базовой поисковой системе Google: **site:docs.google.com SEARCHTERM**. Это будет поиск для указанного термина поиска на веб-сайте документа Google (docs.google.com). Таким же образом, вы можете искать документы, размещенные на Google Drive - с общедоступным доступом, используя следующий поисковый запрос: **site:drive.google.com SEARCHTERM**.

Для поиска файлов, размещенных на Dropbox, введите следующее в Google: **site:dl.dropbox. com SEARCHTERM**.

Для поиска файлов на Amazon AWS введите следующее в Google: **site:s3. amazonaws.com SEARCHTERM**.

Для поиска файлов на Microsoft OneDrive введите следующее в Google: **site:onedrive.live.com SEARCHTERM**.

Поисковые системы файлов

Некоторые специализированные поисковые системы могут задать запрос на многие сайты.

Fagan Finder

Fagan Finder (www.faganfinder.com/filetype) это старая поисковая система, но все еще работает просто отлично, чтобы найти различные типы файлов в Интернете. Просто введите свой поисковый термин, выберите тип файла, который вы хотите искать, и, наконец, выберите поисковую систему для проведения поиска (см. рисунок4-22).

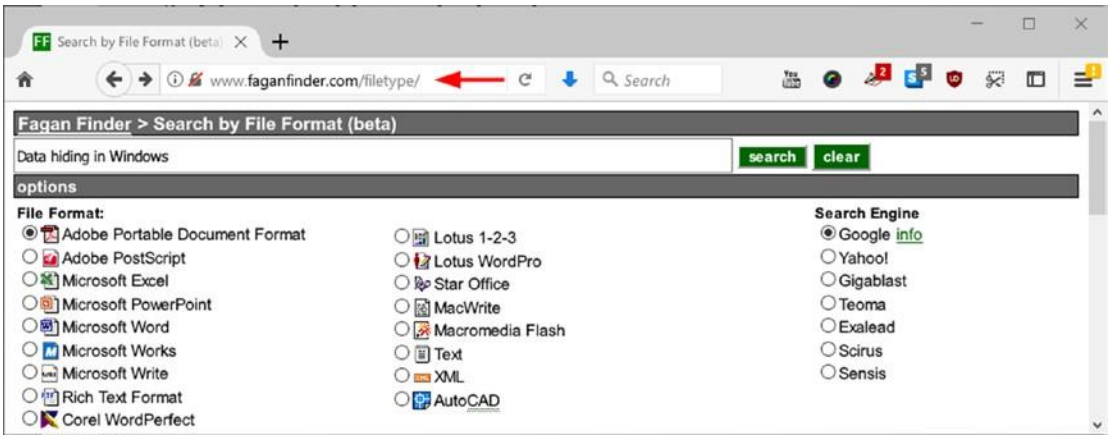

Рисунок 4-22. *Используйте поисковую систему Fagan Finder, чтобы найти различные типы файлов в различных поисковых системах*

Общий-Поиск

General-Search (www.general-search.com) позволяет искать различные типы файлов с помощью 11 файлов хостинг веб-сайтов. Можно выбрать тип файла и установить фильтр до его размера (см. рисунок4-23).

Рисунок 4-23. *Поиск файлов с помощью 11 файл-хостинговых веб-сайтов*

ShareDir

ShareDir (https://sharedir.com) позволяет указать тип файла и одновременно искать более 60 сайтов, файл-хостингов. Уникальный сервис, предлагаемый этим сайтом является то, что он позволяет загружать 500MB ежедневно, не дожидаясь-от премиум файл-хостинга веб-сайтов.

Все, что вам нужно, это зарегистрироваться в бесплатной учетной записи, чтобы использовать эту функцию.

Примечание! Вы можете искать любой файл хостинг веб-сайт с помощью оператора поиска *google сайта.* Например, для поиска файлов на Mediafire.com введите следующего оператора в поисковой системе Google: **site:mediafire.com SEARCHTERM**.

ПОЛЬЗОВАТЕЛЬСКИЙ ПОИСКОВИК

Мы уже рассмотрели различные типы поисковых систем. Тем не менее, мы отложили наше обсуждение пользовательских поисковых систем до сих пор, так что мы могли бы охватить, как использовать этот метод, чтобы сузить поиск для конкретных типов файлов в ограниченном наборе сайтов.

Термин *пользовательский поиск* может вводить в заблуждение на первый взгляд; некоторые пользователи могут думать, что они могут создать новую пользовательскую поисковую систему в соответствии с их предпочтениями. Однако это не так.

Пользовательский поиск позволяет использовать существующий сервис поисковой системы для предварительного выбора веб-сайтов, необходимых для ограничения поиска, типов возвращенных результатов (например, только pdf-файлов), и как результаты будут расставлять приоритеты.

Основным поставщиком пользовательского поиска является Google, поэтому мы рассмотрим, как создать один в следующих шагах:

1. Перейти к www.google.com/coop/cse.
2. Вы должны иметь учетную запись Google, чтобы использовать эту услугу, так что во-вводом, если вы еще не сделали этого.
3. Нажмите кнопку "Новая поисковая система" на левой стороне.
4. На следующей странице введите сайты, которые вы хотите включить в поиск в разделе "Сайты для поиска". Вы можете включить URL-адреса всего сайта или отдельные URL-адреса страниц. Выберите язык, используемый для отображения графического интерфейса пользовательской поисковой системы; наконец, дать вашему поиску имя.
5. Нажмите кнопку «Создание», чтобы создать пользовательскую поисковую систему (см. рисунок4-24).

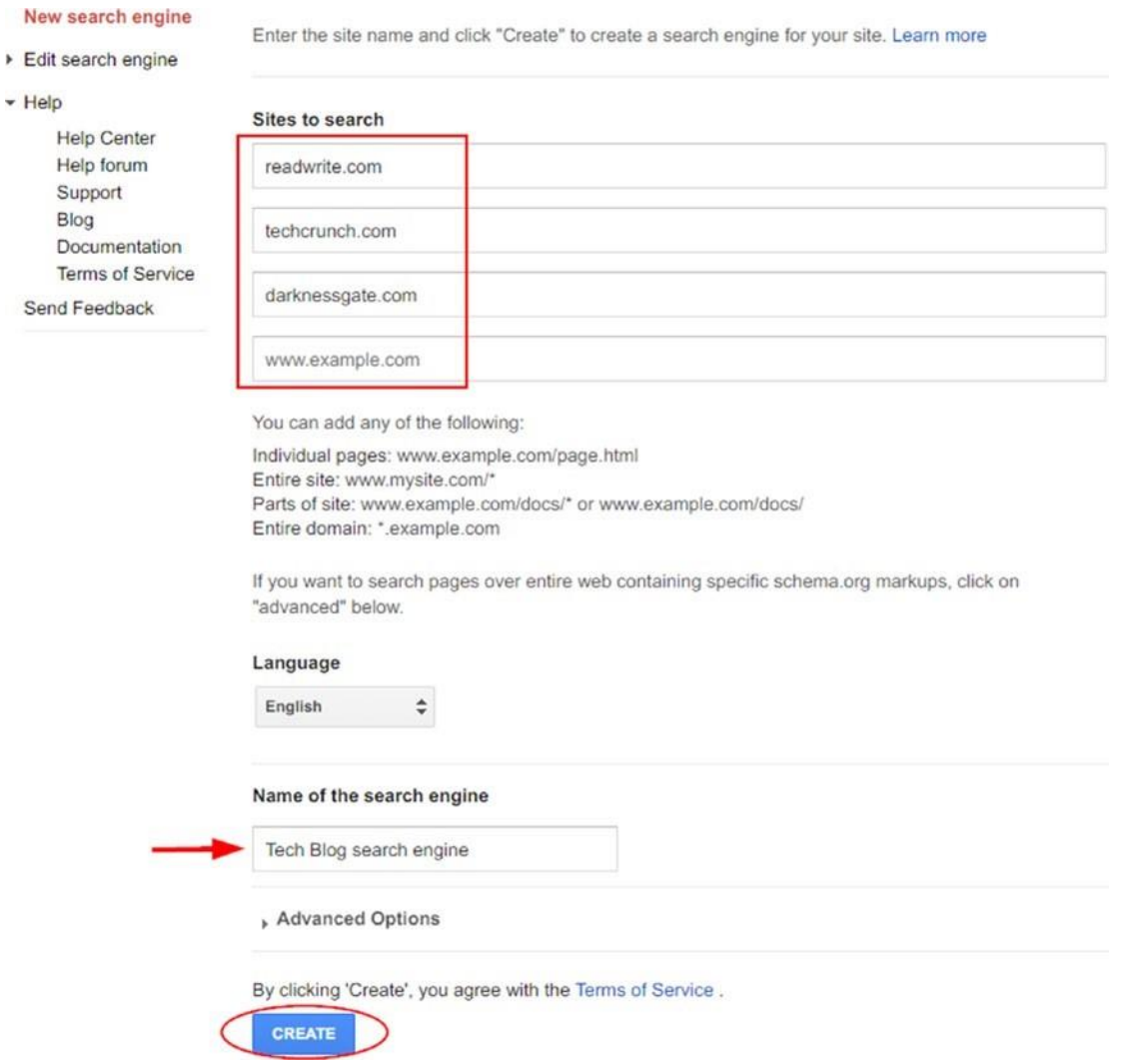

Рисунок 4-24. *Создание пользовательской поисковой системы с помощью пользовательского поиска Google*

6. После успешного создания пользовательской поисковой системы, Google будет отображать страницу, показывающую общедоступный URL вашей пользовательской поисковой системы. Он также покажет фрагмент HTML-кода в случае, если вы хотите разместить его на вашем сайте и ссылку на пользовательскую панель управления поисковой системой для обновления его настроек (см. Рисунок 4-25).

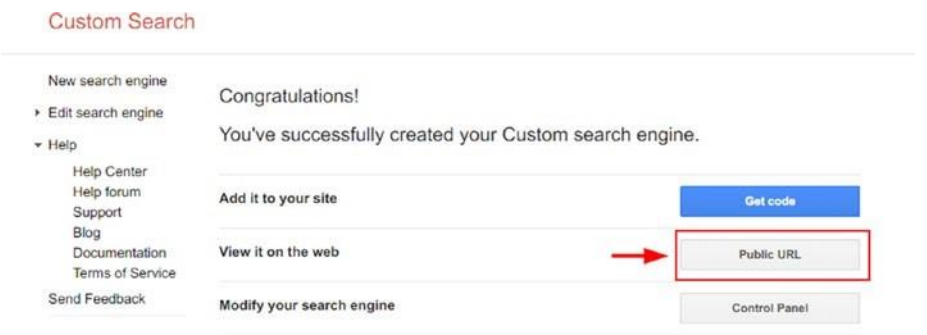

Рисунок 4-25. *Пользовательская поисковая система Google успешно создана*

Чтобы получить доступ к общедоступному URL-адресу вашей пользовательской поисковой системы, перейдите на https://cse.google.

com/cse/all, нажмите на специальное имя поисковой системы, к которого вы хотите получить доступ, перейдите в Setup и выберите общедоступный URL (см. рисунок 4-26).

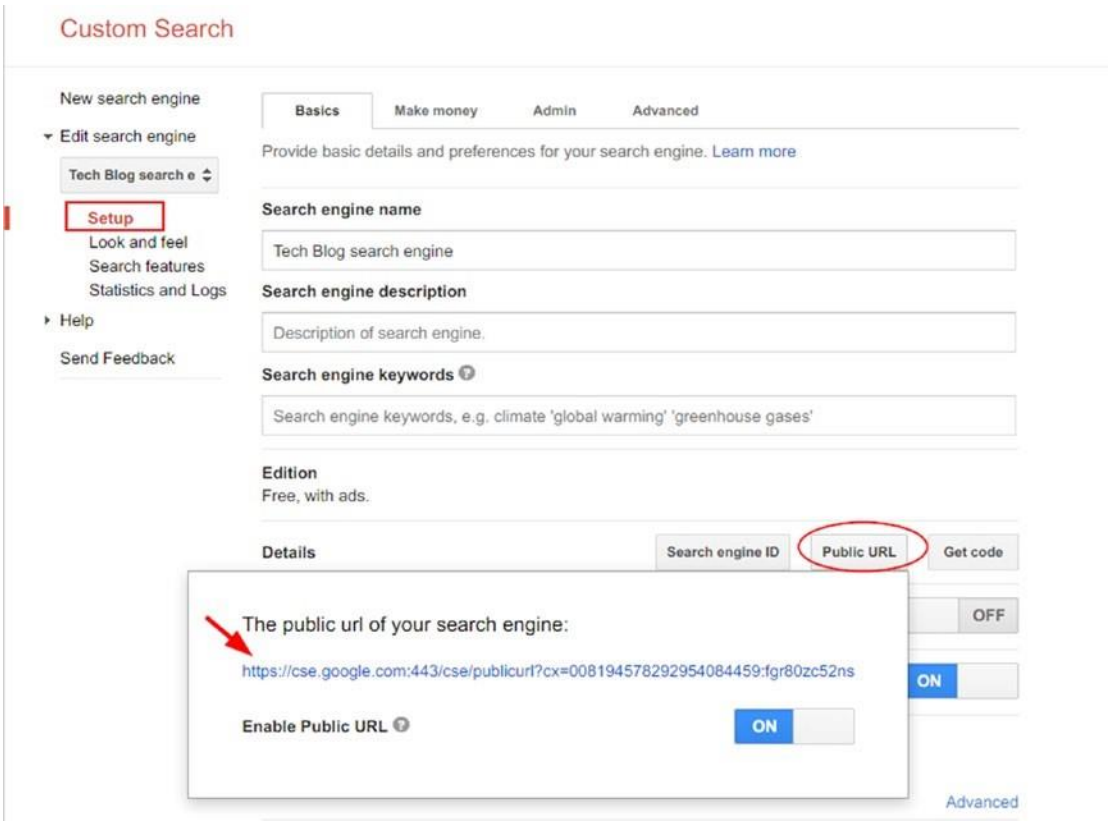

Рисунок 4-26. *Просмотр общедоступного URL-адреса пользовательской поисковой системы Google*

Google будет отображать окно поиска для вас. Введите свой поисковый запрос, и Google будет отображать соответствующие результаты только с веб-сайтов, которые были введены при создании пользовательской поисковой системы.

Многие пользователи Интернета уже создали свои собственные пользовательские поисковые системы Google, чтобы найти файлы и каталоги FTP в Интернете. Один из них расположен в https://cse.google. com/cse/home?cx=014863114814409449623%3Ajc-vjhl_c5g. Чтобы использовать этот пользовательский поиск, введите свой термин поиска (файл или имя каталога); Вы также можете указать тип файла, который вы хотите ограничить результаты поиска, нажав на соответствующее имя ниже окна поиска (см. рисунок4-27).

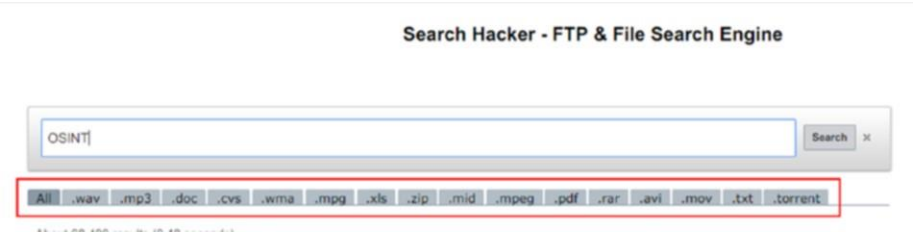

Рисунок 4-27. *Пользовательская поисковая система Google, используемая для поиска различных типов файлов*

Другие полезные Google пользовательских поисковых систем для размещения ресурсов OSINT в Интернете являются следующими::

- 300 Сайты социальных сетей(https://cse.google.com/cse/publicurl?key=AIzaSyB2lwQuNzUsRTH-49FA7od4dB_Xvu5DCvg&cx=0017944 96531944888666:iyxger-cwug&q=%22%22)
- 250 Сайты обмена видео(https://cse.google.com/cse/publicurl?key=AIzaSyB2lwQuNzUsRTH-49FA7od4dB_Xvu5DCvg&cx=0017944965
    - 31944888666:ctbnemd5u7s&q=%22%22)
- Поиск сайтов файловых каипов(https://cse.google.com/cse/publicurl?key=AIzaSyB2lwQuNzUsRTH-49FA7od4dB_Xvu5DCvg&cx=00179449653
    - 1944888666:hn5bcrszfhe&q=%22%22)
- Торрент Поиск(https://cse.google.com/cse/publicurl?key=AIza

- SyB2lwQuNzUsRTH- 49FA7od4dB_Xvu5DCvg&cx=017944965319448886 66:ixpabzzplzy&q=%22%22)

Примечание! Вы можете построить передовой оператор Google для поиска файлов PDF, размещенных на общедоступных серверах, используя следующий Google dork: **intitle:index.of +?last modified? +?parent directory? +pdf “Search Term”**.

•

СЕРАЯ ЛИТЕРАТУРА

Как мы уже говорили в главе 1, серая литература является любой материал, производимый в мире коммерческих издательских систем. Он имеет в основном два типа.

- Серая литература
- Серая информация

Серая литература включает в себя книги, журналы, журналы, и все, что может быть получено публично через традиционные каналы книжных магазинов или академических публикаций. Пользователь обычно платит абонентскую плату, чтобы получить доступ к таким ресурсам или покупает их непосредственно в книжных магазинах (например, покупать книги у Amazon.com). Springer (https://rd.springer.com), которая обеспечивает доступ к миллионам научных документов, таких как журналы, книги, серии, протоколы и справочные работы, является наглядным примером серого канала литературы.

Серая информация, с другой стороны, не может быть легко получена с помощью традиционных маршрутов книжных магазинов. Тем не менее, он имеет некоторые специализированные каналы, где вы можете получить некоторые из них; Вы должны платить за специализированные подписные агентства, чтобы приобрести остальное. Серая информация включает в себя следующие и более:

- Академические работы
- Препринты
- Разберательства
- Конференц-документы и дискуссионные документы
- Отчеты об исследованиях
- Маркетинговые отчеты
- Технические характеристики и стандарты
- Диссертаций
- Тезисы
- Торговые публикации
- Меморандумы

- Правительственные отчеты и документы, не опубликованные на коммерческой основе
- Переводы
- Информационные бюллетени
- Обзоры рынка
- Черновой вариант книг и статей

В этом разделе мы сосредоточимся на академических и научных ресурсах, потому что мы уже охватили бизнес-поисковики, где вы можете получить серую информацию о бизнесе. В следующем списке вы найдете наиболее важные веб-сайты серой литературы, которые могут быть использованы для получения академических и научных ресурсов бесплатно, охватывающих все темы:

- Academia (https://www.academia.edu) является платформой для ученых, чтобы поделиться научно-исследовательских работ- более 19 миллионов работ в настоящее время загружены, охватывающих все академические предметы.
- Academic Index (www.academicindex.net) является научно-академической поисковой системы, которая перечисляет только выбранные наборы качественных веб-сайтов, выбранных учеными, библиотекарями, преподавателями и библиотечными консорциумами.
- Academic Torrents (http://academictorrents.com) является распределенным репозиторием для наборов данных и научных знаний, поддерживаемых сообществом. Здесь проводятся научные исследования, курсы, наборы данных, документы и коллекции с использованием технологии Torrent, где каждый пользователь системы может хранить исследовательскую работу и предлагать ее для скачивания, используя только домашний компьютер. Все, что вам нужно, это клиент Torrent, и вы готовы скачать и поделиться их содержанием.
- American Doctoral Dissertations (www.opendissertations.com) предоставляет бесплатный доступ к более чем 172 000 диссертаций и диссертаций, принятых американскими университетами с 1902 года по настоящее время.
- ArchiveGrid (https://beta.worldcat.org/archivegrid) содержит более пяти миллионов архивных материалов, собранных из архивов, библиотек, музеев и исторических

- обществ. Основные темы включают исторические документы, а также личные и семейные документы и истории.
- Google Scholar (https://scholar.google.com/schhp?hl=en) является поисковой системой Google, чтобы найти научные исследования. Результаты ранжируются на основе количества цитирований (рассчитанных на основе количества людей, которые ссылаются на исследование) и достоверности публикации.
- Вы также можете создавать оповещения (например, Google оповещения уже охвачены), так что вы получите информацию, когда новая научная исследовательская статья будет опубликована, что соответствует вашим критериям поиска.
- The Bielefeld Academic Search Engine (https://www.base-search.net/Search/Advanced) содержит более 100 миллионов документов.
- Archive Portal Europe (www.archivesportaleurope.net) предоставляет доступ к информации о архивных материалах из разных европейских стран, охватывающих многочисленные темы (такие как сельское хозяйство, здравоохранение, правосудие, политика и наука).
- Social Science Research Network (https://www.ssrn.com/en) предоставляет более полумиллиона научных работ, охватывающих 30 тем.
- The National Library of Australia (http://trove.nla.gov.au) имеет более 500 миллионов австралийских и онлайн-ресурсов, охватывающих книги, журналы, ежегодные отчеты, изображения, исторические газеты, карты, музыку, архивы и многое другое.
- ScienceDirect (www.sciencedirect.com) содержит более 250 000 статей открытого доступа (бесплатно для чтения и загрузки) в научных, технических и медицинских исследованиях.
- PQDT Open (https://pqdtopen.proquest.com/search.html) предоставляет открытый доступ к диссертациям и диссертациям бесплатно.
- The National Archive of the United Kingdom (http://discovery.nationalarchives.gov.uk) содержит более 32 миллионов описаний записей, хранятся в Национальном архиве и более 2500 архивов по всей Великобритании, многие из них доступны для скачивания.

- Oxford Academic (https://academic.oup.com/journals) содержит журналы в области права, бизнеса, науки, социальных наук, искусства и медицины.
- Page Press (www.pagepress.org) содержит научные журналы открытого доступа.
- CERN Document Server (https://cdsweb.cern.ch) обеспечивает свободный доступ к тысячам статей, книг, перепечаток, презентаций и переговоров, мультимедиа и информационно-пропагандистской деятельности, охватывающей в основном физическую науку.

  High Wire (http://highwire.stanford.edu/lists/freeart.dtl) имеет бесплатные онлайн полнотекстовые статьи.
- Gray Guide (http://greyguide.isti.cnr.it) имеет ресурсы серой литературы.
- Beyond Citation (www.beyondcitation.org) предоставляет информацию о различных академических базах данных и других цифровых исследовательских коллекциях.
- Crossref (https://search.crossref.org) поиск метаданных (название, автор, DOI, ORCID ID, ISSN) более 92 миллионов журнальных статей, книг, стандартов и наборов данных.
- Databases (https://databases.today) — это каталог общедоступных баз данных для загрузки бесплатных ресурсов для исследователей безопасности и журналистов.

ИНФОРМАЦИЯ ОБ УТЕЧКЕ ДАННЫХ

Утечки данных—иногда называют являются преднамеренным или непреднамеренным обнародованием конфиденциальной информации. Утечки в основном происходят из-за хакерских атак на компьютеризированные системы или недовольных сотрудников, которые могут раскрыть секретную информацию о своих организациях.

Утечки данных могут включать информацию о кредитных картах, PII, медицинскую информацию пациентов, финансовую информацию, электронную почту/социальные имена пользователей и пароли, коммерческую тайну, планы корпораций и будущие работы, информацию об интеллектуальной собственности и военные информация, принадлежащая правительствам.

Ведутся дебаты о правовом статусе информации об утечке данных. Например, некоторые утверждают, что утечка информации стала частью источников OSINT и, таким образом, вы можете справиться с ней, как вы делаете с любой общедоступной информации.

•

Противоположное мнение предполагает, что утечка информации была получена незаконно путем нарушения системы или правовых норм и, следовательно, не должна использоваться в качестве источников OSINT.

Исследование OSINT не могут опустить существование таких просочившихся данных при расследовании некоторых случаев (особенно при работе с утечкой разведывательной информации). Однако предпочтительнее обращаться с этим осторожно на индивидуальной основе. Например, если личная информация или частная корпорация допустила утечку, предпочтительно не обнародовать информацию и отказаться от её в поиске. Вместо этого, вы можете использовать полезные элементы в вашем расследовании, уважая личную информацию человека, которая уже просочилась один раз.

Утечка информации, такой как личная, финансовая и корпоративная информация, может быть найдена в даркнете (уже описана в главе 3),но мы не собираемся ее публиковать, потому что это состоит из незаконных сайтов, пропагандирующих незаконные действия.

Утечка официальных документов распространяется в Интернете с использованием конкретных веб-сайтов, которые сосредоточены на различных областях, в основном военные, разведовательные и тд. Ниже приведены два самых популярных официальных репозитория утечки данных онлайн:

- WikiLeaks (https://wikileaks.org)
- Cryptome (https://cryptome.org)
- Offshore Leaks (https://offshoreleaks.icij.org)

МЕТАДАННЫЕ ДОКУМЕНТОВ

Мы уже говорили о цифровых метаданных файлов и продемонстрировали, как просматривать/ отсеивать их с помощью различных инструментов в главе 2,но имейте в виду, что любые цифровые файлы, приобретенные в Интернете, могут содержать полезные метаданные, которые должны быть исследованы.

Изображения

Цифровые изображения, логотипы и иконки могут быть очень ценны в исследованиях OSINT. Основные поисковые системы, такие как Google, Yahoo и Bing, обеспечивают базовую функциональность поисковой системы изображений. Тем не менее, есть и другие, более

специализированные поисковые системы изображения, которые могут быть использованы для получения более точных результатов.

ОСНОВНЫЕ ПОИСКОВИКИ ИЗОБРАЖЕНИЙ

Следующие сайты предлагают услуги по поиску изображений:

- Google Image Search (https://images.google.com)
- Bing image search (www.bing.com/images)
- Yahoo Images (http://images.yahoo.com)
- Yandex (https://yandex.com/images)
- Baidu (http://image.baidu.com)
- Imgur (https://imgur.com)
- Photobucket (http://photobucket.com)

  Picsearch (www.picsearch.com contains)
- https://ccsearch.creativecommons.org)
- SmugMug (https://www.smugmug.com)

Google предлагает Расширенный поиск изображений, где вы можете установить много критериев вашего поискового запроса, таких как цвет изображения, тип изображения (фото, лицо, клип искусства, рисунок линии, анимированные), регион или страна, сайт или доменное имя, тип формата изображения, и права использования. Google Расширенный поиск изображений можно найти на (https://images.google.com/ advanced_image_search).

Изображения, опубликованные в социальных сетях, можно найти в следующих местах:

- *Lakako* (https://www.lakako.com): Это поиск Instagram, Twitter, и Google для фотографий и людей.
- *Flickr* (https://www.flickr.com)
- Flicker map (https://www.flickr.com/map): Просмотр загруженных изображений на карте в соответствии со страной происхождения загрузчика.
- *My Pics map* (www.mypicsmap.com): Просмотр фотографий Flickr на карте Google. Вам необходимо предоставить имя пользователя Flicker загрузчика изображения или просмотреть фотографии из определенного набора фотографий.

- *idGettr* (https://www.webpagefx.com/tools/idgettr): Найти идентификационный номер Flicker (также работает для групп).
- *Flickr Hive Mind* (http://flickrhivemind.net): Это инструмент для анализа данных для базы данных Flickr фотографии.
- *Instagram* (https://www.instagram.com)
- *Websta* (https://websta.me/search) — расширенный поиск веб-сайта Instagram.
- *Stalkture* (http://stalkture.com) — онлайн-зритель из Сети Instagram.
- *Mininsta* (http://mininsta.net) является передовой поисковой системой Instagram.
- *Pinterest* (https://www.pinterest.com)

Есть специализированные сайты, которые содержат изображения, которые появились в прессе и средствах массовой информации. Для поиска такого типа изображений, попробуйте эти сайты:

- Gettyimages (www.gettyimages.com)
- International Logo List (http://logos.iti.gr/table/)
- Instant Logo Search (http://instantlogosearch.com)
- Reuters Pictures (http://pictures.reuters.com)
- News Press (https://www.news-press.com/media/latest/news)
- Associated Press Images Portal (www.apimages.com)
- PA Images (https://www.paimages.co.uk)
- European Pressphoto Agency (www.epa.eu)
- Canadian Press Images Archive (www.cpimages.com/fotoweb/index.fwx)

Некоторые веб-сайты, например www.DarknessGate.com отключают флэш для защиты от мультимедийного контента. Но многие веб-сайты по-прежнему используют Flash-видео (файлы SWF) для отображения анимации, чтобы загрузить файлы SWF и другие мультимедийные файлы, когда правое нажатие на сайт отключено, используя только браузер Firefox, выполните эти действия:

а. перейдите в меню Firefox и выберите инструменты, а затем информация о странице.

B. перейдите на вкладку Media и найдите свой файл SWF или изображения, которые вы хотите загрузить. Выберите файл, а затем нажмите Кнопку Сохранить (см. Рисунок 4-28).

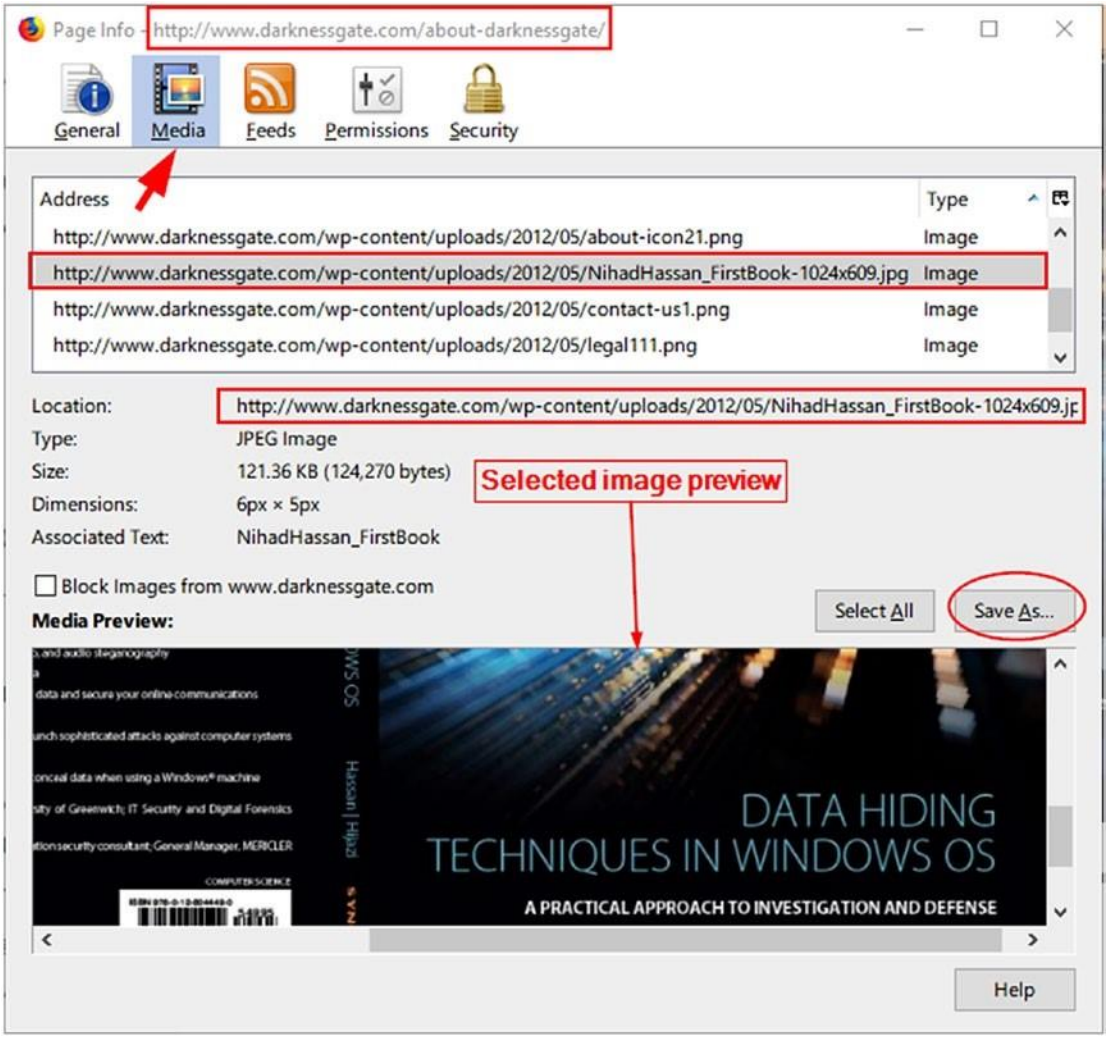

Рисунок 4-28. *Сохранение изображения с защищенного веб-сайта (с ограниченным правом клика с ограниченным и благополучием) с помощью браузера Firefox. Таким же образом можно загрузить файлы SWF (Flash), встроенные в страницы. Тем не менее, вам нужно сначала закончить воспроизведение фильма, прежде чем скачать его.*

пожалуйста, обратите внимание, что мы не поощряем нарушение законов об авторском праве в отношении загрузки мультимедийного контента из Интернета, однако, вам могут понадобиться такие методы в некотором контексте.

всегда читайте веб-сайт "условия использования" и правила и соблюдать законы об авторском праве объявил для каждого сайта, прежде чем собирать любые материалы в Интернете.

ОБРАТНЫЙ ПОИСК ИЗОБРАЖЕНИЙ

Обратный поиск изображений использует образец изображения вместо поискового запроса. Он работает, загрузив изображение или вставив его URL-в обратную поисковую систему изображения, которая, в свою очередь, будет искать свой индекс, чтобы найти, где еще это изображение появляется в Интернете и отображать все другие места. Таким образом, вы можете знать оригинальный источник фотографий, мемов и фотографий профиля. Ниже приведены самые популярные сайты поисковой системы обратного изображения:

- *Google reverse search* (https://www.google.com/imghp): Google имеет специальную поисковую систему для поиска обратного изображения; вы можете вставить URL-адрес изображения в поле поиска или загрузить его в Google (см. рисунок 4-29).

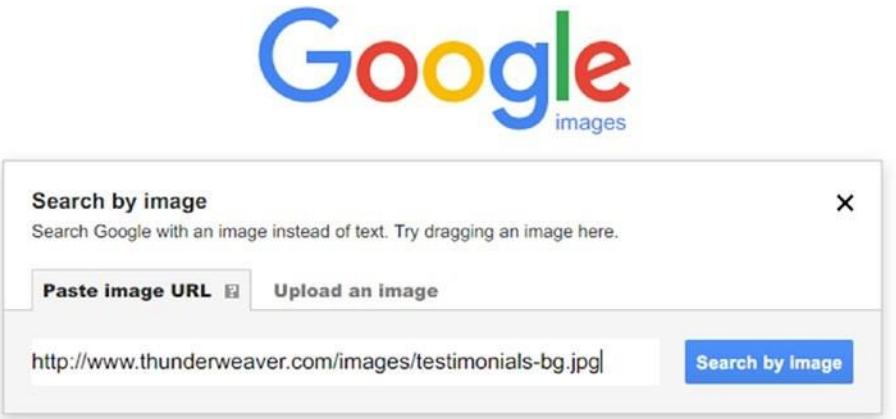

Рисунок 4-29. *Google обратный поиск изображений с помощью URL-адреса изображения*

- *Karmadecay* (http://karmadecay.com): Это обратный поиск изображений на Reddit.com (в бета-версии).

- *TinyEye* (www.tineye.com): Вы можете искать по изображению или URL; более 24 миллиардов изображений уже проиндексированы.
- *Reverse Image Search* (www.reverse-image-search.com): Проведите обратный поиск изображений с помощью Google, Bing и Яндекса.
- *Imagebrief* (www.imagebrief.com): Поиск изображений и использование обратного поиска изображений, а также.
- *Cam Finds App* (http://camfindapp.com): Это приложение доступно как для Android, так и для устройств Apple. Он использует технологию визуального поиска для распознавания загруженных фотографий и дает мгновенные результаты о них, такие как связанные изображения, локальные результаты покупок, а также широкий выбор веб-результатов.
- *Image Identification Project* (https://www.imageidentify.com): При этом используется технология визуального поиска для распознавания загруженных изображений.

ПРОВЕРКА МАНИПУЛИРОВАНИЯ ИЗОБРАЖЕНИЯМИ

Мультимедийные поиски OSINT пересекаются во многих областях цифровой криминалистики. Как онлайн-следователь, вы не должны доверять всем мультимедийным файлам, которые вы приобретаете. Если вы сомневаетесь в какой-либо мультимедийный файл (изображение или видео), вы должны тщательно проверить, чтобы убедиться, что он не был подделан, то есть манипулировать нарочно, чтобы скрыть или изменить некоторые факты. Анализ изображений начинается с идентификации исходного устройства (камеры или мобильного телефона), используемого для съемки фотографии. Эта информация является частью метаданных изображений.

Как мы уже упоминали в главе 2, все типы цифровых файлов могут включать метаданные (который является данными о данных). Метаданные могут включать в себя множество полезной информации для вашего исследования. В главе 2 мы упомянули некоторые инструменты для просмотра/отсечения метаданных в изображениях, видео, PDF-файлах и документах Microsoft Office. Мы будем продолжать здесь и упомянуть дополнительные инструменты, которые специально полезны для цифровых изображений:

- *Forensically* (https://29a.ch/photo-forensics/#forensic- magnifier): Этот сайт предлагает бесплатные инструменты для анализа изображений судебно-медицинской экспертизы; она включает в себя обнаружение клонов, анализ уровня ошибок, извлечение метаданных и многое другое.
- *Fotoforensics* (http://fotoforensics.com): Это предлагает анализ судебно-медицинской экспертизы файлов JPEG и PNG для проверки на наличие каких-либо манипуляций с использованием методов анализа уровня ошибок (ELA).
- *Ghiro* (www.getghiro.org): Это инструмент с открытым исходным кодом, который может анализировать изображения оптом и извлекать информацию о метаданных, использовать метаданные GPS для поиска близлежащих изображений и выполнять ELA для определения того, было ли изображение обработано. Вы можете скачать эту программу в качестве виртуального устройства, которое готово к использованию (он поставляется установлен в Linux Ubuntu).
- *ExifTool* (https://sno.phy.queensu.ca/~phil/exiftool): Вы можете читать, писать и редактировать мета-информацию в самых разнообразных файлах. Он поддерживает различные форматы метаданных, такие как EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP и ID3.
- *Exif Search* (https://www.exif-search.com): Это коммерческий поиск изображений с помощью их метаданных.
- *JPEGsnoop* (www.impulseadventure.com/photo/jpeg-snoop.html): Это анализирует источник изображения, чтобы проверить его подлинность.
- GeoSetter (www.geosetter.de/en): Вы можете манипулировать/просматривать геоданные и другую информацию о метаданных — другие изображения.
- *Lets Enhance* (https://letsenhance.io): Вы можете увеличить размер фотографии, не теряя ее качества. Бесплатная учетная запись позволяет для 14 изображений. Тем не менее, вам все еще нужно загрузить целевое изображение на сервер, и это наложит проблемы конфиденциальности на загруженные файлы.

OCR ИНСТРУМЕНТЫ

Во время поиска вы можете столкнуться с текстом, написанным внутри изображений. Этот текст должен быть извлечен сначала, чтобы он мог быть отредактирован, отформатирован, проиндексирован, отправлен в поиск или переведен. Ниже приведены популярные инструменты и веб-сервисы для извлечения текста из изображений, известный как оптическое распознавание символов (OCR):

- FreeOCR (www.paperfile.net/index.html)
- Free Online OCR (www.i2ocr.com)
- NewOCR (www.newocr.com)

Google Drive и Google Docs имеют интегрированную OCR поддержку включённую по умолчанию. Чтобы воспользоваться этой услугой, вам нужно загрузить изображение

в Google Drive через аккаунт Вы должны иметь учетную запись Google в первую очередь) на https://www.google.com/drive. Затем нажмите правое нажатие загруженного изображения, выберите Open With и выберите Документы Google (см. рисунок4-30).

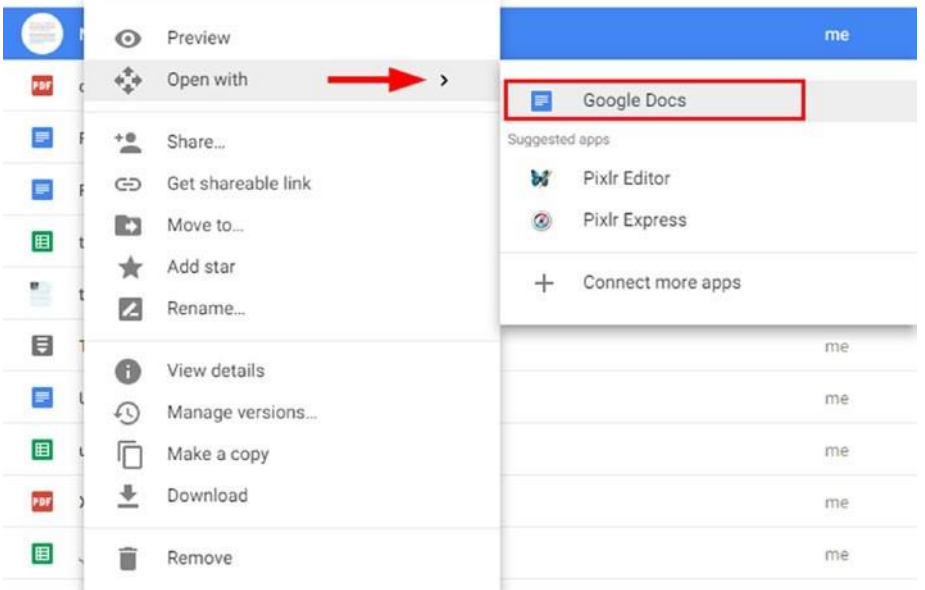

Рисунок 4-30. *Открытие файла изображения с помощью Google Doc*

Вы заметите, что Google представил загруженное изображение в верхней части документа и создал редактируемый текст OCR под ним (см. рисунок4-31).

