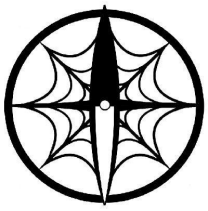
ОБЩИЙ ОБЗОР НЕТСТАЛКИНГА (v. 1.0.1)

РУКОВОДСТВО

Archivist et al.

Актуальная версия руководства доступна по ссылке:
https://t.me/netstalking_documents

2017-2020



ИНСТИТУТ ИНТЕРНЕТ СТАТИСТИКИ

В этой книге изложены основные понятия и методы нетсталкинга. Вы узнаете, как путешествовать по различным сетям, осуществлять два основных вида поиска, анализировать и хранить найденное, делиться им с сообществом. Раскрыта история нетсталкерского движения, развития веба и сетевого искусства - нет-арта. Приводятся советы по использованию программных инструментов и их комбинаций. Кроме того, вы научитесь способам обезопасить себя в Интернете.
Книга выполнена как обзор тематики и даёт отправные точки для самостоятельного углублённого изучения. По мере развития нетсталкерского сообщества она будет исправляться и дополняться.

(v. 1.0.1), 112 pages (2017-2020)

Актуальная версия руководства доступна по ссылке:
https://t.me/netstalking_documents

Содержание

1. Общая концепция

Добро пожаловать в руководство, посвящённое тематике «нетсталкинга». По ходу прочтения вы ознакомитесь с историей тематики и перейдёте от таких азов, как изучение языка запросов[1] Google, сканирование IP-адресов с помощью программ Nmap[2] и masscan[3], к более сложным темам: анализ находок на различных протоколах, проникновение в анонимные и заброшенные сети, особенности игр в альтернативной реальности, защиту от слежки и пузыря фильтров и т.д. Упоминаемый в тексте софт по умолчанию относится к ОС семейства Windows, если не указано обратное. Возможно, вы уже задались вопросом о том, чем же является нетсталкинг. Помимо этимологии этого слова, восходящей как к сталкингу[4], так и к сталкерству[5], существует и определение. По нему «Нетсталкинг – это деятельность, осуществляемая в пределах сети методом поиска, направленная на обнаружение малоизвестных, малодоступных и малопосещаемых объектов с их возможным последующим **анализом**, **систематизацией** и **хранением**, с целью эстетического и информационного удовлетворения искателя». Для разных индивидуумов это имеет разный оттенок: поиск максимально особенной и значимой для личности информации; неформальные исследования сети, где можно позволить себе быть иррациональным; путешествие в новые неизведанные места, куда не ступала нога обывателя; поиск странного, таинственного.

Приведу пример, иллюстрирующий ход нетсталкинга. Представьте себе, как некий индивид интересуется системами видеонаблюдения, т.е. просмотром трансляций с IP-камер реального мира. Вы наверняка неоднократно замечали такие устройства в общественных заведениях: например, в закусочных и торговых центрах. Дело в том, что все эти камеры делятся на два типа. Первый — аналоговые, подключенные специальным кабелем к системе мониторинга. Второй — цифровые, объединённые в локальную сеть или имеющие выход ко глобальной. Последние бывают доступны через веб-страницы, которые часто не защищены, либо защищены простейшей связкой заводских логина и пароля. Интерес для нетсталкера представляет только категория цифровых камер, поскольку получение доступа к аналоговым не связано с «деятельностью, осуществляемой в пределах сети».

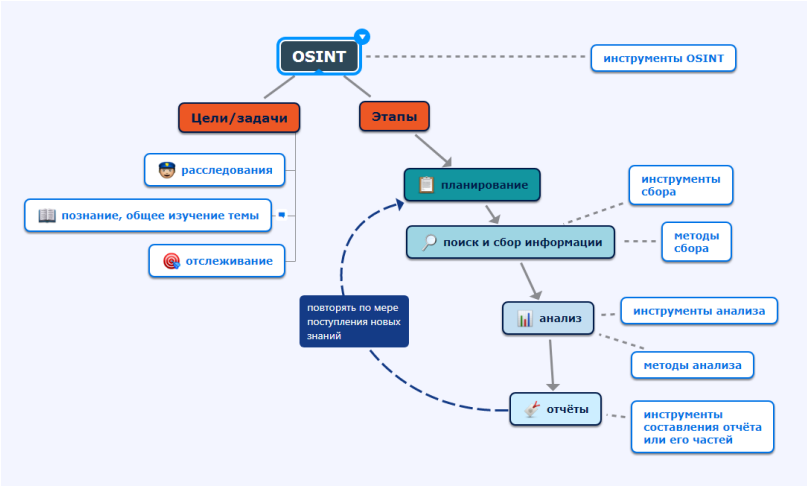
Таким образом, если исследователь хочет понаблюдать за подключенными к сети камерами, сначала он должен их найти. Существуют разные методы поиска, и сейчас я не буду упоминать каждый, ограничившись использованием языка запросов Google. Введя верный запрос, человек осуществляет **поиск** и получает список IP-адресов трансляций. Внимательно просматривая страницу, он изучает её содержание, исходя из своих целей. Например, индивида могут интересовать камеры, установлен-

[1] https://ru.wikipedia.org/wiki/Язык_запросов
[2] https://nmap.org/
[3] https://github.com/robertdavidgraham/masscan
[4] https://ru.wikipedia.org/wiki/Сталкинг_(преследование)
[5] https://ru.wikipedia.org/wiki/Индустриальный_туризм_и_городские_исследования

ные только на заводах, или только в офисах, либо и в офисах, и на заводах. Точно так же он может отсеивать лишь камеры определённого производителя.

Словом, выбор объектов для **анализа** зависит от ваших желаний — **критериев**. Важным критерием считается редкость, и это заводит нетсталкеров в малоизвестные, труднодоступные или заброшенные уголки. Сведение движения до «поиска странного» связано с тем, что нетсталкинг популяризировался среди любителей паранормального, и теперь, из-за таких некомпетентных публикаций журналистов, как статьи[6] Александры Степанищевой, ассоциируется с этим. По факту же нетсталкеры удовлетворяют естественную тягу к исследованию непознанного, сочетая критичность и впечатлительность, способность удивляться и действовать прагматично. Каждый обретает что-то своё, иногда просто интересное, а иногда сакральное, меняющее мировоззрение, поскольку данное занятие вытаскивает человека из эхо-камеры[7]. Для обнаружения чего-то необычного зачастую требуется перебрать огромное количество обыденного контента и мусора, например, архивов семейных FTP. Этим и отличается досуг нетсталкера от пассивного прокручивания ленты соцсетей, предлагающей вам лишь уже знакомые либо «хайповые» темы, отфильтрованные алгоритмами или администраторами пабликов.

Поиск является первым и основным искусством, которому учится начинающий нетсталкер. Он пригодится и на последующих этапах работы с находками. Первейший шаг в овладении этим навыком - прочувствовать гипертекстовость Сети. Всякая ссылка ведёт к новой информации, которая затем используется для уточнения поиска и получения новых ссылок. Это несколько напоминает методику разведчиков, работающих с открытыми источниками (Open Source Intelligence):



Когда собранных ссылок становится слишком много, возникает нужда в их система-

[6]https://lenta.ru/articles/2016/06/06/netstalkingstory
[7]https://ru.wikipedia.org/wiki/Эхо-камера

тизации, т.е. в обобщении всех находок, выделении связей между ними и составлении из них базы данных. Обычно этим занимаются для упрощения **хранения** или **анализа** - рассмотрения и изучения какого-либо признака объекта. Например, нетсталкер, исследовав параметры камер *одинаковой* модели, способен выработать новый метод их поиска. Так, работая с современными камерами компании AXIS, можно заметить, что у всех из них видеопоток вещается по прямому URL формата /mjpg/video.mjpg. Эта особенность применяется для поиска новых трансляций через оператор Google «inurl:» — ввод «inurl:mjpg/video.mjpg» в поисковую строку даёт около 9 страниц результатов по 10 ссылок. **Автоматизация** рутинных сторон процессов, в том числе всё того же поиска однотипных объектов [8] освобождает новые ресурсы для разумной работы с находками.

Вне зависимости от вида ресурсов или сетей всю поисковую активность нетсталкера можно свести к двум типам или методикам: это **нетрандом** и **делисёрч**. У обеих есть свой набор приёмов и программных инструментов.

Нетрандом (образовано «net» (сеть) и «random» (случайность)) — это скитание, поиск чего-то неизвестного в одной из сфер нетсталкинга. Некоторые сравнивают его с поиском иголки в стоге сена. Это сравнение некорректно, т.к. сено и иголка исчерпаемы, они не расширяются, как делает это Интернет. Ежесекундно создаются новые вебсайты, сообщения на форумах и т.п. — охватить весь объём глобальной сети невозможно. Поэтому практичнее аналогия с рыбалкой в море или океане. Причаливая на определённую точку, рыбак забрасывает удочку и ожидает улов, подобно тому, как это происходит в спутниковой рыбалке[9]. Не зная заранее, что именно он получит в итоге, ищущий часто собирает по пути всё, что покажется ему интересным. Поэтому такую деятельность иногда называют «сетевым бомжингом».

Основные способы нетрандома:

- Сканирование сети.
- Использование рандомайзеров - сервисов, выдающих случайную ссылку на ресурсы определённого класса: сайты, документы, видеозаписи YouTube и т.п.
- Просмотр последних загруженных или созданных объектов определённого класса (т.н «ресенты», recents). Некоторые файлообменники, картинкообменники и даже хостеры сайтов заводят для этого отдельные страницы. (примеры из core) Обычно их интерфейс интуитивно понятен: пользователь нажимает на кнопку или обновляет страницу, и генерируется новый сайт или файл. Процедура повторяется, пока нетсталкер не найдёт что-нибудь интересное.

[8] https://telegra.ph/Grabber-fajlov-dlya-netstalkinga-11-14
[9] https://ru.wikipedia.org/wiki/Спутниковая_рыбалка

- Использование в поисковиках т.н. дорков (комбинаций фильтров поиска), составленных таким образом, чтобы выдавались все известные поисковику ссылки на объекты определённого класса. Примером может служить т.н. «яндекс-гейт»[10], когда пользователи обнаружили множество открытых документов Google в выдаче Яндекса. Другой пример - составление запроса, включающего стандартное имя для фотографий или видео: IMG_0123.jpg, DSC_0123.jpg и другие, некоторые из которых встречаются чаще[11].

Как видим, даже при нетрандоме обычно не используется чистая случайность. Искатель выбирает (или создаёт) инструмент, исходя из своего особого интереса к какому-либо виду контента: видео с малым количеством просмотров, снятые на камеру любительские записи, документы, сайты надсети Tor и т.п. Однако вне зависимости от личных вкусов и выбранного метода работы, фактор непредсказуемости остаётся.

Приведу пример с поиском IP-камер посредством сканирования сети. Ничего не зная о камере заранее, индивид не может наверняка сказать, что именно он на ней увидит: комнату в жилом доме или складское помещение. Если бы этот человек занимался парсингом видеохостинга YouTube, то ему бы приходилось открывать сотни и тысячи видеороликов с похожими названиями типа MOV_002 или VID_1523. Не глядя на скриншоты или превью с таких записей, нельзя определить, что на них запечатлено.

Делисёрч (образовано «deliberate» (осознанный) и «search» (поиск)) — это осмысленный поиск предсказуемого объекта, признаки которого известны, в одной или нескольких сферах нетсталкинга. Приведу очередной пример. Недавно в Интернете было опубликовано[12] более 13 млн рассекреченных документов ЦРУ в рамках библиотеки с сайта CIA[13]. Ввод тэга «UFO» в поисковую строку выдаёт порядка 1500 совпадений. Уфологу достаточно сделать один запрос, чтобы достичь своей цели, но сначала ему необходимо узнать: где, как и когда можно сделать этот запрос. Таким образом, делисёрч учит нетсталкера, ставящего перед собой цель, понятиям места, времени и действия.

Основные способы делисёрча

- Использование поисковиков, как общеизвестных (Google, DuckDuckGo), так и специализированных: по типу ресурса, по оверлейной сети, принадлежащих библиотекам и др. организациям, метапоисковиков.

- Поиск избранных файлов в конкретных файловых хостингах с помощью тэгов или поисковых запросов.

[10] https://www.youtube.com/watch?v=OffE_zGRs8E
[11] http://muz4in.net/news/ehlektronnye_imena_fotografij/2013-07-25-33382
[12] https://habr.com/ru/post/400699/
[13] https://www.cia.gov/library/readingroom/

- Мониторинг ресурсов (новостных, соцсетей и пр.) на предмет упоминания определённой темы.

Делисёрч и нетрандом могут и будут пересекаться. Оба задействуют схожие навыки. Кроме того, целевой поиск становится естественным продолжением случайного. Это может происходить в рамках детального анализа рандомно найденного объекта, а также в результате обогащения нетсталкера новой информацией. Новые знания могут попасть к нему в руки неожиданно, однако дополнять их он будет уже осознанно.

2. Хронология развития

Историю нетсталкинга можно разделить на три условных этапа по три года. Проекты **ИСКОПАЗИ** и **Synthetical Science** стояли у истоков, т.е. наиболее повлияли на развитие нетсталкинга в период с 2009 по 2012 гг., а сообщество **Project Trailhead** и смежные с ним в основном развивали уже начатое и активно работали с 2012 по 2015 гг. Дальнейший рост движения породил множество малых и крупных проектов.

2.1 ИСКОПАЗИ

Расшифровка: Интерактивная Сетевая Конференция по Поиску Аномальных и Загадочных Интернетов. Судя по всему, публичная история этой организации начинается на доске /b/ имиджборды 2ch.so в августе 2010 года. В темах с названием «сетевые сталкеры» (из которых в архивах сохранился только неполный тред №3[14] без картинок), люди обсуждали «необычные, примечательные, странные и пугающие» сайты, не индексируемые в поисковиках, обменивались находками и травили байки[15]. В то время в основном использовался nmap, но некоторые пробовали писать и свои IP-сканеры. В сентябре 2010 г. исследователи **do_not_scan**, *nouitfvf, pekayoba, doctor.A* организовали форум[16] и канал общения на IRC (irc.freenode.org, #netstalkers), обособившись от имиджборд. Параллельно некий аноним на HiAsm[17] написал простой сканер диапазонов доменов и IP-адресов, приостановив его разработку на версии 4.7.

5 июля 2011 г. владелец почты sosacher1@gmail.com зарегистрировал домен **netstalking.ru**.

7 июля 2011 г. на нём открылся форум, а на следующий день он в шутку был дефейснут ИСКОПАЗИ. 9 числа сайт восстановили и ввели закрытую регистрацию по приглашениям, но действовал он недолго и вскоре отключился. Осенью 2013 года

[14] https://mega.nz/#!QcZSCa4L!o7Ae-mnP3JebXgqqets24eAVYRkE05MFYRUjQRSB1RE
[15] https://mrakopedia.org/wiki/Веб-трансляции
[16] http://web.archive.org/web/20110603075140/http://netstalking.0bb.ru/viewforum.php?id=2
[17] http://ru.wikipedia.org/wiki/HiAsm

его перекупил Лев Ртутин, державший на нём до 2015 года имиджборду[18]. Сейчас домен выкуплен Рескором под форум и небольшой музей, а до того долго продлевался Ртутиным, несмотря на отсутствие активности[19].

В 2011 г. ISKOPASI выпустили утилиту ipsa[20] – консольный IP-сканер, со временем переросший в аналогичный продукт, но уже с графическим интерфейсом и расширенным функционалом: NESCA[21]. 30 октября 2012 г. вышел BGRT — портативный IRC чат-клиент (с возможностью DDoS-атаки) для соединения с запасным IRC-каналом (dreamterra.ru, #netstalking). Примерно в тех же числах на форуме появилась переадресация на cryptochan[22] — основанное пользователем anony сообщество криптоанархистов с собственной IRC-сетью, пришедшей на замену Нульчату[23].

Крипточан умер в начале 2014 года из-за разногласий администрации, а ИСКОПАЗИ подняли имиджборду[24] на зарегистрированном ещё в мае 2013 года вебсайте D3W.org[25], где ранее лежали NESCA и API для доступа к NESCA DB — хранилищу находок. 25 марта 2014 состоялся[26] релиз ScanLab[27] — созданной anony поисковой системы по базе данных IP-адресов, обновляемой пользователями с помощью nmap. 14 апреля 2014 г. на D3W стартовала публичная раздача NESCA: желающий мог оставить gpg-ключ с ником и получить ключ для активации программы. 9 мая там же опубликовали peka_scan[28] — скрипт на Python, по словарю перебирающий каталоги и файлы веб-сервисов.

Весной 2016 г. D3W закрылся, т.к. его хостинг обанкротился. После гибели всех проектов остатки исследователей долгое время собирались на IRC-канале #0chan сервера anus.hacked.jp:6667, нынешнее местоположение неизвестно. Для подключения к IRC рекомендуются клиенты KVIrc[29] и X-Chat[30].

2.2 Synthetical Science

Нетсталкинг, начинавшийся как хаотичное и стихийное движение по поиску странностей в сетях, оброс мифологией и слухами благодаря Докладчику — иссле-

[18] http://web.archive.org/web/20131020125425/http://netstalking.ru/b/wakaba.html
[19] http://github.com/rtutin/netstalking.ru
[20] https://github.com/wegwarte/netstalking_archive/blob/master/ipsa.rar
[21] http://github.com/ChronosX88/nesca
[22] http://web.archive.org/web/20130223215541/http://crypt0.in/
[23] http://lurkmore.to/%C3%98chat
[24] http://archive.li/1Sovp
[25] https://who.is/whois/d3w.org
[26] https://arhivach.org/thread/17538/#50546
[27] https://github.com/digital-ghost/scanlab
[28] https://github.com/wegwarte/netstalking_archive/blob/master/peka_scan.rar
[29] http://www.kvirc.ru/
[30] http://xchat.org/

дователю меметики[31], автору проекта Synthetical Science. Ему принадлежат понятия Тихого Дома, Города Идей и Ран — вымышленные концепции из сеттинга ARG[32] Докладчика. Его целью было заражение окружающих идеями с помощью мистификации и наблюдение за их мутацией. Именно так случилось с идеей Тихого Дома, простого макгаффина, смысл которому придавали сами нетсталкеры, а также посетители имидборд и сайта крипипасты 4stor. Порой даже доходило до абсурда[33]: отождествления с Нирваной или жизнью после смерти. Среди до сих пор актуальных концепций Докладчика можно выделить IDIOINFECTED[34] — децентрализованную систему обмена сообщениями.

Всё началось с карты Интернета[35] — иллюстрации важных для проекта культурных ценностей и идей, которая была вдохновлена одной старой шуточной схемой[36], а та, по-видимому, происходит из латиноязычной легенды об уровнях дипвеба[37] Докладчик опубликовал карту как кроличью нору на Дваче в июне 2011 года, при этом первый тред из всех оставшихся, где упоминается изображение, датируется[38] 02.07.2011. В дальнейшем картинку много раз редактировали и пародировали. Написанное Докладчиком 01.08.2013 FAQ[39] поясняет те пункты карты, смысл которых неясен новичку. Список всех нетсталкинг-тредов, на протяжении которых развивалась игра, доступен в специальном каталоге.

23.12.2011 на blogbin.net был создан ныне удалённый блог[40] SynSci, посвящённый вопросам инфорнографии, меметики и мысленных экспериментов. О них можно прочесть в незавершенной книге Джона Оно «Infornography: The Tao of Memetic (Meta)Engineering»[41]. 12.06.2013 было сообщено об окончании исследований, и все прошлые записи, кроме титульной, были удалены [42] Докладчиком.

С момента закрытия блога ARG была отпущена в свободное плавание, и Докладчик (под ником unss) минимизировал своё вмешательство. 15.07.2013 в ныне заброшенную XMPP-конференцию нетсталкеров play@conf.netlab.cz, изучавших следы прошедшей ARG, зашел unss, ранее постивший на Хаосаче[43]. Докладчик ответил

[31] https://ru.wikipedia.org/wiki/Меметика
[32] https://ru.wikipedia.org/wiki/Игра_в_альтернативной_реальности
[33] https://4stor.ru/strashno-interesno/61144-tihiy-dom-i-49406.html
[34] https://urbanculture.in/IDIOINFECTED
[35] http://imgur.com/a/vgYoO
[36] http://imgur.com/a/HgL3e
[37] http://d5fdxua4kdbbjo6zvdbch4xiybadk7vb43nzxsokbzbwtwzeehuppbqd.onion/116457616-Manual-Para-La-Deep-Web-2.pdf
[38] http://web.archive.org/web/20130525021155/http://2ch.hk/sn/arch/res/46521.html
[39] http://arhivach.org/thread/4409/
[40] http://web.archive.org/web/20130604052053/http://blogbin.net/blog/1463
[41] https://drive.google.com/file/d/0B2it8L7haRYHNWlkV01rbjhBV2c/view
[42] http://web.archive.org/web/20130629145542/http://blogbin.net/blog/1463
[43] https://chaos.cyberpunk.us/fm/x/res/77.html

на несколько вопросов, подтвердил завершение проекта и пообщался[44] с неким unw о концепции Города Идей, приоткрыв ещё одну цель: усиление «ощущения Города» за счёт внимания игроков.

2.3 Project Trailhead

Многое из того, что известно о существовании этой исследовательской группы в 2010-2012 гг., дошло от Фомы (Курултая; Григория) — её участника. Учтите, что информация по данному периоду времени **не проверена**.