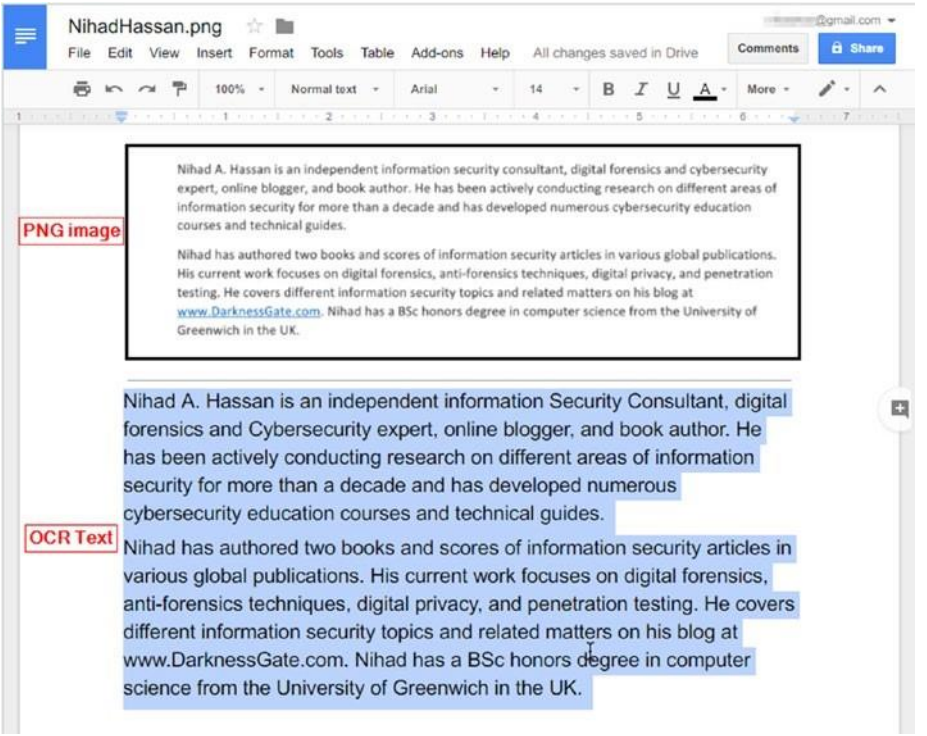

Рисунок 4-31. *Google Doc изменил текст в загруженном изображении в отображаемый текст*

Видео

Технологическая революция повлияла на то, как люди общаются. Например, скорость интернета неуклонно растет и стала более доступной в большинстве стран мира. Вычислительные устройства, такие как столы и смартфоны, дешевеют, и почти любой может приобрести их. Многие из этих устройств оснащены мощными камерами. В самом деле, люди привыкли к записи своих ежедневных моментов с помощью видео; веб-сайты обмена видео позволяют любому загружать видео файл с помощью простого клика с помощью приложения каждого сайта.

Видео содержание может быть большой ценностью в любом онлайн-расследовании. В этом разделе мы перечислим наиболее важные сайты для обмена видео, где вы можете найти различные виды видео. Затем мы рассмотрим некоторые методы и инструменты для изучения видео-контента.

ОСНОВНОЙ ПОИСК ВИДЕО

Вот самые популярные сайты:

- YouTube (https://www.youtube.com)
- Google videos (https://www.google.com/videohp)
- Yahoo video search (https://video.search.yahoo.com)
- Bing videos (https://www.bing.com/videos)
- AOL (https://www.aol.com/video)
- StartPage video search (https://www.startpage.com/eng/video.html)
- Veoh (www.veoh.com)
- Vimeo (https://vimeo.com)
- 360daily (www.360daily.com)
- Official Facebook video search (https://www.facebook.com/pg/ facebook/videos)
- Crowd Tangle (Facebook video search) (www.crowdtangle.com/ videosearch)
- Internet archive open source movies (https://archive.org/ details/opensource_movies)
- Live Leak (https://www.liveleak.com)
- Facebook live video map (http://facebook.com/livemap); see Figure 4-32

Рисунок 4-32. *Facebook живой видеопоток является еще одним источником для расследования OSINT*

Вот некоторые другие видео-сайты:

- *Meta Tube* (www.metatube.com): Это как YouTube.com.
- *Geo Search Tool* (http://youtube.github.io/geo-search-tool/ search.html): Это выполняет поиск всех фильмов в соответствии с определенным запросом, введенным пользователем. Набор результатов будет фильтроваться в зависимости от расстояния от конкретного места (город, деревня, перекресток) и в зависимости от конкретных временных рамок (последний час, последние два или три часа и т.д.).
- *Earth Cam* (www.earthcam.com): Это глобальная сеть живых камер, предоставляющих потоковое видео из разных регионов мира.
- *Insecam* (www.insecam.org): Это каталог онлайн-камер наблюдения безопасности.

Примечание! Вы можете использовать Google для поиска в любом сайте обмена видео, введя следующий поисковый запрос:

site: *youtube.com* SEARCHTERM

Это заменить *YouTube*.

ВИДЕОАНАЛИЗ

Это самые популярные сайты:

- *YouTube DataViewer from Amnesty International* (https:// citizenevidence.amnestyusa.org): Это онлайн-сервис, который позволяет извлекать скрытую информацию из видео, загруженных на YouTube (см. рисунок4-33) как дата загрузки / время и эскизы (вы также можете сделать обратный поиск изображения на извлеченных эскизов с помощью поиска изображений Google обратного изображения).

Рисунок 4-33. *Использование YouTube DataViewer для извлечения метаданных о любом видео YouTube*

- *Ez Gif* (https://ezgif.com/reverse-video): Это обратный поиск видео и предлагает много других полезных инструментов преобразования видео.
- *Print YouTube Video* (https://www.labnol.org/internet/print- youtube-video/28217/): Чтобы распечатать видео раскадровку YouTube, перейдите по предоставленной ссылке и добавьте печатающее видео YouTube в панель инструментов для закладок браузера. Чтобы распечатать любой фильм YouTube, просто доступ к видео странице YouTube и нажмите на закладку (см. Рисунок 4-34). Появится новая страница, содержащая сгенерированные изображения раскадровки видео.

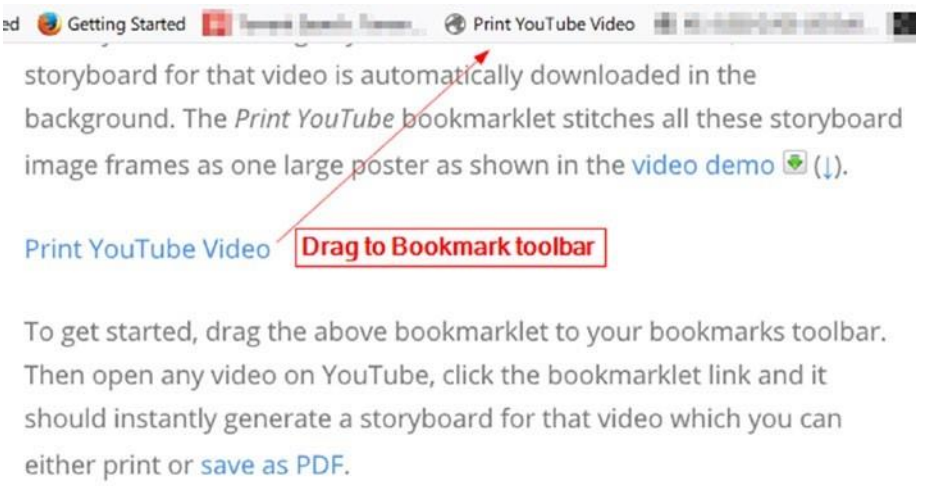

Рисунок 4-34. *Печать видео YouTube (источник: https://www.labnol.org/internet/print-youtube-video/28217/)*

- *Видео на текстовый конвертер*(www.360converter.com/conversion/video2TextConversion): Это преобразует видео/ аудио файлы в текст.
- *Montage* (https://montage.storyful.com): Это позволяет совместно использовать совместную работу для анализа видеоконтента.

File Extension and File Signature List

Зная расширения файлов и подписи поможет вам определить и исследовать цифровые файлы во время сбора OSINT. Ниже приведены два веб-сайта для этой проблемы:

- *File Extensions* (https://www.file-extensions.org/): Эта библиотека содержит тысячи расширений файлов и их описания.
- *File Signature Table* (https://garykessler.net/library/ file_sigs.html): Список расширений файлов и связанная с ними подпись Hex.

Инструменты для повышения производительности

В главе 2, мы рассмотрели некоторые полезные инструменты для принятия ваших онлайн-исследований более организованной. Мы отложили упоминание оставшихся инструментов до сих пор, как они относятся к файл-поиск методов.

ЗАХВАТ ЭКРАНА

Иногда вам нужно взять захват экрана всего экрана или части экрана, чтобы захватить важную информацию (например, для захвата всплывающее сообщение или часть онлайн-карты) и включить его в отчет о расследовании. Есть много инструментов для достижения этой цели; это два популярных решения:

- *Awesome Screenshot Plus* (https://addons.mozilla.org/en-US/firefox/addon/screenshot-capture-annotate/): Это дополнение Firefox; он может быть использован для захвата всей страницы или любой его части; аннотировать его прямоугольниками, кругами, стрелками, линиями и текстом; размытие конфиденциальной информации; и многое другое.
- *Greenshot* (http://getgreenshot.org): Это программа скриншота с открытым исходным кодом для Windows. Это позволяет создавать скриншоты выбранной области, окна или полного экрана. Он имеет встроенный редактор изображений, чтобы аннотировать, выделить или запутать части захваченных скриншотов (см. Рисунок4-35).

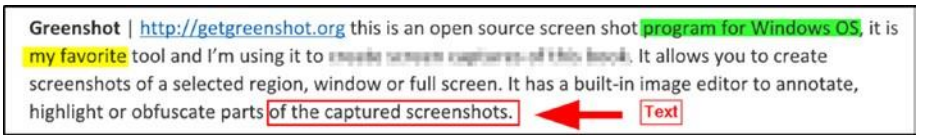

Рисунок 4-35. *Greenshot может выполнять различные действия аннотации на захваченных изображениях и прост в использовании*

- *Screenshot Machine* (https://screenshotmachine.com): Этот сайт позволяет принимать онлайн захват экрана любого указанного URL. Захваченное изображение можно загрузить на устройство.
- *PDF My URL* (http://pdfmyurl.com): Это онлайн-сервис для создания PDF-документов из любого URL в вашем браузере.

СКАЧАТЬ ОНЛАЙН ВИДЕО

Онлайн-расследования требуют от вас поиска и расследования видеофайлов для извлечения полезной скрытой информации. Иногда вам может понадобиться сохранить (загрузить) видео из Интернета, например, с веб-сайта YouTube, чтобы включить его в свое

исследование или проанализировать его дальше. Есть много способов загрузки видео из Интернета; Самый простой способ заключается в использовании браузера дополнений.

Easy YouTube Video Downloader Express

Это firefox дополнения для загрузки видео с YouTube. Это позволяет прямой загрузки высококачественного видео / аудио с YouTube (1080p full-HD и 256Kbps MP3) с одним щелчком мыши. Вы можете найти его на https://addons.mozilla.org/en-US/firefox/addon/ easy-youtube-video-download.

YooDownload

Если вы предпочитаете использовать веб-сервис для загрузки видео с различных социальных сайтов в Интернете, YooDownload поможет достичь этого легко. Перейти к https://yoodownload.com/ index.php и вставить URL-адрес видео с социальной платформы (YouTube, Facebook, Instagram, Twitter, Vid и SoundCloud музыка); Вы также можете выбрать качество видео перед загрузкой. Веб-сайт также предлагает расширение браузера для браузера Chrome.

Dredown

В https://www.dredown.com, Вы можете скачать видео со всех основных сайтов обмена видео, таких как YouTube, Facebook, Instagram, Keek, Twitter, Twitch, Vimeo, Vevo, Tumblr и многое другое.Вы можете найти другие веб-сайты для загрузки видео контента в Интернете на http://deturl.com.

ВИДЕО/АУДИО КОНВЕРТЕР

Вы можете столкнуться с случаями, когда вы не можете открыть определенный файл видео/аудио из-за типа формата файла. Чтобы противостоять таким проблемам, можно использовать программное обеспечение для преобразования видеофайла из текущего формата файлов в другой, чтобы он мог работать на поддерживаемых устройствах.

- HandBrake (https://handbrake.fr): Это программа с открытым исходным кодом для обработки мультимедийных файлов и любого DVD или Blu-ray диска в читаемый формат на поддерживаемых устройствах; он также поддерживает кодирование различных типов аудио файлов.

- Convert2mp3 (www.convert2mp3.net): Это онлайн-сервис, который преобразует видео с различными форматами файлов в MP3 и другие форматы аудио файлов.

Предупреждение! Есть много веб-расширений уже доступны для загрузки / преобразования медиа-файлов из Интернета. однако, мы предпочитаем не использовать такие дополнения, поскольку они могут получить доступ к нашей истории веб-браузера, и это может привести к вторжению в частную жизнь, особенно при работе над деликатными случаями, которые требуют секретности.

Использование онлайн-сервисов должно быть более безопасным при использовании этих двух мер предосторожности:

A. Не предоставляйте информацию при использовании этой услуги (например, электронная почта, номер телефона и т.д..)

1. доступ к таким услугам через vpn соединение (или с помощью tor Browser).

ИНСТРУМЕНТЫ ПОИСКА ФАЙЛОВ

После сбора большого количества файлов в рамках онлайн-расследования, вы можете испытывать трудности с поиском одной конкретной части информации, когда вам это нужно. Все операционные системы имеют встроенную функцию поиска для поиска файлов и папок на диске компьютера. Тем не менее, им не хватает расширенной функции поиска, как те, которые предлагаются некоторые специальные инструменты. Они также, как известно, трудоемкие, особенно при использовании функции поиска Windows на компьютерах со старым оборудованием. (Windows выполняет индексацию фонового поиска и потребляет значительное количество оперативной памяти системы, потому что она выполняет тысячи операций записи на жестком диске, в результате чего замедление работы компьютера; эта проблема явно появляется на Windows Vista.)

Возможность поиска через файлы, которые вы собрали является неотъемлемой частью ваших навыков анализа OSINT. Ваша способность быстро находить файлы с помощью автоматизированного поиска сэкономит значительное время, чем при проведении таких поисков вручную.

Чтобы ускорить поиск файлов на компьютере, необходимо иметь индекс сохраненных файлов. Идея похожа на то, как люди используют поисковые системы. Когда кто-то запрашивает Google для поиска термина, Google будет искать этот термин в своей базе данных индекса. При обнаружении совпадения URL-адреса, связанные с результатами поиска индекса, извлекаются и отображаются в браузере пользователя. Поиск файлов на компьютерах похож. Вы должны иметь индекс всех имен файлов и их расположение на жестком диске компьютера. Список (индекс) будет храниться в базе данных. Всякий раз, когда вы ищете что-то, вы будете запрашивать базу данных вместо того, чтобы просить Windows искать вручную во всех файлах и папках на диске. Это даст вам самые быстрые результаты, особенно если у вас есть миллионы файлов на жестком диске компьютера.

Windows может создать такой индекс, чтобы быстрее найти файлы. Тем не менее, Есть лучшие программы, которые могут сделать работу лучше и имеют более продвинутые функции поиска. Вот некоторые из них:

- *Locate32* (http://locate32.cogit.net): При первом запуске необходимо перейти в меню файлов и выбрать базы данных обновлений. Это позволит создать файл базы данных, который содержит имена всех файлов/ папок вместе с их расположением на всех жестких дисках (см. рисунок4-36).

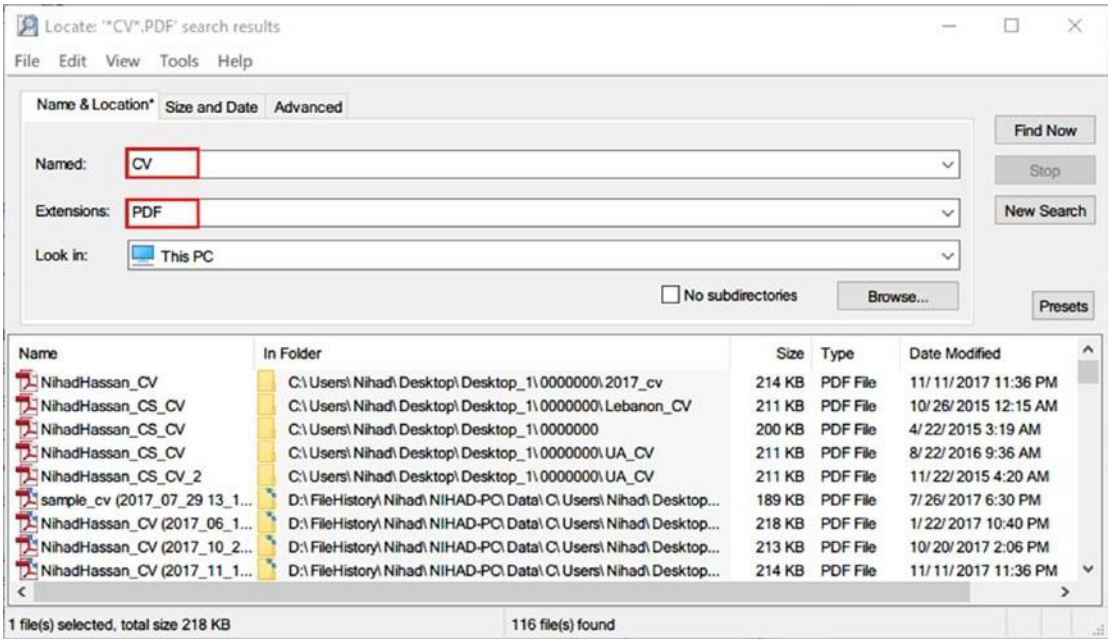

Рисунок 4-36. *Результат поиска наданных 32 образцов*

- *Everything* (www.voidtools.com): Это небольшая программа, которая потребляет очень мало системных ресурсов; он автоматически создает базу данных индексов при запуске и может индексировать файлы очень быстро (для индексации 1 000 000 файлов требуется одна минута) и может искать содержимое файла. Вы можете искать с помощью различных методов, таких как Boolean, regex, подстановочные знаки, типы файлов и макросы.
- *FileSeek* (free edition) (https://www.fileseek.ca): Это использует технологию многопоточности для ускорения поиска и может синхронизировать результаты поиска на разных компьютерах в дополнение к поиску содержимого файла с помощью регулярных выражений.
- *Open Semantic Search* (https://www.opensemanticsearch.org): Эта поисковая система с открытым исходным кодом поставляется с интегрированными исследовательскими инструментами для облегчения поиска, мониторинга, аналитики, обнаружения и интеллектуального анализа текста неоднородные и большие наборы документов и новости. Он может быть установлен на вашем собственном сервере или корпоративном сервере и поставляется с большим количеством отличных функций поиска. Он подходит для групп, проводящих исследования OSINT по большому объему наборов данных.

Итоги

В этой главе мы подробно рассмотрели, как использовать основные и передовые методы поисковой системы, чтобы найти информацию в Интернете. Хотя большая часть вашей работы в этой главе была сосредоточена на извлечении данных из поверхностного интернета, мы показали методы извлечения данных из глуб и предоставили прямые ссылки на различные глубокие веб-хранилища для извлечения информации из нее.

Основные поисковые системы позволяют своим пользователям искать мультимедийный контент, такой как видео и изображения. Тем не менее, существуют специализированные поисковые системы для серверов FTP и мультимедийного контента, которые могут вернуть еще больше результатов. Имейте в виду, что изображения и видео, извлеченные из Интернета, могут содержать полезную информацию, связанную с ними, известную как *метаданные,* которые должны быть извлечены в первую очередь. Эти файлы также должны быть исследованы с помощью специализированных инструментов,

чтобы убедиться, что они не были манипулированы каким-либо образом, прежде чем считать их действительными.

В следующей главе, мы будем продолжать наше обсуждение методов поиска в Интернете, но там мы сосредоточимся на использовании различных методов и сервисах, чтобы найти информацию о конкретных людей, использующих социальные медиа-сайты и другие специализированные люди поиска двигателей.

Примечания

i. Netcraft, “January 2017 Web Server Survey” December 05, 2017 https://news.netcraft.com/archives/2017/01/12/january-2017-web-server-survey.html ii. WWW Size, “The size of the World Wide Web (The Internet)”

December 05, 2017 www.worldwidewebsize.com iii. Smart insights “Search Engine Statistics 2017” December 05, 2017 https://www.smartinsights.com/search-engine-marketing/ search-engine-statistics

iv. IEEE, “FTP: The Forgotten Cloud” December 05, 2017 https://www.computer.org/csdl/proceedings/ dsn/2016/8891/00/8891a503.pdf

Глава 5

Социальная медиа разведка

В современную цифровую эпоху редко можно встретить человека, подключенного к Интернету, у которого нет аккаунта на одном или нескольких сайтах социальных сетей. Люди используют социальные сайты для общения, игры, магазин, общаться в Интернете, и искать информацию обо всем, что вы можете себе представить. Facebook, Twitter, YouTube, LinkedIn и Google стали неотъемлемой частью нашей жизни, и сотни миллионов людей ежедневно проводят на этих платформах значительное количество времени.

Проверьте эти статистические данные о глобальном использовании социальных медиа сайтов:

- По состоянию на октябрь 2017 года общая численность населения мира составляла 7,6 миллиарда человек. [я]Из них 3,5 миллиарда человек имеют подключение к Интернету, и 3,03 миллиарда из этих подключенных пользователей имеют активное присутствие на одной или нескольких социальных медиа-платформы.[ii]
- Каждый пользователь Интернета имеет в среднем семь учетных записей в социальных сетях.[iii]
- Facebook имеет 2,07 миллиарда активных пользователей в месяц по состоянию на третий квартал 2017 года.[iv]
- По состоянию на третий квартал 2017 года, Twitter имеет 330 миллионов активных пользователей в месяц.
- По состоянию на апрель 2017 года, LinkedIn имеет 500 миллионов пользователей в 200 странах.[v]

Социальные медиа сайты открывают многочисленные возможности для любого расследования из-за огромного количества полезной информации, которая может быть найдена на них. Например, вы можете получить много личной информации о любом человеке по всему миру, просто проверив страницу этого человека на Facebook. Такая информация часто включает в себя интересующие лица связи на Facebook, политические взгляды, религия, этническая принадлежность, страна происхождения, личные изображения и видео, имя супруга (или семейное положение), дома и рабочие адреса, часто посещаемых местах, социальной деятельности (например, посещение спорта, театра и ресторана),

N. A. Hassan and R. Hijazi, *Open Source Intelligence Methods and Tools*, https://doi.org/10.1007/978-1-4842-3213-2_5

история работы, образование, важные даты событий (такие как дата рождения, дата окончания, дата отношений, дата отношений, или дата, когда работа неурочная / или начата новая работа), и социальные взаимодействия. Все это можно найти, например, в одном профиле Facebook. Facebook также помогает стороннему наблюдателю понять, как тот или иной пользователь Facebook воспринимает жизнь, просто проверяя текущую деятельность пользователя и социальные взаимодействия.

Многие оценки показывают, что 90 процентов полезной информации, полученной разведывательными службами, поступает из открытых источников (OSINT), а остальная часть поступает из традиционной скрытой разведывательной разведки. Службы безопасности собирают информацию оптом с социальных сайтов, чтобы получить представление о возможных будущих событиях по всему миру и профилировать людей в национальном масштабе.

Помимо сбора разведданных, правоохранительные органы используют сайты социальных сетей в качестве следственных ресурсов для борьбы с преступлениями. Например, проверка страницы подозреваемого в Facebook, а также страниц его родственников и друзей – может раскрыть важную информацию об уголовном деле. Иногда подозреваемый может быть анонимным, но полиция может сфотографировать его, снятые камерами наблюдения. В таких случаях полиция использует сайты социальных сетей для привлечения общественности к выявлению подозреваемых. Социальные сайты также могут быть использованы для отслеживания и обнаружения подозреваемых в дополнение к пониманию их поведения. Однако имейте в виду, что использование информации, собранной с сайтов социальных сетей в судебном деле, как правило, допускается в этих двух условиях:

- При получении разрешения от суда на сбор информации о конкретном пользователе, судебный приказ отправляется на сайт социальной сети для официального передачи информации властям.
- Если информация доступна публично (например, публичные сообщения, изображения или видео), то правоохранительные органы могут приобрести ее без разрешения, что является сутью концепции OSINT.

Данные разведки, собранный из социальных сетей, также могут быть полезны в корпоративном мире. Например, работодатели могут провести проверку потенциальных кандидатов, прежде чем предлагать им вакансию. То же самое относится и к страховым компаниям и банкам, прежде чем предлагать своим клиентам некоторые услуги (например, договор страхования или банковский кредит). Глобальные компании, работающие в разных странах, должны иметь некоторую форму разведки о новых рынках, прежде чем входить в них. Действительно, эксплуатация социальных сетей интегрировалась в большинство предприятий для поддержки процесса принятия решений.

Предупреждение! Использование информации, опубликованной на социальных сайтах для получения информации о перспективе сотрудника, должны быть обработаны тщательно в соответствии с законом, чтобы избежать инициирования претензии дискриминации со стороны потенциального сотрудника.

В этой главе мы покажем иследователям, как найти информацию на сайтах социальных сетей. Есть множество инструментов и онлайн-сервисов, чтобы выйти за рамки основных функций поиска, доступных для каждого социального сайта. Мы продемонстрируем, как использовать такие услуги / инструменты для агрегирования информации о любой цели в Интернете, но прежде чем мы начнем нашу дискуссию о том, как получить информацию из самых популярных социальных медиа-сайтов, мы сначала объяснить термин *социальных медиа разведки* и дифференцировать между различными типами социальных медиа сайтов в настоящее время.

Что такое социальные медиа разведки?

Разведка социальных сетей (SOCMINT) ссылается на информацию, собранную с социальных медиа-платформ. Ресурсы, доступные на сайтах социальных сетей, могут быть открыты как для общественности (например, публичные посты на Facebook), либо частные. Частная информация не может быть доступна без соответствующего разрешения (например, личные сообщения Facebook или сообщения, которыми делятся друзья). Существует дискуссия между защитниками конфиденциальности и другими экспертами по безопасности о том, является ли информация, доступная на сайтах социальных сетей, OSINT. Хотя большинство социальных медиа-сайтов требуют, чтобы их пользователи регистрировались перед доступом к содержимому сайта в полном объеме, многие опросы показывают, что пользователи социальных сетей ожидают иметь некоторую форму конфиденциальности для своей деятельности в Интернете (даже при размещении контента с публичным доступом).

Тем не менее, эксперты по безопасности обычно считают, что информация, распространяемый на сайтах социальных сетей, принадлежит к домену OSINT, поскольку она является общедоступной информацией, распространяемой на общедоступных онлайн-платформах, и поэтому может быть использована в различных целях.

Примечание! Многие штаты США (около 25 штатов в 2017vi) ввели различные ограничения в отношении доступа работодателей к счетам работников (заявителей или сотрудников) в социальных сетях. наблюдается-тайно- так или иначе.

Существуют различные типы социальных медиа-сайтов, но прежде чем перечислить их, давайте сначала посмотрим, какой контент люди могут публиковать на платформах социальных сетей, чтобы узнать типы информации, которую вы можете ожидать, чтобы собрать.

Типы контента в социальных сетях

Помимо просмотра контента, люди взаимодействуют с социальными сетями для различных целей. Ниже приведены общие взаимодействия, используемые в различных социальных медиа-сайтах:

- *Сообщение/комментарий*: Люди получают доступ к социальным сайтам, чтобы размещать или писать абзацы текста, которые могут быть замечены другими пользователями. Каждая социальная платформа имеет свое название. На Twitter это называется *чирикать*, в то время как на Facebook это называется *сообщение* или *комментарий* при комментировании на другой пользователь пост. Этот текст можно комбинировать с изображениями, видео и URL-адресами. Посмотреть рисунок 5-1 для примера публикации LinkedIn.

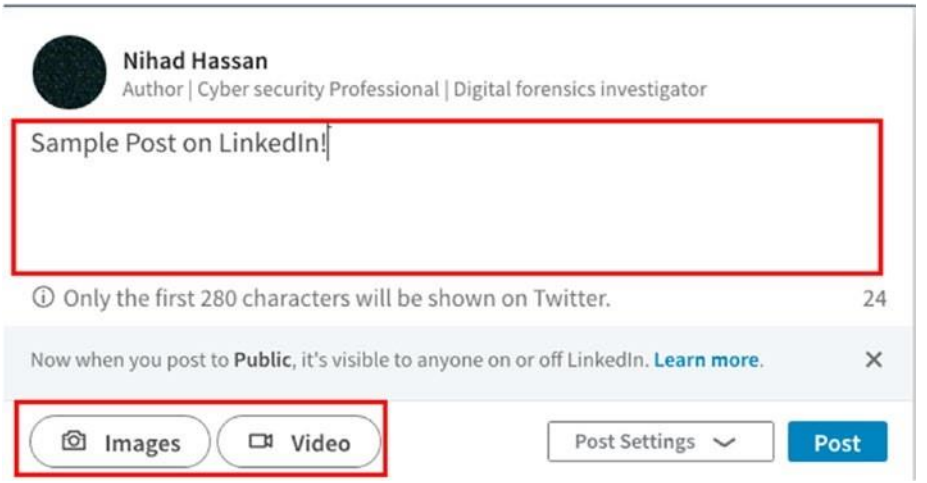

Рисунок 5-1. *Пример поста в LinkedIn, который может быть связан с изображением или видео. Тот же пост также может быть общим на Twitter (который требует подключения вашей учетной записи Twitter с вашим профилем LinkedIn).*

- *Ответ*: это текстовое сообщение (также может быть изображение, видео или URL), которое отвечает на сообщение другого пользователя, статус обновления или комментарий.
- *Мультимедийный контент (изображения и видео)*: Мультимедиа популярен; пользователь может загрузить видео или изображение в рамках своего поста. Многие социальные платформы позволяют своим пользователям загружать несколько изображений/ видео для формирования альбома. Прямые трансляции также доступны на многих социальных платформах, таких как Facebook и YouTube. Эта функция позволяет пользователю транслировать видео в прямом эфире и отображать запись в своих профилях для последующего просмотра.

- *Социальные взаимодействия*: это суть социальных медиа-сайтов, где люди подключаются к сети, отправляя / отвечая на запросы друзей, отправленные их друзьями, коллегами по работе и учебе, соседями по комнате, соседями, членами семьи и любимыми знаменитостями или актерами. Набор онлайн-отношений формирует так называемое *социальные сети*.

- *Метаданные*: Результаты из суммы взаимодействия пользователей с социальной платформой. Примеры включают дату и время загрузки видео / изображения, дату и время принятия запроса на добавление в друзья, данные геолокации, если включено, загруженного мультимедийного файла или публикации, а также тип устройства, используемого для загрузки содержимого (мобильного или стандартного Компьютере).

Онлайн следователи хотят приобрести все эти типы контента, если это возможно, при проведении своих расследований. Эта возможность сделать это зависит от уровня контроля конфиденциальности, установленного каждым пользователем при публикации сообщений/ обновлений в Интернете. Например, невозможно увидеть обновления других людей на Facebook (см. рисунок 5-2), если они ограничивают видимость публикации некоторым кругам друзей или устанавливают ее на "Только я".”

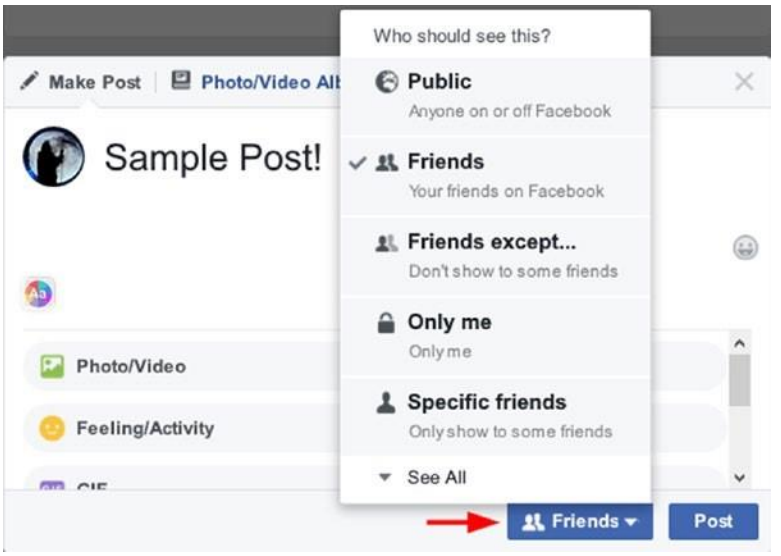

Рисунок 5-2. *Facebook конфиденциальности варианты ограничить видимость поста*

Имейте в виду, что информация, распространяемые на сайтах социальных сетей с семьей или друзьями, не может быть гарантирована конфиденциальной. Например, когда вы делитесь личной фотографией себя с другом, и этот друг делится этой фотографией в публичном статусе, другие могут увидеть вашу личную фотографию, даже если вы поделились ею в частном порядке сначала.

Классификация социальных медиа-платформ

Многие люди используют термины *социальных медиа* и социальных *сетей* взаимозаменяемы для обозначения Facebook, Twitter, LinkedIn, и связанных с ними социальных платформ. Это не абсолютно неправильно, но это не точно, потому что социальные медиа является основой, который содержит другие категории, как "социальные сети", которая содержит сайты, как Facebook. Социальные сети содержат другие типы, которые играют схожие роли в облегчении взаимодействия между людьми в Интернете.

Ниже приведены основные типы социальных медиа классифицируются в соответствии с функцией:

- *Социальные сети*: Это позволяет людям общаться с другими людьми и предприятиями (брендами) онлайн для обмена информацией и идеями. Наиболее очевидными примерами такого типа являются Facebook и LinkedIn. (Последний больше ориентирован на корпоративный мир, но разделяет много аналогичных функций с Facebook.)

- *Фото sharing*: Такие веб-сайты предназначены для обмена фотографиями между пользователями в Интернете. Самыми популярными из них являются Instagram (https://www. instagram.com) и Flicker (https://www.flickr.com).

- *Видео sharing*: Такие веб-сайты предназначены для обмена видео, в том числе прямые видеотрансляции. Самый популярный из них https://www.youtube.com. Обмен мультимедийным контентом возможен через сайты социальных сетей, такие как Facebook (который предлагает прямую видеотрансляцию) и LinkedIn. Тем не менее, видео-сайты обмена, как YouTube.com- предназначены для обмена мультимедийным контентом и содержат ограниченное количество текста в них (в основном позволяет пользователям комментировать загруженные видео).

- *Блоги*: Это тип информационного веб-сайта, содержащий набор постов, относящихся к одной теме или теме, организованных в порядке убывания в соответствии с датой публикации. Первые блоги были основаны на статичном HTML-контенте и созданы/управляются одним автором. С продвижением веб-инструментов публикации и появление web 2.0 технологии, которая упрощает размещение контента в Интернете

нетехнических пользователей-блог использование было повышено и стать доступнымдля для всех, кто хочет иметь место в Интернете, чтобы поделиться своими идеями. Самые популярные блог-платформы WordPress (https:// wordpress.com) и Blogger (https://www.blogger.com), который работате от Google.

- *Микроблог*: это позволяет пользователям публиковать короткий текстовый абзац (который может быть связан с изображением или видео) или ссылку (URL), которая будет совместно с другой аудиторией в Интернете. Самыми популярными микроблогами являются Twitter (https://twitter.com) и Tumbler (https://www.tumblr.com).
- *Форумы (доска сообщений)*: это один из старейших типов социальных медиа. Это позволяет пользователям обмениваться идеями, мнениями, опытом, информацией и новостями и обсуждать их с другими пользователями в форме размещенных сообщений и ответов. Форумы обычно приходят организованные в темы. Самыми популярными из них сейчас являются Reddit (https://www.reddit.com) и Quora | (https://www.quora.com).

- *Социальные игры*: Это относится к игре онлайн с другими игроками в разных местах. Социальные игры позволяют пользователям сотрудничать из разных частей по всему миру, чтобы сформировать команды или бросить вызов другим людям/ группам. Facebook имеет много социальных игр, которые могут быть воспроизведены в веб-браузере пользователя; Вы можете проверить их на https://www.facebook.com/games.
- *Социальные закладки*: Эти веб-сайты предлагают аналогичную функцию типичной закладки вашего веб-браузера. Тем не менее, они позволяют делать это в Интернете и поделиться своими интернет-закладок среди ваших друзей в дополнение к добавлению аннотаций и тегов к сохраненным закладкам. Многие службы закладок позволяют своим пользователям синхронизировать закладки с любым устройством или браузером, делая ваши закладки доступными на нескольких устройствах одновременно. Самые популярные услуги закладок - Atavi (https://atavi.com), Pinterest (www.pinterest.com), и Pocket (https://getpocket.com).
- *Обзор продуктов/ сервисов*: Эти веб-сайты позволяют своим пользователям просматривать- дать обратную связь- о любом продукте или сервисе, которые они использовали. Другие люди найдут такие отзывы полезными, чтобы помочь им в их решениях о покупке. Самые популярные сайты обзор Yelp (https://www. yelp.com) и Angie's List (www.angieslistbusinesscenter.com).

Популярные сайты социальных сетей

Не все сайты социальных сетей имеют одинаковую популярность среди пользователей по всему миру. На рисунке 5-3 показана статистика, опубликованная Statista.com в сентябре 2017 года, в списке самых популярных сайтов социальных сетей, ранжированных по количеству активных пользователей (в миллионах). Характер социальных медиа-сайтов быстро меняется, поэтому ожидается, что в течение года такая статистика будет часто меняться. Тем не менее, ожидается, что основные игроки продолжат доминировать на рынке социальных медиа в ближайшем будущем.

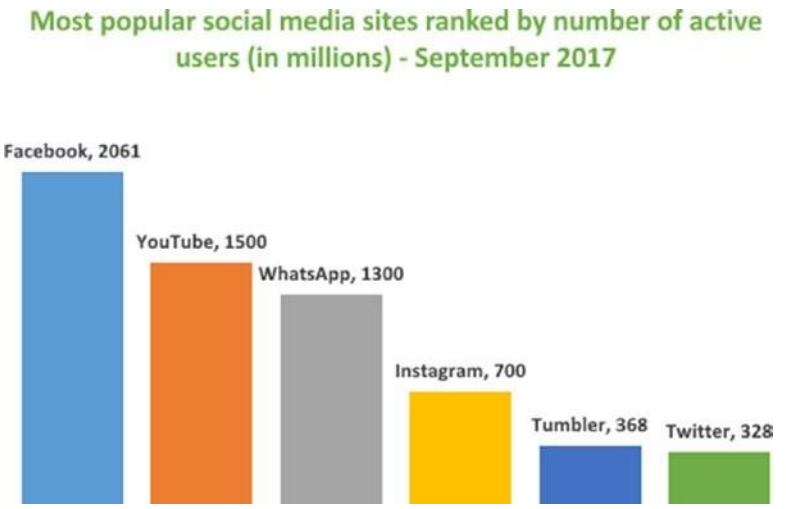

Рисунок 5-3. *Популярные сайты социальных сетей (источник: https://www.statista.com/ statistics/272014/global-social-networks-ranked-by-number-of-users/)*

Исследование социальных медиа сайтов

В этом разделе мы обсуждаем самые популярные сайты социальных сетей и демонстрируем, как проводить более разумный поиск по каждому из них, чтобы извлечь полезную и скрытую информацию, которую нельзя получить, используя стандартную функцию поиска каждого сайта. Основное внимание будет уделено сайтам социальных сетей, поскольку поиск в мультимедийном контенте был рассмотрен в предыдущей главе. Эти сайты содержат огромное количество личной информации и социальных взаимодействий, которые могут быть полезны для онлайн-исследований.

Facebook

Facebook (www.facebook.com) является самым популярным сайтом социальной сети с самой большой активной базой пользователей на Земле. Facebook в настоящее время имеет более 2 миллиардов активных пользователей по всему миру. Facebook является американской компанией; Основанная Марком Цукербергом в 2004 году, она была первоначально разработана для студентов Гарвардского университета для обмена социальной информацией.

Тем не менее, позже она расширила свое членство, приняв студентов из различных университетов США. В 2006 году Facebook разрешил любому человеку старше 13 лет с действительным адресом электронной почты стать зарегистрированным участником и пользоваться его услугой.

Facebook настолько популярен, что любой, кто имеет подключение к Интернету по всему миру, как ожидается, есть учетная запись Facebook! Facebook облегчает обмен различными типами онлайн-контента (изображения, видео, текстовые сообщения, прямая трансляция, регистрация) между людьми, что делает его популярным среди различных групп пользователей по всему миру.

Много информации можно найти в каждой учетной записи пользователя Facebook. Например, чтобы создать учетную запись Facebook, необходимо предоставить свою электронную почту (или номер телефона) в виде имени пользователя, пароля, даты рождения и пола. После создания и активации учетной записи Facebook вы можете добавить больше информации о себе, например, о работе и образовании, местах, где вы жили, контактной информации (электронная почта, номер телефона, адрес, открытый ключ для получения зашифрованных сообщений), религиозные и политические взгляды, языки, другие социальные аккаунты (Twitter и LinkedIn), ваш личный блог или веб-сайт, семья и отношения, а также другая информация о вас в дополнение к живым событиям.

Facebook позволяет своим зарегистрированным пользователям делать различные социальные взаимодействия, такие как следующие:

- Делитесь обновлениями, фотографиями, видео и данными о геолокации (например, ваше текущее местоположение с помощью функции регистрации) с друзьями.
- Смотрят обновления/сообщения друзей, отвечают комментариями, а также любят или делятся своими обновлениями
- Пригласите своих друзей присоединиться к группам и посетить мероприятия
- Чат с помощью Facebook Messenger и отправка прямых личных сообщений другому участнику Facebook
- Играйте в онлайн-игры в вашем веб-браузере (поддерживаются многопользовательские игры)
- Следите за новостями компании / бренда

- Создание связи с любимыми актерами, знаменитостями и другими общественными организациями
- Используйте учетные данные Facebook для вхотворения в различные службы в Интернете
- Сделать прямые видеотрансляции с помощью Facebook Live(https://live.fb.com)
- Получите поддержку Facebook, которая реализует различные настройки конфиденциальности на весь контент, опубликованный его пользователями, чтобы ограничить видимость контента в зависимости от потребности каждого пользователя

Как уже отмечалось, сумма личной информации и социальных взаимодействий, доступных публично на Facebook, предоставляет огромное количество информации для любого сбора OSINT. Как мы уже говорили, сбор личной информации от Facebook о какой-либо цели зависит от контроля конфиденциальности, установленного для их обновлений и социальных взаимодействий. Тем не менее, многие исследования показывают, что большинство пользователей Facebook не дают много думал о вопросах конфиденциальности при использовании этой платформы.