По словам Фомы, костяк составляли трое: Кузьма, якобы основатель, а также LadyBug и SearcherTheOne — рядовые участники. Курултай прибился к их XMPP-комнате по наводке от Кузьмы, которого он поверхностно знал в реальной жизни: в эпоху расцвета жанра смертельных файлов в Мурманске организовывалась сходка подписчиков тематического паблика во ВК. Именно на ней Григорий, как он сам утверждал, познакомился с Кузьмой, приехавшим из своего Петрозаводска.

Конференция, где проходило общение, называлась «11», хотя содержала только четыре человека. Периодически Кузьма покупал места на платных видеоконференциях TrueConf[45] и приводил своих знакомых: количество народа ненадолго увеличивалось, а потом снова спадало.

К середине проекта Григорий укрепился во мнении, что Кузьма — сумасшедший, а к концу пользователи поссорились друг с другом. Сёрчер говорил, что LadyBug (в жизни якобы Наталья Каштанова), пропавшая из конференции, была сбита автомобилем, и он обвинял в её смерти Кузьму.

SearcherTheOne покинул состав после инцидента с чемоданчиком[46] в 2012 году, а Фома с Кузьмой основали сообщество Трейлхеда в социальной сети ВК, к которому позднее присоединились Иван Иванов[47] и Максим Клевцов[48] — самые активные участники следующих двух лет. Вскоре бесследно исчез Кузьма.

Теперь к фактам. Впервые Trailhead был упомянут 14.10.2012 в комментариях к посту пользователя Хз Хз[49] в сообществе 333-333-333. Григорий ответил[50] ему, что пока узнать об организации нельзя, но грядут новости. Самое важное упоминание

[44] https://pastebin.com/tkSaUWZe
[45] https://trueconf.ru/
[46] https://imgur.com/a/FOZkX
[47] https://vk.com/crihan
[48] https://vk.com/blintzeln_kapitan
[49] https://vk.com/x3_x3
[50] https://imgur.com/a/SQzMy

произошло 02.11.2012 — в то время в ту же группу написал Сумасшедший Фрэнки[51], запрашивая контакты нетсталкеров, и опять ответил[52] Курултай. На этот раз он пояснил методологию проекта, сказал, что *никакой конференции нет*, и дал ссылку[53] на закрытую группу во ВК.

На сегодняшний день весь контент сообщества удалён Григорием, но осталась архивная копия , взятая 19.11.2016. Судя по ней, группа была создана ещё в 2009 г., но простаивала 3 года, пока Фома не запостил адрес нет-арта trackybirthday.com[54]. В 2013 г. она временно открылась, о чём свидетельствует страница[55] в Интернет-Архиве. Некоторые записи того времени отсутствуют в копии 2016 г. — видимо, стена иногда очищалась. Примечательно, что 01.10.2014 на Дваче неизвестный пытался мистифицировать[56] историю организации.

07.12.2014 в сообществе появилось объявление[57] о вербовке в возрождение Trailhead: на ныне неактивный форум trailheadgroup.ru, созданный Рэем Мэтсоном[58], Скрюченным Человеком[59] и Rescor Warden[60]. Кандидату требовалось заполнить анкету,пройти психологическое тестирование СМИЛ[61] и прочесть руководство по нетсталкингу[62]. Судя по посту[63] во ВК и треду[64] на 2ch.hk, кандидаты искались среди тех, кто не знал о тематике. В августе 2015 г. сообщество распалось, а 19 ноября вебсайт был окончательно отключен[65] Рескором.

Общее представление об атмосфере внутри проекта в дни его расцвета даёт комментарий одного из его давних участников, Dematerium Neogen:

Обычно было так: в целом околотематические обсуждения материалов, событий, совместные вылазки в «миры»[Worlds.com] и т.д. Это для большинства. Все довольны и получают то, что хотят (как и эстетическое удовлетворение, так и расширение кругозора и т.д.).

---

[51] https://vk.com/agemo_lla
[52] https://imgur.com/a/Lt2mN
[53] https://vk.com/deepwebproject
[54] http://trackybirthday.com
[55] http://web.archive.org/web/20130404073749/http://vk.com/deepwebproject
[56] https://arhivach.ng/thread/39303/#241147
[57] https://imgur.com/a/pB94Q
[58] https://vk.com/raymatson
[59] https://vk.com/scarletsixpence
[60] https://vk.com/rwarden
[61] https://www.psychol-ok.ru/statistics/mmpi/
[62] https://t.me/netstalking_documents/3
[63] https://imgur.com/a/l5AYK
[64] https://a2ch.ru/2015/08/03/s-utra-uvidel-takoe-soobschenie-pacany-ia-tipo-neo-izbrannyj-komu-nibud-98987157.html
[65] https://vk.com/wall225688945_1308

И было несколько участников, постоянно что-то копавших, ищущих, переводящих, адаптирующих и т.д., которые периодически делали вбросы — причём превью-вбросы с намёком на заинтересовывание и дальнейшее уже совместное продолжение деятельности именно по материалу из вброса. Обычно подключается подавляющее большинство (если не все) из первых — да, многие могут тупо ридонлить или отписывать лишь что-то в духе «я удивлён», «интересно» и т.д.

И вне зависимости от исхода всего этого (то есть удачи в финальной раскопке или её провалу) как правило подавляющее большинство присутствующих получает незабываемый экспиренс и опыт. Опять же все удовлетворены.

2.4 Развитие сообществ во ВКонтакте

H.I.D.D.E.N[66] — основанная Артёмом Коноваловым команда и группа ВК, где в основном постятся находки по IP-камерам, нет-арту и ARG. На первом этапе своей деятельности (19.07.2016 - 22.09.2016) основным направлением был нетрандом, в том числе по onion-сервисам, с упором на сетевое искусство, а также просмотр файлообменников. С 23.09.2016 по 2.01.2017 группа была в относительном стазисе, частично развеянном прибытием в неё участников Лапушкина и Дематерия с опытом в нетсталкинге. В результате дискуссий группа решила сосредоточиться на сканировании камер.

В период, названный Артёмом «вторым H.I.D.D.E.N» команда успешно освоила скан, брутфорс и наблюдение за камерами, которые теперь составляли абсолютное большинство контента, публикуемого в группе. Также вышло два видео[67] по основам тематики. В этот период сообщество начинает становиться известным в нетсталкерских кругах. Но под конец периода текущий уровень работы и зацикленность на камерах перестали удовлетворять искателей. Начался второй стазис группы (17.06.2017 - 4.08.2017), после которого она значительно разнообразила деятельность: включила исследование радио, освоение методологий OSINT, повышение общей сетевой и разработческой грамотности своих членов и сообщества в целом. В этот период Коновалов записал определение нетсталкинга, а Дематерий и Архивист подтвердили его корректность. На внутреннем совещании 22.09.2017 население рабочей конференции выбрало «демократический» способ активности: каждый вкладывается соответственно своим желаниям и интересам. Так команда просуществовала до 23.09.2018, чередуя внутренние и внешние конфликты (26.03.2018 один из администраторов попытался уничтожить ВК-группу) со спокойными периодами.

[66] https://vk.com/stalkers_it

[67] https://www.youtube.com/channel/UC6FcefoE9lM9fPe8Zfd-PdA

2.5 Развитие сообществ в Telegram

Отправной точкой можно считать создание **Института Интернет Статистики**. Попадание в конференцию было возможно через пригласительную ссылку, распространявшуюся на имиджбордах[68]. В течение некоторого времени чат был открытого типа, по адресу @netstalking[69], затем снова закрылась, сгенерировав инвайт-линк.

Создан ИИС был 6.06.2016 неким yolo. Цель: завести сообщество, которое позволило бы заинтересованным в нетсталкинге людям общаться не на различных анонимных бордах (ВК тогда не рассматривался), а удобнее и оперативнее в мессенджере. Изгонялись лишь неадекваты и откровенно незаинтересованные люди. С самого начала и на протяжении всего существования конференции в ней активно присутствовали участники ИСКОПАЗИ и Архивист - один из ключевых людей Trailhead, известный как историк нетсталкинга и каталогизатор огромного числа находок.

Дискуссии велись на самые разные темы, от технических до философских, психологических и паранормальных, однако тяготение к техническим обсуждениям сохранялось. Вбрасывались ресурсы из клирвеба, ссылки на софт и сервисы. Предлагались и обсуждались идеи: собственной нетсталкерской платформы для коллаборации и совместной деятельности; способов определения и систематизации нетсталкинга. Последнее затем стало целью конференции **UNEG** (United Netstalking Evolution Group): закрытого чата по приглашениям, созданного 11 июля 2016, где собрались некоторые персоны из Trailhead и перспективные новички из ИИС.

Вспоминаются две интересных инициативы. Так как развитие командной работы было одной из повесток конфы, пара вечеров была посвящена типизации обитателей ИИС с помощью психологических тестов, в том числе на роль в команде. Другая инициатива, направленная на повышение общего актива, породила череду тредов[70] [71] в разделе /б/ двача: принимались заявки на поиск редких материалов от имени несуществующей «Организации Крот» (с указанием e-mail для обратной связи). Наиболее адекватные заявки пытались выполнить силами конфы.

Распад Института был связан с потерей админом доступа к своему аккаунту. Впоследствии его пересобрали в конференцию с таким же названием, но потеря логов и части некогда активных участников, существование на тот момент уже активной Точки Сбора, внутренние разногласия привели к новому распаду. Ценным проектом ИИС-2 было изучение инструментов DARPA, так и не доведенное до конца. Также планировались статистические исследования контента и устройств Сети. Многие темы инициировались или прорабатывались участником с ником Pantene Pro-

[68] https://2ch.hk/b/res/135628631.html#135632394
[69] https://t.me/netstalking
[70] https://2ch.hk/b/arch/2016-08-26/res/134855863.html
[71] https://2ch.hk/b/arch/2016-08-28/res/134979886.html

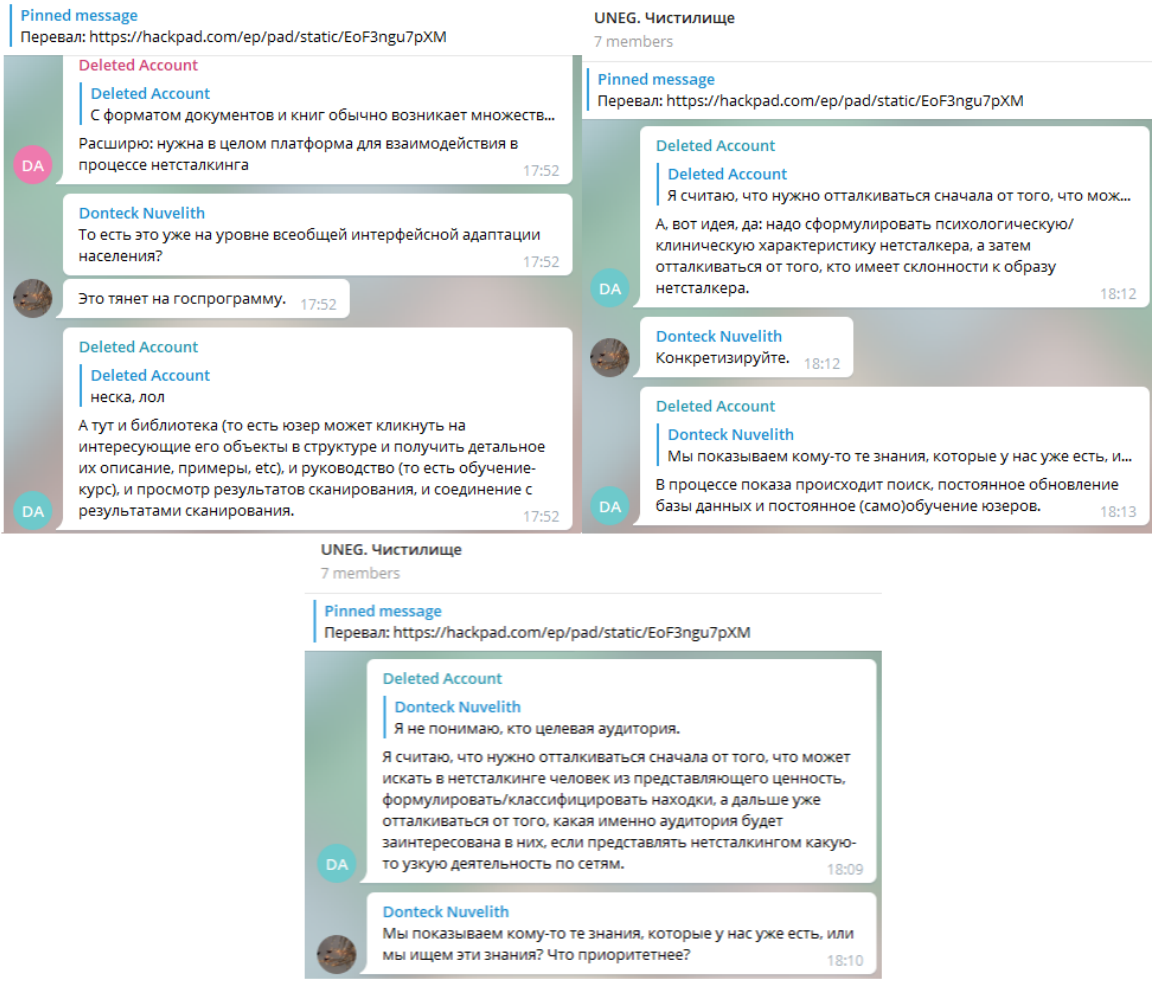


Fig. 1. Несколько фрагментов логов UNEG с обсуждениями направлений развития

V, который впоследствии создал полностью открытую тематическую конференцию: **Точку Сбора**. После исчезновения Пантина в ночь 2-3 мая 2017 конференция перешла к последнему активному админу Wegwarte. 15.10.17 она переехала на новый адрес, чтобы администратор владел полными правами. Старая же сохранила все логи и осталась «точкой входа». Помимо чата, администрация держит каталог ссылок[72], доску объявлений @netstalking_bulletin[73] и хранилище ключевых знаний по теме @netstalking_documents[74].

ТС, доступная и по сей день по адресу @netstalking, создана 17.01.2017 в качестве центральной площадки обсуждения нетсталкинга, технически доступной для прочтения и общения любому, кто заинтересовался бы темой. Наличие открытой конференции позволило одиночкам просить помощи и объединяться в однократные или

[72]https://github.com/netstalking-core/netstalking-catalogue
[73]https://t.me/netstalking_bulletin
[74]https://t.me/netstalking_documents

долгосрочные проекты, искать единомышленников и разрабатывать общенетсталкерские инструменты. Из значимых сообществ, родившихся таким образом, стоит упомянуть:

- Сетевое Соседство (@netstalking_networks[75]) - посвящена обсуждению сетевых технологий, исследованию и колонизации малоизвестных сетей, о которых речь пойдёт далее. Создана Abslimit'ом.
- Asleep Cams (@asleep_cg[76]) - сканирование и просмотр камер, создание инструментов и руководств. Создана Разиэлем 02.06.2018. Вокруг конференции быстро появились личные каналы с подборками эстетически ценных скриншотов или записей, нередко почерпнутых из работающего при ней сканбота.
- Netstalking Expedition Team - команда по расследованию и возможному разоблачению аномалий, теорий заговора и ложных сведений. Концепт такой группы впоследствии многократно перерождался и переименовывался, на момент написания к этим задачам имеет отношение чат под названием h0d.
- BlackNode Research - группа по исследованиям сети с использованием статистических методов и машинного обучения. Объявила о себе 14.11.2017 вместе с открытием онлайн-сервиса, где миллион скриншотов с камер был кластеризован по внешним признакам, а пользователь мог выбирать кадры из разных частей получившейся карты.
- Netstalking Godnota (@netstalking_godnota[77]) - архив наиболее примечательных находок и дискуссий. Создан Яном Майклом Винсентом, Разиэлем и Хранителем Маяка.
- NIAC (Netstalking Initiative Architectural Committee) - группа разработчиков универсальных решений для нетсталкинга. Создана 26.10.2019 Яном Майклом Винсентом. Предпосылки: с одной стороны, активное развитие самых разных ищущих ботов, унификация которых позволила бы легче создавать новых; с другой - опыт заморозки сообществом наиболее масштабных проектов.

3. ПОИСК В СЕТЯХ

Общеизвестный Internet - наследник закрытой сети ARPANET[78], созданной в США для передачи засекреченных военных данных и способной работать даже в условиях потерь сигнала. Первое соединение содержало всего два узла, а в 1970 году

[75]https://t.me/netstalking_networks
[76]https://t.me/asleep_cg
[77]https://t.me/netstalking_godnota
[78]https://en.wikipedia.org/wiki/ARPANET

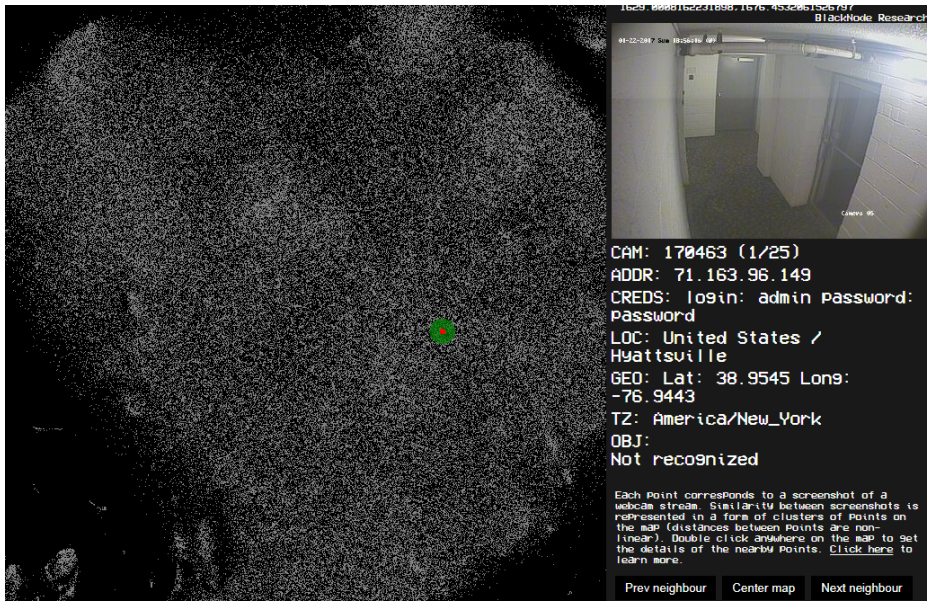


Fig. 2. Интерфейс сервиса с навигацией по кластеризованным камерам от BlackNode

расширилось на десяток государственных университетов. Проектов подобных систем в то время возникало много, и все они разрабатывались в НИИ на основе существующей инфраструктуры. Для подключения использовались линии телефонной связи, что позволило интернету быстро разрастись, а с появлением трансатлантического кабеля проникнуть и в Европу.

Из числа прочих сетей того времени известны CSNet[79], Bitnet[80] и ещё живой Usenet[81], ну а Россию не обошёл стороной FidoNet[82], взрастивший целые поколения пользователей.

С развитием протоколов передачи информации и продвижением стандартов спецификаций все сети постепенно сливались в единое целое, пока, наконец, не стали тем, что принято называть Интернетом. Протоколы передачи сигналов прописаны на уровнях от канального, где идёт получение бинарного кода из электрических импульсов, до пользовательского, которым пользуется самое знакомое и доступное для нас ПО: браузеры, мессенджеры, клиенты игр и др. Развитие сети не останавливается, ведь её пользователи могут создавать собственные протоколы поверх существующих.

Изучение технических редкостей и альтернатив является предметом интереса нетсталкеров наравне с получением прочей информации; методы нетрандома и де-

[79]https://en.wikipedia.org/wiki/CSNET
[80]https://en.wikipedia.org/wiki/BITNET
[81]https://en.wikipedia.org/wiki/Usenet
[82]https://ru.wikipedia.org/wiki/Фидонет

лисёрча также играют тут свою роль. Примером может быть история, рассказанная участником ИСКОПАЗИ: был найден сервер, выдававший поток непонятных данных через нетипичный порт. Сервер был найден нетрандомом (сканирование), а делисёрчем удалось определить, что происходит трансляция аудиопотока.

3.1 Всемирная паутина (WWW)

Зачастую понятие Интернета употребляется как синоним WWW (World Wide Web), хотя в действительности эти термины различаются. Всемирная паутина вместе с первым в мире браузером была изобретена Тимом Бернерсом-Ли значительно позже как проект внутренней сети CERN. Её основа лежит в концепции гипертекста — разновидности текста, обогащённого ссылками. Вскоре она была расширена до «гипермедиа», включив различные объекты, такие как картинки, звук, видео. Концепция воплощена в языке разметки HTML, описывающим отображение гипертекстовых страниц, а также протоколе HTTP (Hypertext Transfer Protocol), передающем эти страницы. Изначально концепция заключалась в построении системы, где каждый участник редактировал бы содержимое, о чём попытались напомнить в 2003 году в проекте Read-Write Web[83]. Наш опыт использования сети формируется **браузером**, а он, за исключением похороненного ViolaWWW[84], позволяет лишь одностороннее потребление. Только с развитием веб-сервисов до т.н. Web 2.0, где посетитель может сам наполнять некоторые страницы, это ограничение удалось преодолеть. Установка дополнений, вроде графической истории[85], даёт возможность ещё больше изменить ощущения от самого процесса сёрфинга.