Объем данных, хранящихся в базе данных Facebook, огромен. Facebook хранит около 300 петабайт данных (в марте 2017 года). [vii] Это равно 300 000 000 гигабайт. Каждую минуту на Facebook выкладывается 510 000 комментариев, обновляется 293 000 статусов и загружается 136 000 фотографий. [viii] Чтобы найти информацию в этих джунглях, Facebook разработала свой собственный механизм поиска для упрощения поиска различных типов контента, генерируемых взаимодействиями его пользователей, и это то, что мы рассмотрим в следующем разделе.

ПОИСК ГРАФИКА FACEBOOK

Facebook предлагает расширенную семантическую поисковую систему, чтобы найти что-либо в своей базе данных, используя естественные фразы на английском языке и ключевые слова. Эта семантическая поисковая система называется Graph Search и впервые была представлена в начале 2013 года; это позволяет пользователям Facebook вводить свои запросы в поле поиска Facebook, чтобы вернуть точные результаты на основе их вопросов / фраз или комбинированных ключевых слов. Вернули результаты довольно информативны и отличаются от традиционного поискового подхода, который работает, возвращая списки ссылок, основанных только на поисковых ключевых словах. Например, можно ввести **Pages liked by my friends** и Facebook вернет список страниц, понравившихся всем вашим друзьям

список, или вы можете просто ввести **Pages liked by ********, замена звездочек наимяпользователя Facebook, чтобы вернуть список страниц, понравившихся указанному пользователю.

Примечание! Вы должны иметь учетную запись Facebook для проведения поисков, используемых в этой главе. целесообразно использовать фиктивный почтовый ящик при создании этой учетной записи, чтобы избежать раскрытия вашей истинной личности при проведении расширенных поисков на Facebook (специально применимыки для правоохранительных органов).

Предупреждение! Политика Facebook запрещает открывать аккаунты с фальшивыми удостоверениями личности. Это надо учитывать при использовании видимых данных Facebook для судебного иска.

Теперь, чтобы использовать поиск на Facebook Graph Search, вам нужно сначала войти в свою учетную запись Facebook, а затем изменить настройки языка учетной записи, чтобы использовать английский язык (US). После этого ваша учетная запись готова к использованию поиска на графике Facebook. Чтобы изменить язык учетной записи Facebook, выполните следующие действия:

1. Войти в свой аккаунт Facebook и нажмите на стрелку вниз, показанную в правом верхнем углу экрана.
2. Нажмите Настройки, чтобы получить доступ к настройкам учетной записи, где вы можете изменить все настройки учетной записи Facebook (см. Рисунок 5-4).

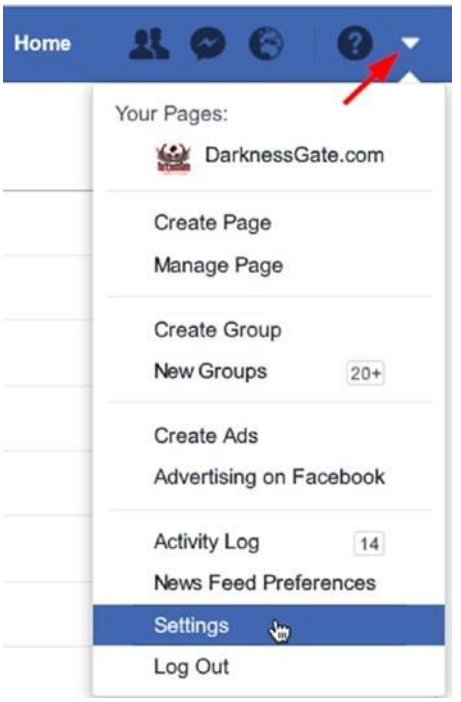

Рисунок 5-4. *Доступ к настройкам учетной записи Facebook*

3. Нажмите Языки на левой стороне страницы, и убедитесь, что параметр "На каком языке вы хотите использовать Facebook в?" Установлен на английском языке (США), как показано на рисунке 5-5.

Рисунок 5-5. *Настройка языка учетной записи Facebook на английский язык (США) для семантической поисковой системы Facebook, известной как Graph Search*

После обновления учетной записи Facebook, чтобы использовать английский (US) язык и таким образом активировать Графический поиск, вы можете ввести в панели поиска Facebook все, что вы хотите искать. Например, вы можете искать людей, друзей вашей цели,

места (города, страны, исторические места), вещи, фотографии, страницы, группы, приложения, события, и рестораны, в дополнение к развлечениям, таким как музыка , фильмы или игры . Как только критерии поиска будут внесены в панель поиска, Facebook покажет список предложений; вы можете выбрать что-то из списка или выбрать вводимый один (см. рисунок 5-6).

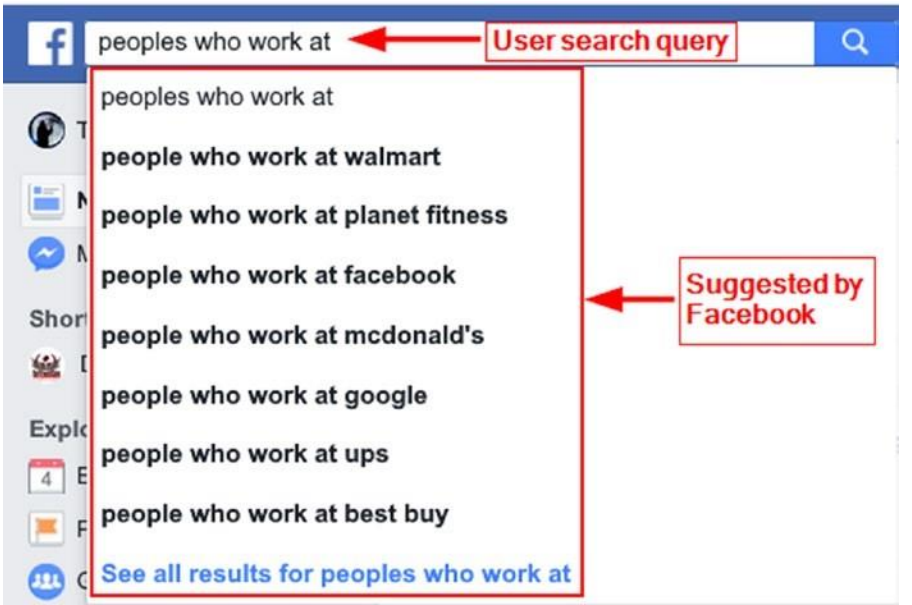

Рисунок 5-6. *Facebook показывает предлагаемые поиски на основе ввода поискового запроса*

Зная, как использовать Facebook Graph Search важно для онлайн следователей использовать Facebook в хранилище данных. Каждая учетная запись Facebook или страница связана с его социальными взаимодействиями пользователей (например, тег, доля, список друзей, работа, университет / школа и образование информации, фильм, песня, события, данные геолокации и места). Следователь должен ввести правильный поисковый запрос, чтобы получить такие результаты. В двух словах, Graph Search поможет вам сопоставить каждый аккаунт Facebook с его связанной деятельностью на Facebook.

Теперь мы дадим несколько примеров Facebook Graph Search запросы, чтобы активировать ваше воображение о том, как построить различные поисковые запросы для получения точных результатов от Facebook.

Для поиска людей на Facebook используйте эти запросы:

- *Поиск людей [Фамилия Имя] которые живут [Город район]*. Вот пример: **people named Nihad Hassan who live in Buffalo, New York**.
- *Люди, которые живут в «городе, государстве» и являются «одинокими/женатыми» и любят «что-то».* Вот пример: **people who work in Seattle, Washington and are single and like Lebanese restaurants**.
- *Люди, которые являются «Имя профессии» и живут в «Городе, государстве». Вот пример:* **People who are Programmer and live in London, UK**.
- *Люди, которым нравится «Имя страницы»* и живут в «Городе». Вот пример:
  people who like apress and live in New York, USA.
- *Люди, которые работают в*«Компании». Вот пример: **people who work at Apress**. Этот запрос может быть уточнен для поиска людей, работающих в компании Apress в качестве авторов: **people who work at Apress as author** (смотрите рисунок5-7).

Рисунок 5-7. *Поиск людей, которые работают в конкретной компании с определенной ролью*

- *Люди, которые живут в «Стране» и любят «Имя*страницы». Вот пример: **people who live in USA and like Al-Qaeda**.

Для поиска определенных страниц на Facebook попробуйте следующие запросы:

- *Страницы под названием «Имя»*. Вот пример: **pages named Al-Qaeda**.

1. *Страницы, понравившиеся по* «Имя». Вот пример: **Pages liked by Mark Zuckerberg**.

- *Страницы понравились* «Профессии». Вот пример: **pages liked by teachers**.

Для поиска профессий, предприятий или служб попробуйте следующие поисковые запросы:

- *Стоматолог в*«Городе». Вот пример: **Dentist in Manhattan, New York**.

- *(Имя профессии) под названием*«Имя». Вот пример: **Teachers named John Walker**.

Для поиска сообщений используйте эти:

- *Сообщения понравились людям, которые любят*«Page». Вот пример: **Posts liked by people who like Apress**.
- *Сообщения понравились людям, которые живут в «городе, государстве» и работают в* «компании». Вот пример: **Posts liked by people who live in Dallas, Texas and work at Google**.
- *Сообщения от «FirstName LastName» с года*. Вот пример: **Posts by Nihad Hassan from the year 2011**.

Подсказка! Мониторинг "почтового времени" цели на Facebook может показать, во сколько человек просыпается каждый день.

Примечание! Использование графика Facebook Поиск может вернуть большое количество результатов. для уточнения результатов поиска можно использовать фильтры поиска графика на левой стороне страницы (см. рисунок5-8).

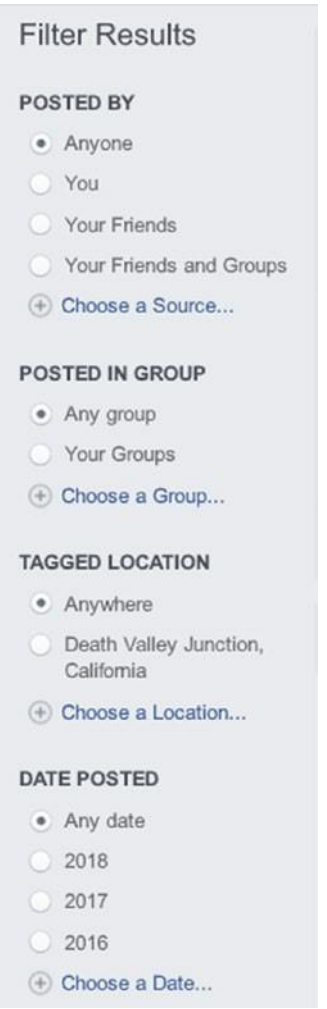

Рисунок 5-8. *Фильтры поиска графиков Facebook помогут вам уточнить результаты поиска*

Чтобы использовать расширенный поиск на графике Facebook, необходимо знать идентификатор профиля Facebook (страницы и группы также имеют свои собственные идентификаторы). Чтобы получить идентификатор профиля Facebook цели вручную, сделайте следующее:

1. Перейдите на страницу цели на Facebook, нажмите правой кнопкой мыши на страницу и выберите Источник страницы просмотра (см. Рисунок 5-9).

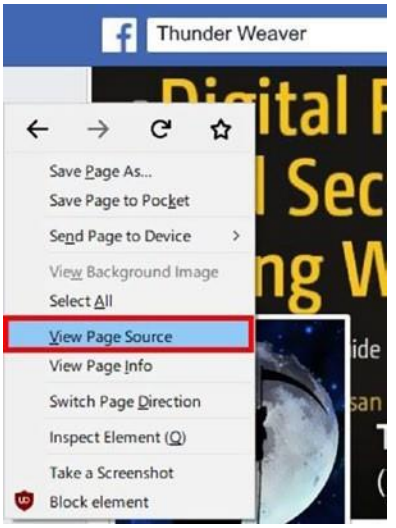

Рисунок 5-9. *Просмотр HTML-кода на странице Facebook, чтобы найти идентификатор профиля*

2. Нажмите на Ctrl-F (в IE, Firefox, Chrome или Opera) для поиска в исходном коде HTML. Введите **профиль в** качестве критериев поиска. Номер рядом с ним является целевой Facebook уникальный профиль ID (см. Рисунок5-10).

Рисунок 5-10. *Поиск уникального идентификатора профиля Facebook*

После того, как узнать, как найти идентификатор профиля Facebook (то же самое относится и к страницам facebook и группам), давайте использовать его для поиска списка публично просматриваемых фотографий цели. На этот раз вы введете свой поисковый запрос в адресную строку браузера вместо того, чтобы использовать панель поиска Facebook.

Веб-адрес Поиска графика всегда начинается с этого: https://www.facebook.com/поиск/.

Для поиска фотографий, понравившихся целевому пользователю Facebook, введите запрос, отображаемый на рисунке 5-11, в адресной строке браузера (выделенное число указывает на идентификатор профиля facebook цели).

Рисунок 5-11. *Поиск фотографий, понравившихся целевому пользователю Facebook*

Таким же образом можно изменить запрос, чтобы вернуть фотографии, которые были отмечены целевым пользователем.

Примечание! заменить номер 100003886582037 с вашим целевым идентификатором профиля Facebook во всех следующих запросах.

Использовать https://www.facebook.com/search/100003886582037/photos-commented чтобы найти фотографии прокомментировал целевой.

Use https://www.facebook.com/search/100003886582037/photos-tagged найти все фотографии с тегами целевого профиля.

Фотографии запроса возвращают все фотографии, загруженные профилем цели в дополнение ко всем фотографиям, где цель была помечена или упомянута; рассмотрите этот запрос как контейнер для отображения всех общедоступных фотографий целевого профиля: https://www.facebook.com/ search/100003886582037/photos-of.

Примечание! Фотозапросы Facebook также работают для Видео. заменить фотографиивидео в поисковом запросе.

Чтобы просмотреть список мест, посещенных вашим целевым профилем, используйте это: https://www.facebook. com/search/100003886582037/places-visited.

Чтобы увидеть список мест, понравившихся целевому профилю, используйте этот: https://www.facebook.com/ search/100003886582037/places-liked.

Чтобы увидеть список мест, зарегистрированных в, используйте это: https://www.facebook.com/ search/100003886582037/places-checked-in.

Чтобы увидеть список друзей цели (если он установлен для общественности), используйте следующее: https://www.facebook.com/search/100003886582037/friends. Это также покажет, когда каждая дружба Facebook началась (см. Рисунок 5-12).

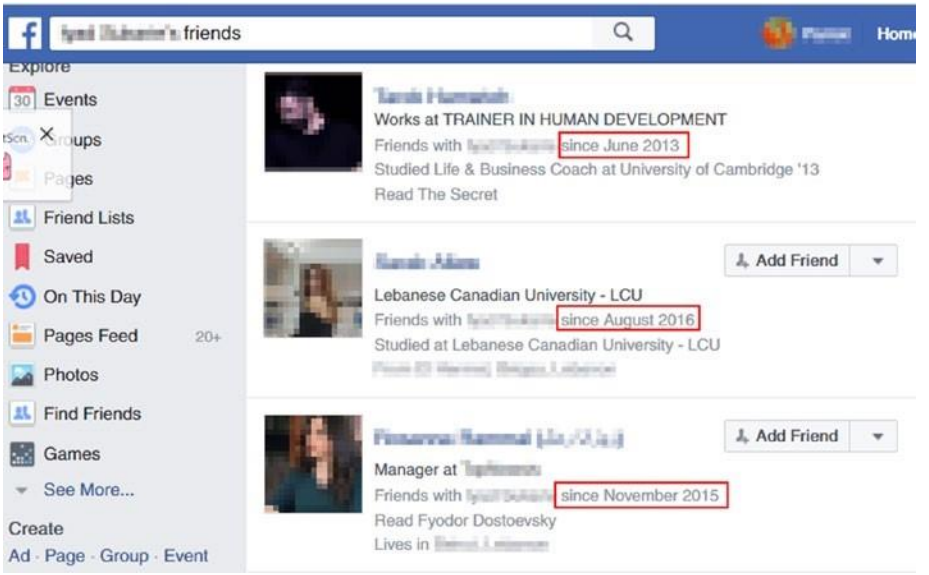

Рисунок 5-12. *Исследование списка друзей Facebook цели покажет, когда начались отношения дружбы с целью*

Чтобы просмотреть список мероприятий, в которых присутствует целевой профиль, используйте это: https://www.facebook. com/search/100003886582037/events-joined.

Если ваша целевая учетная запись Facebook не ограничила список друзей из общего доступа, вы также можете провести следующие запросы в ваших целевых друзьях на Facebook:

- Чтобы просмотреть список фотографий, загруженных целевыми друзьями, введите следующий запрос: https://www.facebook.com/search/100003886582037/friends/photos-uploaded.
- Чтобы увидеть список фотографий, понравившихся друзьям-мишеням, используйте это: https://www.facebook.com/search/100003886582037/friends/photos-liked.
- Чтобы увидеть список фотографий, которые комментируют друзья-мишени, используйте это: https://www.facebook.com/search/100003886582037/friends/photos-commented.

- Чтобы увидеть места, которые посещают целевые друзья, используйте этоhttps://www. facebook.com/search/100003886582037/friends/places-visited.
- Чтобы увидеть друзей целевых друзей, используйте это: https://www.facebook. com/search/100003886582037/friends/friends.

Примечание! Прежде чем использовать поиск графика Facebook, всегда начинайте поиск на Facebook, используя полное имя вашей цели (если оно у вас есть). хотя Facebook запрещает регистрацию с фальшивыми именами, существует большое количество учетных записей Facebook с фальшивыми именами, поэтому вы не всегда можете зависеть от поиска по имени. в качестве второго варианта, попробуйте найти с помощью адреса электронной почты facebook цели и номер телефона (если они у вас есть). пожалуйста, обратите внимание, что поиск с использованием электронной почты и телефонных номеров не даст результаты, если установлен контроль конфиденциальности цели, чтобы предотвратить их появление при поиске на Facebook . Если ничто не дает требуемых результатов, попробуйте получить доступ к известным ассоциированным профилям целевой цели; Вы можете найти что-то, что может помочь вам найти реальный профиль вашей цели.

ДРУГИЕ ПОЛЕЗНЫЕ КОМАНДЫ ПОИСКА ГРАФИКА FACEBOOK

Для поиска всех людей, которым нравится конкретная страница на Facebook, введите запрос, показанный на рисунке 5-13, в панели адресов браузера, заменив выделенный номер идентификатором профиля целевой страницы.

Рисунок 5-13. *Поиск всех людей, которым нравится конкретная страница на Facebook*

ОТСЛЕЖИВАНИЕ ФОТОГРАФИЙ, ЗАГРУЖЕННЫХ ИЗ FACEBOOK В ЕГО ПРОФИЛЬ ИСТОЧНИКА

Когда пользователь загружает фотографию на Facebook, его имя будет изменено после сохранения его в базе данных Facebook. Новое имя обычно состоит из трех длинных чисел, а файл будет находиться в формате JPG. Второй номер имеет отношение к профилю Facebook, которые загружают это изображение на Facebook первоначально. Чтобы узнать источник учетной записи Facebook за это изображение, скопировать второй номер и вставить его после facebook веб-адрес www.facebook.com/. Это должно принять вас к профилю источника Facebook (см. Рисунок 5- 14). Для того чтобы этот совет работал, изображение интереса должно быть опубликовано публично или ваша учетная запись Facebook должна быть другом целевого профиля, если изображение было первоначально совместно с кругом друзей.

Рисунок 5-14. *Отслеживание изображения, загруженного из Интернета в его источник Загрузчик аккаунта Facebook*

Примечание! Многие пользователи Facebook используют одни и те же фотографии профиля на разных социальных платформах. для проведения обратного поиска изображений, чтобы увидеть, где конкретное фото профиля Facebook появляется в Интернете, используйте услугу, как Google images (https:// images.google.com) или tineye (www.tineye.com).

ИСПОЛЬЗОВАНИЕ GOOGLE ДЛЯ ПОИСКА КОНТЕНТА FACEBOOK

Google может быть эффективно использован для поиска в Facebook общедоступных страниц с помощью оператора поиска *site:facebook.com,* который ограничивает поиск Google только указанный веб-сайт. Другие продвинутые поисковые операторы Google, уже охваченные в главе 4, могут быть использованы для поиска точной информации в Facebook.Посмотреть рисунок 5-15 например,

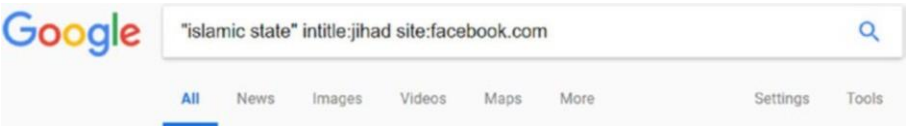

Figure 5-15. *Using a Google advanced search operator to locate information within Facebook*

ПОИСК ХЭШТЕГОВ НА FACEBOOK

Для поиска сообщений, фотографий или страниц с хэштегами введите адрес Facebook в адресной строке веб-браузера с последующим указанным хэштегом, как в https://www.facebook.com/*hashtag*.

Например, ввод **https://www.facebook.com/hashtag/Terrorism** будет отображать связанные с ними содержимое на Facebook, которые несут*#Terrorism* hashtag.

Совет! Вы можете искать несколько социальных медиа-сайтов (Facebook, Twitter, pinterest, instagram) для конкретного хэштега, перейдя к https://www.hashatit.com.

ИСПОЛЬЗОВАНИЕ АВТОМАТИЗИРОВАННЫХ СЛУЖБ ДЛЯ ОБЛЕГЧЕНИЯ ПОИСКА ГРАФИКА FACEBOOK

Поиск с помощью Facebook Graph Поиск легко; Вам нужно использовать свое воображение и создавать запросы, которые наилучшим образом соответствуют вашим потребностям. Есть онлайн-сервисы, которые облегчают использование Graph Search; всё, что вам нужно сделать, это ввести целевое имя пользователя Facebook или идентификатор профиля, и онлайн-сервис будет проводить расширенные поисковые запросы- уже обсуждается для вас (конечно, только общедоступной доступной информации появится). Ниже приведены самые популярные генераторы поиска на Facebook Graph.

Сканер Facebook

Этот веб-сайт (https://stalkscan.com) позволяет исследовать общедоступную информацию любого пользователя Facebook. Чтобы воспользоваться этой услугой, введите URL-адрес Facebook целевого профиля, и сайт заполнит страницу всеми общественными социальными взаимодействиями, созданными по интересуемому профилю (см. рисунок 5-16).

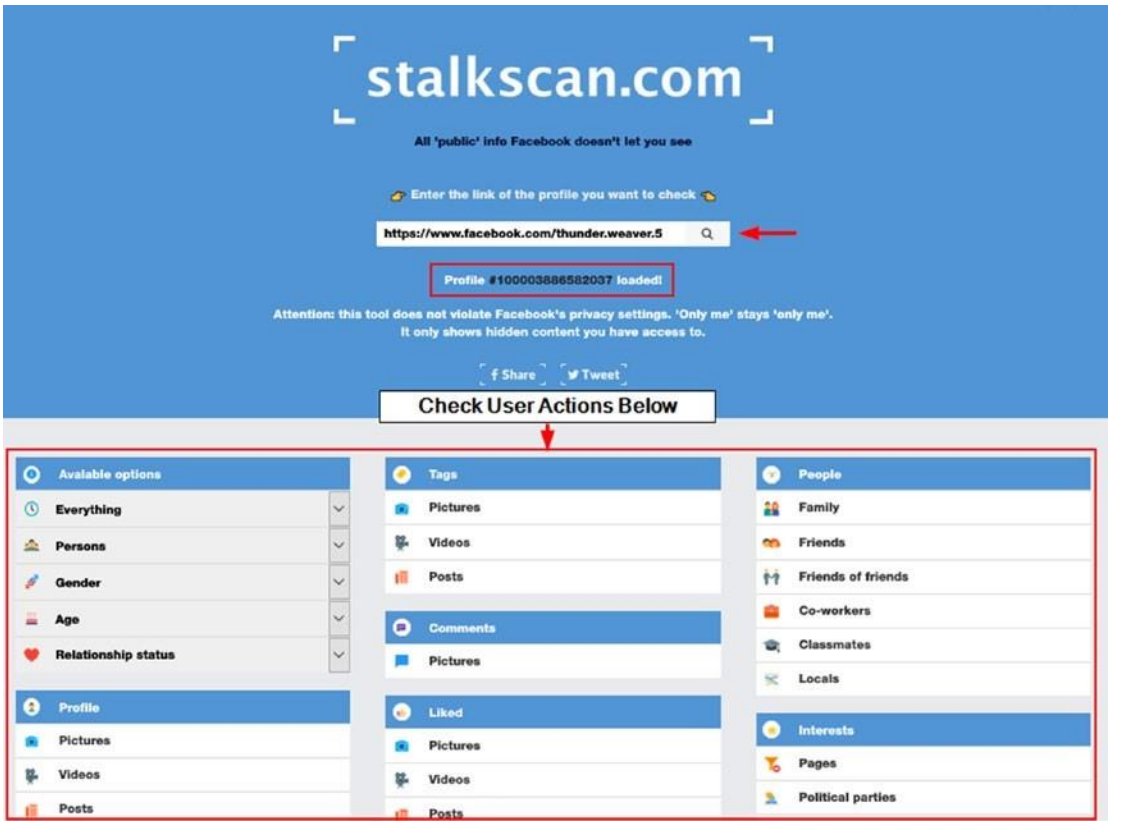

Рисунок 5-16. *Этот сайт может раскрывать общедоступную информацию из любого профиля Facebook*

График

Этот сайт(http://graph.tips) предлагает простой графический пользовательский интерфейс для использования Поиска графика Facebook для поиска общедоступной информации о любом пользователе Facebook. Вы должны предоставить имя пользователя Facebook цели (которое может быть извлечено из посещения страницы профиля цели facebook, как показано на рисунке 5-17),и веб-сайт будет делать оставшуюся работу за вас.

Рисунок 5-17. *Имя пользователя Facebook (выделено) отличается от имени, выбранного пользователем при создании учетной записи (которая появляется в панели поиска Facebook при посещении страницы профиля цели)*

peoplefindThor

Этот сайт (https://peoplefindthor.dk) — генератор поиска на Facebook с наиболее часто используемыми фильтрами (см. Рисунок 5-18).

Рисунок 5-18.*peoplefindThor Facebook поисковый фильтр*

Socmint

Этот сайт(http://socmint.tools) облегчает получение информации с помощью поиска графика Facebook.Поиск графика Facebook постоянно развивается, как и его команды. Успех в использовании этой поисковой системы требует проб и ошибок, чтобы найти запрос, который возвращает лучшие результаты. Это можно достичь, попробовав различные варианты одного и того же запроса (изменение формулировки запроса), чтобы получить желаемый результат. Имейте в виду, что Graph Search может как-то зависеть от вашего друга и общих списков друзей; распространение и разнообразие вашей сети Facebook может повлиять на результаты общего поиска графика.

ONLINE FACEBOOK SEARCH TOOLS/SERVICES

Есть много онлайн-сервисов, которые упрощают процесс получения/анализа информации из учетных записей Facebook. Ниже приведены наиболее полезные:

- *Lookup ID* (https://lookup-id.com): Этот сайт поможет вам найти личные ID на Facebook. Эти ID необходимы для проведения расширенных поисков с использованием Facebook Graph Search.
- *FindMyFbid* (https://findmyfbid.com): Найдите свой личный номер на Facebook ID.
- *Facebook Page Barometer* (http://barometer.agorapulse.com): Этот сайт дает статистику и информацию о конкретных профилях или страницах Facebook.
- *Facebook Search Tool* (http://netbootcamp.org/facebook.html): Проведение расширенных поисков на Facebook.
- *LikeAlyzer* (https://likealyzer.com): Анализ и мониторинг страниц Facebook.
- *Facebook Live video search* (https://www.facelive.org): Показ видео в прямом эфире Facebook braodcast.
- *Wallflux* (https://www.wallflux.com): Этот сайт предоставляет RSS-каналы и обновления для последних сообщений в группах и страницах Facebook.
- *Facebook People/Pages/Places name directory* (https://www.facebook.com/directory/people): Этот сайт списки людей, которые имеют публичные списки поиска доступны на Facebook.

- *Information for Law Enforcement Authorities* (https://www.facebook.com/safety/groups/law/guidelines): Предлагает информацию и правовые руководящие принципы для правоохранительных органов / органов при поиске информации из Facebook и Instagram.
- *Who Posted What?* (https://whopostedwhat.com/staging): Это генератор поиска ключевых слов Facebook. Он ищет сообщения facebook и ограничивает результаты определенной датой.
- *Signal* (https://www.facebook.com/facebookmedia/get-started/signal): Эта услуга используется журналистами для сбора соответствующих тенденций, фотографий, видео и постов из Facebook и Instagram, чтобы включить их в свои медиа-трансляции. Услуга доступна бесплатно для журналистов.

СБОР ЛОКАЛЬНОЙ КОПИИ ЦЕЛЕВЫХ ДАННЫХ FACEBOOK

Если вы собираете доказательства от Facebook для судебного иска, убедитесь, что сохранить копию ваших выводов (доказательства) где-то на вашем компьютере. Facebook управляется его пользователями, и любой публичный пост/фото может быть внезапно удален или закрыт его владельцем. Чтобы сохранить копию публикаций или общедоступных профилей, сохраните страницу с помощью браузера, выбрав файл, а затем сохраните страницу As. Или вы можете просто распечатать указанную страницу на бумаге. Вы также можете взять захват экрана страницы и сохранить его в качестве изображения на локальном компьютере.

Аналитикам OSINT может понадобиться офлайн-версия данных Facebook цели для продвинутого офлайн-анализа или создания отчетов о конкретном профиле или странице пользователя. Родной пользовательский интерфейс Facebook не предоставляет никаких средств для сохранения или печати данных профиля для автономного использования, и сохранение страницы общедоступного профиля в качестве страницы HTML может быть неудобным решением, особенно если вы хотите сохранить длинную страницу. http://le-tools.com разработал инструмент под названием ExtractFace для автоматизации извлечения данных из профилей Facebook. Чтобы использовать этот инструмент, выполните следующие шаги:

1. Скачать инструмент из https://sourceforge.net/projects/extractface/?source=typ_redirect. В настоящее время перед использованием этого инструмента необходимо ЗинединЗидан:

- Вам необходимо получить доступ к своей учетной записи Facebook с помощью издания Firefox ESR, который можно загрузить из https://www.mozilla. org/en-US/firefox/organizations/all/.

1. Вам нужно дополнение MozRepl, которое можно найти вhttps:// addons.mozilla.org/en-US/firefox/addon/mozrepl/. После установив это дополнение, вам нужно запустить его или установить опцию "Активировать на запуске", чтобы запустить его автоматически, когда Firefox запускает (см. Рисунок 5-19).

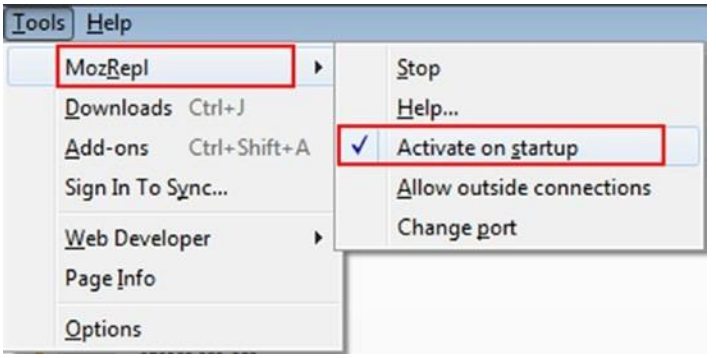

Рисунок 5-19. *Запуск дополнения MozRepl или установка его, чтобы начать автоматически при запуске Firefox*

- И, конечно, вы должны иметь действительный аккаунт Facebook, и вы должны войти в него при использовании этого инструмента.

Предупреждение! отключить брандмауэр или разрешить соединения в порт 4242 перед использованием этого инструмента.

---

2. Чтобы начать сбор данных о Facebook, перейдите в профиль цели и нажмите справа на значок ExtractFace, который находится в панели задач Windows, чтобы запустить меню опций (см. Рисунок 5-20).

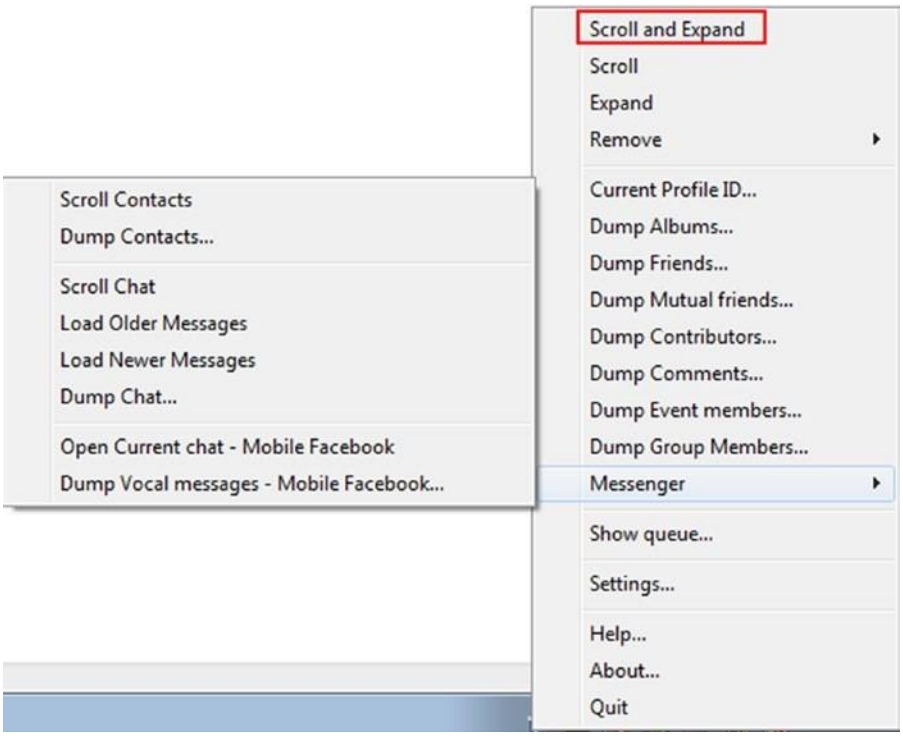

Рисунок 5-20. *Просмотр опций ExtractFace*

3. Первый вариант в меню прокрутки и расширения. Рекомендуется использовать эту опцию, прежде чем собирать друзей цели, сроки и комментарии (сообщения, фотографии и видео комментарии), как это будет автоматизировать процесс прокрутки через всю страницу до конца, прежде чем собирать свои данные. Это необходимо, чтобы избежать получения частичных результатов от этого инструмента при посещении длинных страниц или при медленном подключении к Интернету.

Например, чтобы собрать список друзей на Facebook, перейдите сначала на страницу друга цели на Facebook, нажмите опцию Scroll and Expand, чтобы начать прокрутку по всей странице, и нажмите Dump Friends. Всплывающее меню будет отображаться с просьбой выбрать, где вы хотите хранить файлы дампа. Выберите местоположение и, наконец, нажмите кнопку "Свалка сейчас" (см. Рисунок 5-21).

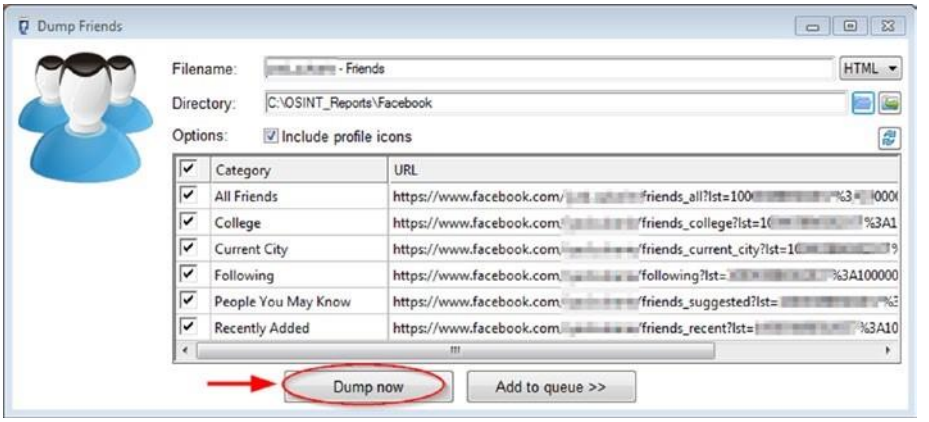

Рисунок 5-21. *Сброс списка друзей Facebook с помощью инструмента ExtractFace*

Большинство функций инструмента ExtractFace работают со всеми людьми, страницами и группами.

Совет! Facebook не уведомляет пользователя, когда кто-то посещает его профиль facebook или просматривает его фото или видео.

если вы столкнетесь с заблокированным профилем Facebook (мы имеем в виду здесь учетную запись, которая ужесточила контроль конфиденциальности, скрывая свой список друзей), вы можете изменить список друзей из "Нравится" и тегов, связанных с этой учетной записью.

Twitter

Twitter является самой популярной платформой микроблогов социальных медиа со средним 330 миллионов активных пользователей ежемесячно (по состоянию на третий квартал 2017 года).[ix] Он начал в 2006 году с основным акцентом на отправку SMS мобильных сообщений связи в Интернете. Twitter разрешил своим пользователям размещать твиты со 140 символами. В 2017 году Twitter расширил количество своих персонажей, чтобы позволить 280 символов. Твиты могут содержать фотографии, короткие видео и URL-адреса в дополнение к тексту.

Twitter в основном используется для подключения людей с теми же интересами на основе размещенного контента. Для создания интернет-сообществ Twitter использует хэштеги (как префикс, #) помогая группировать аналогичные темы. Люди, даже если они не знают друг друга, могут участвовать в разговоре на основе хэштега.

Зарегистрироваться на Twitter, для активации учетной записи необходимо иметь номер телефона или адрес электронной почты. В дополнение к паролю, Twitter не применяет использование реальных имен при регистрации учетной записи. Twitter использует *псевданим* имени для того, чтобы назначить имя пользователя Twitter. В Twitter псевданим начинается с собаки (@) за знаком следуют алфавитные символы без пробелов(e.g., @darknessgate). В Twitter псевдоним может быть использован для упоминания кого-то в публичных твитов или для отправки кому-то личного сообщения. При использованииTwitter, Вы можете иследовать другие общедоступные профили Twitter и их обновления будут отображаться в вашей Хронике.

Twitter позволяет вести прямые видеотрансляции с помощью сервиса Twitter Periscope; Вам нужно использовать официальное приложение Twitter для этого для работы с помощью android или устройства Apple.

Хотя характер Twitter не обеспечивает богатство личной информации, предоставляемой Facebook или LinkedIn,он по-прежнему считается мощной социальной медиа-платформы, которые могут выявить полезную информацию OSINT о некоторых целях при правильном расследовании . Например, данные о геолокации, личные интересы, политические и религиозные взгляды, поездки и друзья могут быть выявлены путем проверки чьей-то учетной записи Twitter.

TWITTER SEARCH

Twitter имеет простую функцию поиска, расположенную в верхней правой части экрана – при использовании веб-интерфейса Twitter – после входа в свой аккаунт Twitter. А
Простой поиск Twitter позволяет выполнять основной поиск в базе данных Twitter. Тем не менее, не стоит недооценивать этот маленький ящик, как вы можете добавить передовые поисковые операторы,по аналогии с Google передовых поисковых операторов,для вашего поискового запроса, чтобы заставить его погрузиться глубоко и вернуть точные результаты, как вы собираетесь видеть следующий.

Лучшее место, чтобы начать поиск twitter, чтобы перейти к щебетать поиск дома наhttps://twitter.com/search-home (см. рисунок 5-22). Отсюда вы можете либо проводить простой поиск (например, поиск профилей Twitter или твитов), либо нажмите

"продвинутый поиск", чтобы перейти на расширенную страницу поиска Twitter, где вы можете установить различные фильтры на поиске.

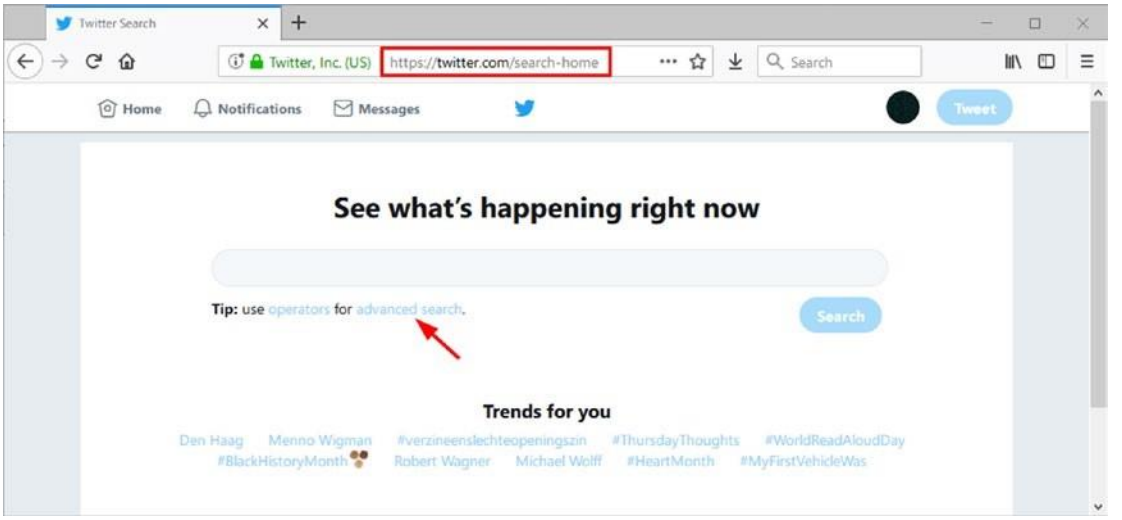

Рисунок 5-22. *Страница домашнего поиска Twitter*

ОПЕРАТОРЫ РАСШИРЕННОГО ПОИСКА TWITTER

База данных Twitter становится все больше с каждым днем. Каждую секунду публикуется около 8000 твитов. [x] Это равно 480000 твитов каждую минуту. Чтобы найти свой путь в этом огромном объеме данных, необходимо использовать передовые поисковые операторы для уточнения поиска. Следующие поисковые операторы могут быть включены в простой поиск Twitter, чтобы найти связанные твиты более точно:

- Используйте оператора "" для поиска точной фразы или слова. Вот пример: **“OSINT intelligence”**.
- Для поиска более одного поискового термина используйте *оператор OR.* Вот пример: **OSINT OR intelligence** (это будет искать твиты, содержащие либо слово *OSINT* или слово разведки или оба).
- Оператор отрицания (-) используется для исключения определенных ключевых слов или фраз из результатов поиска. Вот пример: **virus -computer**. (Это будет поиск твитов со словом *Вирус,* но не связанных с компьютерными вирусами.) Запрос отрицания может быть расширен, чтобы исключить больше слов/фраз с помощью *OR* оператора Пример:

Eiffel tower(trip OR new year OR vacation). Это позволит искать *Eiffel tower* исключать твиты о *trip* и *new year* и *vacation*.