Конкурентов у WWW было не так много. Project Xanadu [86] начал разрабатываться более 50 лет назад и противопоставлялся «простым бумажным страничкам» гипертекста. Делался упор на разнотипные, визуально отображаемые связи между фрагментами информации и их первоисточниками и создателями. На текущий момент не закрыт, но реализовал лишь начальные возможности в своём языке разметки EDL[87]. Hyperwave (старое название Hyper-G) предполагал централизованное хранение единой базы разнотипных ссылок, обладающих также метаданными. Это позволяло легко отыскивать связанные друг с другом материалы, определять права доступа к ним. Hyper-G работал с протоколом HG-CSP вместо HTTP и интерпретировал собственный язык разметки HTF вместо HTML. Разработчики прогнозировали ему скорое превосходство над WWW[88], но вместо этого на сегодня могут предложить[89] лишь корпоративную систему управления внутренней сетью — интранетом.

[83] https://readwrite.com/2003/04/19/the_readwrite_w
[84] https://en.wikipedia.org/wiki/ViolaWWW
[85] https://chrome.google.com/webstore/detail/brancher-visual-history-m/dfanhpdcmhemhkjafmannijhneiplgec
[86] https://ru.wikipedia.org/wiki/Проект_Xanadu
[87] http://xanadu.com/xuDemoPage.html
[88] http://jaschke.net/hyperwave.html
[89] https://www.hyperwave.com/en/

Интранет — частная сеть, обычно принадлежащая некоторому учреждению или организации и доступная только для сотрудников. Аналогична Интернету по архитектуре, но может даже не иметь выхода в глобальную сеть. Если же выход имеется, его стараются защитить как от внешних проникновений, так и от слива данных изнутри. Важно помнить, что любой человек может создать собственный протокол, поэтому в правительственных и внутрикорпоративных сетях могут применяться наработки, незнакомые широкой общественности.

Открытость информации ещё не делает её доступной любому. Требуются определённые умения, чтобы получать желаемое от поисковых систем, библиотек и архивов, форумов, соцсетей. Даже найдя зацепку, рядовой пользователь не всегда способен ею воспользоваться, так как не обладает должными навыками навигации, понимания механизмов работы сети и быстрого схватывания прочитанного[90]. Единицы безошибочно решают поисковые челленджи[91]. В результате развития сети, умение ориентироваться в гипертекстовом пространстве стало новым видом грамотности – т.н. Internet literacy. Простейший вид передвижения - «бессистемное просматривание Интернета путём перехода от одной страницы к другой» – называется **интернет-сёрфингом** [92] Такое поведение в сети обусловлено именно гипертекстовой парадигмой. Сеть изменила даже саму манеру чтения и вкусы в нём. В частности, люди стали читать[93] куда больше новостей и меньше литературы. Исследования показывают, что сконцентрированность чтения падает, когда материал перемежается привлекательными ссылками и яркими анимациями. Как следствие, поведение нетсталкера в сети отличается от поведения обывателя и становится по сравнению с ним искусством.

Закон «шести рукопожатий» здесь превращается в закон 19-ти ссылок. Он гласит, что с любой веб-страницы Сети можно попасть на любую другую в среднем за 19 нажатий мышки[94]. Этот предел не будет сильно увеличиваться с ростом сети: до 21 или 22 ссылок к концу века.

3.2 Поисковики

Скачкообразное развитие и создание первых примитивных поисковых систем произошло в начале 90-х, начавшись с успешных проектов Archie[95] и W3Catalog[96]. Ручное пополнение каталогов веб-страниц – тогдашних основных источников серверов – быстро теряло актуальность. С повышением популярности Интернета новые

[90] http://www.webology.org/2012/v9n1/a94.html
[91] http://vas3k.ru/challenge/2/
[92] Polly, J.A. (1992). Surfing the Internet: An introduction. Wilson Library Bulletin, 66(1Telnet и SSH0), 38-42.
[93] http://www.webology.org/2012/v9n1/a94.html
[94] Albert R, Jeong H, Barabási A-L. 1999 Diameter of the world-wide web. Nature 401, 130–131.(doi:10.1038/43601)
[95] https://en.wikipedia.org/wiki/Archie_search_engine
[96] https://en.wikipedia.org/wiki/W3Catalog

сервисы появлялись слишком часто, чтобы поспевать за ними, и люди решили автоматизировать процессы поиска и индексации. Всё это привело к многообразию поисковых систем и их конкуренции на цифровом рынке.

Сегодняшние поисковики используют разнообразные нововведения, но всё это лишь надстройки над основной структурой, мало изменившейся за всю историю. Основу поисковой системы составляют:

1. Веб-краулер, называемый иначе «поисковым роботом» или «пауком». Это бот, переходящий от одной сетевой ссылки к другой. Копии посещённых им страниц сохраняются в специальной базе, называемой индексом поисковика. Соответственно, процесс посещения - индексация. Такая тактика объясняет существование «глубокой сети». Множество ресурсов существуют, не имея ни одной внешней ссылки на себя.

2. Индекс, база известных сервису страниц. Специальный алгоритм обходит её в поисках наиболее релевантной к полученному запросу информации. У особо крупных поисковиков в базе может храниться больше ресурсов, чем они выдают. Их алгоритм может сокрыть результат, посчитав его недостаточно релевантным.

3. Система ранжирования выдачи. Определяет, какие параметры страницы делают её наиболее подходящей (т.е. релевантной) к поисковому запросу пользователей. Самые релевантные страницы появляются наверху выдачи, то есть юзер видит на первой странице то, что поисковая система «считает» наиболее качественным материалом к его требованию.

Ниже приведены лишь некоторые из факторов, влияющих на индексацию страниц.

- Для разработчика бессмысленно засорять поисковую выдачу тем, что не потребуется конечному пользователю, ведь главное — юзабилити. Его целевой аудитории нет дела до динамической генерации одноразовых ссылок подтверждения регистрации, форм заказа в магазинах или бесконечности страниц vesna.nologin.ru.

- Обычно доступность ссылок из базы данных поисковика регулярно проверяется, чтобы посетитель не наткнулся на нерабочие сайты. Именно поэтому не сохраняются текущие треды /b/, ведь дольше дня они обычно не живут. Однако архивные копии умерших страниц прекрасно индексируются.

- Веб-краулеры способны находить только то, что либо скармливается им вручную, либо упоминается на сайтах третьих лиц, которые уже проиндексированы поисковиком. На практике это означает, что IP-адреса с открытыми TCP портами без привязанных к ним доменов не будут автоматически проиндексированы, как и другие данные, никогда не светившиеся в Интернете.

- Сисадмин может ограничить индексацию всего сайта или части его страниц во всех поисковых системах через файлы robots.txt[97], .htaccess[98] или мета-тег HTML-а noindex[99]. Это имеет негативные последствия: такие сайты нельзя добавить на Internet Archive[100] и похожие сервисы. Гораздо практичнее блокировать конкретный поисковик утилитами типа Google Removal Tool[101], но так делают не все администраторы. Игнорирование robots.txt считается дурным тоном. Одно время создавались каталоги таких злодейских краулеров, а пойманный за этим занятием китайский поисковик Baidu[102] после крупного скандала принял общие правила игры. Google также убирает результаты из-за официальных заявлений, оповещая искателя курсивной плашкой (см. рисунок). Уточнить подробности позволяет сервис https://www.lumendatabase.org/.

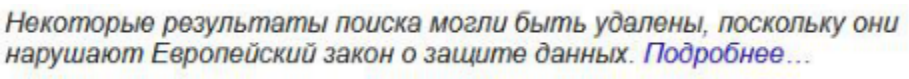


Fig. 3. Пометка про убранные из выдачи результаты

Необходимость выводить коммерческие ресурсы «в топ», то есть в первые строчки результатов того же Гугла, привела к развитию SEO. Вместе с тем, СЕО-инструменты можно использовать для неформальных исследований содержимого клирвеба. Приёмы поисковой оптимизации позволили заполонить целые страницы выдачи т. н. поисковым спамом, мешающим нетсталкеру. Помимо него, можно натолкнуться на дорвеи — странно выглядящие ресурсы, наполненные сгенерированными или ворованными текстами, работающими на цепях Маркова. Подробнее рассмотрим в разделе анализа находок.

Приём избавления от поискового спама описан Фравией: нужно перейти сразу на середину выдачи и двигаться обратно до появления осмысленных результатов; иначе перейти ещё глубже.

Грамотная работа с поисковиками подразумевает знание языка запросов[103]. Именно верная формулировка поискового запроса отличает обывателя от нетсталкера. Например, если простой человек вводит: «*скачать Photoshop бесплатно и без смс*», то исследователь использует операторы цитирования и поиска по сайту: «*site:rg-mechanics.org "photoshop cs6"*», а в сложных случаях[104] обращается к специализированным сетям[105]. Свой синтаксис запросов имеют все поисковики, включая самые

[97] https://en.wikipedia.org/wiki/Robots_exclusion_standard
[98] http://web.archive.org/web/20170627193056/hosting.nic.ru/support/htaccess.shtml
[99] https://ru.wikipedia.org/wiki/Noindex
[100] http://web.archive.org/
[101] https://google.com/webmasters/tools/removals
[102] https://moz.com/community/q/baidu-spider-appearing-on-robots-txt
[103] https://ru.wikipedia.org/wiki/Язык_запросов
[104] https://geektimes.ru/post/245180/#comment_8253502
[105] https://habrahabr.ru/post/318400/

известные: Google[106], Яндекс[107] и DuckDuckGo[108]. Для составления эффективного запроса внимательно рассматривайте url-ы своего целевого сайта или сайтов, пробуйте разные команды, изощряйтесь при выделении признаков вашего искомого объекта. Одно из преимуществ хорошо составленной поисковой фразы – она отсеивает множество однозначно лишних для вас результатов.

Пример постепенного уточнения запроса. Вы хотите найти сорт мороженого, о котором в памяти остался только красный цвет англоязычной этикетки и примерный год. Введём *красное мороженое* -– даёт слишком много вариантов, поэтому исключаем марки, которые не могли создать обёртку на английском. Получаем *красное мороженое -бабаевское -"красный октябрь"*. Чтобы отсечь современные образцы, укажем "мороженое красного цвета" 1997 год -бабаевское -"красный октябрь" ...и так далее.

Готовые фразы на языке поисковика, заточенные под какую-либо задачу делисёрча или нетрандома, называются дорками. Пример первого: поиск книги или конкретного официального документа. Пример второго: все Excel-таблицы с сайтов на домене .gov; все пользователи всех русских форумов на выбранном движке с конкретными интересами в профиле .

Дорки позволяют запросить массив специфических результатов с различных ресурсов. Таким образом вполне легально можно получить доступ к данным, хранящимся на сервере и не предназначенным для сторонних глаз. Можно одним махом собирать однотипные страницы для последующего ручного или машинного перебора. Добывают базы и документы, а также созданные на веб-сервисе ресурсы. Так, с открытых досок Trello можно получить[109] персональные данные и пароли, бизнес-стратегии предприятий и подобную чувствительную информацию, которую пользователи не озаботились скрыть. Аналогично нетсталкерами был сохранён перечень из многих тысяч майндкарт wisemapping.com.