- Для поиска твитов, содержащих определенный хэштег, используйте (#). Вот пример: **#OSINT** (это будет искать все твиты, содержащие #*OSINT*).
- Для поиска твитов, отправленных из определенной учетной записи Twitter, используйте оператора *from*. Вот пример: **from:darknessgate** (это позволит получить все твиты, отправленные из учетной записи darknessgate. Вы можете отфильтровать результаты на основе людей, фотографий, новостей и т.д. (см. Рисунок 5-23).

Рисунок 5-23. *Вы можете использовать фильтры по умолчанию Twitter, чтобы сузить результаты поиска в определенном наборе результатов после использования оператора From*

- Оператор *to* за которыми следуют Twitter никнейм будет отображать все твиты, отправленные конкретному человеку. Вот пример: **to:darknessgate** (это позволит получить все твиты, отправленные в учетную запись *darknessgate*). Вы можете отфильтровать результаты на основе людей, фотографий, новостей и т.д., как мы это делали с оператором from.
- Чтобы найти все твиты, которые ссылаются на конкретную учетную запись Twitter, используйте оператор @ . Вот пример: **@darknessgate** (это позволит получить все твиты, которые ссылаются на учетную запись *darknessgate*).
- Для поиска твитов, отправленных из определенного места, используйте *near* оператор, за которым следует название местоположения. Вот пример: **“happy birthday” near New York** (это будет искать твиты, содержащие точную фразу *happy birthday* и послал из ближнего *New York*).
- Для поиска твитов, отправленных из определенного расстояния от определенного используйте оператор *within*. Вот пример: **near:LA**

within:15mi (это будет возвращение tweets отправлены в 15 милях от Лос-Анджелеса).

- Для поиска твитов, отправленных с определенной даты, используйте оператор since с последующей датой. Вот пример: **OSINT since:2014-11-30** (это вернет все твиты, содержащие *OSINT* и отправленные с 11 ноября 2014 года).
- Для поиска твитов, отправленных до определенной даты, используйте оператор *until*. Вот пример: **OSINT until:2015-11-30** (это вернет все твиты, содержащие *OSINT* и отправленные до даты 30 ноября 2015 г.).
- Чтобы найти все твиты, которые задают вопрос, используйте оператор *?* . Вот пример: **OSINT?** (это вернет все твиты, содержащие *OSINT* с ококнчанием на вопросительный знак).

Оператор *Filter* является мощным для фильтрации результатов на основе различных критериев. Ниже приведены примеры самых популярных фильтров:

- Для поиска в твиттере используйте оператор *filter* с *replies* ключевыми словами. Вот пример:**OSINT Filter:replies** (это вернет все твиты, которые содержат ключевое слово *OSINT* и являются ответами на другие твиты).
- Использование ключевого слова *images* для возвращения твитов, содержащих изображение с твитами . Вот пример:**OSINT Filter:images** (это вернет все твиты, которые содержат ключевое слово *OSINT* и имеют изображение, встроенное в них).
- Чтобы вернуть твиты с видео, встроенного в них, используйте ключевое слово *videos* (аналогично ключу *images*). Вот пример:**OSINT Filter:videos**.
- Вернуть твиты, содержащие загруженное видео, Amplify video, или Periscope video, используй оператор *native_video*. Вот пример: **OSINT filter:native_video** (это вернет все твиты, содержащие ключевое слово поиска *OSINT,* которые имеют загруженное видео, Amplify video, or Periscope video).
- Чтобы вернуть твиты с изображением, и видео, используй оператор *media*. Вот пример: **OSINT Filter:media**.

- Чтобы вернуть твиты с url-адресом новостей, связанным с ними, используйте ключь *news*. Вот пример: **OSINT Filter:news** (это будет возвращать твиты, содержащие *OSINT* в них, которые упоминаются источником новостей).
- Чтобы вернуть твиты, содержащие ссылку (URL) внутри них, используйте ключь *links*. Вот пример: **OSINT Filter:links**.
- Чтобы вернуть текстовые твиты, используйте ключь *text*. Вот пример: **OSINT Filter:text**.
- Для возврата твитов только от проверенных пользователей (проверенные учетные записи имеют синий контрольный знак рядом с их именами), используй ключь *verified*. Вот пример: **OSINT Filter:verified**.

Совет! Вы можете использовать Оператор отрицания(-) с оператором *фильтра,* чтобы изменить уже упомянутые примеры. Например, ввод **OSINT -Filter:images** вернет все твиты, содержащие ключевое слово *поиска OSINT,* но не содержащие изображения, встроенные в них.

- Для поиска видео, загруженного с помощью Twitter Periscope service, используется *Periscope* filter. Вот пример: **OSINT filter:periscope** (это будет искать все твиты, содержащие ключевое слово *OSINT* с URL-адресом видео Periscope).

Для поиска твитов в зависимости от количества лайков, ответов и ретвитов используйте следующие операторы:

- Использовать *min_retweets*: оператора, за которым следует номер. Вот пример: **OSINT min_retweets:50** (это вернет все твиты, содержащие ключевое слово *поиска OSINT,* которые были ретвитнуты по крайней мере 50 раз).
- Использовать оператор *min_replies*:, чтобы вернуть все твиты с числом или более ответов. Вот пример: **OSINT min_ replies:11** (это вернет все твиты, содержащие ключевое слово *поиска OSINT,* которые имеют 11 или более ответов).

- Используйте *min_faves*: затем число, чтобы вернуть все твиты с числом более лайков. Вот пример: **OSINT min_faves:11**
  (это вернет все твиты, которые имеют по крайней мере 11 или более лайков и которые содержат ключевое слово поиска *OSINT*).

- Чтобы исключить ретвиты, используйте -*RT* оператор. Вот пример: **OSINT—RT** (это будет искать все твиты, содержащие ключевое слово *поиска OSINT,* но исключит все ретвиты).

- Для поиска твитов из определенного источника используйте *source* оператор с последующим именем источника. Вот пример: **OSINT source:tweetdeck** (это вернет все твиты, содержащие *OSINT* и отправленные из *tweetdeck* (общие источники *являются tweetdeck*, *twitter твиттер-веб-клиент*).

- Чтобы ограничить результаты, полученные в Twitter на определенном языке, используйте оператор *lang*. Вот пример: **OSINT lang:en** (это вернет все твиты, содержащие *OSINT* только Английский язык). Чтобы просмотреть список языков, поддерживаемых Twitter, перейдите на https://dev.twitter.com/web/overview/languages.

Примечание! Twitter позволяет сэкономить до 25 сохраненных поисков на счет. Чтобы сохранить текущий результат поиска, нажмите кнопку "Больше действий поиска" в верхней части страницы результатов, а затем нажмите кнопку "Сохранить этот поиск.”

Пожалуйста, обратите внимание, что вы можете объединить более одного расширенного поискового оператора Twitter для проведения более точного поиска. Например, тип**“OSINT intelligence” from:darknessgate -Filter:replies lang:en**чтобы получить только твиты, содержащие точную фразу *OSINT intelligence* от пользователя *darknessgate* которые не являются ответами других пользователей и только на английском языке.

СТРАНИЦА РАСШИРЕННОГО ПОИСКА TWITTER

Расширенная страница поиска в Твиттере(https://twitter.com/search-advanced) позволяет установить различные фильтры (язык, местоположение, ключевые слова, дата / диапазон

времени), чтобы вернуть лучшие результаты. Вы можете искать людей, хэштеги и фотографии в любой теме (см. рисунок5-24).

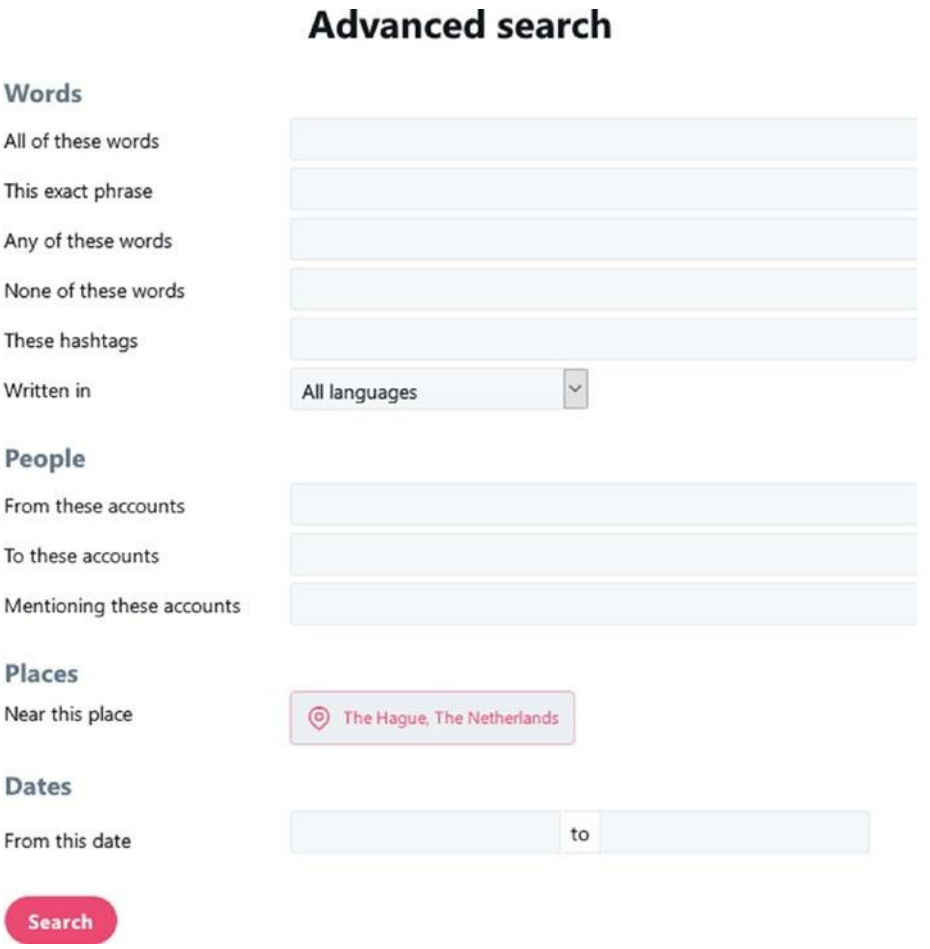

Рисунок 5-24. *Расширенная страница поиска Twitter*

ОНЛАЙН ПОИСК TWITTER ИНСТРУМЕНТЫ/СЕРВИСЫ

Ниже приведены онлайн-сервисы, которые помогут вам найти информацию о Twitter:

- *TweetDeck* (https://tweetdeck.twitter.com): Это приложение панели мониторинга социальных сетей для управления учетными записями Twitter в веб-браузере, таких как Chrome или Firefox. Он популярен среди пользователей настольных компьютеров и дает вам гибкость, чтобы управлять более чем одной учетной записи Twitter с помощью простого, гладкий интерфейс. Он также позволяет совместно использовать учетную запись с вашей командой, не делясь паролем, так как вы можете установить различные разрешения доступа на принадлежащие вам учетные записи. TweetDeck

показывает все действия, связанные с Twitter (деятельность, сообщения, уведомления и поиск) на одном экране. Вы можете добавить на экран больше типов столбцов (например, уведомления, поиск, список, сбор, активность, сообщения, упоминания, последователи, расписание, тренд); прокрутите страницу слева направо, чтобы увидеть всестолбцы. TweetDeck может быть эффективно использован для поиска в Twitter и сохранения текущих поисков, чтобы увидеть любое обновленное содержимое, отраженное автоматически. Вы также можете уточнить свой поисковый запрос с помощью продвинутых операторов поиска Twitter с помощью простого в использовании графического пользовательского интерфейса.

- *All My Tweets* (https://www.allmytweets.net): Просмотр всех общедоступных твитов, размещенных в любой учетной записи Twitter на одной странице.
- *Trendsmap* (https://www.trendsmap.com): Это показывает вам самые популярные тенденции, хэштеги и ключевые слова на Twitter из любой точки мира.
- *Foller* (http://foller.me): Анализ данных публичного аккаунта Twitter (например, публичная информация профиля, количество твитов и подписчиков, темы, хэштеги, упоминание).
- *First Tweet* (http://ctrlq.org/first/): Найти первый твит любого поискового ключевого слова или ссылки.
- *Social Bearing* (https://socialbearing.com/search/followers): Проанализируйте подписчиков Twitter по какой-либо конкретной учетной записи (максимум 10 000 подписчиков могут быть загружены).
- *Twitter Email Test* (https://pdevesian.eu/tet): Это проверяет, используется ли адрес электронной почты для учетной записи Twitter. Полезно знать, есть ли у конкретного пользователя учетная запись Twitter, возможно, под чужим именем.
- *Twicsy* (http://twicsy.com/): Поиск более 7,374,661,011 фотографии Twitter.
- *Follower Wonk* (https://moz.com/followerwonk/analyze): Проанализируйте подписчиков пользователя Twitter.
- *Sleeping Time* (http://sleepingtime.org/): Предсказать график сна любого на Twitter.
- *Simple Twitter Profile Analyzer* (https://github.com/x0rz/tweets_ analyzer): Это скрипт Python.

- *Tag Board* (https://tagboard.com): Поиск хэштегов в Twitter, Facebook и Google.
- *TINFOLEAK* (https://tinfoleak.com): Получите подробную информацию о любом аккаунте Twitter и посмотрите, что происходит с утечками каждой учетной записи. Для получения подробного отчета необходимо предоставить свой адрес электронной почты.
- *TET* (https://pdevesian.eu/tet): Проверить, используется ли введенный адрес электронной почты для учетной записи Twitter.
- *Spoonbill* (https://spoonbill.io): Мониторинг изменений профиля людей, за которыми вы следите в Твиттере.
- *Export Tweet* (https://www.exporttweet.com): Это передовой аналитический сервис Twitter; Вы можете скачать генерируемый отчет для автономного использования. Чтобы разблокировать все функции, вам нужно заплатить.

Предупреждение! Многие сервисы анализа социального медиа могут потребовать от вас, чтобы дать им широкий доступ к вашей учетной записи Twitter. если вы используете фиктивный счет, вы можете сделать это безопасно; в противном случае убедитесь, что не давали разрешения службам, требующим доступа к вашей учетной записи (см. рисунок5-25).

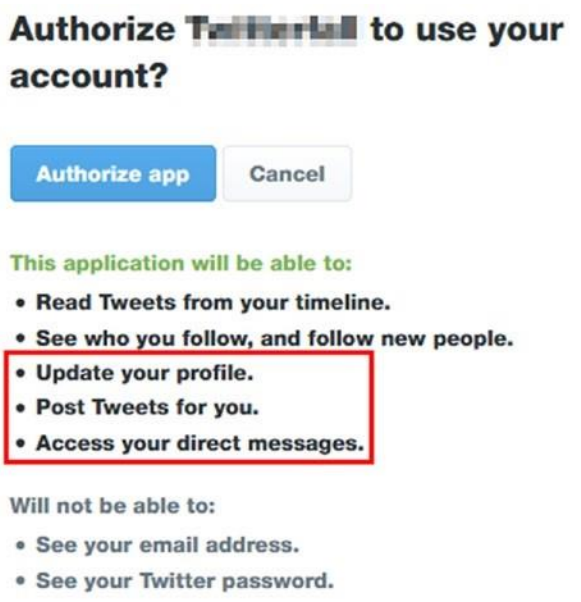

Рисунок 5-25. *Пример предупреждения, выданного Twitter о третьей стороне, которая требует разрешения на широкий доступ к вашей учетной записи*

Google+

Это сайт социальной сети, принадлежащий Google. Теоретически он считается вторым по величине сайтом социальных сетей после Facebook – по количеству зарегистрированных пользователей. (Google имеет более чем 1,2 миллиарда активных ежемесячных пользователей своего бесплатного сервиса электронной почты Gmail.) Тем не менее, мы не можем заключить, что такое же количество пользователей действительно использует социальную платформу Google+.

Самым популярным сервисом, предлагаемым Google, является Gmail, который предоставляет бесплатный сервис электронной почты любому зарегистрированному пользователю Google по всему миру, с отличными функциями с точки зрения надежности, доступности и места для хранения. Для использования любого из продуктов Google (например, YouTube, Google Drive, Gmail, Google Maps, Google Docs) необходимо иметь учетную запись Google.

После регистрации на аккаунт Google вы можете одним щелчком мыши активировать учетную запись Google. Характер этого означает, что фактическое число пользователей Google может быть гораздо меньше, чем объявленная статистика. На самом деле,

исследование, проведенное в 2015 году xi, показывает, что число активных пользователей на Google составляет менее 1 процента от общего числа пользователей Google. Недавняя статистика, проведенная 4 сентября 2017 г., показала, что общее число уникальных ежемесячных посещений Google составляет 34 миллиона, что намного меньше, чем его прямой конкурент Facebook.

Google+ предлагает аналогичные социальные взаимодействия с Facebook; люди могут размещать обновления статуса, и эти обновления могут быть только текст или содержать, в дополнение к тексту-фото, опрос, ссылка (URL), или местоположение. Уровень конфиденциальности каждой публикации может быть скорректирован в соответствии с потребностями пользователя.ПодходGoogleи к управлению конфиденциальностью используется через *круги*. В отличие от Facebook, любой может добавить кого-то в свой круг (который концептуально список людей) без необходимости для другого человека, чтобы добавить запрашивающего обратно. Этот подход аналогичен Twitter; люди могут следовать друг за другом, чтобы увидеть их обновления, но последующие отношения могут происходить только в одном направлении (например, Нихад может следовать Сьюзен, но Сьюзен не должна следовать Nihad).

Имена круга по умолчанию Google' — друзья, семья и Знакомые. Пользователь может создавать столько кругов по мере необходимости и добавлять к ним других людей. При размещении обновлений в Google пользователь выбирает круги, с которыми он хочет поделиться этими обновлениями (см. рисунок 5-26). Пожалуйста, обратите внимание, что круги являются частными, так что другие люди не будут знать, в каком круге вы положили их.

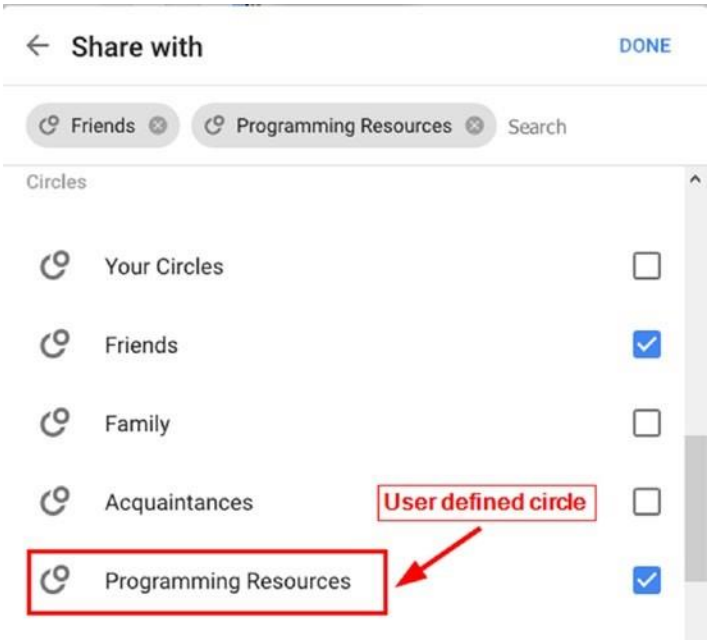

Рисунок 5-26. *Элементы управления конфиденциальностью Google*

Мы не будем углубляться в Google, так как фактическое число активных пользователей значительно невелико. В следующем разделе мы покажем некоторые методы поиска людей в рамках этой платформы.

ПОИСК В GOOGLE+

Как и в других социальных сетях, Google позволяет своим пользователям иметь профиль, который показывает некоторую личную информацию о них. Они могут настроить настройки конфиденциальности каждого раздела профиля. Некоторые сведения о профиле Google также будут отображаться во всех службах Google. Общие данные с другими службами Google включают в себя следующие: контактная информация, образование, места (по аналогии с функцией регистрации Facebook), ссылки (например, личный блог или профиль LinkedIn), личная информация (пол, день рождения), навыки и личные фотографии.

Чтобы начать поиск, начните с панели поиска, расположенной в верхней части страницы, и введите человека, который вы хотите искать. При вводе ввода google'a будет давать свои предложения. Возвратные результаты на следующей странице будут сгруппированы по четырем категориям: сообщества, люди и страницы, коллекции и сообщения (см. Рисунок 5-27).

Рисунок 5-27. *Поиск в Google с использованием встроенной функциональности поиска*

РАСШИРЕННЫЙ ПОИСКОВЫЙ ОПЕРАТОР GOOGLE

Как и Twitter, Facebook и LinkedIn, у Google есть специализированные поисковые операторы, которые помогут вам легко найти точные результаты. Ниже приведены самые популярные из них.

Примечание! Перед использованием продвинутых поисковых операторов Google, вы должны знать, как найти идентификатор профиля Google (имя пользователя).

1. Войти в свой профиль Google.
2. Нажмите на вкладку профиля на левой стороне экрана.
3. посмотрите на Url в адресной панели. набор символов после http://plus.google.com/ ваш Google ID(см. Рисунок 5-28).

Рисунок 5-28. *Извлечение идентификатора Google из URL*

4. чтобы увидеть идентификаторы Google других пользователей, перейдите к каждому профилю пользователя и проверьте Url в адресной панели для целевого идентификатора профиля Google. Пожалуйста, обратите внимание, что многие профили Google по-прежнему используют номера. однако, активные пользователи имеют возможность использовать индивидуальный Url, который отражает их реальные имена. Получение идентификаторов Google, состоящих из букв, похоже на те, с цифрами; Вам нужно скопировать буквы из Урла (начиная с знака).

- Для поиска хэштегов, похожих на Twitter, используйте символ фунта. Вот пример: **#OSINT**.
- Используйте *форму* оператора для поиска сообщений, размещенных конкретным пользователем. Вот пример: **from: 106061931199710505959** (replace номер с вашим целевым идентификатором Google, который также может состоять из писем для некоторых учетных записей).

- Для поиска сообщений по определенному типу содержимого используется оператор поиска. Вот пример: **OSINT has:photo** (это вернет все сообщения, содержащие *OSINT,* которые имеют изображение, встроенное в них).
  Фоточасть может быть заменена на любой из следующих типов: *вложение, опрос, видео, документ, слайды, электронная таблица*.

- Для поиска сообщений до или после определенной даты используйте оператор *до* или *после.* Формат даты должен быть следующим: YYYY-MM-DD. Вот пример: **OSINT before:2017-01-16** | **OSINT after:2018-01-01**.

- Чтобы найти сообщения, комментируемые конкретным пользователем, используйте оператора *комментатора,* за которым следует целевой идентификатор Google ID. Вот пример: **commenter:106061931199710505959**.

- Чтобы найти все сообщения, в которых упоминается конкретный пользователь, используйте оператора *упоминания.* Вот пример: **mention: 106061931199710505959**.

- Для поиска сообщений в определенном сообществе или коллекции используйте *оператора.* Прежде чем привести примеры того, как искать в сообществах/коллекциях, выполните следующие действия, чтобы найти сообщество или идентификатор коллекции в Google.

  1. Войти в свой профиль Google.
  2. Перейти к целевому сообществу / сбору, проверить адресную строку браузера, и скопировать строку цифр и букв в конце URL (см. Рисунок5-29).

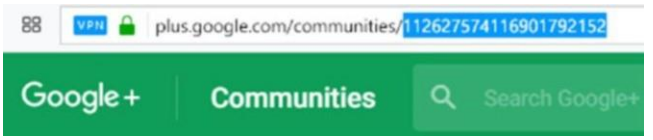

Рисунок 5-29. *Идентификатор сообщества (выделен в цветах), извлеченный из URL-адреса сообщества Google*

- Для поиска в сообществах Google используйте *«Поисковое ключевое слово» in:community* (заменить *сообщество* слов на сообщество целиID). Вот пример: **pentesting in:112627574116901792152** (это будет искать ключевое слово *pentesting* в сообществе цели, которая имеет Google ID 112627574116901792152).

- Для поиска в коллекциях Google используйте *«Поисковое ключевое слово»] in:collection* (заменить *коллекцию* слов коллекцией целевой ID). Вот пример: **hacking in:gAAAZ** (это будет поиск *для взлома* в коллекции имени *gAAAZ*).
- Google позволяет использовать трех логических оператора (AND, OR, NOT), но вы должны написать их заглавными буквами. Вот пример для использования каждого из них:
- Использование оператора NOT для отрицания. Вот пример: **from:106061931199710505959 NOT has:photo** (это будет поиск для всех сообщений, отправленных пользователем, чьи Google ID 106061931199710505959 и не содержащие фото). Пожалуйста, обратите внимание, что оператор NOT может быть заменен на знак минус (-) (**from:106061931199710505959—has:photo**).
- Оператор AND используется для поиска нескольких ключевых слов поиска. Google+ автоматически добавит его при разделении ключевых слов поиска с пробелом, так что нет необходимости добавлять его вручную. Вот пример: **from:106061931199710505959 AND from:101607398135470979957** (это будет поиск сообщений из двух учетных записей Google).
- Оператор OR оператор используется для поиска сообщений для одного или нескольких ключевых слов поиска. Вот пример: **OSINT has:doc OR has:photo OR has:spreadsheet** (это будет поиск ключевого слова *OSINT* в сообщениях, которые содержат *документ* или *фотографию* или *электронную таблицу* в нем).

ИСПОЛЬЗОВАНИЕ GOOGLE ДЛЯ ПОИСКА В GOOGLE+

Поисковая система Google может быть эффективно использована для поиска в Google+. Как вы делали много раз, используйте оператора *сайта,* чтобы ограничить поиск только Google(site:plus.google.com). Вот несколько примеров:

- **“PERSON NAME” site:plus.google.com** (Заменить PERSON NAME целевым именем)

1. **“Work at COMPANY NAME” site:plus.google.com** Заменить КОМПАНИЯ ИМЯ на название целевой компании)

ПОИСК В GOOGLE С ПОМОЩЬЮ ПОЛЬЗОВАТЕЛЬСКОГО ПОИСКОВОГО СЕРВИСА GOOGLE

Вот самые популярные пользовательские поисковые системы Google для поиска в профилях Google Plus:

- Google+ Коллекции и сообщества (http://goo.gl/A8MB7z)
- Google Плюс Сталкер(https://cse.google.com/cse/publicurl?cx=0 01394533911082033616%3Asvzu2yy2jqg)
- Google+ Фотографии Пользовательский поисковая система (https://cse.google.com/ cse/publicurl?cx=006205189065513216365:uo99tr1fxjq)
- Google-Плюс профили (https://cse.google.com/cse/publicurl?cx= 009462381166450434430:cc5gkv2g7nk)
- Retrieve Google+ профили, которые имеют адрес электронной почты и номер телефона(https://cse.google.com/cse/publicurl? cx=009462381166450434430:cotywcrgpru)
- **Другие полезные услуги для Google+**

Вот еще несколько сайтов, чтобы проверить:

- *Google+ to RSS* (https://gplusrss.com): Создайте RSS-канал любого профиля или страницы Google. Бесплатная версия позволяет для двух каналов.
- *Google+ User Feed* (http://plusfeed.frosas.net): С помощью этого сайта вы можете следить за каналами пользователей Google. Полезно следить за публикациями вашей цели, не посещая их страницу Google.

LinkedIn

LinkedIn это социальная сеть, посвященная профессиональному взаимодействию в деловом мире. Физические лица поддерживают профиль, подобный резюме, где они представляют свои навыки, историю занятости и достижения в работе/проекте, в то время как корпорации поддерживают страницу для продвижения своей деловой деятельности и объявляют о вакансиях.

LinkedIn началась в 2003 году, поэтому считается одним из старых социальных медиа-сайтов. LinkedIn предлагает свои услуги в 200 странах, и его интерфейс поддерживает 20 языков. Большинство пользователей LinkedIn находятся в США; второй по величине сегмент приходит из Индии, за которой следует Бразилия. В декабре 2016 года Microsoft приобрела

LinkedIn. В настоящее время LinkedIn имеет более 546 миллионов активных пользователей по всему миру.[xiii]

Чтобы иметь профиль LinkedIn, необходимо предоставить свои имена и фамилии, электронную почту и пароль. LinkedIn имеет политику для обеспечения соблюдения с использованием реальных имен только; на самом деле это не имеет смысла иметь ложный профиль здесь, как суть LinkedIn заключается в том, чтобы сделать соединения в деловом мире, и вы должны предложить реальную информацию, чтобы сделать полезные деловые связи. Для людей, настроенных на конфиденциальность, LinkedIn предлагает различные разрешения доступа, которые позволяют каждому пользователю адаптировать данные своего профиля для просмотра.

Большинство содержимого LinkedIn невозможно увидеть без предварительного входа в учетную запись LinkedIn. Если вы попытаетесь увидеть профиль LinkedIn, пока вы не вошли в систему, вы столкнетесь с страницей с просьбой зарегистрироваться или войти в свой аккаунт (см. рисунок 5-30). Некоторые пользователи LinkedIn устанавливают высокие настройки контроля конфиденциальности в своих учетных записях, чтобы другие участники LinkedIn не просматривали части своего профиля, включая фотографию профиля, если только они не подключаются к LinkedIn.

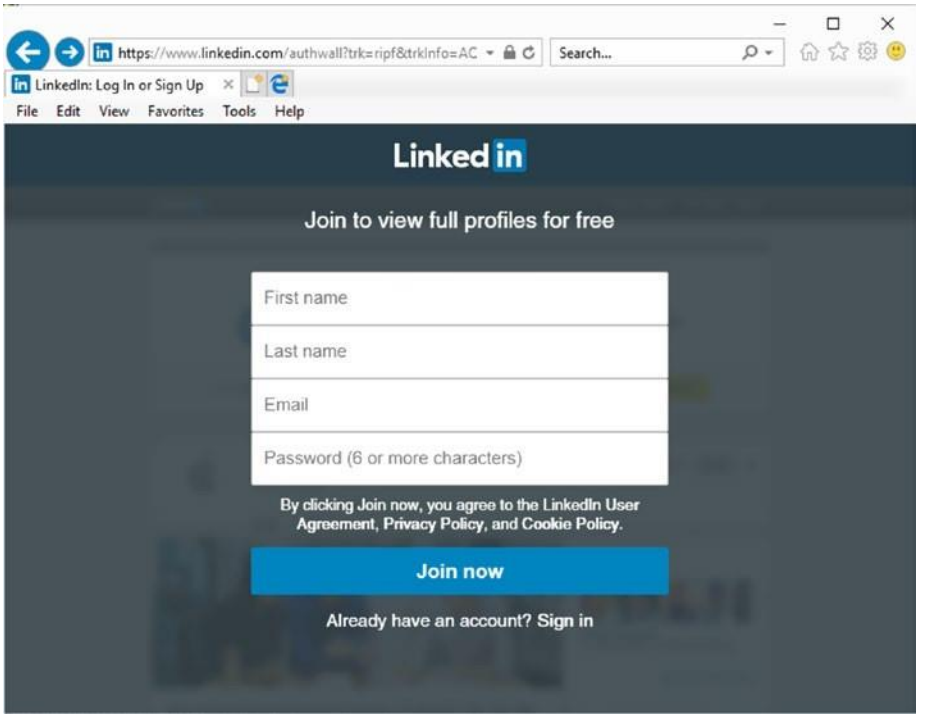

Рисунок 5-30. *Представление профиля, когда запрашиваемый не вошел в LinkedIn*

Индивидуальные профили на LinkedIn (см. Рисунок 5-31) держать свое имя, профессию, образование, историю работы (текущая и предыдущая занятость), признакам навыки и одобрения, рекомендации, достижения, Языки говорят, почести и награды , проекты и интересы. Люди могут общаться с другими профессионалами linkedIn; они также могут следить за другими людьми или корпоративными страницами, и их обновления будут отображаться в ленте времени пользователя.

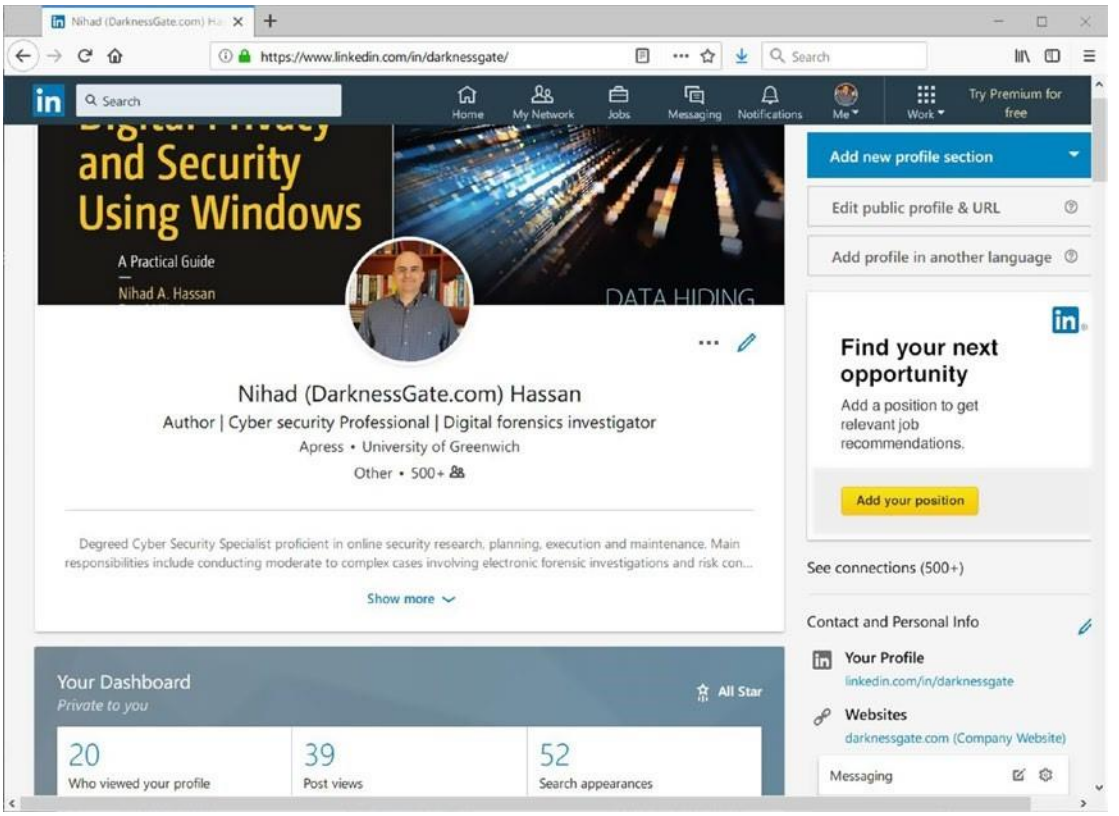

Рисунок 5-31. *Пример отдельного профиля LinkedIn с профилем автора в LinkedIn*

ПОИСК В LINKEDIN

Пока вы не вошли в LinkedIn, вы можете выполнить простой поиск людей, использующих их имена и фамилии. Форма поиска расположена в нижней части главной страницы (см. рисунок5-32).

Рисунок 5-32. *Использование простой формы поиска LinkedIn, расположенной на главной странице рядом с разделом "Найти коллегу", для поиска людей, пока вы не вошли в систему*
Linkedin

Результат поиска LinkedIn, в то время как вы не вошли в систему, это список совпадающих имен с резюме для каждого из них. Если вы хотите получить доступ к дополнительной информации о любом профиле, вам нужно войти в LinkedIn.

Для пользователей, зарегистрированных в журнале, LinkedIn предоставляет панель поиска поверх страницы для поиска людей, рабочих мест, сообщений, компаний, групп и школ. Используя эту панель поиска, вы можете начать простой поиск, и после получения результатов, вы можете уточнить набор результатов с помощью

Передовые фильтры LinkedIn.

Например, для поиска ключевого слова *Apress,* введите ключевое слово поиска Apress в панели поиска и нажмите кнопку Enter. (Обратите внимание, что при вводе ключевых слов поиска, LinkedIn даст поисковые предложения, которые появляются в списке выпадающих вниз при вводе.) Посмотрите в верхней части страницы результатов и нажмите все фильтры (см. рисунок 5-33), чтобы отфильтровать результаты в соответствии с вашими потребностями (см. рисунок 5-34). Обратите внимание, что на некоторых страницах LinkedIn могут отображаться поисковые фильтры LinkedIn в правой части страницы.

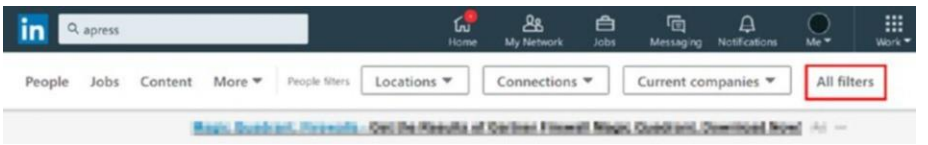

Рисунок 5-33. *Доступ к расширенным поисковым фильтрам LinkedIn для сужения*

Результаты

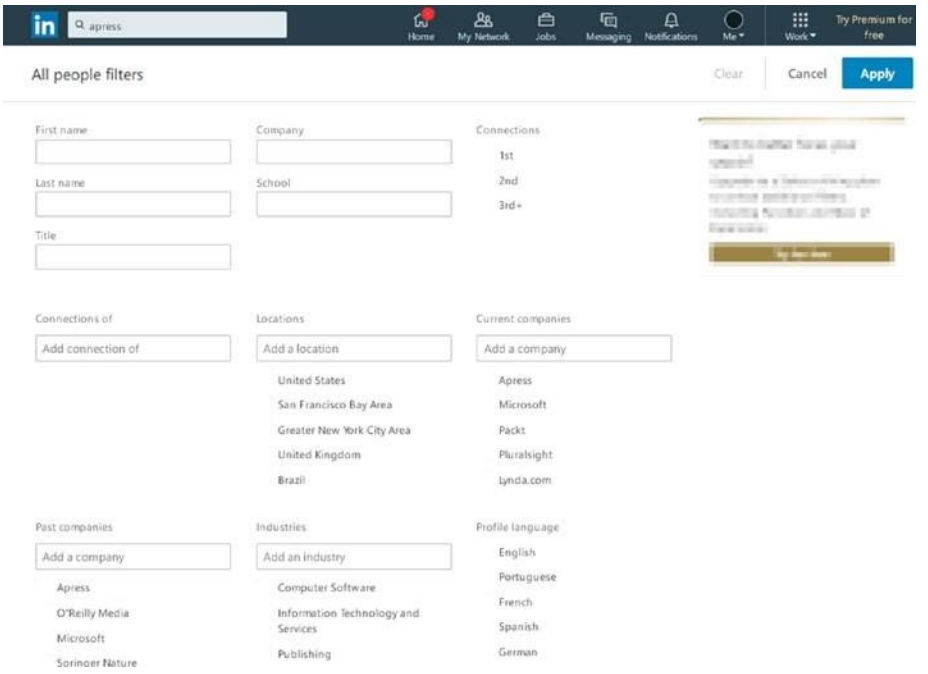

Рисунок 5-34. *Передовые поисковые фильтры LinkedIn*

Предупреждение! Всякий раз, когда вы посещаете чей-то профиль на linkedin, ваш визит записывается, и посещаемый профиль будет знать об этом. Вы можете просматривать linkedin анонимно после изменения настройки конфиденциальности (параметры просмотра профиля), но вы, в свою очередь, потеряете возможность узнать, кто просматривал ваш профиль. пожалуйста, обратите внимание, что пользователи с премиум linkedin счета будут знать, кто просмотрел их профиль, даже если посетитель использует linkedin в частном режиме.

Расширенный поиск LinkedIn позволяет искать в соответствии с именами и фамилиями цели, компанией, школой и названием. Вы также можете указать географическое местоположение цели, чтобы ограничить поиск только одной областью. Поиск может быть уточнен, чтобы добавить других членов LinkedIn, которые могут иметь связь с этой целью. Кроме того, можно фильтровать в соответствии с языком профиля и целевую текущую/предыдущую работу.

РАСШИРЕННЫЕ ОПЕРАТОРЫ ПОИСКА LINKEDIN

Как и в Twitter, LinkedIn позволяет использовать продвинутых поисковых операторов для уточнения поиска. Ниже приведены самые популярные из них:

- Чтобы найти точную фразу, приложить его в кавычки. Тот же метод можно использовать для поиска профилей, которые имеют несколько слов. Вот пример: **“OSINT intelligence”** (это будет искать точную фразу, заключенную в кавычки).
- Использование оператора NOT что бы исключить конкретный термин. Вот пример: **developer NOT designer**.
- Используйте OR оператор, чтобы включить один или несколько терминов вместе. Вот пример: **developer OR designer** (поиск разработчика или дизайнера или обоих).
- Use the AND оператора, чтобы включить два или более терминов вместе. Вот пример: **developer AND designer** (поиск как дизайнера, так и разработчика). Нет необходимости использовать AND оператор в поиске, потому что LinkedIn будет добавлять его автоматически, когда вы ищете более одного термина вместе; просто введите пространство между условиями поиска.
- Используйте скобки для объединения терминов поиска. Вот пример: **penetration tester NOT (developer OR designer)**. В будет поиск отабражено пейнтестер и игнорирован запрос как разработчик и дизайнер из результатов поиска.
- Вы можете использовать Google для поиска в LinkedIn с помощью оператора гугла *site*. Вот пример:**“Nihad Hassan” site:linkedin.com**.