Как уже упоминалось в 1-ой главе, благодаря служебным операторам можно искать не только незащищённые IP-камеры, но и другие устройства: роутеры, админпанели CMS, SCADA-системы и прочее. Тем не менее, обычно такие дорки[110] уступают сканированию диапазонов и поисковикам особого назначения: Shodan[111], Censys[112] и ZoomEye[113]. Какими бы полезными ни были обычные поисковики, найти с их помощью можно далеко не всё. Они не видят порядка 80-90% страниц в слепой зоне, образующей Deep Web — «Глубокую Сеть» . Зримая же часть называется клирвебом – «Ясной Сетью» либо «Поверхностной Сетью». Иногда исследователи сужают значе-

[106] https://bynd.com/news-ideas/google-advanced-search-comprehensive-list-google-search-operators
[107] https://yandex.ru/support/search/query-language/qlanguage.html
[108] https://help.duckduckgo.com/results/syntax/
[109] https://roem.ru/24-08-2017/257566/trello-llo/
[110] https://www.exploit-db.com/google-hacking-database
[111] https://www.shodan.io/
[112] https://censys.io/
[113] https://www.zoomeye.org/

ние термина до оверлейных сетей, однако это некорректно, т.к. в отдельных случаях можно проиндексировать вебсайты анонимных сетей. Например, благодаря tor2web[114] и ему подобным веб-гейтам для Tor, поисковики научились проверять и парсить html-содержимое сайтов .onion пространства. Более того, даже в Tope есть свои поисковые системы, охватывающие, впрочем, менее половины всех существующих скрытых ресурсов. Ещё чаще названием для совокупности оверлейных сетей служит термин Dark Net: оно широко используется даже в СМИ[115].

Пример: дорк, позволяющий искать обычным поисковиком среди onion-ресурсов, проиндексированных через гейты.
(site:onion.link | site:onion.cab | site:tor2web.ch | site:tor2web.org | site:onion.sh | site:tor2web.fi | site:onion.direct | site:onion.gq | site:onion.top | site:onion.rip | site:onion.guide | site:onion.to | site:onion.gold) ваш запрос

Пример: классический дорк для поиска ресурсов с «секретными материалами»

intitle:"index of" intext:"secret"

Пример: поиск конфиденциальных документов на русском:
"экз №" filetype:pdf

Иногда кастомный поисковик интегрирован в вебсайт и/или не основан на поисковой выдаче других сервисов. Почти все открытые файлообменники, равно как и видеохостинги: YouTube[116], Dailymotion[117], RuTube[118], и Vimeo[119], имеют свои формы для поиска. Помимо общего удобства, они упрощают сбор файлов по тегам. Например, снятые на фотоаппарат марки Nikon фотографии или видеоролики имеют в названии префикс DSCN и порядковый номер: DSCN0257, DSCN1821 и т.д. Есть и другие префиксы: MVI, MOV, IMG, VID, REC, MAH. Порой для сортировки результатов бывает полезно добавить постфиксный формат файла из списка Open-File[120]. Попрактиковаться можно в т.ч. на Документах ВКонтакте[121], где, впрочем, часто распространяются ДП[122] и изображения закладок — мест, где спрятаны пакетики с наркотиками.

Некоторые идут ещё дальше и создают **рандомизаторы** файлов со стандартны-

[114] https://www.tor2web.org/
[115] https://9net.ru/191-darknet-kak-voyti.html
[116] https://www.youtube.com/
[117] https://dailymotion.com
[118] https://rutube.ru/search/
[119] https://vimeo.com/
[120] https://open-file.ru/
[121] https://vk.com/docs
[122] https://ru.wikipedia.org/wiki/Детская_порнография

ми названиями. Так появился PetitTube[123], выдающий YouTube-записи с малым числом просмотров. По состоянию на 06.01.2016 в своей базе он содержит 5951 ссылку[124]. Аналогично работает Astronaut[125], имеющий открытый репозиторий на GitHub[126].

Таким образом, для нетсталкеров представляют интерес не только неиндексированные, но и непосещаемые или труднодоступные из-за избытка мусорной информации и технических ограничений ресурсы.

Литература

[1] John Matherly (в переводе LavenderTram), Complete guide to Shodan, 2016 г.

3.3 Файлообменники

На фоне облаков[127] многие забывают о файлообменниках, которые по сей день используются для быстрого обмена файлами, а исследователями — ещё и для их массового скачивания.

В рамках нетсталкинга файлообменники можно разделить на три категории:

1. Те, что генерируют порядковые ссылки или имеют публичные каталоги. Работа с ними вручную заключается в частом обновлении страницы и своевременном скачивании заинтересовавшего файла. Процесс можно автоматизировать с помощью парсера для извлечения ссылок из XML или HTML-документов или брутфорса для перебора порядковых чисел в URL. Если вам наскучат файлообменники этой книги, вы можете найти другие. Рекомендуется проверять их на наличие корневых sitemap.xml и sitemap_recent.xml запросами типа inurl:sitemap.xml.

- RGhost[128]. Один из крупнейших российских файлообменников, во время написания руководства сменивший концепцию и удаливший старые файлы. Обновляемый каталог за последний день был доступен[129] в XML. Также была полная история[130] неудалённых публичных файлов. Срок хранения выборочен: от 1 до 90 дней. В работе с РГхостом характерен скоростной парсинг. Заключается он в следующем. После загрузки на сервер файл сразу не меняет ссылку со стандартной 9-значной (7bDfKcfTJ) на сложную приватную (private/7C75Q9FXs/*md5 hash*), зато добавляется в каталог. Нетсталкер может успеть поставить файл на скачку до того, как его запривatит владелец, и изменится ссылка. Хакеры

[123] http://petittube.com/
[124] https://paste.ee/p/INclI
[125] http://astronaut.io/
[126] http://github.com/wonga00/astronaut
[127] https://ru.wikipedia.org/wiki/Облачное_хранилище_данных
[128] https://rghost.net/
[129] https://rghost.net/sitemap.xml
[130] https://rgho.st/releases

используют этот метод, чтобы достать сканы паспортов, частное порно и базы аккаунтов — всё, что плохо лежит. Технически это не взлом, т.к. файл общедоступен на момент скачивания.

- Файлообменник[131]. Вместо каталога есть постраничная таблица[132] с более чем 300000 ссылками. Точный срок хранения файлов неизвестен, т.к. их удаляет администрация по своему усмотрению, но в правилах[133] указан диапазон от 20 до 150 дней. Прямая ссылка находится в значении метода document.getElementById("link").innerHTML JS-функции linker(). Из защиты возможен только пароль.

- zFile[134]. Таблица на всю страницу содержит[135] лишь файлы за последние 3,5 дня, хотя всего их более 20000. Срок хранения: 14 суток. Приватизации нет, но запароливание есть. Перед скачиванием файла включается таймер на 10 секунд, заскриптованный JS-функцией *countdown()*. Его можно обойти, т.к. в методе *document.getElementById("link").innerHTML* первого вложенного if лежит прямая ссылка. Критичнее другое: скачивание возможно не чаще раза в минуту, поэтому советую использовать анонимайзеры. На сервер также нельзя загружать одинаковые файлы.

- 4shared[136]. Коммерческий международный файлообменник с мобильными приложениями на Android, IOS и Windows Phone, премиум подпиской и облачным хранением. Каталог[137] рассортирован по файловым расширениям и содержит более 80000000 файлов. Срок хранения не ограничен, но аккаунт деактивируется, если не логиниться дольше 180 дней. Безопасность описана[138] отдельно.

2. Те, что не имеют уязвимостей, обеспечивают конфиденциальность пользователя и пресекают попытки парсинга или брутфорса. Чаще всего это выражается в отсутствии каталогов и генерации сложных буквенно-цифровых ссылок. Тем не менее, какую-то часть их файлов, упоминавшихся в Интернете, можно найти с помощью операторов site:, inurl: и цитирования. Список таких файлообменников: Sendspace[139] (искать по /file/); Troloload файлообменник.рф DepositFiles[140] и т.д. Особо интересен MyFile[141], имеющий свой ханипот[142] и отслеживающий[143] скачивания государствен-

[131] http://fayloobmennik.cloud/
[132] http://fayloobmennik.cloud/files/list.html
[133] http://fayloobmennik.cloud/pravila.html
[134] https://zfile.in.ua/
[135] https://zfile.in.ua/files
[136] https://www.4shared.com/
[137] https://4shared.com/web/q
[138] https://www.4shared.com/security.jsp
[139] https://www.sendspace.com/
[140] https://dfiles.ru/ru/
[141] https://myfile.is/
[142] http://ru.wikipedia.org/wiki/Honeypot
[143] https://myfile.is/creeper

ными структурами и СМИ.

3. Наконец, существуют файловые хостинги. Принцип их работы такой же, как и у любых файлообменников, но есть ключевое отличие: поддержка одного, максимум двух типов файлов. С целью экономии места далее перечислены основные публичные хостинги.

Imgur[144]. Крупнейшая площадка для обмена картинками и анимациями, которые можно заприватить. Новые публичные изображения публикуются в специальной ленте[145]. Популярность сайта привела к появлению рандомайзеров, например: random imgur[146], Imgur Roulette и RandomGur[147]. Есть возможность узнать источник файла, если он загружен по ссылке. Другие хостинги изображений: Радикал[148] и Tinypic[149]. Оба имеют неограниченный срок хранения, строгую модерацию и два каталога, однако первый сервис менее организован, чем второй, из-за отсутствия пользовательских категорий.

Lightshot[150]. Обменник, хранящий скриншоты, взятые одноименным ПО. Его парсит нетсталкерский бот RandomShots.

Pastebin[151]. Первое в мире хранилище текстовых файлов неограниченного размера. Срок хранения выборочен. Подобные сайты популярны среди пользователей мессенджеров из-за неудобности чтения больших текстов прямо в чатах. Похожие функции выполняют pastebin.ru , Slexy[152], Upaste[153] и Pastiebin[154] , некоторые из которых генерируют удобные порядковые ссылки. Парсинг Пастебина возможен, но из-за того, что в архиве[155] хранятся 50 последних ссылок, потребуется либо постоянное обновление его страницы, либо покупка платного доступа к API[156].