ПОИСК LINKEDIN С ПОМОЩЬЮ ПОЛЬЗОВАТЕЛЬСКОГО ПОИСКА GOOGLE

Google пользовательских поисковых систем может стать удобным, чтобы получить некоторые результаты, которые не могут быть извлечены легко с помощью типичных поисковых систем. Ниже приводится выбранный набор пользовательских поисков Google, которые оказались полезными при извлечении данных из LinkedIn:

- *Недавно обновленные профили*(https://cse.google.com/cse/publicurl?cx=009462381166450434430:luit7gbqx2a): Это позволит получить недавно обновленные профили из LinkedIn.

- *Экстрактор контакта LinkedIn*(https://cse.google.com/cse/publicurl?cx=001394533911082033616:tm5y1wqwmme): Это позволит извлечь профили LinkedIn, которые имеют доступ к своим контактам. Извлеченная информация включает поля Контакт, Электронная почта, Email2 и Email3.
- *Резюме LinkedIn*(https://cse.google.com/cse/publicurl?cx=010561883190743916877:qa_v6ioerxo#gsc.tab=0): Это будет поиск обновленных профилей LinkedIn, которые были обновлены в течение последнего месяца или двух.
- *Поиск людей LinkedIn (международный)*(https://cse.google.com/cse/home?cx=009679435902400177945:psuoqnxowx8): Фильтр результатов в соответствии со следующими странами: США, Канада, Великобритания, Ирландия, Индия, Новая Зеландия, Китай и Австралия.

Для вашей поисковой работы OSINT LinkedIn считается первым местом для поиска людей, которые работают в определенной профессии, чтобы найти свою историю занятости. Например, вы можете выяснить опыт пользователя, увидев его навыки одобрения и истории занятости. Люди, которые одобряют цель, также могут стать мишенью для вашего поиска, чтобы увидеть их связь с основной целью (например, их рабочие отношения, дата, когда работали вместе, и какие проекты они работали). Не забудьте настроить настройки конфиденциальности учетной записи, чтобы другие не знали вашу личность при проведении поиска в LinkedIn.

Общие ресурсы для размещения информации на сайтах социальных медиа

Есть много онлайн-сервисов, которые могут быть использованы в соответствии с уже обсуждаемыми методами поиска, чтобы найти полезную информацию о любой цели, которая имеет присутствие на одном или нескольких сайтах социальных медиа.

- *Buzz Sumo* (http://buzzsumo.com): Найти наиболее общую тему или тему, которая в настоящее время в тренде на основных платформах социальных медиа.
- *Key Hole* (http://keyhole.co): Это предлагает отслеживания хэштегов и ключевых слов через различные сайты социальных медиа; Вы можете отслеживать учетные записи Twitter, упоминания и URL-адреса.

- *MIT PGP Public Key Server* (http://pgp.mit.edu): Поиск на PGP Public Key Server, который может раскрыть адрес электронной почты цели. Вы можете использовать его для проведения дальнейших расследований, если цель загрузила свой открытый ключ к таким серверам.

Примечание! Вы можете увидеть список всех pgp открытых ключевых серверов и проверить их статус на https://sks-keyservers.net/status.

Другие социальные медиа-платформы

Мы упомянули самые популярные сайты социальных медиа в этой главе. Однако, говоря о всех социальных платформах, которые существуют в мире сегодня потребуется книга сама по себе. Существуют сотни активных социальных медиа-сайтов в мире, и некоторые из них популярны только в своих собственных обществах (например, китайские сайты). Таблица 5-1 перечисляет другие менее популярные - сайты социальных сетей, которые также должны быть рассмотрены при проведении онлайн-расследований.

Table 5-1. *Less Popular Social Media Sites*

Name	Category	URL	Comments
		International Sites	
reddit	Social news	https://www.reddit.com	Агрегация социальных новостей, рейтинг веб-контента и веб-сайт для обсуждения
instagram	photo sharing	https://www.instagram.com/?hl=en	
tumblr	Microblogging	https://www.tumblr.com	
tinder	location-based social search mobile app	https://tinder.com	
pinterest	Social network	www.pinterest.com	Мультимедийный - шаринг вебсайт

Flickr	photo sharing	https://www.flickr.com	
classmates	Social sharing	www.classmates.com	

Table 5-1. (*continued*)

Name	Category	URL	Comments
		China	
Qzone	Social network	http://qzone.qq.com	Крупнейшая Китайская социальная сеть активных пользователей 500 миллионов
Sina Weibo	Microblogging social platform	http://weibo.com/	смесь между Facebook и Twitter
Baidu	Social forum network	https://tieba.baidu.com/index.html	
		Russia	
Moemesto.ru	Bookmarking service	http://moemesto.ru	
Vkontakte	Social network	https://vk.com	популярны в России, Украине, Беларуси и Казахстане
diary.ru	Bookmarking site	www.diary.ru	
		Other Countries	
draugiem	Social network	www.draugiem.lv	Латвия
hatena	Bookmarking site	http://b.hatena.ne.jp	Япония

Facenama	Social network	www.facenama.com	Иран
taringa	Social network	www.taringa.net	Латинская америка

Сайты Pastebin

Pastebin — это служба обмена текстовыми сообщениями; это позволяет любому пользователю Интернета размещать большой объем текстовых данных, даже не регистрируясь на сайте Pastebin. Хотя он предназначен для обмена законными данными, многие хакеры black hat используют его для распространения украденных данных, таких как скомпрометированные учетные записи социальных сетей (имя пользователя и пароли), частные IP-адреса и подсети, принадлежащие различным корпорациям по всему миру, и учетные данные пользователей, взятые из различных нарушенных онлайн-сервисов.

Ниже приведены некоторые популярные сайты Pastebin и услуги:

- *Pastebin* (https://pastebin.com/trends): Это служба обмена текстовыми сообщениями.
- *PasteLert* (https://andrewmohawk.com/pasteLert): Это служба оповещения Pastebin, посвященная веб-сайту Pastebin.com.
- *Custom PasteBins Search Tool* (https://inteltechniques.com/osint/menu.pastebins.html): Эта пользовательская страница поиска индексирует 57 сайтов пасты.
- *Dump Monitor* (https://twitter.com/dumpmon): Это учетная запись Twitter, которая отслеживает несколько сайтов пасты для сбросов паролей и другой конфиденциальной информации.

Психологический анализ социальных медиа

Сайты социальных сетей интегрировались в нашу повседневную жизнь. Люди используют их все чаще публиковать все типы цифрового контента в Интернете. До сих пор мы сосредоточились на сборе данных с социальных сайтов. Однако, есть пункт, который мы не должны опускать при проведении анализа собранных данных: психологическое состояние человека размещения содержимого на их профиле может также дать важную информацию, даже больше, чем само содержание (в некоторых случаях). Например, истинная личность анонимного

Аккаунт Twitter может быть раскрыт путем проведения лингвистического анализа подозрительного аккаунта. Кроме того, подозреваемые могут быть отслежены в Интернете, изучая, как они используют язык, когда они в чате или когда они транслируют свои мысли в Интернете (например, как цель использует капитализацию, опускает или включает в себя слова, и произносит некоторые слова). Достижения в системах искусственного интеллекта сделают анализ аккаунтов в социальных сетях более эффективным и помогут следователям раскрыть истинную личность анонимных учетных записей в социальных сетях.

Примечание! Анализ онлайн-контента, особенно контента, найденного на платформах социальных сетей, становится важным для судебно-медицинского контекста расследования преступлений, разведки, кибер-эксплуатации, судебных процессов и судебных процедур. эта наука известна как *судебно-лингвистика*.

Анализ психологического состояния целевого онлайн-контента выходит за рамки этой книги. Тем не менее, есть некоторые онлайн-сервисы, которые могут помочь вам проанализировать содержание в Интернете и предсказать психологическое состояние цели при его размещении.

Tone Analyzer

Этот онлайн-сервис (https://tone-analyzer-demo.mybluemix.net) предлагает бесплатный лингвистический анализ для обнаружения человеческих чувств, таких как радость, страх, печаль, гнев, аналитические, уверенные в себе и предварительные тона– найденные в тексте, таких как твиты, электронные письма и сообщения Facebook (см. Рисунок 5-35).

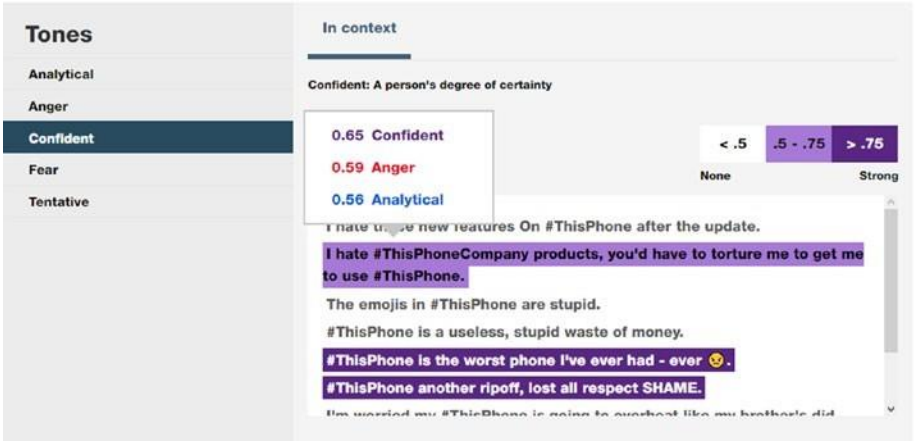

Рисунок 5-35. *Проведение лингвистического анализа для понимания психологического статуса автора текста*

Watson Tone Analyzer

Это (https://www.ibm.com/watson/services/tone-analyzer/) — облачный сервер, созданный IBM. Он анализирует эмоции и тона в онлайн-контенте (например, сообщения facebook, отзывы и твиты), чтобы предсказать эмоциональное состояние писателя. Эта услуга может использоваться в различных сценариях, помимо разведки, например, понять, что клиент должен лучше обслуживать их.

Прогноз Facebook и Twitter

Этот сайт(https://applymagicsauce.com/demo.html) предсказывает ваш психо-демографический профиль. Служба может анализировать ваши сообщения На Facebook и Twitter и дать представление о вашей личности, что полезно, чтобы увидеть, что ваш текущий социальный профиль говорит о вас или о какой-либо цели. Вы также можете вставить любой текст на сайте, чтобы предсказать психодемографический профиль его автора.

Fake Sport

Этот сайт(https://www.fakespot.com) анализирует отзывы пользователей Amazon, Yelp, TripAdvisor и Apple App Store, чтобы проверить достоверность их.

Review Meta

С этим сайтом(https://reviewmeta.com) Вы можете исследовать отзывы пользователей на Amazon, чтобы проверить, какой из них может быть поддельным или вводящим в заблуждение.

TweetGenie

Это (www.tweetgenie.nl/index.php) — голландский проект, который предсказывает возраст и пол цели от имени пользователя Twitter.

Итоги

В этой главе мы освещали самые популярные сайты социальных сетей по всему миру, сосредоточив внимание на одном с наибольшим числом ежемесячных активных посетителей. В цифровую эпоху редко можно увидеть интернет-пользователя, который не имеет хотя бы одной учетной записи на одном или нескольких сайтах социальных сетей. Люди используют социальные медиа-сервисы для размещения всех типов содержимого в Интернете, таких как фотографии, видео, текстовые сообщения и данные геолокации. Они также упоминают свое образование, историю занятости и адреса, где они живут. Личная информация, такая как социальные связи, посещаемые места, привычки, симпатии и антипатии, члены семьи, супруги и многое другое, все это может быть легко найдено. Хотя сайты социальных сетей позволяют своим пользователям ужесточить контроль за конфиденциальностью, чтобы другие не видели размещенного контента, мало кто заботится о таких проблемах и публикует многие из своих действий, особенно текстовые сообщения и

чек-инс - в публичном статусе. Это делает большой объем доступных данных легко доступным для различных видов онлайновых расследований.

В этой главе объясняется, как искать популярные сайты социальных сетей, чтобы найти информацию за пределами типичной функциональности поиска, предлагаемой каждой службой. В следующей главе, мы будем продолжать обсуждение того, как найти информацию о людях в Интернете, сосредоточив внимание на конкретный тип поисковых систем, известных как люди поисковых систем. Эти двигатели похожи на типичные поисковые системы. Тем не менее, они индексируют содержание, связанное только с отдельными лицами. Следующая глава будет также охватывать правительственные отчеты (также известный как *публичные записи).* Это конфиденциальные записи, подготовленные местными органами власти, и они содержат ценную информацию о конкретных гражданах страны. Объединив информацию из

поисковых систем и правительственных записей людей с информацией, собранной с сайтов социальных сетей, вы можете почти найти всю имеющуюся информацию о конкретном человеке в Интернете.

Заметки

i. Worldometers, “Current World Population,” February 5, 2018, www.worldometers.info/world-population/.

ii. We Are Social Singapore, “Global Digital Statshot Q3 2017,” February 14, 2018, https://www.slideshare.net/ wearesocialsg/global-digital- statshot-q3-2017

iii. Globalwebindex, “Internet users have average of 7 social accounts,” February 14, 2018, https://blog.globalwebindex. net/chart-of-the-day/internet-users- have-average-of-7social-accounts

iv. Statista, “Number of monthly active Facebook users worldwide as of 4th quarter 2017 (in millions),” February 14, 2018, https:// www.statista.com/statistics/264810/number-of-monthlyactive-facebook-users-worldwide/

v. LinkedIn, “The Power of LinkedIn's 500 Million Member Community,” February 10, 2018, https://blog.linkedin. com/2017/april/24/the-power-of-linkedins-500-million community

vi. National Conference of State Legislatures, “STATE SOCIAL MEDIA PRIVACY LAWS", February 11, 2018, www.ncsl.org/research/ telecommunications-and- information-technology/statelaws-prohibiting-access-to-social-media- usernames- andpasswords.aspx

vii. Smartdatahq, “The Data Volume Stored By Facebook Is… “, February 12, 2018, https://smartdatahq.com/data-volumestored-by-facebook/

viii. Microfocus, “How Much Data is Created on the Internet Each Day?,” February 11, 2018, https://blog.microfocus.com/howmuch-data-is-created-on-the-internet - each-day

ix. Statista, “Number of monthly active Twitter users worldwide from 1st quarter 2010 to 4th quarter 2017 (in millions),” February 14, 2018,

x. Internet Live Stats, “Twitter Usage Statistics,” February 12, 2018, www.internetlivestats.com/twitter-statistics/

xi. stonetemple, “Hard Numbers for Public Posting Activity on Google Plus,” February 14, 2018, https://www.stonetemple.com/ real-numbers-for-the-activity-on-google-plus/

xii. Statistic Brain Research Institute, “Google Plus Demographics & Statistics,” February 14, 2018, https://www.statisticbrain.com/ google-plus-demographics- statistics/

xiii. LinkedIn, https://about.linkedin.com, February 14, 2018, https://press.linkedin.com/about-linkedin

Глава 6

Поисковые машины и публичные записи

В цифровую эпоху, большинство людей имеют какой-то присутствие в Интернете, прямо или косвенно. Другие организации, такие как государственные и местные органы власти, также хранят некоторую информацию о своих гражданах в общедоступных базах данных. Поиск кого-то не всегда так просто, как вводить свое имя в Google или Facebook; люди с небольшим присутствием в Интернете не будет отображаться легко при поиске их в Интернете. В предыдущей главе мы продемонстрировали важность социальных медиа-сайтов, чтобы найти людей в Интернете. В этой главе, мы будем продолжать наше обсуждение о том, как найти людей в Интернете с помощью специализированных веб-сайтов, известных как *люди поисковых систем* в дополнение к поиску людей в государственных отчетах (также известный как публичные *записи*).

Освещение этих тем в одной главе удобно, потому что при поиске людей в Интернете, значительный объем информации выводится из общедоступных баз данных. В этой главе, мы перечислим основные люди поисковых систем в настоящее время (с упором на бесплатные услуги) и кратко поговорить о различные функции, предлагаемых каждым из них. Мы также будем охватывать правительственные сайты записей и классифицировать их в соответствии с предлагаемой информацией. Информация в этой главе в сочетании с предыдущей главой поможет вам найти информацию о большинстве целей в Интернете.

Что такое поисковая система людей?

Люди поисковые системы похожи на типичные поисковые системы; люди поисковые системы индекс онлайн-контента, но сосредоточиться на личных данных людей и хранить результаты в огромных базах данных, чтобы вернуть информацию по запросу. Различные параметры используются для поиска людей на этих сайтах, таких как адрес целевой электронной почты,

номертелефона, имяпользователя социального пользователяи полное имя. Некоторые веб-сайты предлагают дополнительные параметры поиска, такие как относительные

N. A. Hassan and R. Hijazi, *Open Source Intelligence Methods and Tools*, https://doi.org/10.1007/978-1-4842-3213-2_6

имена, почтовый адрес, дата рождения, известные псевдонимы, возраст и даже фотографии с использованием обратной техники поиска изображений. Базы данных, используемые поисковыми системами людей для поиска информации, разнообразны. Например, многие люди поисковых систем поиска в глубокой сети для извлечения информации из исходных баз данных, что типичные поисковые системы не могут достичь; к ним относятся базы данных о рождении и смерти, публичные записи (такие, как криминальные и налоговые отчеты) и другие упущенные источники (такие, как информация, хранящаяся в собственных базах данных). Пожалуйста, имейте в виду, что люди поисковые системы будут также индексировать результаты социальных медиа-платформ, таких как Facebook и LinkedIn, что делает их удобным решением для возвращения всеобъемлющих наборов результатов.

Онлайн следователи (такие как правоохранительные органы и разведывательные службы) нужны люди поисковых систем для получения точной информации о своих целях; другие стороны также заинтересованы в использовании таких услуг. Например, работодатели могут проводить проверку своих перспективных сотрудников, а физические лица могут искать объем личной информации, которая раскрывается о себе в Интернете.

Что такое публичные записи?

Мы уже говорили о людях поисковых систем; эти сайты получают часть их результатов из публичных хранилищ. Итак, что мы имеем в виду, когда мы говорим *публичные записи*?

Публичные записи состоят из информации, которая была, в основном, произведена государственными органами и должна быть неконфиденциальной.

Каждый человек на Земле имеет набор публичных записей. Например, наиболее важным – обязательным – публичными записями каждого человека является его рождение и смерть! Различные страны обрабатывают публичные записи по-разному, так как публичные записи будут содержать личную информацию (PII) о людях, и разоблачение таких деталей для общественности подлежит закону.

В Соединенных Штатах доступ к национальным государственным документам регулируется Законом о свободе информации (FOIA),[в] котором четко говорится, что любое лицо имеет право на получение доступа к правительственной информации в отчетах органов исполнительной власти. До сих пор Соединенные Штаты были единственной страной в мире, которая

предоставляет неограниченный доступ к публичным записям своих граждан. Это означает, что поиск граждан и жителей Соединенных Штатов возвращает более богатые результаты по сравнению с другими странами.

Правительственные записи бывают разных типов, таких как текст, фотографии и карты, и они хранятся в бумажных и электронных форматах, а также, таких как CD/ DVDs, ленты и компьютерные базы данных.

Помимо законов, регулирующих доступ к публичным записям, вам нужно знать, что многие онлайн-сервисы предлагают доступ к таким данным бесплатно или в обмен на небольшую плату.

Пример публичных записей

Публичные записи содержат различные типы информации. Следующий список классифицирует записи на группы на основе типа информации; однако следующий список не включает в себя все типы:

- Записи о рождении
- Записи о смерти
- Записи о браке
- Записи о разводе
- Записи адресов
- Судимости
- Суд / судебные записи
- Записи голосования
- Записи водительских прав
- История образования
- Запись собственности
- Налоговая/финансовая отчетность
- Разрешения на оружие
- Нарушения правил дорожного движения
- Записи о банкротстве

- Записи о сексуальных преступниках
- Профессиональные лицензии
- Записи электронной почты
- Телефонные записи
- Переписи Записи

Поиск личных деталей

Это основной раздел этой главы. Мы начнем с разговора об общих поисковых системах людей, а затем сузить наше обсуждение, чтобы охватить конкретные услуги, в основном публичные записи, специализирующиеся на поиске конкретных типов информации.

Общий поиск людей

Ниже приведены самые популярные сайты, используемые для поиска информации о людях в Интернете.

Примечание! перед тем, как начать поиск с помощью этих служб, убедитесь, что, если возможно, чтобы подготовить как можно больше деталей о вашей цели.

1. Полное имя
1. Электронная почта, номер телефона
1. Почтовый адрес

- Друзья, бывшие, члены семьи, имена социальных кругов, товарищи по учебе, деловые партнеры, известные соседи, или любое, кто может знать цель
- Где они жили или жили раньше (страна, город, государство)
- История образования (школа, университет)
- Возраст

TRUTHFINDER

TruthFinder (https://www.truthfinder.com) является одним из самых популярных людей поисковых систем; это публичный поиск записи, которая дает мгновенный доступ к широкому набору личной информации о тех, кто живет в Соединенных Штатах. TruthFinder имеет огромную базу данных профилей социальных сетей, истории адресов, контактной информации, публичных записей (федеральных, страновых и государственных источников данных) и других коммерческих источников. Вы можете искать, используя первую и/или фамилию цели в дополнение к городу/государству, где цель живет или жила раньше.

TruthFinder сканирует глубокую сеть интернет-ресурсов, чтобы получить результаты из мест, которые обычные поисковые системы не могут работать; он также ищет темную паутину для

разоблаченная личная информация, предоставление отличного сервиса для тех, кто может подозревать, что их личные данные были проданы на dark web (он предлагает бесплатный dark web служба мониторинга для своих зарегистрированных членов). Действительный поиск в TruthFinder будет производить доклад с подробной информацией о цели, такие как рождение и смерть записей, имущественные записи, судимости, истории образования, истории работы, истории местонахождения, социальных медиа и знакомств профилей, родственников ' имена, члены семьи, контактная информация и многое другое.

411

На 411 (https://www.411.co) Вы можете искать людей в Соединенных Штатах. Параметры поиска включают полное имя, местоположение, обратный поиск телефона, электронную почту и бизнес. Бесплатная учетная запись возвращает основные сведения, такие как местоположение, контактная информация и возможные родственники; однако платная подписка возвращает глубокие результаты.

PIPL

Pipl (https://pipl.com) является еще одной популярной поисковой системы людей, которая охватывает весь мир. Это позволяет искать людей, использующих их адрес электронной почты, номер телефона или имя пользователя в социальной сети. Pipl сотрудничает с другими поисковыми службами людей, чтобы вернуть всеобъемлющие результаты. К этим службам можно получить доступ, нажав на спонсируемые ссылки, которые отображаются на странице результатов поиска. Нынешними партнерами являются Peoplelooker.com, Archives.com и Spokeo.com. Эти услуги взимают плату за предоставление более подробной информации о человеке, представляющем интерес.

ДРУГИЕ

Перечень других важных поисковых систем людей, которые вы должны рассмотреть во время поиска:

- *Spokeo* (https://www.spokeo.com): Это коммерческая поисковая система людей, которая дает подробные отчеты о какой-либо цели.
- *TruePeopleSearch* (https://www.truepeoplesearch.com): Вы можете искать по целевому имени, последний телефон, и последний адрес. Услуга бесплатна и показывает контактную информацию (телефон и электронную почту) в дополнение к текущим и предыдущим адресам.

- *US Search* (https://www.ussearch.com): Это дает основную информацию о человеке, представляющем интерес, такие как адрес, родственники, работа и возраст. Чтобы разблокировать полный профиль, необходимо оплатить премиум-подписку. Услуга ограничена только Соединенными Штатами.
- *Peek You* (https://www.peekyou.com): Это агрегирует информацию из профилей социальных сетей, источников новостей, блогов и других общедоступных баз данных. Чтобы разблокировать полную информацию, вам нужно заплатить.
- *Zaba Search* (www.zabasearch.com): Вы можете найти людей в Соединенных Штатах, используя имя или номер телефона. Услуга бесплатна, и вы можете зарегистрироваться с помощью учетной записи Facebook бесплатно, чтобы получить преимущества премиум-услуги.
- *White Pages* (https://www.whitepages.com): Вы можете искать людей в Соединенных Штатах, используя их имя, номер телефона, бизнес или адрес. База данных «Белые страницы» насчитывает более 500 миллионов человек. Бесплатный подписной аккаунт дает следующую информацию о интересуянии лица: стационарные номера, текущие и предыдущие места жительства, родственников и партнеров.
- *Been Verified* (https://www.beenverified.com): Вы можете искать людей в Соединенных Штатах, используя их имя, телефон, электронную почту или почтовый адрес. В базовом докладе приводится общая информация по данному вопросу, в то время как коммерческая подписка дает подробный отчет о ком-либо, включая судимости (там, где это возможно) и отчеты о налоге на имущество. Эта услуга популярна в Соединенных Штатах и используется миллионами каждый год.
- *Address Search* (https://www.addresssearch.com): Вы можете искать чей-то адрес электронной почты или рассылки, используя имя и местоположение. Услуга ограничена Соединенными Штатами.

    1. *Lullar* (http://com.lullar.com): Вы можете искать веб-сайты социальных сетей, используя адрес электронной почты цели или имя и фамилии или пользователя.

- *Yasni* (www.yasni.com): Вы можете искать людей на основе их истории работы.
- *My Life* (https://www.mylife.com): Это показывает оценку репутации любой цели на основе информации, собранной из правительственных, социальных и других источников, а также

личные отзывы, написанные другими. Чтобы разблокировать полный отчет, необходимо зарегистрироваться и оплатить услугу.

- *Snoop Station* (http://snoopstation.com/index.html): Вы можете искать людей, используя их полное имя и местоположение. Это коммерческая услуга.
- *Advanced Background Check* (https://www.advancedbackgroundchecks. com): Вы можете предоставить основные сведения о цели, такие как почтовый адрес, телефон и электронная почта; чтобы разблокировать полную информацию, вы должны платить.
- *Family Tree Now* (http://familytreenow.com): Откройте для себя свое генеалогическое древо, ища с иными именами и городом/государством. Это бесплатная услуга.
- *Radaris* (https://radaris.com): Это публичная запись глубокой поисковой системы; он возвращает исчерпывающую информацию о цели. В нем также перечислены онлайн-упоминания о цели, такие как резюме, бизнес-записи, публикации, видео и изображения, профиль социальных сетей и веб-ссылки.
- *Profile Engine* (http://profileengine.com): Это поисковик по социальным сетям.

- *Info Space* (http://infospace.com): Это механизм метапоиска, который возвращает всеобъемлющие результаты из различных открытых источников данных и других сайтов поисковых систем людей.
- *Cubib* (https://cubib.com): Вы можете искать миллионы онлайн записей данных бесплатно. Агрегированные данные получены из поиска людей, маркетинговых данных, записей о собственности, записей о транспортном средстве, судебных записей, патентов, регистрации бизнеса, регистрации доменных имен и записей посещений Белого дома.
- *Fast People Search* (https://www.fastpeoplesearch.com): Это поиск по имни, адресу или поиск телефона бесплатно.
- *Speedy hunt* (https://speedyhunt.com): Вы можете искать людей в Соединенных Штатах и вернуть подробный отчет, где это возможно- о них, которые включают арест и записи сексуальных преступников. Вы должны заплатить, чтобы воспользоваться этой услугой.
- *That's Them* (https://thatsthem.com/people-search): Вы можете искать людей, использующих их имя, адрес, телефон и электронную почту бесплатно.

- *Webmii* (http://webmii.com): Вы можете искать людей и для их оценки видимости бесплатно.
- *How Many of Me* (http://howmanyofme.com/search/): Вы пишете имя, и сайт будет возвращать число людей в Соединенных Штатах, которые соответсвуют вами веденным данным.
- *Genealogy* (www.genealogy.com): Вы можете искать записи семейной истории, используя информацию, первоначально размещенную в GenForum.
- *Sorted By Name* (http://sortedbyname.com): Это список ссылок на генеалогию детали на основе первой буквы фамилии человека, упомянутых на других сайтах.

Онлайн-реестры

Интернет-реестр является своего рода список пожеланий опубликованы в Интернете. Наиболее очевидным примером таких реестров является, когда пара формулирует список вещей, которые они должны купить для их брака. Они составляют список и публикуют его публично. Когда один из их друзей или родственников покупает им товар из списка, поставщик реестра удалит этот товар из списка и отправит приобретенный товар паре.

Для целей расследования OSINT, онлайн-реестры полезны для раскрытия личных данных / пожелания людей, представляющих интерес в дополнение к близким друзьям (так как многие реестры позволяют друзьям размещать свои пожелания на стене владельца реестра), особенно после зная, что многие люди оставляют свои реестры доступны в Интернете после окончания церемонии.

Существуют различные типы онлайн реестров. Наиболее известными типами являются свадьба, ребенок, выпускной, день рождения, праздник, и подарок реестров. Следующий список самых популярных онлайн-реестров:

- *The Knot* (https://www.theknot.com): Найти свадебный реестр пары и веб-сайт.
- *Registry Finder* (https://www.registryfinder.com): Поиск реестров.
- *Amazon Registry* (https://www.amazon.com/wedding/home): Это реестр Amazon.
- *My Registry* (https://www.myregistry.com): Это глобальная онлайн-сервис по регистрации подарков.
- *Checked Twice* (https://www.checkedtwice.com): Это реестр подарков.

Важные записи

Записи жизнедеятельности являются правительственными документами, обычно созданными местными властями. Они включают в себя записи о рождении и смерти, лицензии на брак и развод. При поиске жизненно важных записей, возвращенный результат, как правило, приходят с личными данными цели. Например, запись о рождении обычно приходит с полным именем родителя, именем ребенка и местом, где произошло событие. Запись о смерти будет идти с местом, где человек похоронен, свидетельство о смерти, и имя человека, который сообщил о событии властям. Брак записи будут содержать имена родителей пары и место, где брак был зарегистрирован. Наконец, в записи о разводе будет содержаться информация об именах детей пары. Другие связанные записи, такие как записи о происхождении (предлагаемые некоторыми базами данных) и почтовый адрес заинтересованного лица также могут отображаться при поиске в жизненно важных записях.

Ниже приведены наиболее популярные жизненно важные базы данных записей:

Примечание! как мы уже говорили, большинство публичных записей в Интернете относятся к гражданам США из-за законодательства США. однако, мы перечислим другие международные базы данных публичных записей, где это возможно .

- *Sorted by Birth Date* (http://sortedbybirthdate.com): Этот сайт использует Death Master File по состоянию на март 2014 года. Death Master File является базой данных, публично доступных Администрацией социального обеспечения США с 1980 года, она содержит личную информацию о людях, которые имели номера социального страхования и о чей смерти были сообщено В Администрацию социального обеспечения с 1962 года по настоящее время.
- *DeathIndexes* (www.deathindexes.com): Этот сайт содержит каталог ссылок на веб-сайты с онлайн индексы смерти классифицируются по штату и стране.
- *Family Search* (https://www.familysearch.org/search/ collection/1202535): Это индекс смертности от социального обеспечения США.

- *Find a Grave* (https://www.findagrave.com): Вы можете найти информацию о людях, включая их рождение, смерть и информацию о погребении, и она может включать фотографии, биографии, семейную информацию и многое другое. Сайт содержит более 170 миллионов мемориалов в своей базе данных.
- *Deaths of U.S. citizens in foreign countries* (https://www.archives. gov/research/vital-records/american-deaths-overseas.html): Это база запись смертей за рубежом гражадн США.
- *Obits Archive* (www.obitsarchive.com): Вы можете найти более 53 миллионов некрологов США здесь.
- *U.S., Department of Veterans Affairs BIRLS Death File, 1850–2010* (https://search.ancestry.com/search/db.aspx?dbid=2441): Эта база данных содержит записи о рождении и смерти для более чем 14 миллионов ветеранов и в. А. бенефициаров, которые умерли между 1850 и 2010.
- *Melissa* (https://melissadata.com/lookups/deathcheck.asp): Это отображает список людей, которые умерли в течение последних 24 месяцев в Соединенных Штатах.
- *Deceased Online* (https://www.deceasedonline.com): Это центральная база данных для захоронений и кремаций в ЕС.
- *National Records of Scotland* (https://www.nrscotland.gov.uk/ research/visit-us/scotlandspeople-centre/useful-websites- for-family-history-research/births-deaths-and-marriages): Это включает в себя ссылки на рождения, смерти, и браке записей правительства Шотландии в отдельных странах, как Соединенные Штаты и Канада.
- *Find My Past* (https://search.findmypast.co.uk/search-united- kingdom-records-in-birth-marriage-death-and-parishrecords): Вы можете искать жизненно важные записи в Великобритании, Австралии, Новой Зеландии, США, Канаде и Ирландии.
- *Forebears* (http://forebears.io/germany): Здесь хранятся международные генеалогические записи. Выберите страну и тип записи для отображения связанных результатов (см. рисунок6-1).

Рисунок 6-1. *Международные генеалогические отчеты, предлагаемые* [*http://forebears.io*](http://forebears.io)

Примечание! крупный портал для размещения жизненно важных записей в рамках US является Vitalrec(www.vitalrec.com) территории в US. все, что вам нужно сделать, это выбрать лицо, представляющее интерес государства, а затем просматривать доступные ссылки жизненно важных записей для этой области. это должно быть ваше первое место для поиска жизненно важных записей в US. пожалуйста, обратите внимание, что Vitalrec.com не хранит никакой информации в своей базе данных; он просто предлагает ссылки непосредственно на страницу каждого государства, и он упоминает, где и как получить жизненно важные записи государства. в международном разделе(www.vitalrec.com/links2.html)приводится подробная информация о том, где найти такую информацию в других странах.

Уголовный и судебный поиск

Уголовные и судебные записи включают в себя различные категории информации, такие как люди с ордерами на обыск (ордера на арест и разыскиваемых людей), тюремные записи и сексуальные преступления (эта категория имеет специальный веб-сайт в Соединенных Штатах, который содержит полную информацию о каждом правонарушителе). Любое лицо, осужденное

за преступные деяния, может быть найдено в таких публичных базах данных. Ниже приведены наиболее важные сайты судимости (в основном принадлежащие к базам данных США):

- *National Sex Offender Public Website (NSOPW)* (https://www. nsopw.gov/en): Это дает общественности доступ к данным о сексуальных преступлениях в Соединенных Штатах; результаты включают фотографию преступника.
- *Criminal Searches* (www.criminalsearches.com): Это магазины записей для сотен миллионов взрослых с судимостью по всей территории Соединенных Штатов.
- *Black Book Online* (https://www.blackbookonline.info/ index.html): Это каталог бесплатных публичных услуг поиска записей, охватывающих всю Часть Соединенных Штатов. Просто выберите штат, чтобы увидеть доступные записи окружного суда в области.
- *Ancestor Hunt* (http://ancestorhunt.com/most-wanted- criminals-and-fugitives.htm): Это самые разыскиваемые преступники и беглецы в Америке. Выберите состояние, чтобы увидеть список.
- *The Inmate Locator* (www.theinmatelocator.com): Это списки заключенных лока в Соединенных Штатах.
- *Federal Bureau of Prisons* (https://www.bop.gov/inmateloc): Здесь вы можете найти местонахождение любого федерального заключенного, заключенного в заключении с 1982 года по настоящее время.
- *The Global Terrorism Database* (GTD) (www.start.umd.edu/gtd/): Это база данных с открытым исходным кодом, в котором содержится информация о террористических событиях по всему миру (бот-международных и внутренних) с 1970 по 2016 год.

Примечание! Статистика преступности ФБР может быть полезна в некоторых случаях, когда вам нужно исследовать статистику преступности в конкретной области и в течение определенного года. Вы можете найти его на https://ucr.fbi.gov.

Совет! чтобы увидеть список значков, в основном значки сил безопасности- из всех стран по всему миру, перейдите наhttp://allbadges.net/en.

Отчеты о собственности

Используйте эти сайты, чтобы получить информацию о недвижимости и их жителей:

- *U.S. Realty Record* (https://usrealtyrecords.com): Это крупный поставщик информации о собственности в Соединенных Штатах.
- *Zillow* (https://www.zillow.com): Этот сайт предлагает покупку, продажу, аренду, финансирование и реконструкцию недвижимости в Соединенных Штатах.
- *U.S. Title Records* (https://www.ustitlerecords.com/property- records): В нем перечислены записи свойств, поиск залога, поиск заголовков и документы. Это коммерческая услуга.
- *GOV.UK* (https://www.gov.uk/search-property-information- land-registry): Здесь вы можете найти информацию о недвижимости в Англии или Уэльсе.
- *Neighbor Report* (https://neighbor.report): Это дает данные об адресах, резидентах и номерах телефонов в Соединенных Штатах. Эта услуга уникальна, поскольку она позволяет любому размещать жалобы или спасибо своим соседям.

Налоговые и финансовые отчеты

Вы можете найти налоговую и финансовую информацию о человеке, представляющем интерес для публичного поиска записи.

- *VAT Search* (https://vat-search.eu): Это сайт для проведения поиска ндс налога во всех странах Европейского Союза.
- *Real Property Tax Database Search* (https://otr.cfo.dc.gov/page/ real-property-tax-database-search): Этот сайт предоставляет доступ к информации об имуществе в США.

- *The National Archives (UK)* (www.nationalarchives.gov.uk/help- with- your-research/research-guides/taxation): Это сайт для поиска британских государственных записей о налогообложении.

Очень важный сайт! Перейти к https://publicrecords.netronline.com для U. S. публичные записи онлайн каталог, который содержит ссылки на официальные публичные базы данных, включая U. S. граждан государственных налоговых отчетов.

Поиск номера социального страхования

Вы можете выполнить обратный поиск номера социального страхования (только для Соединенных Штатов), перейдя на https://www.ssn-check.org/lookup/?state=AK&year=1936. База данных содержит номера социального страхования, которые были выпущены в период с 1936 по 2011 год.

Другой сайт, который предлагает бесплатный номер социального страхования поиска и поиска инструментов SSN- Проверить(https://www.ssn-verify.com/tools).

Примечание! Вы можете найти записи регистрации избирателей в США по адресуhttps:/ / voterrecords.com.

Проверка имени пользователя

Вы можете проверить конкретные имена пользователей, чтобы увидеть, где они используются (например, сайты социальных сетей) или узнать, существует ли конкретное имя пользователя на самом деле.

- *Check User Name* (http://checkusernames.com): Проверьте использование конкретного имени пользователя в 160 социальных сетях. Это полезно, чтобы обнаружить целевые учетные записи социальных медиа, чтобы увидеть, если они используют одно и то же имя пользователя на нескольких платформах.

- *Namechk* (https://namechk.com): Проверьте, используется ли указанное имя пользователя для основных доменных имен и сайтов социальных сетей.
- *Namecheckr* (https://www.namecheckr.com): Проверка доступности домена и социального имени пользователя в нескольких сетях.
- *User Search* (https://www.usersearch.org): Сканирование 45 популярных веб-сайтов в социальных сетях.

Поиск по электронной почте и расследование

Бесплатные услуги могут помочь вам найти людей в соответствии с их соответствующим адресом электронной почты. Службы проверки электронной почты проверяют, существует ли адрес электронной почты, и дают другую подробную техническую информацию о нем.

- *E-mail Dossier* (https://centralops.net/co/emaildossier.aspx): Этот сайт дает подробные технические отчеты проверки об электронной почте.
- Emailhippo (https://tools.verifyemailaddress.io): Бесплатная служба проверки адреса электронной почты.
- *Hunter* (https://hunter.io/email-verifier): Этот веб-сайт предлагает бесплатный адрес электронной почты службы проверки / 100 электронной почты в месяц.
- *E-mail Checker* (https://email-checker.net): Вы можете использовать этот сайт, чтобы проверить, является ли адрес электронной почты реальным.
- *Mail Tester* (http://mailtester.com/testmail.php): Этот сайт предлагает проверку адреса электронной почты.
- *Byte Plant E-mail Validator* (https://www.email-validator.net): Вы можете проверять адреса электронной почты оптом.
- *E-mail Format* (https://email-format.com): Найдите форматы адресов электронной почты, которые используются в тысячах компаний.
- *E-mail Permutator+* (http://metricsparrow.com/toolkit/email- permutator): Это бесплатная услуга электронной почты permutator.
- *Emails4Corporations.com*(https://sites.google.com/site/ emails4corporations/home): Предоставление шаблонов адресов электронной почты для более чем 1000 компаний.

- *Scam Dex* (www.scamdex.com): Это огромный архив афера электронной почты.
- *E-mail Header Analysis* (https://www.iptrackeronline.com/ email-header-analysis.php): Получите подробную техническую информацию, полученную из заголовков электронной почты. Это включает в себя IP-адрес отправителя, электронную почту и отправителя ISP в дополнение к географической информации. Чтобы воспользоваться этой услугой, необходимо скопировать заголовок электронной почты и вставить его в движок анализа заголовков электронной почты и нажмите кнопку "Отправить заголовок для анализа". Смотрите следующее примечание, чтобы узнать, как извлечь заголовок сообщения Gmail.

Примечание! Следуйте этим шагам, чтобы извлечь заголовки электронной почты из gmail:

1. открыть целевую электронную почту.
2. Нажмите вниз стрелка, расположенная рядом с кнопкой ответа и выберите "Показать оригинал" (см. рисунокНажмите вниз стрелка, расположенная рядом с кнопкой ответа и выберите "Показать оригинал" (см. рисунок6-2).

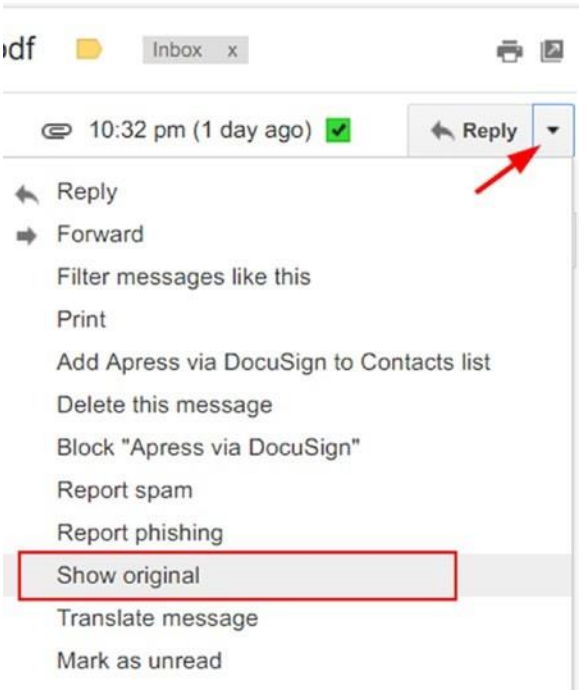

Рисунок 6-2. *Отображение заголовка электронной почты Gmail*

Веб-сайты репозитория данных, скомпрометированные

Эти сайты содержат список веб-сайтов, которые пострадали от утечки данных в прошлом. Когда сайт страдает от утечки данных, зарегистрированные данные пользователей, особенно имена пользователей и пароли, обычно становятся раскрытыми общественности. Многие люди имеют плохую практику использования одного и того же пароля для более чем одной учетной записи (например, используя тот же пароль для Facebook и для учетной записи электронной почты), так что знание одного пароля может предоставить доступ к другим социальным счетам / услугам, принадлежащим одному и тому же пользователю.