SlideShare[157] - сервис хранения и распространения файлов презентаций. Это дочерний проект LinkedIn - соцсети для рекрутинга и профессиональных контактов. Задуман как социальная медиаплощадка, аналогичная ютубу: предоставляет возможности по комментированию, отметкам лайков и избранного, выходу в топы ресурса, анализу статистики посещаемости. Основным направлением контента предполагается обучающий материал, презентации конференций и компаний. Здесь хранятся учеб-

[144] https://imgur.com
[145] https://imgur.com/new/time
[146] http://www.maxitter.com/imgur/
[147] http://jasonb.io/randomgur/
[148] https://radikal.ru/
[149] http://tinypic.com/
[150] https://prnt.sc/
[151] https://pastebin.com/
[152] https://slexy.org/slexy/recent
[153] https://upaste.me/archive
[154] https://pastiebin.com/view_pasties
[155] https://pastebin.com/archive
[156] https://pastebin.com/api
[157] http://slideshare.net/

ные курсы, научные и научно-популярные материалы, диссертации. Это определено контекстом сервиса, но по факту ограничений на содержание заливаемых файлов нет. К примеру, можно найти копии печатных СМИ[158]. Поддерживаемые форматы[159]: pdf, odp, txt, форматы MS PowerPoint и MS Word. Сервис делит контент на презентации, документы и инфографику, исходя из свойств залитого файла. Хотя справка SlideShare этого не поясняет, позволяется заливать и видео. Для удобства краулера создаётся транскрипт: тексты на презентациях по возможности распознаются и включаются в страницу. Поиск по сервису возможен несколькими путями: по ключевым словам, по алфавиту (требует логина), сёрфингом по топам (не позволяет опускаться ниже определённого уровня) и сёрфингом по приглянувшимся профилям, подысканным в комментариях или из предыдущих поисковых результатов (пример[160] с интересным для нас, хотя и устаревшим контентом). Существует аналогичный MyShared , ориентированный на русскоязычный сегмент и поддерживающий только форматы PowerPoint.

Помните, что среди внешне непримечательных картинок могут оказаться rarjpeg'и[161] разных расширений: .jpg, .png, .gif, .mp3, .wav, .aac, .amr, .torrent и .html.

3.4 Парсинг

Автоматический сбор информации с того или иного веб-ресурса путём считывания со страниц называется парсингом, граббингом, а иногда веб-скраппингом. Специальная программа собирает всё либо только некоторые фрагменты по заданному правилу. Результат можно анализировать статистическими методами, с помощью natural language processing (например, через NLTK - Natural Language Toolkit[162]) или же перебирать так же, как это делается с выхлопом сканера портов. Этим способом были получены скриншоты тысяч майдкарт с открытых сервисов, на том же принципе базируются многочисленные боты для перебора сайтов на бесплатных хостингах: narod.ru, sitesity.ru, chat.ru и других. Общая схема подобного бота следующая:

1. Вы задаёте дорк, по которому будет совершаться поиск в google или другом поисковике.

2. Парсер, снабжённый библиотекой для веб-скраппинга, наподобие beautifulsoup, проходит по выдаче поисковой машины и заглядывает на каждую сссылку.

3. С помощью так называемого headless browser берётся скриншот, записываются все необходимые данные о ресурсе: URL, заголовок, любые другие дополнения. Вся эта информация поступает на вывод бота. Он может быть оформлен как сохранение на жёсткий диск или отправлен в какое-либо облако, например,

[158] https://www.slideshare.net/PRESSA2014/spask-vesti-spassk0425-44582501
[159] https://www.linkedin.com/help/slideshare/answer/53682
[160] https://www.slideshare.net/werro33/presentations
[161] http://lurkmore.to/Rarjpeg
[162] https://www.nltk.org/

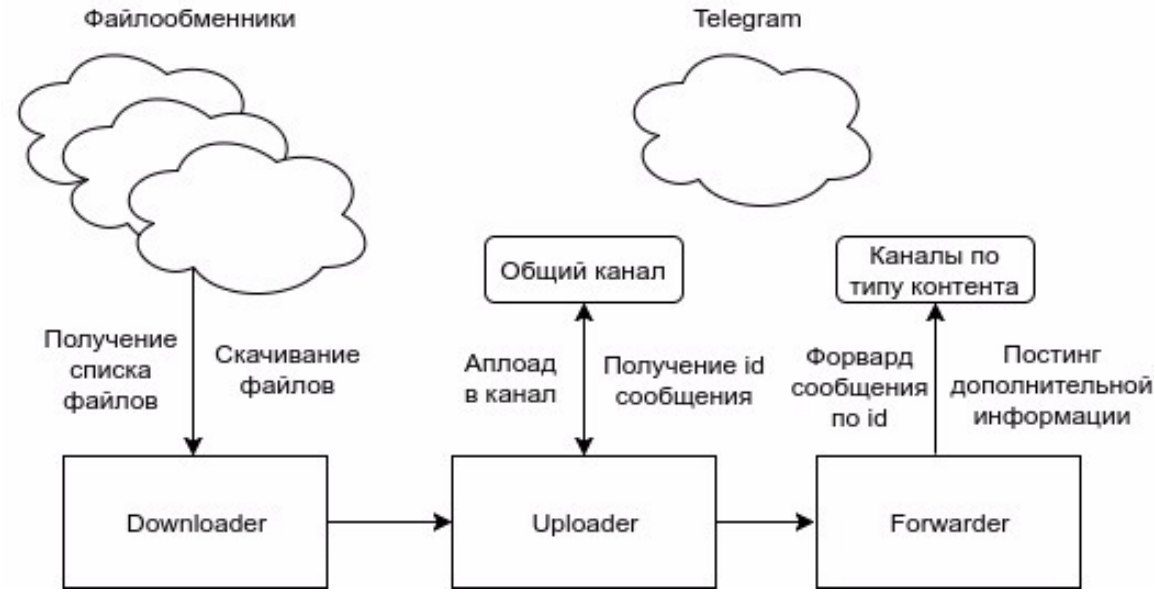


Fig. 4. Условное разбиение частей скрипта бота

Telegram, через API.

Архитектура бота[163], закачивающего файлы с обменника RGhost и фильтрующего их по типам для заливки, схематически выглядит так:

3.5 Сканирование сети

Каждое подключенное к интернету устройство (узел/хост) обладает IP-адресом[164] — уникальным идентификатором для выхода в глобальную или локальную сеть. Существуют две версии межсетевого протокола: IPv4[165] и IPv6[166], но в руководстве рассматривается только 4-ая, т.к. массовый переход на 6-ую требует дорогостоящих процедур замены и модификации оборудования. В России это пока едва осуществимо: лишь некоторые провайдеры поддерживают IPv6, хотя есть масса гайдов[167] по настройке без их согласия. Более того, сканирование его диапазонов сейчас бессмысленно, т.к. мельчайший из них содержит около 655367 возможных адресов, что вчетверо больше[168] числа работающих на IPv6 сайтов.

[163] https://telegra.ph/Grabber-fajlov-dlya-netstalkinga-11-14
[164] https://ru.wikipedia.org/wiki/IP-адрес
[165] https://ru.wikipedia.org/wiki/IPv4
[166] https://ru.wikipedia.org/wiki/IPv4
[167] https://www.ixbt.com/soft/ipv6.shtml
[168] https://security.stackexchange.com/questions/51523/how-do-i-use-nmap-to-scan-a-range-of-ipv6-addresses

IP-адрес стандарта IPv4 состоит из 4 чисел (октетов[169]/байтов[170]) от 0 до 255, разделённых точкой, и читается слева направо по нисходящей иерархии. Общее количество таких реальных адресов — 4 миллиарда, не учитывая диапазоны, которые резервируются[171] для частных сетей. На одном сервере могут быть заняты любые TCP порты[172] (от 1 до 65535), разрешающие приложениям принимать и передавать информацию по интернету. Зачастую открыты всего несколько из них, а прочие закрыты (активны, но отвергают входящие соединения) или отфильтрованы (не отвечают на запросы из-за брандмауэра). Исходя из этого, сканирование сети — автоматическая проверка доступности заданных портов, запущенных служб и номеров их версий на хостах адресного пространства, записываемого двумя способами:

Первый метод заключается в последовательном указании начальных и конечных IP-адресов через дефис. Например, диапазон 79.26.168.3-79.26.169.33 включает в себя все адреса с 79.26.168.3 по 79.26.168.255 (253 штуки) и с 79.26.169.0 по 79.26.169.33 (34 штуки).

Второй способ менее очевиден и подразумевает знание CIDR[173] — нотации, позволяющей записать целую подсеть[174] в виде IP-адреса и битовой маски, которая показывает, сколько первых битов должны остаться неизменными, и принимает значение от 0 до 32. Таким образом, 79.26.168.3/0 означает все возможные адреса (0 битов фиксированы, меняются все байты адреса), 79.26.168.3/24 означает диапазон 79.26.168.0-79.26.168.255 (24 бита фиксированы, меняются последние 8 бит = байт = число от 0 до 255), а 123.56.78.9/32 означает только один адрес — 123.56.78.9 (все 32 бита фиксированы).

Пользуйтесь CIDR, если вы хотите просканировать набор подсетей юридического или частного лица, города или государства, образованный онлайн-калькуляторами[175] и конвертерами[176]. Диапазоны по странам в простом и сложном форматах генерируют CIPB[177] и CIPRG[178], но их результаты устаревают и бывают уже изучены, в отличие от свежих перечней прокси со spys.ru и других каталогов с фильтрацией. Они позволяют узнать whois-информацию по адресам и скопировать значения полей inetnum или route. Чтобы не наживать проблем с законом, без тщательной анонимизации лучше не работать по своей стране и спискам «do not scan», куда входят, например,

[169] https://ru.wikipedia.org/wiki/Октет_(информатика)
[170] https://ru.wikipedia.org/wiki/Байт
[171] https://safezone.cc/threads/zarezervirovannye-ip-adresa-chto-ehto-takoe-i-s-chem-edjat.23225/
[172] https://ru.wikipedia.org/wiki/Список_портов_TCP_и_UDP
[173] https://ru.wikipedia.org/wiki/Бесклассовая_адресация
[174] https://ru.wikipedia.org/wiki/Подсеть
[175] http://www.subnet-calculator.com/cidr.php
[176] https://ipaddressguide.com/cidr
[177] https://www.countryipblocks.net/acl.php
[178] http://services.ce3c.be/ciprg/

военные, научные и засекреченные учреждения США, где, как считается, хранится самое «вкусное». Благодаря bgp.he.net вы можете пополнить их прежде не известными провайдерами, обслуживающими правительственные объекты, университеты и корпорации.

1. Находим в Гугле провайдеров этой страны/города.
2. Копируем их названия.
3. Идём на https://apps.db.ripe.net/search/
4. Вставляем названия в окно поиска.
5. Нажимаем поиск.

В общем случае каждому IP-адресу может быть сопоставлено несколько доменных имён. Это задача DNS-серверов: переводить числовую адресацию в «читабельный формат»вкусное и обратно.

Трудность с поиском на конкретной локации связана с тем, что подсети раскиданы провайдерами так, как им заблагорассудится. При этом в одном и том же месте, как правило, их работает несколько. Для подбора диапазона по стране, городу или даже улице имеется несколько рекомендаций. Если в интересующем месте расположены значительные (к примеру, юридические) организации со своими серверами, то наверняка у них есть своя официальная подсеть. Тогда нужно найти любой их сайт, определить его IP и посмотреть диапазон. Затем найти другие диапазоны[179] выданные этой организации.

Если место находится в шаговой доступности, можно побродить вокруг него и найти открытые WiFi-точки или незапароленные роутеры. Подключиться, определить свой IP аналогично прошлому шагу и посмотреть диапазоны.