Следующие сайты являются популярными веб-сайты, которые перечисляют информацию от утечки данных; Вы можете использовать их, чтобы получить интеллект о любой цели в Интернете:

- Have I been Pwned (https://haveibeenpwned.com/Passwords): На этом сайте перечислены полмиллиарда реальных паролей, ранее обнаруженных в

результате утечки данных. Вы также можете загрузить список Pwned Passwords, который содержит дополнительные данные о каждой нарушенной учетной записи (например, количество случаев, когда пароль был замечен в утечках исходных данных). Этот сайт можно искать с помощью целевого адреса электронной почты или самого пароля, чтобы увидеть, появляется ли он в простом тексте в любом публичном списке дамб (см. рисунок 6-3). Это рекомендуемый сайт.

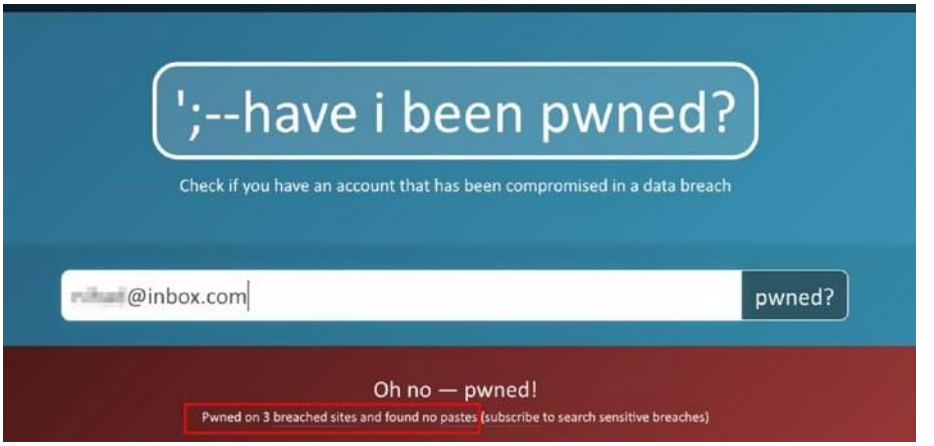

Рисунок 6-3. *Поиск электронной почты, которая была pwned ранее*

- *Breach Alarm* (https://breachalarm.com): Введите свой адрес электронной почты, чтобы узнать, были ли обнаружены пароли связанных с вами учетных записей в ходе предыдущего нарушения данных. Результаты будут отправлены на указанный адрес электронной почты.
- *Global Cyber Vandalism Statistics* (https://defacer.id): Этот сайт содержит информацию о самых активных хакерских веб-сайтах, наиболее активных хакерских группах, о недавно взломаных правительственных и академических веб-сайтах, сообщениях о взломе веб-сайтов.

- *Hacked E-mails* (https://hacked-emails.com): Анонимно проверьте, была ли ваша электронная почта скомпрометирована в результате предыдущего нарушения данных.

Примечание! В даркнете содержит много общедоступных баз данных, которые перечисляет взломаных учетные записи с паролями в виде тексте. последний известный файл дампа, найденный в даркнете, содержал 1,4 миллиарда учетных данных в одном текством файле. [ii]

Для человека, это незаконно, чтобы получить доступ к учетным записям других людей, используя украденные учетные данные на баз данных аккаунтах. Для OSINT иследователей, дискуссия являеться ли утечка информации является законным источником OSINT или нет!

Поиск номера телефона

Обратный поиск телефона полезно, чтобы узнать, кто стоит за конкретный номер телефона. Некоторые службы также указывают имя и тип перевозчика в дополнение к типу номера телефона. Ниже приведены некоторые услуги поиска телефона:

- *Z lookup* (https://www.zlookup.com): Это сайт, который делает международные обратный поиск телефона, включая мобильные телефоны.
- *Reverse Phone Lookup* (https://www.reversephonelookup.com): Этот сайт прослеживает телефон обратно к своему владельцу бесплатно.
- *Inter800* (http://inter800.com/index.html): Поиск телефонных номеров в США.
- *Twilio* (https://www.twilio.com/lookup): Определите форматы телефонных номеров, найдите имена абонентов, найдите типы абонентов (деловые или личные), определите оператора номера телефона и проверьте тип номера телефона (стационарный, VoIP или мобильный).
- *Spy Dialer* (https://www.spydialer.com): Это обратный поиск телефона для сотовых телефонов и стационарных телефонов.

- *Who calld* (https://whocalld.com): Это обратный телефон поиск службы для международных номеров.

  Info Bel (www.infobel.com): Поиск номера телефона человека или компании в любой точке мира.

  Fone Finder (www.fonefinder.net): Поиск телефонных номеров США/Канады.

- *True Caller* (https://www.truecaller.com): Это международный обратный поиск номера телефона.

- *Free Carrier Lookup* (http://freecarrierlookup.com): Это услуга поиска перевозчика.

- *Phone Lookup* (https://www.phonelookup.com): Это обратный номер телефона поиск службы.

Примечание! Вы не можете получить обратный поиск телефона для мобильных телефонов легко бесплатно; однако, есть много платных сайтов, которые предлагают такие услуги.

Профили сотрудников и веб-сайты о вакансиях

Сайты вакансий могут раскрывать большое количество информации о частных лицах и личных данных компаний. Например, вы можете узнать тип аппаратного и программного обеспечения, реализованных в компании, интересующих ее, посмотрев на технические вакансии, размещенные ею (например, размещение технической вакансии для ИТ-администратора с опытом работы в технологии Windows Server означает, что целевая компания использует ОС Windows в своей инфраструктуре). Опыт человека, образование и история работы можно легко найти, посмотрев на их резюме на веб-сайтах вакансий; резюме человека также может раскрывать важную техническую информацию о компаниях, в которых они ранее работали. Ниже приведены самые популярные сайты работу:

- *LinkedIn* (https://www.linkedin.com): Это уже было подробно освещено в главе5.

- *Recruit in* (https://recruitin.net): Это сторонний веб-сайт, который использует Google для поиска профилей на LinkedIn. Это возвращает более глубокие результаты по сравнению с LinkedIn.
- *Byte* (https://www.bayt.com): Это популярный сайт поиска работы на Ближнем Востоке.

  Market Visual (www.marketvisual.com): Поиск профессионалов по имени, компании или названию. Сайт отображает деловые отношения визуально между интересующим лицом и другими организациями. Он отображает дополнительные данные о цели, такие как предыдущие и текущие принадлежности и образования. Полученные данные поиска могут быть загружены в различных формах для последующего анализа.
- *Xing* (https://www.xing.com): Это сайт бизнес-сетей.
- *Indeed* (www.indeed.com): Это сайт по поиску работы.
- *Eluta* (https://www.eluta.ca): Это официальная поисковая система работы Канады 100 лучших работодателей.
- *CareerBuilder* (https://www.careerbuilder.com): Это сайт по поиску работы.
- *Euro Jobs* (https://www.eurojobs.com): Это европейский сайт работы.
- *Glassdoor* (https://www.glassdoor.com/index.htm): Это международный сайт работы.
- *Monster* (https://www.monster.com): Это международный сайт работы.
- *Head Hunter* (https://www.headhunter.com): Это платформа управления и руководящей работы.
- *Jobs* (https://www.jobs.pl): Это польский сайт работы.
- *Job site* (https://www.jobsite.co.uk): Это веб-сайт вакансии U.K..
- *Seek* (https://www.seek.com.au): Это австралийский сайт работы.
- *Simply Hired* (https://www.simplyhired.com): Поиск работы в США.
- *Zip Recruiter* (https://www.ziprecruiter.com): Поиск более 8 миллионов рабочих мест в США.

Поиск сайта знакомств

Полезную информацию о людях и их отношениях можно найти на сайтах знакомств. Эта информация не может быть опущена при проведении расследования OSINT о человеке, представляющем интерес.

Ashley Madison (https://www.ashleymadison.com): Это международный сайт знакомств.

First Met (https://www.firstmet.com/index.php): Это сайт знакомств с 30 миллионами пользователей.

- *Badoo* (https://badoo.us): С более чем 380 миллионов пользователей, эта сеть в настоящее время считается крупнейшей социальной сети открытия на Земле.
- *Plentyoffish* (https://www.pof.fr): Это сайт знакомств.
- *EHarmony* (https://www.eharmony.com/verify): Это международный сайт знакомств с разнообразной группой людей всех возрастов и стран.
- *Zoosk* (https://www.zoosk.com): Это международный сайт знакомств с более чем 40 миллионов пользователей.
- *Black People Met* (https://www.blackpeoplemeet.com): Этот сайт специализируется на поиске одиноких чернокожих.
- *True Dater* (www.truedater.com): Найти отзывы людей на сайтах знакомств; поиск с использованием имени пользователя Найти отзывы людей на сайтах знакомств; поиск с использованием имени пользователя.
- *Our Time* (https://www.ourtime.co.uk): Это сайт знакомств для людей старше 50 лет.
- *Hater Dater* (https://www.haterdater.com): Этот сайт помогает людям, которые ненавидят то же самое, чтобы собрать и общаться в Интернете.
- *UK Match* (https://uk.match.com): Это сайт знакомств U.K.
- *Pheramor* (https://www.pheramor.com): Это приложение знакомств для тех, кто в настоящее время работает в Хьюстоне, штат Техас.
- *Tinder* (https://tinder.com): Это мобильное приложение для социального поиска, которое позволяет людям взаимодействовать в Интернете. Это похоже на сайты знакомств.

- *Beautiful people* (https://www.beautifulpeople.com/en-US): Международный сервис знакомств. Вы можете зарегистрироваться через свой аккаунт Facebook - если у вас есть один.

  Meet Up (https://www.meetup.com): Веб-сайт, облегчающие встречи с людьми с одинаковым интересом/хиппи.

- *Okcupid* (https://www.okcupid.com): Бесплатный международный сайт знакомств, которые используют математические алгоритмы, чтобы найти лучший вариант в соответствии с каждым профилем пользователя.

Примечание! Вы можете найти сравнение сайтов знакомств на https://www. consumerreports.org/dating-relationships/online-dating-guide-match-me-if-you-can.

Другие публичные записи

Существуют и другие типы онлайн-публичных записей, которые могут оказаться полезными в некоторых случаях.

- *Search Systems* ((http://publicrecords.searchsystems.net): Это поисковая система публичных записей; она включает в себя ссылки на базы данных премиум-класса (и требует оплаты).
- *Unites States patent records* (https://www.uspto.gov): В сайт патентных записей.
- *Google Advanced Patent Search* (https://www.google.com/advanced_patent_search): Поиск патентов здесь.
- *Federal Election Commission* (https://classic.fec.gov/finance/disclosure/norindsea.shtml): В нем перечислены индивидуальные взносы, сделанные отдельными лицами, индейскими племенами, партнерствами, индивидуальными предпринимателями, компаниями с ограниченной ответственностью (LLC), а также взносы кандидатов во все политические комитеты.

- *Follow That Money* (https://www.followthemoney.org): В нем перечислены, как тратятся деньги на федеральных выборах.
- *Political Money Line* (www.politicalmoneyline.com): Это отслеживает деньги, потраченные в политике.
- *EHDP* (https://www.ehdp.com/vitalnet/datasets.htm): Это содержит много наборов данных о здоровье в Соединенных Штатах.

  Data.GOV.UK (https://data.gov.uk/data/search): Это огромная коллекция правительственных данных Великобритании.

  Stats (www.stats.govt.nz/browse_for_stats.aspx): Это набор данных правительства Новой Зеландии.

Примечание! местные библиотеки в Соединенных Штатах предлагают доступ к базы данных, как Ссылки США (огромный справочник службы) и газеты Америки (полный текст некрологи) за небольшую плату. во многих случаях такие услуги могут быть предложены удаленно в обмен на действительную библиотечную подписную карту.

Итоги

При поиске человека в Интернете, убедитесь, что попробовать различные веб-сайты, чтобы сделать работу, потому что каждая служба агрегирует свою информацию из различных баз данных. Механизмы индексации также различаются между участками. Также желательно начать поиск в социальных сетях; если вы найдете полезную информацию о цели, вы можете провести более тщательный поиск с помощью сайтов, охватываемых в этой главе.

В следующей главе мы продолжим обсуждение того, как найти людей в Интернете, но на этот раз, используя географическую информацию, которая поставляется с использованием Интернета людей и деятельности социальных медиа.

•

Примечания

i. Archives, “Freedom of Information Act (FOIA)”, March 11, 2018, https://www.archives.gov/foia

ii. Medium, “1.4 Billion Clear Text Credentials Discovered in a Single Database”, March 11,2018, https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentialsdiscovered-in-a-single-database-3131d0a1ae14

Глава 7

Онлайн Карты

Отслеживание геолокационной информации пользователей становится все более популярным с продвижением вычислительных устройств, мобильных коммуникаций и социальных медиа-платформ, потому что эти технологии делают размещение чьего-то текущего местоположения в Интернете вопросом нажатия одна кнопки.

В настоящее время многие типы электронных устройств оснащены спутниковыми датчиками слежения для определения их местоположения на карте. Почти все портативные устройства, такие как смартфоны и носимые устройства, теперь известны. Многие приложения в крупных магазинах программного обеспечения, таких как Apple и Google Play имеют возможность использовать датчик геолокации смартфона / планшета, чтобы предложить индивидуальный опыт или предложить определенные функции для пользователя устройства. На самом деле, большинство приложений, онлайн-сервисов и платформ социальных сетей могут так или иначе отслеживать местоположение пользователя.

В этой главе мы продемонстрируем, как вы можете использовать информацию о геолокации, которая поставляется с онлайн-деятельности многих пользователей, чтобы определить их текущее и предыдущее местоположение. Мы также рассмотрим многие полезные онлайн-сервисы, которые помогут вам отслеживать все онлайн, включая транспортные средства, корабли, грузы, самолеты и людей. Вы также узнаете, как исследовать различные онлайн-хранилища карт для сбора разведданных.

Но прежде, чем мы начнем, мы будем описывать в простых терминах, как навигационные системы, которые отвечают за определение текущих местоположений людей-работы.

Основы геолокации

Большинство людей не заботятся о лежащей в основе технологии, ответственной за предоставление им услуг на основе местоположения. Люди вводят адрес местоположения, нужное им искать на карте, или они используют встроенную функцию, доступную в смартфонах, для геотега цифровых файлов (таких как изображения и видео), чтобы они записывали текущее местоположение изображений/видео в виде мета-тега автоматически. В других случаях многие социальные медиа-платформы,

N. A. Hassan and R. Hijazi, *Open Source Intelligence Methods and Tools*, https://doi.org/10.1007/978-1-4842-3213-2_7

особенно Facebook и Twitter, позволяют своим пользователям размещать свое текущее местоположение в Интернете (так называемый *регистрация* на Facebook) всего одним щелчком мыши, а остальное обрабатывается с помощью электронного устройства.

Чтобы определить чье-то текущее географическое место, устройствам, знающим о местоположении, необходимо связываться со спутниковой навигационной системой, которая, в свою очередь, отвечает за доставку точных координат местоположения на Земле.

Глобальная система позиционирования (GPS) — американская спутниковая навигационная система, разработанная и эксплуатируемых правительством США; она считается самой популярной навигационной системой на Земле и используется большим количеством электронных устройств по всему миру. Конечно, есть и другие навигационные системы, такие как российская система ГЛОНАСС, система BeiDou, принадлежащая Китаю, или Galileo, управляемый Европейским Союзом. Эти системы поддерживаются различными производителями устройств.

Для GPS, чтобы знать ваше текущее местоположение, он должен определить точную координату, где вы в настоящее время стоит. Итак, что мы подразумеваем под географической координатой?

Система географических координат — это система, которая находит точки на Земле, используя два значения координат: широту и долготу. Зная эти два значения, вы можете визуализировать любую точку на Земле на карте.

Как найти GPS Координаты любого местоположения на карте

Чтобы найти GPS координаты (широта и долгота) любого географического места на Земле с помощью Google Maps, выполните эти шаги:

1. Перейти к Картам Google по адресу https://maps.google.com.
2. Нажмите в любом месте на карте, где вы хотите увидеть координаты GPS. Небольшая коробка появляется в нижней части страницы Google Maps, показывающей текущее местоположение GPS координат (см. рисунок7-1).
3. Для дальнейшего изучения выбранного местоположения щелкните номера координат, и Google передаст вам точное местоположения в дополнение к предоставлению вам его почтового адреса (если это применимо).

Примечание! первый номер Gps представляет широту, а второй представляет долготу.

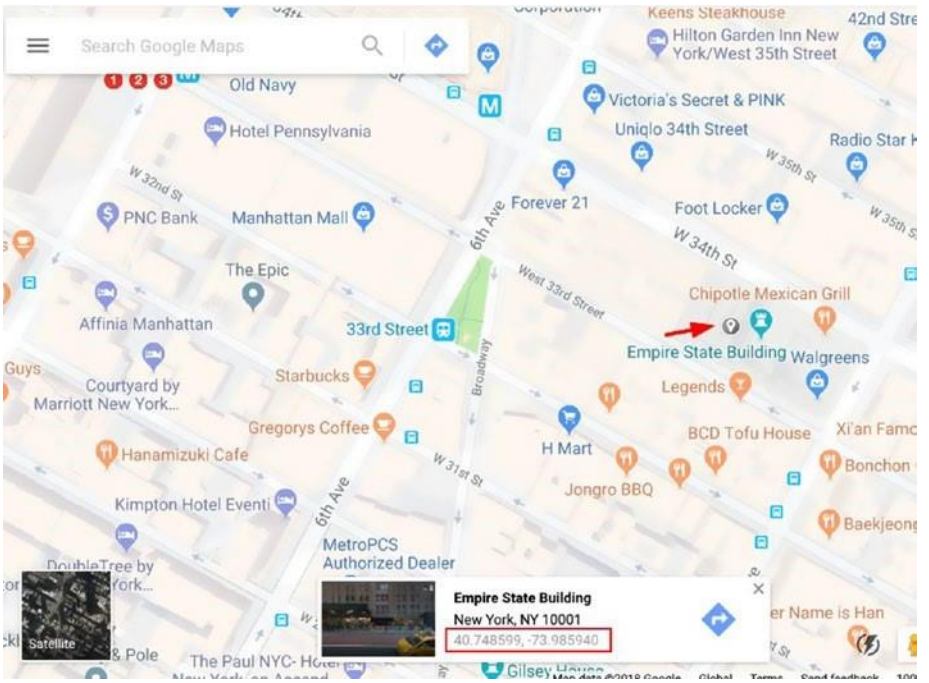

Рисунок 7-1. *Поиск GPS координат любого места на Земле с помощью Google Maps*

Примечание! Вы также можете найти широту и долготу точки, перейдя на http://itouchmap.com/latlong.html. Нажмите на карту и перетащите маркер в нужное место. Вы также можете ввести адрес (улица, город, штат и страна) в поле поиска, чтобы найти координаты Gps на карте.

Что бы преобразовать широту и долготу в десятичную, перейдите кhttps://andrew.hedges. name/experiments/convert_lat_long.

Как найти координаты геокода с адреса рассылки

Если у вас есть адрес для конкретного местоположения на Земле, но вы не знаете, как найти его координаты геокода на карте, перейдите на следующие бесплатные услуги:

- *Batch Geocoding* (https://www.doogal.co.uk/BatchGeocoding. php): Эта служба преобразует несколько адресов одновременно в эквивалентные координаты геокода (широта и долгота) с помощью Google Maps.
- *GPS Visualizer's Quick Geocoder* (www.gpsvisualizer.com/geocode): Эта служба преобразует адрес в эквивалентные координаты геокода (и работает как для Google, так и для Bing).
- *Batch Reverse Geocoding* (https://www.doogal.co.uk/ BatchReverseGeocoding.php): Эта служба преобразует номера координат геокода из различных систем координат в их эквивалентный приблизительный почтовый адрес.

Общие инструменты геопространственных исследований

Есть много онлайн-сервисов, которые могут помочь вам при исследовании онлайн-карты для различных видов информации. Ниже приведены самые популярные услуги:

- *Digital Globe* (https://discover.digitalglobe.com): Это простой в использовании глобальный инструмент изображений карт с расширенными поисковыми фильтрами.
- *Bing Maps* (https://www.bing.com/maps): Это альтернатива Картам Google.
- *Yandex Maps* (http://maps.yandex.com): Это российская альтернатива Google.
- *Baidu Maps* (http://map.baidu.com): Это китайская альтернатива Google.

- *Daum* (http://map.daum.net): Это корейская карта.
- *N2yo* (www.n2yo.com): Этот сайт выдает потоковео видео с разных спутников. Он также предоставляет информацию о следящих спутниках и зоне их покрытия.
- *Wigle* (https://wigle.net): Это показывает, Wi-Fi сети отображения по всему миру. Он показывает имя сети Wi-Fi вместе с адресом точки доступа MAC (аппаратное обеспечение), в дополнение к возможным местам, где бесплатный Wi-Fi может быть доступен.
- *BB Bike* (https://mc.bbbike.org/mc): Здесь вы можете сравнить две карты. Например, можно сравнить одно и то же местоположение на картах Bing и Google Maps, чтобы увидеть различия в целевом местоположении.
- *Newspaper Map* (https://newspapermap.com): Это списки всех газет по всему миру на карте; вы можете отфильтровать их в зависимости от местоположения и газетного языка.
- *USGS* (https://earthexplorer.usgs.gov): Здесь вы можете искать карту мира, используя различные критерии поиска, такие как адрес, имя места или координаты местоположения. Эта версия карты новее, чем Карты Google.
- *Google Street View* (https://www.google.com/streetview): Здесь вы можете просмотреть определенное место (которое должно существовать в базе данных Google Street View), как если бы вы там.
- *Google Maps Street View Player* (www.brianfolts.com/driver): Это показывает вид на улицу, где это возможно - между двумя точками на карте.
- *RouteView* (http://routeview.org/): Это еще один Google уличного обозрения.
- *Street View Movie Maker* (www.streetviewmovie.com): Здесь вы можете увидеть представление улицы Google между двумя местами, где это возможно– и скачать фильм на ваш компьютер для просмотра в автономном режиме.
- *Open Street Cam* (http://openstreetcam.org/): Здесь вы можете просмотреть открытые уличные камеры в определенном месте, где это возможно.
- *Zoom Earth* (https://zoom.earth): Здесь вы можете просматривать международные изображения облаков, обновляемые каждый день со спутников НАСА.
- *Hivemapper* (https://hivemapper.com): Это создает интеллектуальную 3D-карту из воздушно-десантного видео, раскрывая изменения, которые люди не могут видеть.
- *Liveuamap* (https://liveuamap.com): Это медиа-платформа с открытыми данными, которая показывает последние новости, фотографии и видео из различных зон конфликтов по всему

миру на карте. Эта услуга важна для получения информации из различных источников СМИ в зонах конфликтов.

- *Terrapattern* (www.terrapattern.com): Это визуальный инструмент поиска спутниковых снимков; это позволяет искать в широком географическом районе для конкретных визуальных эффектов. В настоящее время поиск овелит в следующих городах: Нью-йорк, Сан-Франциско, Питтсбург, Берлин, Майами и Остин.
- *dominoc925* (https://dominoc925-pages.appspot.com/mapplets/ cs_mgrs.html): Здесь вы можете просмотреть координаты справочной системы военной сетки (MGRS).
- *Google Map Alert* (https://followyourworld.appspot.com): Вы можете получать оповещение, когда новые изображения доступны как в Google Maps, так и в Google Планета Земля. Вы должны предоставить широту и долготу целевого местоположения.
- *Mapillary* (https://www.mapillary.com): Здесь вы можете просмотреть уличные изображения, загруженные людьми по всему миру. Эта услуга дает 3D-представление многих мест (ее база данных в настоящее время имеет 259,200,042 изображений), что полезно для обнаружения / исследовать конкретное место, пока вы не там.
- *Address Lookup* (https://ctrlq.org/maps/address): Найти адрес любого места на Картах Google; просто переместите маркер в определенное место на карте, и соответствующий адрес появится во всплывающем окне (см. рисунок7-2).

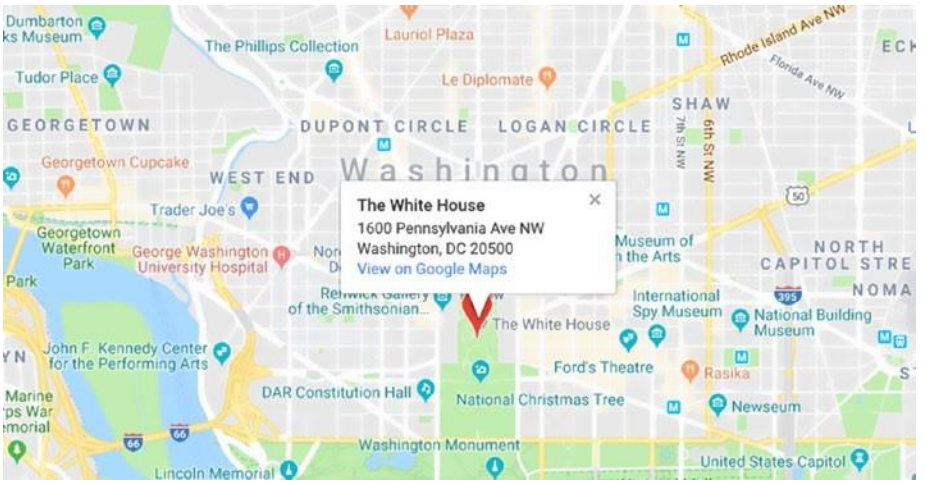

Рисунок 7-2. *Поиск адреса любой географической точки на Картах Google*

- *Inspire Geoportal* (http://inspire-geoportal.ec.europa.eu/ discovery): Этот сайт дает доступ к европейским пространственным данным.

- *Hiking and Biking Map* (http://hikebikemap.org): Это карта для пеших и велосипедных прогулок.
- *Viamichelin* (https://www.viamichelin.com): Это показывает, турист, рестораны, отели, трафик, и погода на карте мира.
- *CORONA Project* (http://corona.cast.uark.edu): В нем перечислено более 800 000 изображений, собранных спутником-шпионом CORONA, запущенным Организацией Объединенных Штатов и действовавшей в период с 1960 по 1972 год. Фотографии с высоким разрешением и охватывают различные географические районы по всему миру, особенно в странах, которые принадлежали к социалистическому блоку во время холодной войны.
- *Ani Maps* (www.animaps.com): Здесь вы можете создавать карты с интерактивной анимацией.
- *Trip Geo* (www.tripgeo.com/Directionsmap.aspx): Здесь вы можете создать карту направления, используя данные Google Street View.
- *GeoGig* (http://geogig.org): Это инструмент с открытым исходным кодом, который импортирует необработанные геопространственные данные (в настоящее время из Shapefiles, PostGIS или SpatiaLite) в репозиторий для отслеживания любых изменений в данных.
- *GRASS GIS* (https://grass.osgeo.org): Это программное обеспечение с открытым исходным кодом Geographic Information System (GIS), используемое для управления и анализа геопространственных данных, пространственного моделирования и визуализации.
- *Timescape* (https://www.timescape.io): Это платформа для повествования на основе карт.
- *Polymaps* (www.polymaps.org): Это библиотека JavaScript для создания динамических интерактивных карт в современных веб-браузерах; он поддерживает различные визуальные презентации для размещения.
- *Mapquest* (https://www.mapquest.com): Это поможет вам найти места на карте (например, отели, рестораны, кафе, продуктовые магазины, аптеки, аэропорты и многое другое). Вы также можете использовать эту услугу, чтобы найти лучший маршрут - кратчайший и предполагаемое время прибытия, когда происходит из одного места в другое (см. Рисунок 7-3).

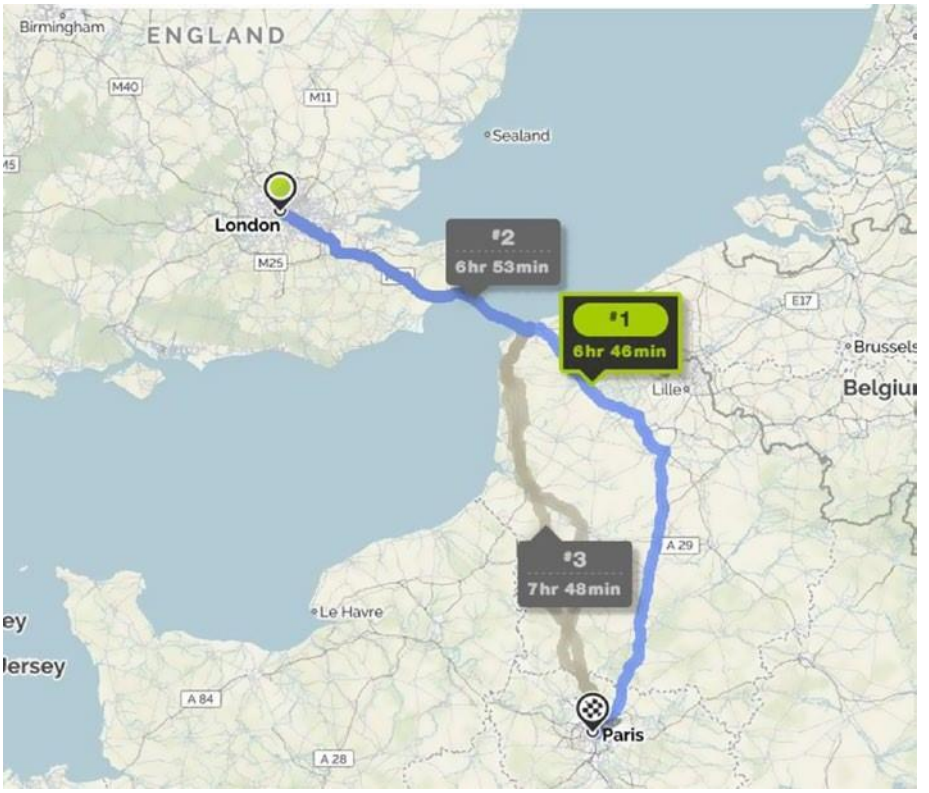

Рисунок 7-3. *Поиск лучших маршрутов между двумя локациями*

- *NGA GEOINT* (https://github.com/ngageoint): Это официальное хранилище национальных геопространственных разведывательных служб, связанных с картами на GitHub.
- *Free Map Tools* (https://www.freemaptools.com/radius-around- point.htm): Здесь вы можете найти радиус вокруг точки на карте.
- *Maphub* (https://maphub.net): Здесь вы можете создать интерактивную карту, добавив точки, линии, полигоны или метки в дополнение к индивидуальным фонам.
- *Crowdmap* (https://crowdmap.com): Это аннотация инструмент, который позволяет визуализировать информацию на карте и сроки.
- *Maperitive* (http://maperitive.net): Это программное обеспечение Windows для рисования карт на основе OpenStreetMap и данных GPS.
- *Perry-Castañeda Library Map Collection* (https://legacy.lib. utexas.edu/maps/index.html): Это списки онлайн-карты текущих интересов по всему миру в дополнение к различным картам, в том числе исторические карты-из разных мест по всему миру.

- *United Nations Geospatial Information Section* (www.un.org/Depts/ Cartographic/english/htmain.htm): В нем перечислены различные типы карт, такие как общие карты стран и миссия Организации Объединенных Наций по картографии.
- *Roundshot* (www.roundshot.com/default.cfm?DomainID=1&TreeI D=172&language=en): Здесь вы можете посмотреть живые камеры из выбранных регионов по всему миру. Дополнительная информация доступна для каждого выбранного местоположения, которое включает в себя физическое покрытие камеры на карте, прогнозы погоды, а также некоторые исторические данные / фотографии.
- *Live Earthquake Map* (http://quakes.globalincidentmap.com): Этот сайт дает в режиме реального времени информацию о землетрясениях, которые произошли по всему миру; он также охватывает важные инциденты, происходящие по всему миру, такие как янтарные предупреждения, вспышка болезней, деятельность банд, вопросы безопасности границ, нетеррористические авиационные инциденты, предикация терроризма и многое другое.
- *Universal Postal Union* (www.upu.int/en/the-upu/member- countries.html): Здесь вы можете найти почтовые индексы для всех стран.

Примечание! база данных имен местоположений с различными орфографическими написаниями на разных языках доступна на www.geonames.org.

чтобы увидеть список городов и поселков по всему миру, перейдите на www.fallingrain . com/world.

Коммерческие спутники

Есть много глобальных поставщиков спутниковых снимков высокого разрешения, которые предлагают свои услуги государственным органам безопасности и гражданским компаниям, чтобы помочь им предсказать будущие угрозы и принимать соответствующие решения. Ниже приведены самые популярные поставщики спутниковых снимков высокого разрешения:

- *European Space Imaging* (www.euspaceimaging.com):

  Обеспечивает -коммерческие - очень высокое разрешение изображения Земли с помощью следующих спутников: DigitalGlobe: WorldView-1, WorldView-2, WorldView-3, GeoEye-1, КвикБерд и IKONOS(archive).

- *Digital Globe* (https://www.digitalglobe.com/industries/ defense-and-intelligence): Это популярный веб ресурс для предоставления спутникового изображения конфликтов по всему миру с высоким разрешением.

Дата/Время вокруг света

Есть много бесплатных услуг, которые предлагают -в дополнение к текущей дате и времени в любом месте по всему миру-важные статистические данные о месте, такие как текущая погода, GPS координаты, важные адреса, близлежащие аэропорты, и известные места. Ниже приведены популярные услуги:

- *Wolframe Alpha* (www.wolframalpha.com): Введите конкретный город/город или любое место, и сайт будет получать важную информацию о нем, такие как население, текущее местное время, текущая погода, близлежащие города, близлежащие аэропорты, географические свойства, и многое другое.
- *SunCalc* (http://suncalc.net): Это показывает движение солнца в течение дня для любого данного местоположения на карте.
- *SunCalc* (https://www.suncalc.org): Это показывает солнечные данные для выбранного местоположения в дополнение к другой географической информации об этом месте.
- *Mooncalc* (https://www.mooncalc.org): Это показывает лунные данные для выбранного местоположения на Земле.

Социальные медиа, основанные на местоположении

Основные социальные медиа-платформы позволяют своим пользователям геотегировать некоторые из своих действий при их использовании. В этом разделе мы обсудим, как вы можете использовать функцию геолокации, предлагаемую основными платформами социальных медиа для сбора разведданных о конкретной цели или предмете.

YouTube

Для поиска видео с геококоординационными данными на YouTube можно использовать специальный инструмент под названием Geo Search Tool(https://youtube.github.io/geo-search-

tool/search. html). Вы можете искать видео по указанному адресу и в заданный таймфрейм. Вы также можете указать расстояние от ввода места; следовательно, поиск может быть столь же широким, как 1000 КМ или как узкий на 1 КМ. Возвратные результаты могут быть отфильтровамины в зависимости от времени загрузки видео. Окончательные результаты отображаются графически на карте в виде красного маркера (см. рисунок7-4).

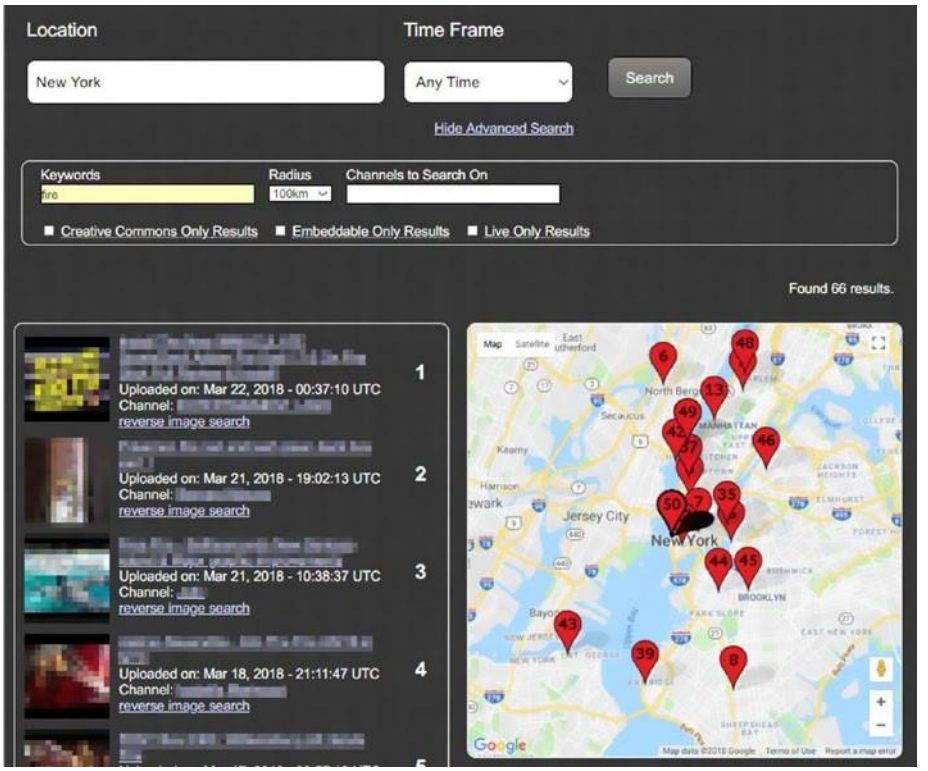

Рисунок 7-4. *Поиск фильмов о геолокации YouTube*

Facebook

Facebook является номером один сайт социальной сети. Это позволяет своим пользователям геотег сообщения, фотографии и видео, в дополнение к размещению обновлений статуса с их текущей геолокации. Мы уже рассмотрели, как искать в Facebook тщательно. В этом разделе мы сосредоточимся на поиске местоположений в пользовательском контенте Facebook.

ИСПОЛЬЗОВАНИЕ ГРАФИКА FACEBOOK В ПОИСКЕ МЕСТОПОЛОЖЕНИЯ

Мы уже рассмотрели, как найти значение профиля конкретного пользователя (или страницы/группы) Facebook. Следующие ссылки продемонстрируют, как использовать поиск графика Facebook для получения результатов на основе геотегированного контента.

Примечание! заменить номер 100003886582037 с профилем вашей цели iD в следующих запросах.

- Чтобы отобразить места, посещенный целевым профилем, введите следующее в панели адресов браузера: https://www.facebook.com/search/100003886582037/places-visited/.
- Чтобы отобразить последние места, которые были "зарегистрированы" целевым профилем, введите следующее в панели адресов браузера: https://www. facebook.com/search/100003886582037/places-checked-in/.
- To display common places where two targets have “checked in” previously, type the following in your browser address bar: https://www.facebook.com/search/Facebook_Profile_ID_1/ places-checked-in/ Facebook_Profile_ID_2/places-checked-in/ intersect/.
- Чтобы отобразить общие события, в которых ранее присутствовали две цели, введите следующее в панели адресов браузера: https://www.facebook.com/search/ Facebook_Profile_ID_1/ events/ Facebook_Profile_ID_2/events/intersect/.
- Чтобы просмотреть список сообщений, написанных в определенном месте, введите следующее в панели поиска Facebook: **Сообщения, написанные в Сиэтле, штат Вашингтон**.

Совет! Обнаружение пересечений между двумя профилями Facebook может выявить отношения между ними и открыть дверь для дальнейшего расследования.

FACEBOOK LIVE

Go to Facebook Live (https://www.facebook.com/live) чтобы увидеть, где Есть живое видео в настоящее время вещания. Видео в реальном времени отображаются на глобальной карте; пользователь может нажать на любое живое видео, представленное как синяя точка, чтобы просмотреть/сохранить ее.

Twitter

Twitter позволяет пользователям размещать твиты в сочетании с текущими данными о местоположении (см. рисунок 7- 5). Такие твиты могут помочь следователям определить текущее/предыдущее местоположение цели в определенный момент времени. В этом разделе мы рассмотрим, как найти твиты на основе их геолокации информации.

Рисунок 7-5. *Публикация твита с информацией о местоположении*

ПОИСК ТВИТОВ В ОПРЕДЕЛЕННОМ ГЕОГРАФИЧЕСКОМ МЕСТОПОЛОЖЕНИИ

Функциональность поиска Twitter позволяет искать твиты, размещенные в определенном месте, с помощью GPS-координат. Чтобы найти все твиты, размещенные в определенном месте на Земле, выполните следующие шаги:

1. Откройте Карты Google, перейдите к целевому местоположению и нажмите на точную точку на карте, чтобы увидеть ее GPS координаты (см. рисунок7-6).

Рисунок 7-6. *Извлечение GPS координат цели на Картах Google*

2. Перейти к окну поиска Twitter и **введите рядом:** затем широта цели и долгота, заключенные в кавычки (см. Рисунок7-7).

Рисунок 7-7. *Поиск всех твитов, которые соответствуют введенным координатам GPS*

3. Вы можете добавить более продвинутые операторы поиска Twitter к предыдущему поиску для дальнейшего фильтрации его результатов (см. рисунок7-8).

Рисунок 7-8. *Добавление расширенных фильтров поиска Twitter для уточнения поиска*

Как показано на рисунке 7-8, обратите внимание, что три фильтра применяются на предыдущем поиске местоположения.

- *Within:3mil*: Это ограничивает результаты тремя милями от целевых координат GPS.
- *Filter:images*: Это возвращает твиты, содержащие изображения в нем.
- *Since:2018-03-18*: Дата твита должна быть с указанной даты и позже.

Чтобы увидеть точное время, когда любой твит был размещен, навистете мыши над его метки времени (см. Рисунок 7-9). Пожалуйста, обратите внимание, что дата/время, которое появляется, в соответствии с часовом поясом настроек учетной записи Twitter, а не датой/временем загрузчика.

Рисунок 7-9. *Поиск даты/времени твита*

TWEET MAPPER

Tweet Mapper (https://keitharm.me/projects/tweet) это бесплатная услуга, которая перечисляет все геотегами tweets (все твиты размещены в то время как функция местоположения ON). Все, что вам нужно сделать, это ввести ручку Twitter цели, а затем нажмите Enter. Карта будет отображаться с красными маркерами (см. рисунок 7-10) по всем географическим местам, где эта цель публикует свои геотеговые твиты. Нажмите любой маркер, чтобы увидеть связанные твиты под картой.

Рисунок 7-10. *Отображение карты твитов для пользователя Apress*

ONE MILLION TWEET MAP

Посмотреть последний миллион твитов в мире на карте в https://onemilliontweetmap.com. Это интересная карта, чтобы увидеть живые твиты со всего мира в режиме реального времени. Для уточнения результатов могут быть применены различные фильтры.

QTR TWEETS

Qtr Tweets (http://qtrtweets.com/twitter) позволяет находить все твиты на определенном расстоянии от целевого местоположения на карте. Вы также можете искать ключевые слова и фильтровать результаты в соответствии с заранее определенными критериями, такими как твиты с изображениями и твиты с данными о нелокации.

TWEET MAP

Tweet Map (https://www.mapd.com/demos/tweetmap) позволяет визуализировать все твиты на глобальной карте. Нажмите на точки, которые представляют твиты, чтобы прочитать содержание твитов. Вы также можете увидеть топ хэштеги и твиты и искать их.

PERISCOPE MAP

Periscope Map (www.periscopemap.live) показывает Twitter Periscope живое видео на карте мира.

Other Social Media Platforms

Существуют сотни социальных медиа-сервисов, и многие из них позволяют пользователям геотег опубликовал содержание, но в этой главе мы сосредоточились на самых популярных двух: Facebook и Twitter.

Чтобы обогатить ваше мышление о широких возможностях сбора OSINT, предлагаемых гео- с поддержкой социальных медиа-услуг, мы кратко рассмотрим дополнительную услугу, которая использует данные геолокации пользователей, чтобы предложить функции. Эта услуга называется Strava, и она используется в основном в качестве приложения для социальных сетей для спортсменов для измерения и обмена своей деятельностью.

STRAVA HEAT MAP

A Strava тепловая карта (https://www.strava.com/heatmap) является показателем производительности спортивное приложение для спортсменов; он работает путем мониторинга спортивной деятельности через датчик GPS, существующий в их смартфоне (поддерживает Apple и Android) или любое другое поддерживаемое устройство, такое как GPS часы и головные узлы, и загружая такие данные на свои серверы, чтобы сделать их доступными для обмена. Это бесплатное приложение, но оно оставляет за собой некоторые премиум-функции для платных пользователей (например, показ расширенной статистики о деятельности пользователей). Наиболее популярным использованием этого приложения является отслеживание деятельности пользователей во время езды на велосипеде и бега.

На тепловой карте Стравы показано "тепло", произведенное агрегированной общественной деятельностью за последние два года; эта карта обновляется ежемесячно. В начале 2018 года Страва раскрыла несколько мест расположения военных баз в Сирии и Афганистане, потому что

военные личности внутри этих -секретных баз использовали это приложение для измерения и отслеживания своих фитнес-упражнений. Расположение базы появилось ясно, как солдаты двигались внутри базы, рисуя четкую границу каждой базы.

То, что произошло со Стравой, ясно показывает, что, несмотря на все меры безопасности, отсутствие подготовки пользователей по вопросам безопасности может привести к раскрытию военных секретов, которые доступны для сбора разведданных.

Примечание! изучение тепловой карты strava может выявить важную информацию о спортивных мероприятиях пользователей и маршрутах выполнения, которые они используют.

Вы можете просматривать фотографии, загруженные на Flickr на карте, перейдя на https://www. flickr.com/map. Snapchat также имеет живую карту, чтобы увидеть снимки событий, последние новости, и многое другое со всего мира в https://map.snapchat.com.

Проведение поиска местоположения в социальных сетях с использованием автоматизированных инструментов

Есть много инструментов, которые могут оказаться полезными при поиске данных (как геотегами, так и негеотегами) в Интернете. В этом разделе мы кратко упомянем некоторые популярные инструменты сбора OSINT для сбора различных видов общественной информации, включая геолокационный контент, как с интернет-платформ, так и с платформ социальных сетей.

- *Creepy* (https://www.geocreepy.com): Это геолокационный инструмент OSINT для сбора информации о геолокации из Twitter, Instagram, Google и Flickr.
- *Oryon OSINT Browser* (https://sourceforge.net/projects/oryon- osint- browser): Это содержит десятки ссылок OSINT на различные службы для обнаружения общественной информации; он также оснащен функциями конфиденциальности для защиты вашей личности при проведении поиска OSINT.

- *Maltego* (https://spreadsecurity.github.io/2016/09/03/open- source-intelligence-with-maltego.htm l): Это инструмент интеллектуального анализа данных с графическим интерфейсом, используемый для сбора информации с открытым исходным кодом; он визуализирует результаты и находит взаимосвязь между ними.
- *Spider Foot* (www.spiderfoot.net): Это автоматизированный инструмент OSINT, который запрашивает более 100 открытых источников данных для поиска информации о цели.

Информационные профили стран

Эти веб-сайты предлагают краткие обзоры и статистические данные о различных странах по всему миру. Такие обзоры включают информацию о географии страны, истории, политике, экономике, международных отношениях, культуре, путешествиях, военных, здравоохранении, образовании и других темах.

Ниже приведены самые популярные поставщики информации о профиле страны:

- *The World Factbook* (https://www.cia.gov/library/publications/ the-world-factbook/index.html): Это справочный ресурс, опубликованный Центральным разведывательным управлением (ЦРУ); он предоставляет информацию об истории, населении, правительстве, экономике, энергетике, географии, связи, транспорте, военных и транснациональных вопросах для 267 субъектов мира.
- *BBC Country Profiles* (http://news.bbc.co.uk/2/hi/country_ profiles/default.stm): Это руководство по истории, политике и экономике стран и территорий, а также справочная информация по ключевым институтам. Она также включает в себя архивное содержание службы Би-би-си.

Отслеживание транспорта

С развитием технологии связи, большинство транспортных средств и общественного / частного транспорта являются местоположение известно, то есть они поставляются с GPS или другим датчиком системы спутникового слежения, чтобы определить его текущее местоположение. Системы слежения предлагают полное представление о местоположении объекта в дополнение к другой информации о нем, такой как название транспортного средства (если это применимо), тип, груз, пункт назначения, владелец и многие другие технические детали. Многие бесплатные онлайн-услуги облегчают доступ к информации о наземных транспортных средствах, судах и самолетах; такая информация может оказаться чрезвычайно полезной во время любого типа онлайн-расследования, особенно если знать, что многие сайты также перечисляют предыдущие записи отслеживания транспортных средств, судов и судов в своих публичных базах данных.

Воздушное движение

Следующие службы отслеживают воздушные рейсы (грузовые, частные и туристические самолеты). Некоторые сайты даже предлагают оплату подписки для отслеживания военных самолетов! Вот список:

- *Flight Aware* (https://uk.flightaware.com): Эта компания считается крупнейшей компанией по отслеживанию данных полетов в мире; он предлагает свои услуги отслеживания полетов бесплатно для частных и коммерческих воздушных перевозок. FlightAware агрегирует свои источники данных из систем управления воздушным небом в 55 странах в дополнение к наземным станциям в более чем 150 странах. Используя эту услугу, вы можете искать рейсы по аэропорту происхождения и назначения или отслеживать конкретный рейс, используя номер рейса или авиакомпании. Частные рейсы также можно отслеживать с помощью этой услуги. При отслеживании конкретного рейса, вы можете увидеть предстоящие следующие рейсы и прошлые рейсы. Чтобы просмотреть всю историю полетов, необходимо оплатить абонентскую плату.
- *Flight Radar 24* (https://www.flightradar24.com; see Figure 7-11): This site offers an international real-time civilian flight-tracking service. It tracks more than 150,000 flights per day and has the ability to track specific types of military jets (like Russian and NATO jets) in some regions. Business subscribers can remove their private jets from public view, so it is essential to use more than one tracking service when investigating a specific target.

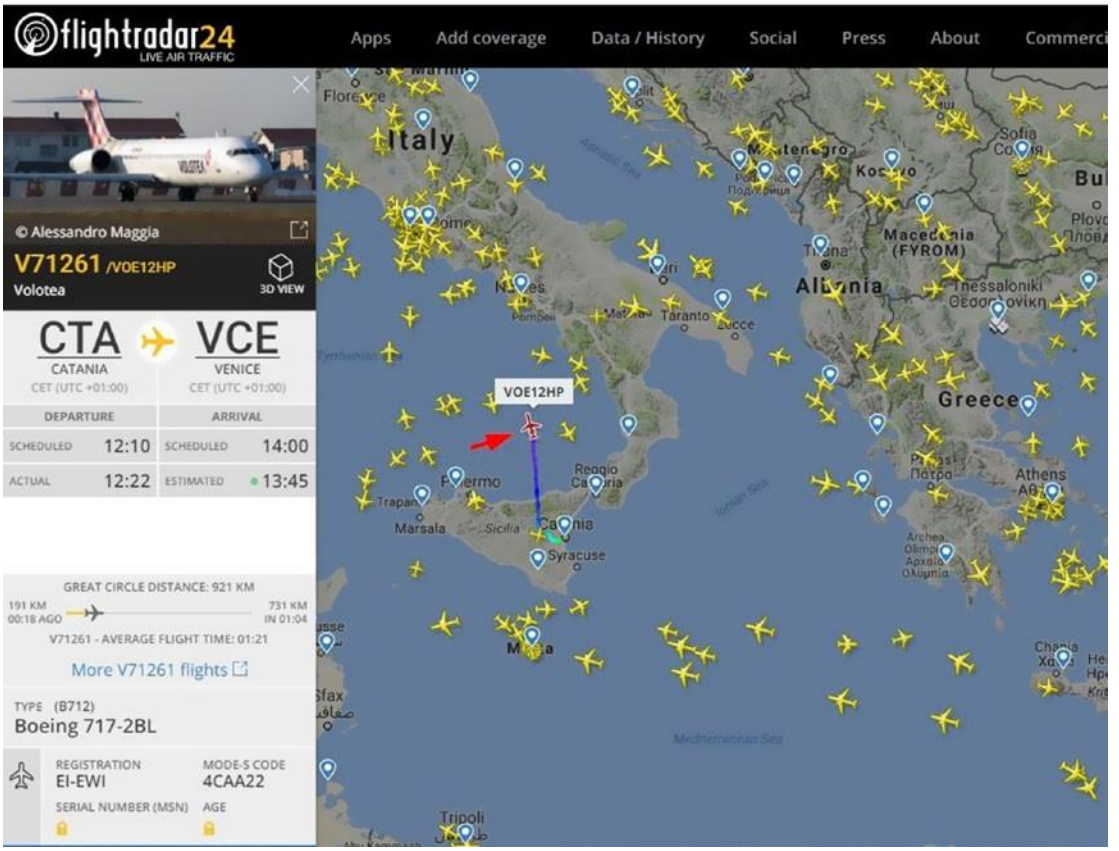

Рисунок 7-11. *Flightradar24 предлагает подробную информацию о каждом рейсе, включая аэропорты вылета и прибытия, маршрут рейса, расписание, предполагаемое время вылета и прибытия, текущую скорость полета и расстояние, а также тип самолета и модель. Другие сведения заблокированы для платных подписок.*

- *Air Cargo Tracker* (www.track-trace.com/aircargo): .
- *Radar Box 24* (https://www.radarbox24.com/): This is an international airplane tracker. The free account shows basic flight information; you need to pay to unlock the full features.

- *PlaneFinder* (https://planefinder.net): Сайт предлагает международное отслеживание самолетов. Бесплатный аккаунт показывает хорошую информацию о каждом рейсе.

- World aircrafts Database (www.planemapper.com/aircrafts)
  содержит информацию о международных авиакомпаниях вместе с самолетами (тип самолета и техническая информация), зарегистрированных на них. один и тот же сайт содержит подробную информацию о каждой авиакомпании по всему миру.

Морские движения

Следующие службы отслеживают движения судов по всему миру.

- *Marine Traffic* (https://www.marinetraffic.com): Это основной сайт морского слежения. Используя этот сайт, вы можете отслеживать любой корабль в мире. Сайт имеет огромную базу данных о судне детали и прошлый тракинг. Чтобы найти корабль, вы можете либо искать его имя с помощью средства поиска сайта или просто просмотреть карту, чтобы увидеть все доступные корабли. Чтобы увидеть конкретные сведения о кораблях, щелкните корабль на карте (корабли отображаются в виде стрелок на живой карте). Вы можете нажать кнопку Детали судна (см. Рисунок 7-12), чтобы увидеть полную информацию об этом корабле, такие как имя, номер MMSI, номер ИМО, флаг, вес, тип судна, размеры, год построен, последняя позиция, история названия судна (если корабль изменил свое название, предыдущие имена и флаги появятся здесь), и многое другое. Вся эта информация доступна с бесплатной учетной записью (на самом деле, я даже не зарегистрироваться для просмотра). Платные учетные записи дают больше информации, особенно в отношении индивидуального представления карты, прошлого отслеживания и истории рейсов.

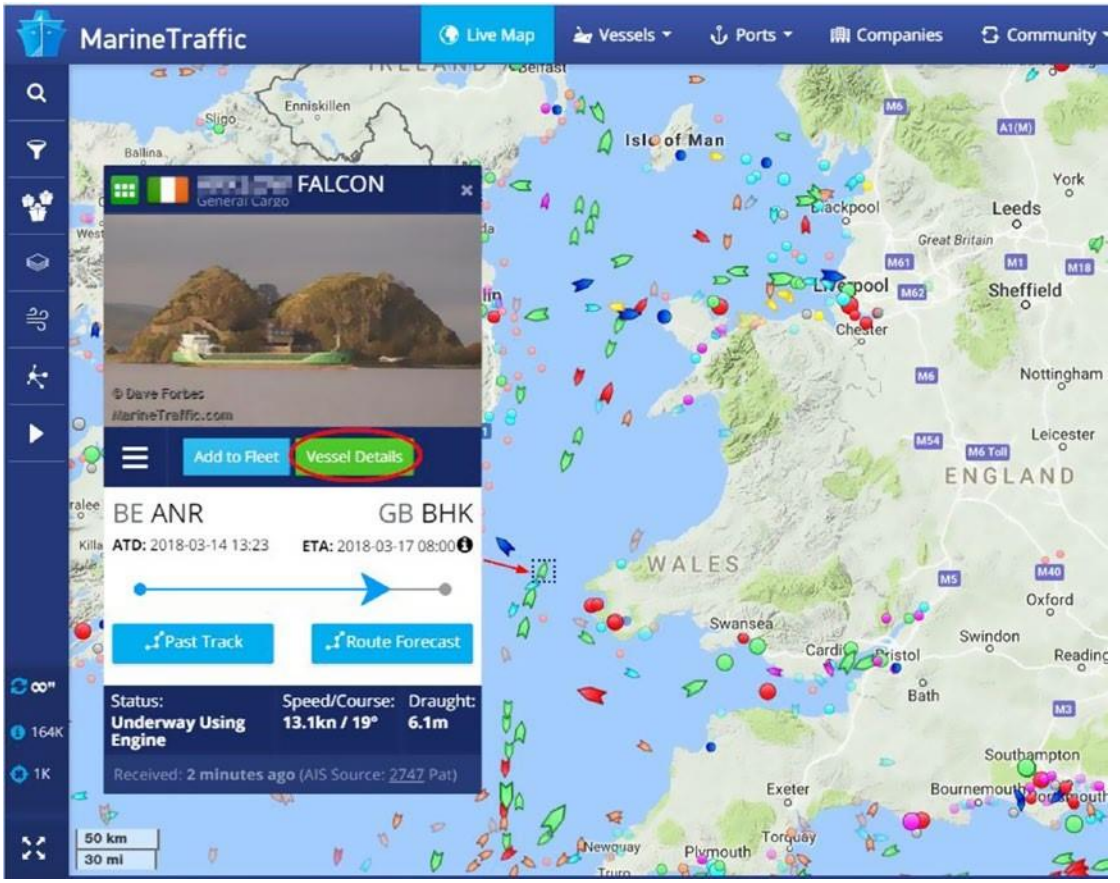

Рисунок 7-12. *Отслеживание судов с помощью веб-сайта Marine Traffic*

- *Container Tracking* (www.track-trace.com/container): Это отслеживает контейнеры для 125 компаний; Вам нужно поставить только номер контейнера.
- *Vessel Finder* (https://www.vesselfinder.com): Это служба слежения за судном.
- *Cruise Mapper* (www.cruisemapper.com): Это показывает треки круизов и дает подробную информацию о каждом из них, в дополнение к их текущим и прошлым местам.
- *Ship Finder* (http://shipfinder.co): Это отслеживает суда и дает подробную информацию о слежении судов.

Это сайты, могут быть полезны при отслеживании судна информация в Интернете:

- Список префиксов контейнера(www.prefixlist.com)
- международные идентификационные коды владельцев контейнеров (https://www.biccode.org/bic-codes/)
- международный портовый код (www.infodriveindia.com/TradeResources/Port.aspx)

Транспортные средства и железные дороги

Следующие сайты дают информацию о движении наземных транспортных средств и железных дорог:

- *ASM* (https://asm.transitdocs.com): Это предлагает в режиме реального времени отслеживание поездов по всей территории Соединенных Штатов.
- *Train Time* (https://traintimes.org.uk/map/tube): Это предлагает живую карту поездов лондонского метро.
- *Aprs* (https://aprs.fi): Это показывает информацию в режиме реального времени, собранную из сети автоматической системы отчетности позиций Интернет.
- *Spoorkaart* (http://spoorkaart.mwnn.nl): Это железнодорожный трекер для Нидерландов.
- *Junatkartalla* (https://junatkartalla.vr.fi/?lang=en-US Track): Это отслеживает поезда в режиме реального времени по всей Финляндии.
- *Travic : клиент транзитной визуализации* (http://tracker.geops.ch/?z=11&s=1&x=529282.4572&y=6853173.3731&l=transport): он предлагает живое отслеживание общественного транспорта (автобус, трамваи, поезда) в Нидерландах.

- *GotoBus* (https://www.gotobus.com/track-bus-status): Это система слежения за автобусами, которая отслеживает автобусы в отдельных регионах по всему миру для автобусных компаний, которые занимаются этой услугой (США, Мексика, Европа и Канада).
- *Germany Train Route Maps* (www.apps-bahn.de/bin/livemap/ query-livemap.exe/dn?L=vs_livefahrplan&livemap): Это предлагает маршрутные карты для Германии.

Примечание! чтобы увидеть сравнение дорожных знаков в разных странах, перейдите на https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Comparison_of_MUTCD-influenced_traffic_signs.html. Эта информация может быть полезна при изучении некоторых изображений, содержащих дорожные знаки. это может помочь определить страну происхождения, и, возможно, местоположение-предмет изображения.

Отслеживание пакетов

Отслеживание пакетов полезно для отслеживания поставок по всему миру. Если ваша работа OSINT требует расследования посылки, отправленной по суше или по воздуху, вы можете использовать следующие ссылки, чтобы найти более подробную информацию о нем:

- *After Ship* (https://www.aftership.com/couriers Track 447): Это отслеживает курьеров по всему миру. Просто введите номер пакета, и он автоматически обнаружит курьерскую компанию.
- *Tracking EX* (https://www.trackingex.com): Это отслеживает 235 трекеров.
- *17 Track* (https://www.17track.net/en): Это услуга отслеживания пакетов.

- *Package trackr* (https://www.packagetrackr.com): Это отслеживает глобальных трекеров и визуализирует путь доставки с помощью Google Maps.
- *Boxoh* (www.boxoh.com): Это сервис отслеживания пакетов для USPS, UPS, FedEx и DHL/AirBorne.
- *Canada Post* (https://www.canadapost.ca/cpotools/apps/track/personal/findByTrackNumber?execution=e1s1): Это отслеживает пакеты в Канаде.
- *Royal Mail* (https://www.royalmail.com/track-your-item#): Это отслеживает королевскую доставку почты. Отслеживание по карте (www.trackonthemap.com) позволяет людям следить за вашим местоположением в Интернете. Вам нужно устройство с gps трекер, smartphone для работаты.

Вебкамеры

Есть много сайтов, предлагающих бесплатный доступ к общественным веб-камерам по всему миру. Ниже приведены самые популярные из них:

- *World Web Cam Search* (http://world-webcams.nsspot.net): Это отображает доступные веб-камеры со всего мира с помощью Google Maps.
- *Earth Cam* (https://www.earthcam.com): Это прямая веб-камера из разных мест по всему миру.
- *Fisgonia* (www.fisgonia.com): Это визуальное представление веб-камеры с помощью Google Maps из разных мест по всему миру. Вы можете фильтровать камеры в соответствии с различными категориями, такими как аэропорты, железнодорожные станции, животные, трафик, университеты и так далее, и вы можете указать страну с помощью Google Maps.

- *World Cam* (https://worldcam.eu): Это списки веб-камер в разных местах по всему миру и предлагает информацию о местоположении, такие как их местоположение на картах и информацию о погоде о целевой области.
- *UM Weather* (http://cirrus.sprl.umich.edu/wxnet/wxcam.php): Это списки сотен метеорологических камер по всей Северной Америке.
- *Opentopia* (www.opentopia.com/hiddencam.php): В нем перечислены общедоступные веб-камеры из разных мест по всему миру.
- *Mila* (https://www.livefromiceland.is/webcams/geysir): Это веб-камера из Исландии.

Как мы уже упоминали в главе 4, Google также может быть использован для поиска общедоступных веб-камер в Интернете. Лучшее место, чтобы сделать такой поиск Google Hacking Database (GHDB) at https://www.exploit-db.com/google-hacking-database13/.

Метаданные цифрового файла

Мы уже рассмотрели в главе 2, как исследовать метаданные цифровых файлов (таких как изображения, видео, файлы Microsoft Office и PDF). Некоторые цифровые файлы, особенно геотегов изображения и видео, могут содержать GPS координаты. Изучение таких файлов легко; все, что вам нужно сделать, это скопировать GPS координаты и использовать услуги в этой главе, чтобы найти адрес на карте объекта фото или видео.

Итоги

Большинство действий пользователей в Интернете могут быть связаны с информацией о геолокации. Обнаружение информации в Интернете с помощью поиска на основе местоположения может сузить результаты поиска и сделать ваше расследование более целенаправленным.

В следующей главе мы поговорим о чем-то, отличаемм от всего уже упомянутого. Вы узнаете, как использовать различные инструменты и методы для сбора разведданных, в основном технической информации, о целевой ИТ-инфраструктуре и веб-сайтах.

Глава 8

Technical Footprinting

Footprinting это первая задача, что хакеры должны делать, прежде чем проводить атаки на компьютеризированные системы. Это акт использования различных инструментов и методов, чтобы получить как можно больше информации, перед атакой цели. В предыдущих главах мы рассмотрели, как использовать широкий спектр инструментов и методов для сбора данных в Интернете о различных организациях (таких как люди и организации). Тем не менее, мы не освещали, как исследовать веб-страницы и сеть цели для получения технической информации.

В главе 1, мы определили OSINT как ссылку на всю информацию, которая находится в открытом доступе. Это означает, что источники OSINT отличаются от других форм разведки в том, чтобы быть юридически доступными для общественности, не нарушая никаких законов о неприкосновенности частной жизни или авторском праве. Это юридическое определение также применяется к техническому следу при определении ИТ-технологий, служб и сетей.

В главе 1мы провели различие между тремя типами сбора информации:
пассивный, полупассивный и активный. В этой главе мы сосредоточиваемся только на методах пассивной разведки, поскольку два других метода могут иметь юридические последствия, если они будут применяться без надлежащего разрешения. Таким образом, вы не можете рассматривать их как принадлежащие к OSINT-сбор сферы.

В пассивной разведке, цель ничего не будет знать о вашей деятельности по сбору информации. Вы не будете отправлять никаких пакетов данных на целевые серверы. Вместо этого, вы будете просматривать целевой веб-сайт, как и любой обычный посетитель Интернет искать интересную информацию. Объем информации, собранной таким образом, ограничен тем, что представлено на целевом веб-сайте. В полупассивной разведке вы отправляете ограниченный трафик на целевой сервер. Тем не менее, этот трафик не запустит сигнализацию систем безопасности, реализованных сетью целевой организации (брандмауэр и IDS), потому что этот трафик будет напоминать любое регулярное поведение интернет-трафика.

N. A. Hassan and R. Hijazi, *Open Source Intelligence Methods and Tools*, https://doi.org/10.1007/978-1-4842-3213-2_8

Как пассивная разведка, так и полупассивная разведка разрешены законом в крупных странах (без получения разрешения), хотя некоторые страны могут также рассматривать некоторые виды полупассивной деятельности как вид незаконной footprinting.

Примечание! Активная разведка предполагает непосредственное взаимодействие с целевой системой; вы можете достичь этого различными способами. Например, можно использовать методы социальной инженерии для получения информации из справочной службы цели.

Делая пассивную разведку, вы можете собрать полезную техническую информацию, такую как идентификация IP-адресов целевой организации, извлечение информации о доменных именах, идентификация имен ее поддоменов и идентификация ИТ-устройств и технологий в использовании. Кроме того, можно собирать традиционные типы информации (например, имена сотрудников, электронные письма и метаданные документов) с целевого веб-сайта, которые могут быть использованы для профиля целевых сотрудников.

Исследуйте целевой веб-сайт

Первое место, куда вам нужно пойти, когда начинается ваш технический footprinting —веб-страницыцелевойкомпании. Исследование веб-сайта компании даст вам чрезмерное количество полезной информации с точки зрения безопасности. Ниже приведены лишь некоторые примеры:

- Адрес компании
- Офисные отделения
- Ключевые сотрудники
- Открытые вакансии и предложение о работеs (предложения о работе могут выявить технологии, используемые в компании)
- Схема электронной почты (глядя на адреса электронной почты сотрудников)

- Номер телефона
- Компании-партнеры – или любая компания, имеющая тесные деловые отношения
- Часы работы и праздники
- Новости о целевой организации (новости о слиянии или приобретении)
- Технология, используемая при создании целевого веб-сайта
- Используется система электронной почты (многие организации используют технологию с открытым исходным кодом, например Horde и Roundcube)
- ИТ-технологии (аппаратное и программное обеспечение), используемые целевой организацией
- VPN-провайдер (если таковые.)
- Цифровые файлы (такие как PDF-файлы и электронные таблицы) и метаданные (некоторые организации даже размещают свой список инвентарных запасов, включая ИТ-оборудование, на своих веб-сайтах)
- Политика конфиденциальности или безопасности, в ней перечислены элементы управления ИТ-безопасностью (например, такие документы могут содержать политику создания паролей)
- Информация о сотрудниках организации

Веб-страницы состоят из HTML-кода, поэтому желательно начать с этого. Вы можете просмотреть источник HTML, чтобы увидеть, оставили ли разработчики какую-либо полезную информацию в комментариях HTML. Необходимо также проверить головной раздел исходного кода HTML для прилагаемых документов, таких как CSS и JavaScript файлов. Эти файлы могут также содержать комментарии их разработчиков.

Примечание! для просмотра исходного кода HTML любой веб-страницы с помощью Firefox, нажмите правой кнопкой мыши на целевую страницу и выберите Источник страницы Просмотра. Вы можете найти полезную информацию в HTML комментарии теги, которые выглядят следующим образом: !-- это комментарий -->.

Многие компании заказывают дизайн сайта у иностранных компаний. Обнаружение этой проблемы из исходного кода HTML сделает аутсорсинговую компанию частью вашей деятельности по расследованию.

Примечание! Firefox имеет встроенную утилиту для оказания помощи веб-разработчиков. Firefox Инструменты разработчика представляют собой набор инструментов веб-разработки, которые могут быть использованы для анализа исходного кода HTML веб-страниц. для запуска инструмента нажмите ctrl-Shift'i или просто перейдите в меню инструментов, выберите веб-разработчика, а затем выберите панель инструментов разработчика.

Исследуйте файл Robots.txt

Веб-роботы также известны как *crawlers* or *spiders*—используются поисковыми системами для автоматического сканирования Интернета для обнаружения нового контента. Они используются всеми поисковыми системами, такими как Google и Yahoo для индексирования веб-контента. Владельцы веб-узлов используют файл robots.txt в корневом каталоге веб-сайта, чтобы дать инструкции веб-роботам на каких страницах они хотят включать или исключать во время процесса сканирования. Когда робот читает Disallow: в файле robots.txt, он будет игнорировать путь файла после него. Для целей разведки, проверка этого файла покажет, что владелец сайта хочет скрыть от общественности. Для просмотра файла robots.txt любого веб-сайта, введите в панели адрес браузера целевое доменное имя, за которым следует передний слэш, а затем robots.txt. См Рисунок 8-1 для образца роботов. txt файл для Apress.com доменное имя.

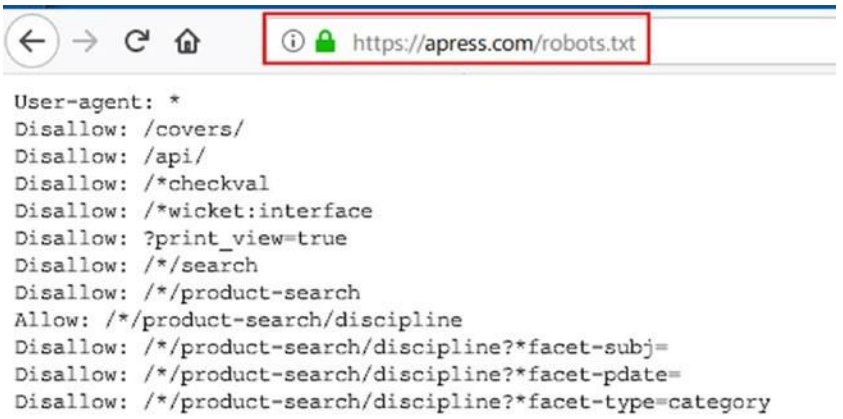

Рисунок 8-1. *Пример файла robots.txt, показывающий, какие страницы могут быть прослежены веб-роботами*

Примечание! robots Disallowed это проект на github (https://github.com/ danielmiessler/RobotsDisallowed) что собирает "Disallow" каталоги из robots.txt файлы лучших веб-сайтов в мире (взято из Alexa 100K глобального рейтинга).

Зеркало атакуемого веб-сайт

Иногда удобнее при просмотре HTML-кода — загрузить весь атакуемы веб-сайт для просмотра/разбора в автономном режиме, и существуют автоматизированные инструменты для выполнения этой задачи. Ниже приведены самые популярные:

- *HTTrack* (https://www.httrack.com): Здесь вы можете скопировать веб-сайт для просмотра в автономном режиме.
- *GNU Wget* (www.gnu.org/software/wget): Здесь вы можете получить файлы с помощью http, HTTPS, FTP и FTPS Интернет-протоколы.
- *BlackWidow* (www.softbytelabs.com/en/BlackWidow): Здесь вы можете скачать полный сайт или его часть. Вы также можете скачать любые файлы, включая видео YouTube, встроенные в сайт.

Извлеките ссылки

Целевой веб-сайт может быть связан с другими приложениями, веб-технологиями и связанными с ними веб-сайтами. Сброс его ссылок позволит выявить такие соединения и дать URL-адреса других ресурсов (таких как CSS и JavaScript файлы) и доменов, связанных с ним. Есть много онлайн-сервисов для извлечения URL-адресов, изображений, скриптов, iframes и встраиваемых целевых веб-сайтов. Ниже приведены самые популярные (Нужно использовать более одного сервиса, поскольку они выдают разные результаты):

- *Link Extractor* (www.webtoolhub.com/tn561364-link-extractor. aspx): Результаты можно экспортировать в файл Excel.
- *Free URL Extractor* (www.bulkdachecker.com/url-extractor): Извлекайте ссылки из URL/Domain (например, ссылки, изображения, скрипты и внедрения).
- *Link Gopher* (https://sites.google.com/site/linkgopher): Это дополнение Firefox, которое извлекает все ссылки с веб-страниц, включая встроенные, и отображает их на новой веб-странице.

Примечание! чтобы узнать, куда перенаправляет целевой веб-сайт Url, используйте следующую услугу: http://redirectdetective.com.

Проверьте обратные ссылки целевого веб-сайта

Следует также рассмотреть возможность проверки всех обратных ссылок на домен целевой организации, так как некоторые связанные веб-сайты могут раскрывать полезную информацию о цели. Чтобы увидеть все связанные веб-сайты с определенным доменным именем, введите следующее в Google: **site:* darknessgate. com** (должно быть пространство между звездочкой и доменным именем).

Это вернет все сайты, которые ссылаются на www.DarknessGate.com. Чтобы уточнить поиск и вернуть только результаты из других доменных имен, исключить все ссылки на целевой домен из себя (см. рисунок Рисунок 8-2).

Рисунок 8-2. *Поиск обратных ссылок на конкретное доменное имя с помощью продвинутых операторов Google*

Мониторинг обновлений веб-сайта

Вы должны регулярно следить за веб-обновлениями целевого веб-сайта. Конечно, это не удобно контролировать веб-сайт с сотнями страниц, так что есть инструменты для автоматизации этой задачи. Популярным инструментом для этого является WebSite-Watcher(http://aignes.com/index.htm), которая является коммерческой программой. Это программное обеспечение будет контролировать веб-страницы, форумы и RSS-каналы для новых сообщений и ответов (даже защищенных паролем страниц) и сообщать об изменениях.

Проверить архивный контент веб-сайта

OSINT следователи должны помнить, что Интернет постоянно меняется. Организации регулярно обновляют свои веб-сайты, и прошлые версии целевого веб-сайта могут сливать важную информацию. Поэтому, убедитесь, что взглянуть на предыдущие версии целевого веб-сайта с помощью Wayback Machine (www.archive.org).

Примечание! чтобы узнать, кто размещает любой веб-сайт, перейдите на https://www. whoishostingthis.com.

Определить используемые технологии

Существуют различные способы обнаружения типа технологии, используемой в целевой организации. Например, вакансии, предлагаемые на сайте целевой организации, а также на других специализированных веб-сайтах вакансий, являются ценным источником информации (вы можете найти необходимый тип навыков, необходимые ИТ-сертификаты, прошлый опыт работы с конкретными продуктами/поставщиками) , и из этого вы можете легко определить тип ИТ-инфраструктуры, ОС и другого программного обеспечения, используемого.

Совет! если целевая организация имеет более одного филиала, тип необходимых навыков, как указано на должностях, для конкретного филиала может быть показателем деятельности, происходящей в этом филиале.

Для определения технологий, используемых для создания целевого веб-сайта, существует множество онлайновых сервисов и инструментов, доступных для этой задачи. Самый популярный сервис Built With (https://builtwith.com). Чтобы воспользоваться этой услугой, введите целевое доменное имя, чтобы просмотреть его профиль технологии и профиль отношений. Технологический профиль будет отображать подробную информацию о целевых веб-сайтах, таких как аналитика и коды отслеживания, виджеты, языки веб-сайтов, оптимизирован ли он для мобильных просмотров, сети доставки контента (CDN), БиблиотекиJavaScript, рекламные сети, e-mail услуги, DNS, SSL сертификат, тип веб-сервера, кодирование и документированиеинформации. Представление профиля отношения предлагает важную информацию о целевом домене; оно показывает историческое использование идентификаторов (таких как идентификаторы Google AdSense), которые передаются другим веб-сайтам. Зная эту информацию, вы можете раскрыть, какие веб-сайты также контролируются одной и той же компанией/отдельным лицом (см. рисунок8-3).

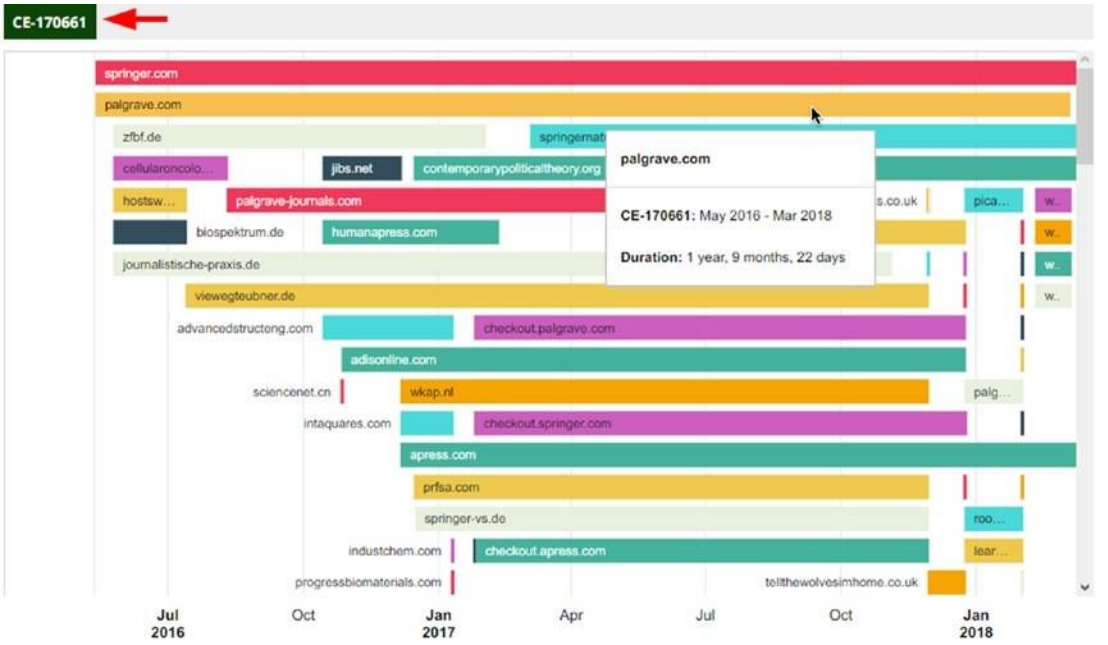

Рисунок 8-3. *Исследование профиля отношений Apress.com показывает использование и историю тегов CrazyEgg (диограмма предоставлена https://builtwith.com)*

Другим инструментом для выявления веб-технологий, используемых на целевых веб-сайтах, является Wappalyzer (https://www.wappalyzer.com). Вы можете установить его в качестве дополнения к вашему браузеру Firefox или Chrome, чтобы исследовать технологии, используемые на любом веб-сайте, который вы посещаете.

Выявление ключевых технологий, используемых как программного обеспечения, так и аппаратного обеспечения, поможет вам провести некоторые целенаправленные исследования для выявления каких-либо уязвимостей в программном обеспечении целевой организации, выявления дефектов, связанных с продуктом, и выявления конкретных приложений проблемы конфигурации. В следующем разделе мы продемонстрируем, как определить целевой сервер ОС с помощью онлайн-инструмента.

Примечание! чтобы найти домены обмена же Google Analytics iD, перейдите на https://dnslytics.com/reverse-analytics.

Примечание! Многие из них оборудования (например, маршрутизаторы, управляемые коммутаторы, брандмауэры, серверы, элементы управления доступом, интернет-камера наблюдения, и даже пакеты программного обеспечения) поставляется предварительно настроенс с именем пользователя по умолчанию и паролем. если тот, кто устанавливает такие устройства, забывает обновить/удалить учетные данные по умолчанию, такие устройства уязвимы. следующие сайты список сотни его оборудования по умолчанию учетных данных:

- *CIRT* (https://cirt.net/passwords)
- *Default Password* (https://default-password.info)
- *Default Password Lookup* (www.fortypoundhead.com/ tools_dpw.asp)
- *Router Passwords* (http://routerpasswords.com)
- *Open Sez Me!* (http://open- sez.me)
- *Hashes* (https://hashes.org)

для выявления уязвимостей нулевого дня любого программного обеспечения, удаленных служб или приложений, включая эксплойты на стороне клиента, проверьте на следующие сайты:

- *Exploit Database (*https://www.exploit-db.com)
- *Packet Storm* (https://packetstormsecurity.com)
- *Security Focus* (www.securityfocus.com/bid)
- *National Vulnerability Database* (https://nvd.nist.gov)
- *CVE Details* (https://www.cvedetails.com)
- *CVE* (http://cve.mitre.org)

- *0day* (http://0day.today)
- *Secunia Research* (https://secuniaresearch.flexerasoftware.com/community/research)

Web Scraping утилиты

Существуют автоматизированные инструменты, которые могут помочь вам легко собирать различные типы информации с целевого веб-сайта. Такие инструменты известны как *web scraping* tools или *web data extraction* tools. Представьте, что вы хотите собирать электронные письма с большого веб-сайта (с тысячами страниц). Делать это вручную было бы сложной задачей, но при использовании автоматизированных инструментов, вы можете сделать это одним щелчком мыши.

THE HARVESTER

The Harvester (https://github.com/laramies/theHarvester) является инструментом для сбора имен поддомейнов, адресов электронной почты, виртуальных хостов, открытых портов/баннеров и имен сотрудников из различных публичных источников, таких как Google, Bing, LinkedIn, Twitter, Yahoo, pgp и многое другое. Поиск, проводимый с помощью этого инструмента, является пассивным, а это означает, что цель не заметит никакой разведывательной деятельности с вашей стороны.

The harvester предустановлен на Kali Linux. Тем не менее, вы можете установить его на любую Linux-ОС, введя следующую команду в терминале:

```
apt-get theharvester
```

Чтобы собрать электронные письма целевой организации, откройте программу и введите следующие:

```
theharvester -d springer.com -b all -l 500 -f results.txt
```

theharvester используется для выполнения инструмента, и это несколько вариантов:

- -d определяет домен для поиска или название компании.

- -b определяет источник данных, такой как google, googleCSE, bing, bingapi, pgp, linkedin, google-profiles, jigsaw, twitter, googleplus, и другие.
- -l ограничивает количество результатов для работы с ними.
- f- сохраняет результаты в HTML или XML файле.

В предыдущем скрипте мы просим инструмент вытащить результаты из всех источников данных и ограничить результат количеством 500. Кроме того, генерируемые результаты должны быть сохранены в файле, названном results.txt в том же рабочем каталоге (см. рисунок 8-4).

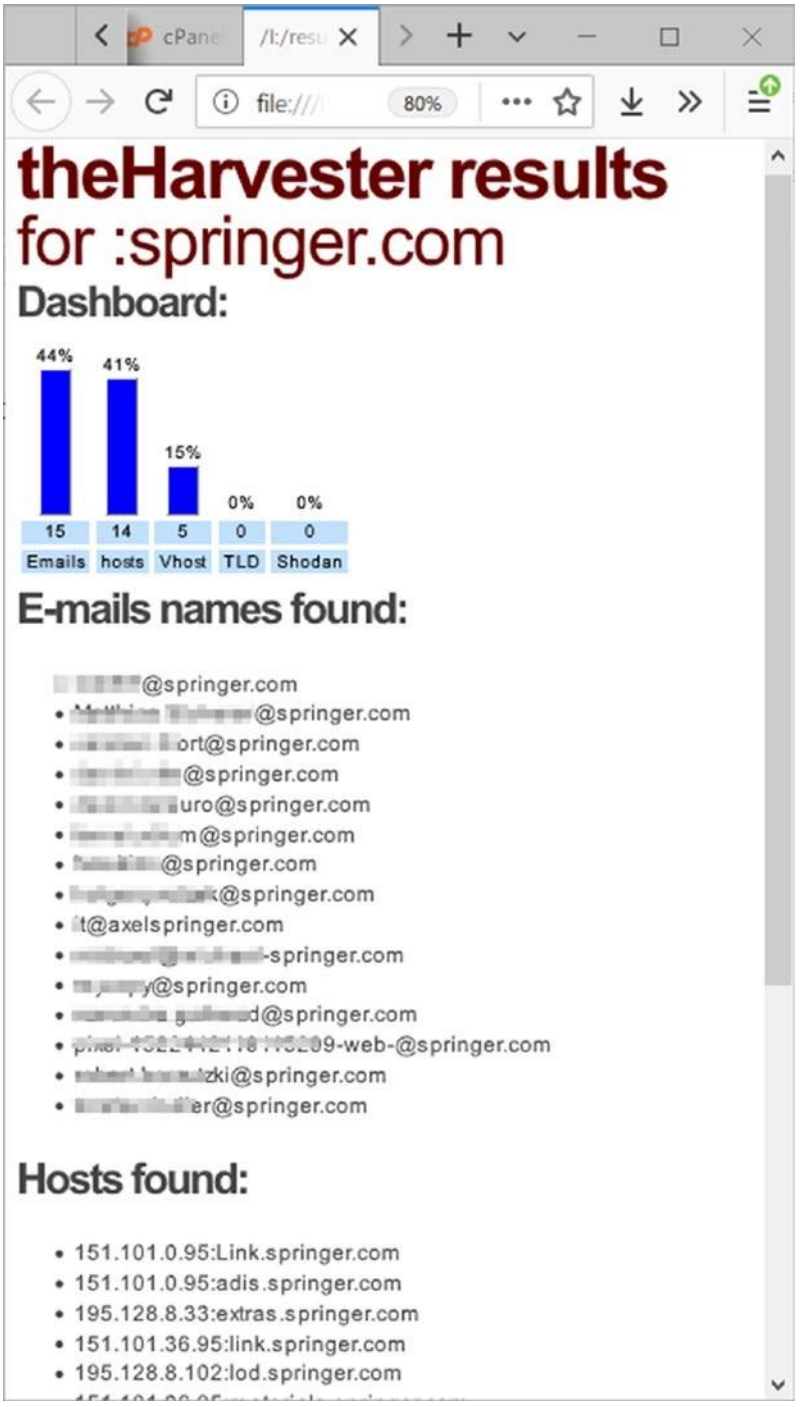
cPanel
/l:/resu
file:///
80%
theHarvester results
for :springer.com
Dashboard:
44%
41%
15%
0%
0%
15
14
5
0
0
Emails
hosts
Vhost
TLD
Shodan
E-mails names found:
@springer.com
@springer.com
ort@springer.com
@springer.com
uro@springer.com
m@springer.com
@springer.com
k@springer.com
t@axelspringer.com
-springer.com
y@springer.com
d@springer.com
09-web-@springer.com
zki@springer.com
er@springer.com
Hosts found:
151.101.0.95:Link.springer.com
151.101.0.95:adis.springer.com
195.128.8.33:extras.springer.com
151.101.36.95:link.springer.com
195.128.8.102:lod.springer.com

Рисунок 8-4. *поиск адресов электронной почты от целевого доменного имени Springer.com с помощью TheHarvester. Инструмент также разрешает целевое доменное имя в свой IP-адрес и обнаруживает много виртуальных хостов, связанных с целевым доменным именем.*

Предыдущий пример — самое простое использование этого инструмента; мы смогли собрать целевые адреса электронной почты в дополнение к обнаружению многих поддоменных имен целевого основного домена. Этот поиск также обнаруживает виртуальные хосты (имеется в виду несколько веб-сайтов, размещенных на одном сервере). После получения некоторых целевых адресов электронной почты, вы можете использовать методы в предыдущих главах, чтобы построить профиль для каждого из них.

ЭКСТРАКТОР ВЕБ-ДАННЫХ

Web Data Extractor (www.webextractor.com) это коммерческая программа, которая собирает различные типы данных, включая URL-адреса, номера телефонов и факсов, адреса электронной почты, а также информацию мета-тега и текст тела.

ЭКСТРАКТОР ЭЛЕКТРОННОЙ ПОЧТЫ

Email Extractor (https://www.email-extractor.io) — это дополнение Chrome, которое извлекает все сообщения электронной почты из веб-страниц, которые в настоящее время посещаются.

Исследование доменного имени компании является второй задачей после первоначального исследования веб-страницы. Различные типы поисков могут быть проведены на доменных имен. Начнем с поиска информации WHOIS о целевом домене.

Исследуйте метаданные файлов целевого веб-сайта

При просмотре веб-сайта целевой компании вы можете столкнуться с различными типами файлов, размещенных на нем, таких как файлы рекламы продуктов в JPEG или PDF форматах, электронныетаблицы, содержащие каталоги продуктов и другие файлы. Эти файлы должны быть загружены и исследованы в автономном режиме для извлечения их метаданных. Мы уже рассмотрели метаданные в главе 2. В этом разделе мы перечислим дополнительные инструменты для анализа метаданных в цифровых файлах:

- *Metagoofil* (https://code.google.com/archive/p/metagoofil): Вы можете извлечь метаданные публичных документов с веб-сайта целевой компании.
- *OOMetaExtractor* (https://archive.codeplex.

com/?p=oometaextractor): Можно извлечь метаданные документа OpenOffice.

- *Fingerprinting Organizations c Collected Archives* (https://www.elevenpaths.com/labstools/foca/index.html): Это инструмент анализа метаданных; он собирает публичные файлы из Интернета с помощью трех поисковых систем: Google, Bing и DuckDuckGo. Затем вы можете искать их для метаданных и скрытой информации.

Поиск сертификации веб-сайта

Чтобы показать криптографические сертификаты, связанные с любым доменным именем, воспользуйтесь этими поисковыми службами:

- *Censys* (https://censys.io)
- *Certificate Search* (https://crt.sh)

Инструменты статистики и аналитики веб-сайта

Инструменты статистики веб-сайтов предоставляют полезную маркетинговую, техническую и историческую информацию о любом доменном имени. Вам нужно предоставить только целевое доменное имя, и создается подробный отчет. Ниже приведены самые популярные инструменты в этой области:

- *Alexa* (https://www.alexa.com/siteinfo): Предложения богатых веб-сайтов статистика и аналитическая информация.
- *Moon Search* (http://moonsearch.com): Предлагает веб-сайты аналитические услуги и Backlinks checker службы.
- *Spy On Web* (www.spyonweb.com): Сбор различной информации о целевом доменном имени, как его IP-адрес и использовать DNS-сервер.
- *W3bin* (https://w3bin.com): Здесь вы можете узнать, кто является хостером конкретного веб-сайта.
- *Visual Site Mapper* (www.visualsitemapper.com): Этот инструмент показывает исходящие и входящие ссылки на целевой веб-сайт.
- *Site Liner* (www.siteliner.com): Этот инструмент показывает дубликат содержимого и связанные с ним доменные имена.

- *Clear Web Stats* (https://www.clearwebstats.com): Этот инструмент показывает подробную техническую информацию о любом доменном имени.
- *Website Outlook* (www.websiteoutlook.com): Различные инструменты статистики веб-сайта, такие как социальная популярность, анализ ключевых слов и техническая информация на сайте.
- *Informer* (http://website.informer.com): Этот инструмент показывает статистическую информацию о веб-сайтах.
- *Security Headers* (https://securityheaders.io): Здесь вы можете проанализировать http заголовки ответов целевых веб-сайтов.

Инструменты проверки репутации веб-сайта

Есть много организаций, которые предлагают бесплатные онлайн-услуги, чтобы проверить, является ли конкретный веб-сайт является вредоносным. Некоторые из этих сайтов также предлагают историческую информацию о целевом веб-сайте. Ниже приведены различные услуги анализа веб-репутации:

- *Threat Miner* (https://www.threatminer.org/index.php): Этот сайт предлагает анализ информации об угрозах доменов.
- *Urlquery* (http://urlquery.net): Это онлайн-сервис для обнаружения и анализа вредоносных программ на основе Интернета.
- *URLVoid* (www.urlvoid.com): Это инструмент проверки репутации веб-сайта.
- *Threat Crowd* (https://www.threatcrowd.org): Это поисковая система для поиска угроз.
- *Reputation Authority* (www.reputationauthority.org/index.php): Здесь вы можете проверить оценить поведение доменного имени.
- *Sucuri SiteCheck* (https://sitecheck.sucuri.net): Это веб-сайт вредоносных программ и сканер безопасности. Он также покажет список ссылок и список скриптов, включенных в целевой веб-сайт.
- *Joe Sandbox* (https://www.joesandbox.com): Эта служба обнаруживает и анализирует потенциальные вредоносные файлы и URL-адреса.

- *Safe Browsing* (https://developers.google.com/safe- browsing/?csw=1): Этот сайт предлагает APIs для доступа к Google Safe Browsing списки небезопасных веб-ресурсов.
- *abuse.ch ZeuS Domain Blocklist* (https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist): Это черный список доменных имен.
- *Malware Domain Blacklist* (http://mirror1.malwaredomains.com/files/domains.txt): Содержит список доменов, которые, как известно, используются для распространения вредоносных программ в Интернете.
- *MalwareURL* (https://www.malwareurl.com/index.php): Вы можете проверить подозрительный веб-сайт или IP-адрес здесь.
- *Scumware* (https://www.scumware.org): Это список вредоносных веб-сайтов.

Примечание! чтобы увидеть список веб-сайтов, которые были взломаны раньше, перейдите на http:// zone-h.org/archive и в поиске целевого доменного имени. если есть предыдущий взлом, он покажет вам взломали страницу (которая заменяет оригинальную главную домашнюю страницу), хакер team, кто ответственной за этот хак, если таковой имеется, и дата / время, когда взлом состоялся.

Пассивная техническая разведка

Проведение пассивной разведывательной деятельности для получения технической информации означает, что вы пытаетесь определить поддомены, IP-адреса, делать DNS след, и получать информацию WHOIS о целевом домене.

WHOIS Lookup

С помощью поиска WHOIS вы можете узнать, кто зарегистрировал целевое доменное имя в дополнение к другой полезной информации, такой как владелец доменного имени и личная информация, платежный контакт и технический контактный адрес (см. рисунок 8-5). Эта информация является общедоступной и должна быть такйора со стороны организации

ICANN, ответственной за надзор за системой доменных имен. Информация WHOIS о каждом домене хранится в общедоступных центральных базах данных под названием WHOIS databases. Эти базы данных могут быть запрошены для получения подробной информации о любом зарегистрированном доменном имени. Пожалуйста, обратите внимание, что некоторые регистраторы доменов могут сделать свои регистрационные данные конфиденциальными. (Эта услуга называется чем-то другим в каждом регистре доменов и требует уплаты дополнительной платы, но наиболее распространенными терминами являются *конфиденциальность домена* или *защита WHOIS.)* В этих случаях личная информация регистратора доменов будет скрыта в базах данных WHOIS.

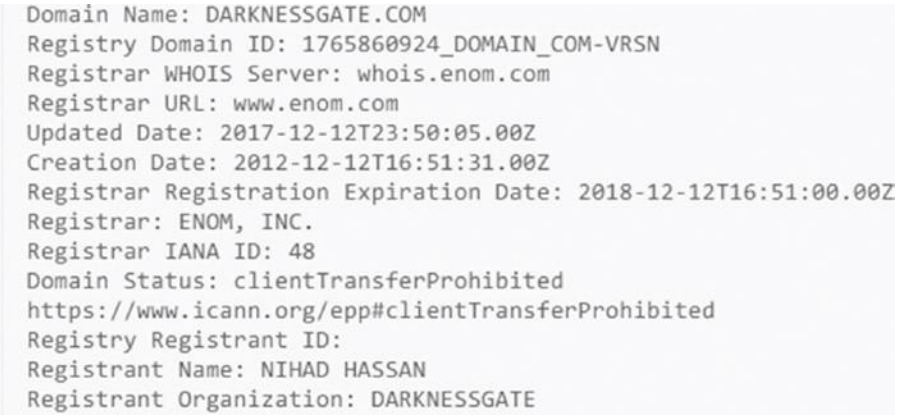

Рисунок 8-5. *Частичный отчет WHOIS о доменном имени DarknessGate.com извлечены изhttps://whois.icann.org*

Многочисленные сайты предлагают информацию WHOIS. Однако основным ответственным за предоставление этой услуги является ICANN. ICANN и ее местные региональные интернет-реестры управляют распределением и регистрацией IP-адресов и доменных имен для всего мира.

- *ICANN* (https://whois.icann.org/en): Это головная организация, ответственная за координацию Интернет DNS и IP-адресов.
- *AFRINIC* (https://www.afrinic.net) Это отвечает за африканский регион.
- *APNIC* (https://www.apnic.net): Это отвечает за Азиатско-Тихоокеанский регионregion.
- *LACNIC* (www.lacnic.net) Это отвечает за Латинскую Америку и Карибский бассейн.

Многие другие онлайн-сервисы дают больше информации о зарегистрированных доменных имен, перечисленных здесь:

- *Domain History* (www.domainhistory.net): Это показывает архивную информацию о доменных именах.
- *Whoisology* (https://whoisology.com/#advanced): Это архив владения доменным именем.
- *Robtext* (https://www.robtex.com): Это содержит различную информацию о доменных именах.
- *Who* (https://who.is): Это предлагает WHOIS поиск доменного имени, веб-сайта и IP утилит.
- *Operative Framework* (https://github.com/graniet/operative- framework): Здесь вы можете найти все домены, зарегистрированные по тому же адресу электронной почты.
- *URL Scan* (https://urlscan.io): Это показывает различную информацию о целевом веб-сайте, такую как детали IP, субдомены, деревья доменов, ссылки, сертификаты и технологии, используемые для его создания.

Теперь, узнав, кто несет ответственность за целевое доменное имя, вы можете начать открывать, как целевая компания организует свои интернет-ресурсы через веб-хостов и поддоменов.

Открытие поддоменов

Поддомен — это веб-адрес, созданный под текущим адресом доменного имени. Он обычно используется администраторами веб-сайта для организации их содержания в Интернете. Например, www.darknessgate.com может использовать поддомен http://shop.darknessagte.com для покупок и поддомена http://blog.darknessgate.com для блога.

Многие администраторы веб-сайтов могут создавать поддомены для тестирования новой технологии, прежде чем применять ее на главном сайте. Такие сайты являются небезопасными, поскольку они используются на стадии разработки и могут быть оставлены открытыми для атак. Обнаружение таких небезопасных поддоменов может обеспечить важную информацию о целевой компании (например, она может выявить код веб-сайта или документы подверженые утечки, забытые на сервере).

Есть много инструментов / методов для обнаружения субдоменов. Ниже приведены самые популярные из них.

ИСПОЛЬЗОВАНИЕ ПОИСКОВОГО ОПЕРАТОРА GOOGLE

Использовать *site:target.com -inurl:www* и Google покажет все связанные имена субдоменов цели. Например, ввод **site:yahoo.com -inurl:www** покажет все поддомены целевого доменного имени yahoo.com с помощью страницы поиска Google (см. Рисунок 8-6).

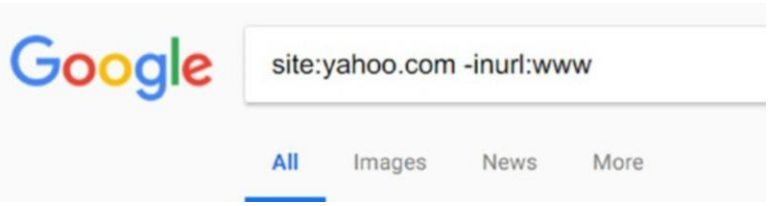

Рисунок 8-6. *Использование google передовых поисковых операторов для обнаружения поддоменных имен*

ИСПОЛЬЗОВАНИЕ VIRUSTOTAL.COM

Служба VirusTotal проверяет подозрительные файлы и URL-адреса на наличие вредоносного кода. Эта услуга может быть использована для обнаружения субдоменов. Перейти кhttps://www.virustotal.com/#/home/search

(убедитесь, что выберите вкладку Поиска, если она еще не выбрана. Введите целевое доменное имя и нажмите Enter. Прокрутите до конца страницы, чтобы найти раздел "Наблюдаемые поддомены" (см. рисунок 8-7).

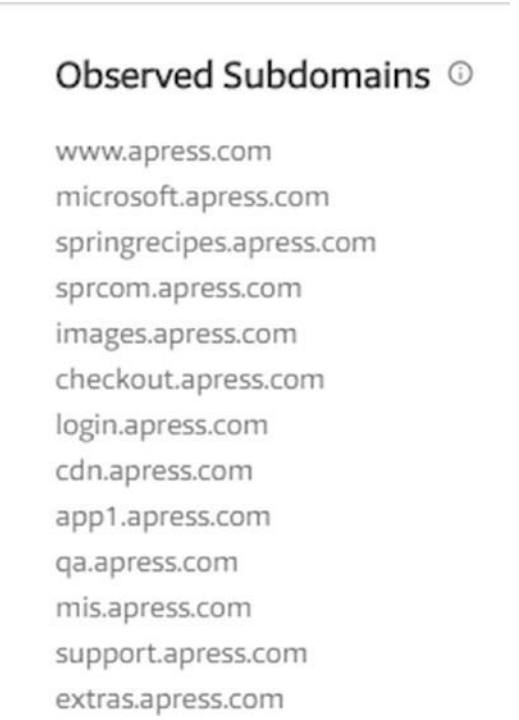

Рисунок 8-7. *VirusTotal показывает раздел "Наблюдаемые субдомены" для Apress.com*

DNSDUMPSTER

С DNSdumpster (https://dnsdumpster.com), Вы можете найти информацию о доменных именах о поддоменах, DNS-серверах и записях MX.

Вот другие инструменты для работы с поддоменами:

- *Dnsmap* (https://tools.kali.org/information-gathering/ dnsmapComes): Это предустановленное на Linux Kali. Он выполняет обнаружение поддоменных имен и показывает связанные IP-адреса для каждого найденного поддоменных имени.
- *Certificate Search* (https://crt.sh): Эта услуга также обнаруживает имена поддоменных доменов целевого домена.
- *Gobuster* (https://github.com/OJ/gobuster): Этот сайт обнаруживает поддомены и файлы / каталоги на целевых веб-сайтах. Этот инструмент используется в качестве активной разведывательной техники для сбора информации.

- *Bluto* (https://github.com/darryllane/Bluto): Здесь вы можете собирать имена поддоменов пассивно через Netcraft.
- *PenTest Tools* (https://pentest-tools.com/information- gathering/find-subdomains-of-domain): Здесь вы можете обнаружить имена поддоменов, найти виртуальные хосты, а также сделать веб-сайт разведки и извлечения метаданных с целевого веб-сайта.
- *Sublist3r* (https://github.com/aboul3la/Sublist3r): Здесь вы можете обнаружить имена поддоменов, используя как пассивные, так и активные методы разведки.

Совет! Используйте более одной службы для обнаружения субдоменов, поскольку некоторые службы могут возвращать частичные результаты на основе метода обнаружения.

DNS Reconnaissance

После сбора информации о записях WHOIS и целевых поддоменных именах вы можете получить более пассивную информацию о целевом домене. В этом разделе мы перечислим методы пассивной разведки для сбора информации о DNS-серверах и записях DNS. Следующим этапом является сканирование портов и другие активные методы разведки, которые считаются вне сферы нашей книги OSINT-сбора деятельности.

ROUTE MAPPING

Чтобы определить путь к целевой сети, необходимо использовать команду tracert. Пожалуйста, обратите внимание, что, когда информация проходит через сети, она не идет по тому же пути каждый раз; он проходит через различные маршрутизаторы, брандмауэры и другие вычислительные устройства, прежде чем добраться до места назначения. Для сайтов с высокой ценностью команда tracert будет отключена, но это не повредит протестировать ее для вашего целевого веб-сайта. Есть много инструментов для выполнения трассировки. На ОС Windows откройте запрос командной строки и введите **tracert,** за которым следует целевое доменное имя (см. Рисунок 8-8).

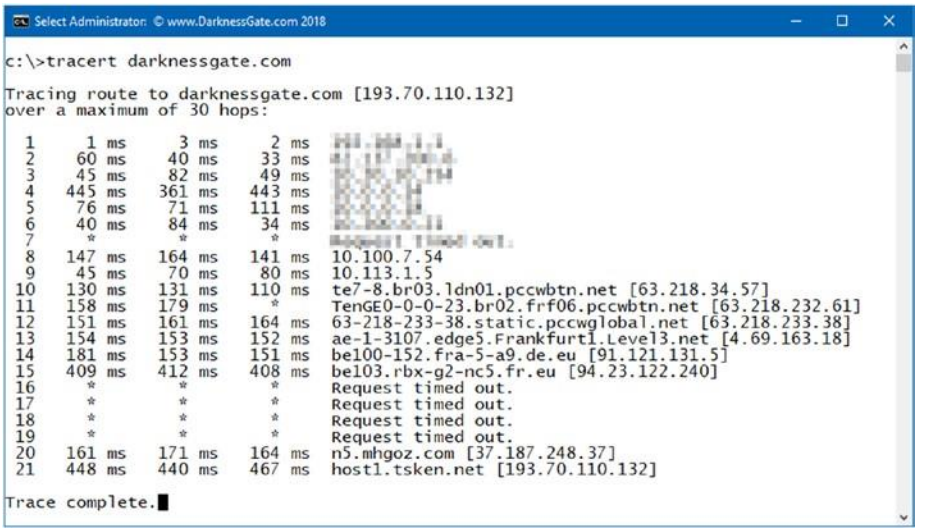

Рисунок 8-8. *Выполнение трассировку на целевом веб-сайте*

ОБЩИЕ ТИПЫ ЗАПИСЕЙ DNS

Прежде чем собирать информацию из целевых DNS, необходимо знать основные типы записей DNS. Система доменных имен имеет много записей, связанных с ним. Каждый из них дает различный набор информации о связанных доменное имя. Это наиболее распространенные записи DNS:

- **A** обычно используется для отображения имен хоста на IP-адрес узла. Используется для записей IPv4.
- **AAAA** является таким же, как тип **записи,** но используется для записей IPv6.
- **CNAME** является каноническим имя записи. Эту запись часто называют *псевдонимом записи,* потому что она отображает псевдоним к каноническому названию.
- **MX** является запись обмена почтой. Он отображает доменные имена на свой почтовый сервер, ответственный за доставку сообщений для этого домена.
- **NS** — запись сервера имен. Он обрабатывает запросы, касающиеся различных услуг, связанных с основным доменным именем.

- **TXT** текстовая запись. Он ассоциирует произвольный текст с доменным именем.

NSLOOKUP КОМАНДЫ

Эта команда поможет вам обнаружить различную DNS информацию о целевом доменном имени в дополнение к его разрешенному ip-адресу. Команда доступна как на Windows, так и на Linux. Начнем с поиска записи целевого доменного имени (см. Рисунок 8- 9).

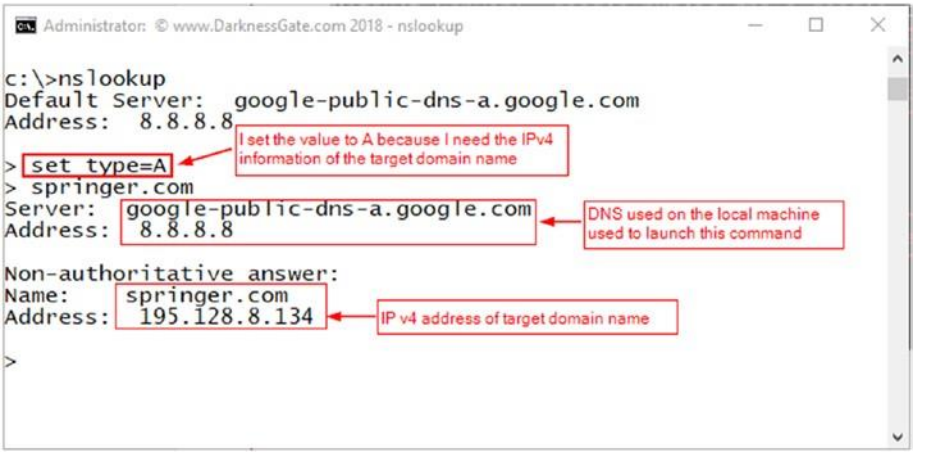

Рисунок 8-9. *Поиск записи целевого доменного имени с помощью nslookup*To увидеть записи MX (записи почтового сервера), связанные с целевым доменным именем, введите команду, показанную на рисунке 8-10.

Рисунок 8-10. *Отображение записей MX с целевым доменным именем*

Таким же образом, вы можете извлечь IP-адрес из любого почтового сервера целевого доменного имени, введя **set type=a** а затем ввести адрес почтового сервера, чтобы выяснить его в IP-адрес (см. рисунок 8-11).

Рисунок 8-11. *Просмотреть IP сервера обмена почты в номер IPv4*

Зная IP-адрес почтового сервера, вы можете в дальнейшем реализовать методы поиска IP на этом IP-адресе, чтобы найти больше информации о нем, как вы увидите дальше.

Вы можете использовать nslookup так же, как с помощью веб-инструментов; давайте практиковать его с помощью веб-сайта MXtoolbox.

Перейти к https://mxtoolbox.com и ввести целевое доменное имя в поле поиска. Сайт предоставляет DNS информацию о целевом доменном имени, таком как поиск DNS, поиск MX, поиск WHOIS, поиск политики отправителя (SPF) и распространение DNS. Вся эта информация отображается в графическом пользовательском интерфейсе. Важной особенностью этого сайта является то, что он дает вам авторитетный сервер имя целевого доменного имени (см. Рисунок 8-12). Авторитетный означает, что DNS-сервер является сервером, который содержит фактические записи DNS (A, CNAME, MX и так далее) для целевого доменного имени. Пожалуйста, обратите внимание, что во время наших предыдущих тестов nslookup, мы получали "неавторитетный ответ" при запросе целевого доменного имени. Это потому, что мы получаем ответ от кэшированной версии или от локального DNS-сервера (DNS-сервер вашего ISP).

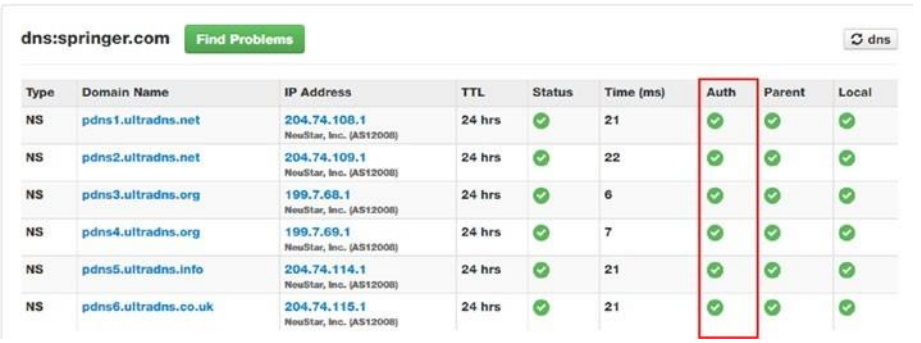

Рисунок 8-12. *Авторитетный сервер имен целевого доменного имени*

Ниже приведены другие полезные веб-сайты, которые предлагают DNS и веб-инструменты поиска:

- *W3DT* (https://w3dt.net): Это предлагает различные услуги DNS поиска и другие сетевые и интернет-инструменты.
- *DNS Stuff* (https://www.dnsstuff.com/tools): Это предлагает различные инструменты анализа DNS, сетей и электронной почты.

NETCRAFT

Netcraft является популярным сайтом сканера безопасности, который дает подробную информацию о безопасности любого веб-сайта. Чтобы использовать его, перейдите на https://searchdns.netcraft.com, введите целевое доменное имя в текстовом поле и нажмите кнопку поиска (см. рисунок 8-13). Netcraft будет создавать подробный отчет о безопасности целевого веб-сайта, который включает в себя следующие):

- Сетевая информация (IPv6, реестр доменов, сервер имен, контакт администратора DNS, хостинговая компания и многое другое)
- Запись истории хостинга
- Рамки политики отправителя (SPF)
- Проверка подлинности сообщений на основе домена, отчетность и запись соответствия
- Веб-трекеры, связанные с этим сайтом, такие как виджеты социального обмена, файлы JavaScript и изображения
- Технологии сайта и рекламные сети

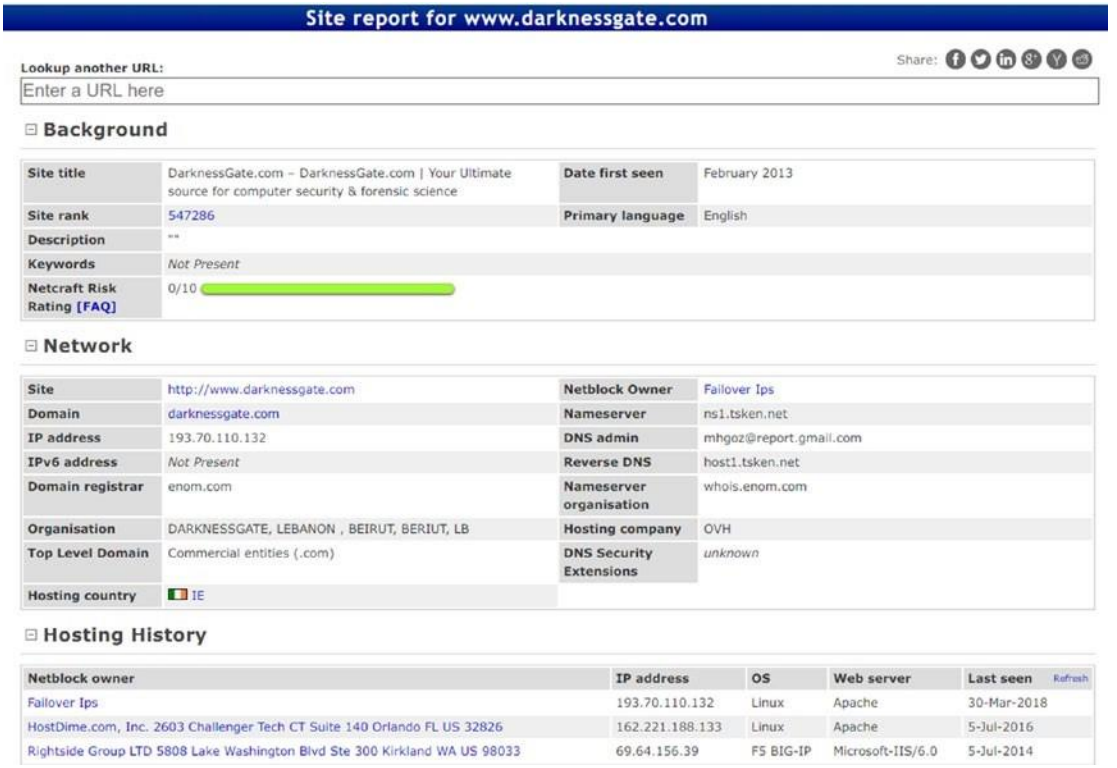

Рисунок 8-13. *Netcraft предоставляет подробную информацию о безопасности любого веб-сайта*

Отслеживание IP-адресов

В главе 2, мы тщательно рассмотрели концепцию IP-адресов и как они могут быть использованы для отслеживания пользователей в Интернете через различные веб-сайты. В этом разделе мы перечислим самые популярные и бесплатные инструменты, которые помогут вам найти более подробную информацию о любом IP-адресе или доменном имени.

Вот инструменты для информации о геолокации IP:

- *IPverse* (http://ipverse.net): Это показывает списки блоков адресов IPv4 и IPv6 по коду страны.
- *IP2Location* (www.ip2location.com/demo.aspx): Это бесплатная служба ip расположения.

- *Ipfingerprints* (www.ipfingerprints.com): Этот сайт позволяет показывать, IP-адрес географическое местоположение .
- *DB-IP* (https://db-ip.com): Это показывает геолокацию IP и сетевую разведку.
- *IPINTEL* (https://ipintel.io): Это показывает IP-адрес на карте и показывает ISP.
- *IP Location* (https://www.iplocation.net): Это показывает данные геолокации IP.
- *UTrace* (http://en.utrace.de): Найдите IP-адрес и доменные имена.

Вот инструменты для получения информации об Интернет-протоколе(IP):

- *Onyphe* (https://www.onyphe.io).
- *CIDR REPORT for IPv4* (www.cidr-report.org/as2.0).
- *IP to ASN* (https://iptoasn.com): Это показывает IP-адрес базы данных ASN обновляется ежечасно.
- *Reverse DNS Lookup* (https://hackertarget.com/reverse-dns- lookup): Это показывает обратные записи DNS для целевого IP-адреса.
- *Reverse IP lookup* (https://dnslytics.com/reverse-ip).
- *Same IP* (www.sameip.org): Это показывает сайты, размещенные на том же IP-адресе.
- *CIDR REPORT for IPv6* (www.cidr-report.org/v6).
- *IP Address Tools* (www.ipvoid.com).
- *ExoneraTor* (https://exonerator.torproject.org): Здесь вы можете проверить, использовался ли конкретный IP-адрес в качестве ретранслятора Tor до.

Вот инструменты, чтобы узнать информацию о протоколе пограничных шлюзов(BGP):

- *BGP4* (www.bgp4.as/tools).
- *Hurricane Electric BGP Toolkit* (https://bgp.he.net).
- *BGP Ranking* (http://bgpranking.circl.lu).
- *BGP Stream* (https://bgpstream.com).

Вот инструменты, чтобы узнать информацию о черный список IP-адресов:

- *Block List* (www.blocklist.de/en/index.html): Здесь вы можете сообщить о злоупотреблениях IP-адресов для своих операторов сервера, чтобы остановить атаки или скомпрометированной системы.
- *FireHOL* (http://iplists.firehol.org): Здесь вы можете собирать IP-каналы киберпреступности для создания черного списка IP-адресов, которые могут быть использованы на различных сетевых устройствах для блокирования вредоносного доступа/ веб-сайтов.
- *Directory of Malicious IPs* (https://www.projecthoneypot.org/ list_of_ips.php): Каталог вредоносныхIPs.

Итоги

Сбор технической информации о целевом веб-сайте и сетевой системе известен как *технический след.* В этой книге мы сосредоточились на методах пассивной разведки, так как суть сбора OSINT связана с получением общедоступной информации, которая не нуждается в разрешении для ее сбора. В этой главе мы рассмотрели инструменты и методы, которые могут быть использованы для проведения OSINT разведки о веб-сайте цели и сетевой инфраструктуры пассивно.

В следующей главе мы поговорим о будущем и о том, как широкое использование Интернета, мобильной связи и социальных медиа-платформ повлияет на будущее методов сбора OSINT.

Глава 9

Что дальше?

OSINT стал предпочтительным методом сбора информации для разведывательных органов во всем мире. Традиционно разведывательные службы опирались на другие каналы для получения информации с различной степенью надежности и полезности; однако по мере того, как вычислительная технология продолжает развиваться, а Интернет и социальные сети становятся еще более доступными во всем мире, разведывательные службы перевели значительную часть своей деятельности по сбору разведывательной информации в сферу действия OSINT. Некоторые эксперты разведки считают, что более 90 процентов разведывательной информации идет сейчас из источников OSINT.

OSINT не ограничивается разведывательными службами, правоохранительными органами и военными ведомствами. OSINT стала неотъемлемым компонентом в процессе принятия решений для правительств, бизнес-корпораций, учреждений ООН, неправительственных организаций, научных кругов, средств массовой информации и гражданских обществ, таких как группы защиты прав граждан и профсоюзы. В настоящее время корпорации используют OSINT для расследования внутренних утечек, сбора информации о конкурентах и прогнозирования тенденций на зарубежных рынках. OSINT также используется киберпреступниками и преступными организациями для изучения данных, которые могут быть использованы для лучшей атаки или социальной инженерии.

Где будет OSINT Идем дальше?

Информационный век привел к взрывному количеству потенциальных источников разведки и будет определять будущее сбора OSINT. В разведывательной сфере прогнозируется, что практика сбора онлайн-данных для борьбы с терроризмом и раскрытия преступности будет возрастать. Кроме того, OSINT будет продолжать предлагать дешевый метод для получения информации о любом сообществе по всему миру. Например, многие исследования показывают, что недавние протесты в арабских странах были предсказаны западными службами безопасности после анализа поведения арабских пользователей на социальных платформах в то время.

N. A. Hassan and R. Hijazi, *Open Source Intelligence Methods and Tools*, https://doi.org/10.1007/978-1-4842-3213-2_9

В гражданской области предприятия будут более охотно развивать свои собственные возможности OSINT, чтобы получить конкурентные преимущества и обеспечить свои инвестиции в постоянно меняющемся мире. Крупные организации будут работать над созданием собственных команд OSINT, в то время как коммерческие поставщики OSINT будут продолжать предлагать свои услуги малым и средним корпорациям, которые не могут позволить себе иметь независимый отдел по сбору OSINT.

Примечание! Многие корпорации уже используют OSINT для прогнозирования рисков, которые они называют *конкурентной разведкой* или бизнес-*аналитикой*.

С точки зрения информационной безопасности, сбор OSINT будет по-прежнему будет ступенькой для большинства оценок тестирования на проникновение для оценки слабых мест системы и работы по их быстрому устранению. Организации будут работать над интеграцией своей разведки OSINT в общую стратегию организации в области киберзащиты для защиты своих активов и укрепления своей безопасности.

Основным препятствием на пути сбора OSINT является массовый объем данных, которые должны быть обработаны. Действительно, огромные достижения в области мобильных вычислений и увеличение скорости Интернета сделает людей более готовыми размещать значительный объем данных в Интернет. Этот огромный поток общедоступных данных сделает анализ чрезвычайно трудоемким. Правительства и гигантские корпорации постоянно тестируют новые технологии для преодоления этой проблемы. Инвестиции в аналитические технологии стали приоритетом для многих правительств и гигантских ИТ-корпораций, поскольку это приведет к обработке огромных объемов данных, с тем чтобы превратить их в данные, которые могут быть запрошены и смоделированы для быстрого создания выводов.

Примечание! Данные, генерируемые с устройств Интернета вещей (IoT), также считаются серьезной проблемой. Ожидается, что в ближайшем будущем у нас будут миллиарды работающих устройств IoT.

Полученные данные/метаданные с этих устройств огромны и требуют сложных аналитических инструментов для получения полезной развединформации от них.

Еще одной проблемой для сбора OSINT является прогнозируемый рост "фейковых новостей" в Интернете. В настоящее время основные социальные сети платформ, как Facebook и Twitter сталкиваются с реальной проблемой для борьбы с такой деятельностью. Новые алгоритмы и политики использования должны быть разработаны для автоматической проверки источников новостей, прежде чем рассматривать их действительными источниками OSINT.

Достижения в области вычислительных технологий, безусловно, приведут к созданию эффективных алгоритмов для обработки огромного объема данных и отделения нерелевантных данных от целевых данных. Достижения в области искусственного интеллекта и технологий машинного обучения вновь преобразуют OSINT в ближайшие годы.

Процесс OSINT

В процессе написания этой книги, мы прямо не говорили о процессе, или конкретных шагах, которым должны следовать, чтобы собрать OSINT. Мероприятия по сбору OSINT не могут проводиться в определенном порядке в зависимости от каждого случая или цели. Тем не менее, поток глав в этой книге также может считаться хорошим способом организации поисковой деятельности OSITN.

В целом, есть пять основных этапов для любой деятельности по сбору OSINT, как поясняется здесь:

1. *Определить источники*: Вы определяете источники, где вы хотите собрать эти данные (например, Интернет, газеты, журналы, коммерческие базы данных и так далее).
2. *Сбор данных*: Вы используете различные инструменты и методы для сбора данных из целевых источников; имейте в виду, что вы должны следовать пассивным методам для сбора этих данных.
3. *Обработка и проверка*данных: Вы обрабатываете собранные данные и проверяете неопределенные данные из нескольких источников, если это возможно. Следует также определить текущие и устаревшие данные и исключить нерелевантные данные из дальнейшего анализа.

4. *Проанализируйте данные*: Вы анализируете данные и пытаетесь найти связи между ними, чтобы сформулировать полную картину о цели.
5. *Доставка* результата: Вы представляете отчет о своих выводах соответствующей стороне. Этот шаг имеет важное значение и, как правило, упускается из виду многими сборщиками OSINT. Необходимо представить свои ключевые выводы в простом для понимания в доступном формате для конечного пользователя.

Заключительные слова

В заключение, мы считаем, что будущее OSINT является чрезвычайно ярким! Как государственные, так и частные организации будут работать над интеграцией сбора OSINT в их общие процессы принятия решений. Новые отрасли промышленности будут стремиться использовать огромные данные, полученные в результате информационной революции, для поддержки своих бизнес-стратегий и разведки.

Мы надеемся, что эта книга поможет пролить свет на эту важную концепцию, которые широко используются с самого начала истории под разными именами.

Index

A

B

C

D

N. A. Hassan and R. Hijazi, *Open Source Intelligence Methods and Tools*,
https://doi.org/10.1007/978-1-4842-3213-2

E

F

G

H

I

J

K

L

M, N

O

P, Q

R

S

T

U

V

W, X

Y

Z