Если же возможности добраться до места нет, можно воспользоваться информацией других исследователей. Каждой WiFi-сети соответствует уникальный номер - BSSID. Это позволяет собирать и каталогизировать точки доступа вместе с их местоположением и адресами. Создаются публичные базы [180] и целые WiFi-карты.
Инструкция по использованию базы, созданной коммьюнити сканера RouterScan:

1. Зайти на страницу карты. Авторизоваться под antichat / antichat (гостевой лог/пасс).
2. Выбрать на карте желаемое местоположение.

[179]https://apps.db.ripe.net/db-web-ui/#/query
[180]https://www.mylnikov.org/archives/1170

3. Зайти в интерфейс поиска IP по местоположению: третья слева кнопка в правом верхнем углу, с цифрами 192. В форму после клика будут переданы координаты с карты. Радиус поиска можно поменять. Можно зайти туда сразу по URL и вводить координаты вручную.

4. По кнопке Найти получаем диапазоны по заданным координатам. Нажав Список получим их в текстовом виде, пригодном для вброса в сканер сети.

Автоматизация массового скана с арендуемого сервера нежелательна у большинства хостингов, за исключением независимого CockBox[181] и сервисов типа linode.com. Эти будут сотрудничать с вами до первых жалоб блэклистам: скажем, spamhaus.org. Помните, что сканирование юридически не запрещено, если вы не занимаетесь пентестингом без разрешения. Даже в обычном режиме ваша рабочая машина отправляет сотни GET/POST-запросов на загрузку медиаконтента. Уголовный кодекс РФ предусматривает несанкционированное копирование, модификацию и уничтожение информации, но не её просмотр. Грубо говоря, нетсталкер осматривает и изучает устройство замка, разбираясь в типах отмычек, а взломщик вскрывает и эксплуатирует его в корыстных целях.

На гитхабе и форумах скриптkидди находятся[182] сотни любительских и профессиональных IP-сканеров вроде российских Advanced IP Scanner[183] и Advanced Port Scanner[184] на разные ОС, однако флагманским стандартом де-факто принят **Nmap**, консольный инструмент с опциональным GUI, кратким FAQ[185] и полной справкой[186]. Лучше запускать его с правами администратора, необходимыми для проведения низкоуровневых операций с сетевыми пакетами. Среди недостатков упоминают низкую скорость и отсутствие сортировки, из-за чего требуется сторонняя обработка XML. На сервере или локалке её проводят фреймворками типа IVRE[187], благодаря фильтрации составляющие частотную статистику WoT-устройств на мировой карте по странам, ленточной диаграмме и графе связей. Если вам не нужны свои свежие результаты, можете импортировать датированные базы scans.io, доступные на Censys с ограничениями (без графиков и пассивной слежки за состоянием хоста).

Гораздо шустрее, но не информативнее, будет **masscan**, способный просканировать всю Сеть за 6 минут на широком канале, пропускающем до 10 млн. пакетов в секунду. Но провайдер не обойдёт такую активность вниманием. Если вы не обладатель Linux'а, то придётся компилировать CLI-программу в виде проекта Visual Studio[188]

[181] https://cockbox.org/
[182] https://github.com/search?utf8=%E2%9C%93&q=ip+scan&type=
[183] https://www.advanced-ip-scanner.com/ru/
[184] http://advanced-port-scanner.com/ru/
[185] https://github.com/pantyusha/ultimate-netstalking-guide/blob/master/nmap-guide.md
[186] https://nmap.org/man/ru/index.html
[187] https://ivre.rocks
[188] https://visualstudio.microsoft.com/

или вручную через MiniGW[189]. К ней также имеется готовый веб-интерфейс[190] для табличной агрегации с поиском по заголовкам, сервисам, портам и октетам. Категоризацию HTML-страниц предлагает **Nesca**, некогда кооперативный сканер с активацией по ключам, опороченный пафосным дизайном и слухами о троянах и пересылке статистики на (уже недоступные) серверы. На сегодня[191] отправка данных отключена, исправлена часть багов. Неска визуализирует находки графиками, брутит BA по словарям из папки pwd_lists и имеет режим DNS-скана, перебирающего символы адреса в алфавитном порядке с прибавлением ДВУ (.ru) или поддомена (.narod.ru) по инструкции do_not_read.txt.
Далее приведён список наиболее частых целевых портов и соответствующих протоколов:

- 21: FTP — протокол передачи файлов меж клиентом и сервером, не потерявший актуальности с 1971 года. Сегодня многие вебсайты оснащены FTP-сервером, откуда подгружаются важные для работы ресурсы, и пусть он зачастую защищён, но встречается и свободный доступ по логину anonymous. Если вы найдёте рабочий анонимный FTP, и он вдруг умрёт, то лучше сохраните ссылку и проверьте её позже вручную или с помощью самописного скрипта. Некоторые сисадмины нечасто пользуются сервером, поэтому они отключают его на время простоя для экономии электроэнергии. Часто попадаются «пустые» FTP с директорией /incoming/, в которую можно заливать файлы, но скачивать их нельзя, т.к. после загрузки на сервер они видны лишь владельцу. Это результат настройки правил на чтение и просмотр файлов и необходимо для защиты от злоумышленников.

  Современные браузеры умеют открывать ссылки вида ftp://188.242.2.232, но поддерживают лишь скачивание. Поэтому полезны расширенные клиенты: FileZilla[192] и WinSCP[193], позволяющие загружать файлы на сервер или создавать их напрямую, скачивать папки и изменять режим передачи (ASCII или двоичный). Если сканирования недостаточно, то можете опробовать поисковики Krasfs[194], Mamont[195] и старинный проект Куличек.ком: FileSearching. В Телеграме также был канал[196], куда регулярно транслировались находки ИИС, ныне его сменил FTP-бот[197] Яна Майкла Винсента.

- 80, 8080: HTTP – протокол передачи в виде сообщений произвольных данных, в том числе гипертекстовых документов (HTML), потокового видео и звука.

[189] http://mingw.org
[190] https://www.offensive-security.com/offsec/masscan-web-interface/
[191] https://github.com/S0Ulle33/nesca
[192] https://filezilla.ru/
[193] https://winscp.net/eng/download.php
[194] https://www.krasfs.ru/
[195] https://www.mmnt.ru/int/
[196] https://t.me/aiWeipeighah7vufoHa0ieToipooYe
[197] https://t.me/netstalking_ftp2

Важными элементами являются стартовая строка и заголовок. Изучая их, можно определить тип передаваемых данных, что в сочетании с другой информацией о сервере может дать представление об их содержимом, если оно непонятно или не просматривается напрямую.

Порт 80 является портом по умолчанию при открытии URL либо ip-адреса в любом браузере.

- 443: HTTPS – шифрованное расширение протокола HTTP.
- 23: Telnet — Подключаться к telnet-серверам можно как вводом одноименной команды в терминалах Windows[198] и Linux[199], так и с помощью кроссплатформенной программы PuTTY[200] или веб-гейта[201] в браузере. Также действуют каталоги: BBS Guide содержит перечень публичных BBS (Bulletin Board Systems)[202], а Offbeat Internet[203] — просто часть известных серверов. Исследования компании Rapid7[204] показали, что около 15000000 хостов висят с открытым 23 портом. Популярен среди владельцев ботнетов.
- 3389, 5900-5906: RDP/VNC. Система удалённого доступа к рабочему столу компьютера, использующая протокол RFB. Часто устанавливается для управления объектами на предприятиях, частями инфраструктуры, поэтому требует бережного и ответственного обращения с вашей стороны. Проще говоря: ничего не трогайте. Для подключения[205] используются VNC клиенты: TightVNC, VNCViewer. Поскольку хосты с удаленным доступом часто становятся мишенью хакеров, эксперты безопасности частенько оставляют ханипоты, имитирующие уязвимые хосты, так что настоятельно рекомендуем использовать VPN.

Клиентской программе на тот или иной протокол указывает URI-схема: специальный идентификатор в начале адреса. Помимо общеизвестных http:// и mailto: вы встретите ftp://, gopher://, news:, geo: и многое другое - перечень см. в официальном реестре IANA [206]. Разнообразие же неофициальных URI потенциально неограничено и зависит от разработчиков клиентских программ.
Целенаправленное сканирование камер и получение доступа к ним осуществляется аналогично, но с учётом дефолтных портов устройств (см. подробно 4.4, также Литература, [1]) и особенностей их прошивок. Софт для этой задачи тоже зачастую

[198] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb491013(v=technet.10)?redirectedfrom=MSDN
[199] https://www.computerhope.com/unix/utelnet.htm
[200] https://putty.org.ru/
[201] http://telnet-online.net/
[202] https://ru.wikipedia.org/wiki/BBS
[203] http://www.jumpjet.info/Offbeat-Internet/Public/TelNet/url.htm
[204] https://information.rapid7.com/rs/495-KNT-277/images/rapid7-research-report-national-exposure-index-060716.pdf
[205] https://habr.com/ru/post/76343
[206] http://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml

адаптирован к конкретным вендорам. Например, Asleep Scanner - ПО, разработанное группой Camshift[207] для брутфорса и каталогизации камер Dahua, а в перспективе и других. Умеет находить и брутфорсить камеры dahua, делать скриншот, постить результат с геолоакцией и Shodan API в Telegram.

3.5.1 Telegram-сканеры Интернета

В октябре 2016го нетсталкер Pantene занялся разработкой сканера ip, который бы пришел на смену сканеру NESCA. Цитаты:
неска не взлетела почему то, хотя туда приделали все эти фишки: и распределенного скана, и даже встроенного общения. как думаешь почему? (я не знаю)
с неской же была стори что набежали школьники и борда d3w на которой сидели разрабы окуклилась.
Чтобы не нагружать новый проект на начальных этапах с поднятием файлового хранилища, было решено использовать сервера Telegram для хранения данных о хостах. Тогда сохранялись скриншоты веб-страниц, geo-ip и постились в канал https://t.me/netstalking_screenshots. Сканирование хостов осуществлялось через python-библиотеки, работающие с Tor и Selenium. Скачать исходный код этого сканера можно по ссылке: https://github.com/pantyusha/netstalking-telegram-bot
Предполагалось, что в последствии с помощью скриншотов и html создадут инструмент, который будет фильтровать выдачу методами машинного обучения, решая задачу кластеризации с эвристиками.
На основе этого проекта предпринимались попытки создания аналогичного сканера для доменных имён .onion, одна из таких попыток — https://t.me/onionnetstalk.
После ухода Pantene эстафету улучшения сканера перехватил Vechur, создав проект Medved, в принципе выдача ничем не отличалась от предыдущего проекта, поменялся инструментарий, добавились возможности распределенного скана для владельца бота, добавление результатов сканирования в MongoDB, убрано сканирование через Tor. Увидеть результат работы сканера можно в канале
https://t.me/xai7poozengee2Aen3poMookohthaZ, исходный код для улучшения: http://github.com/ChronosX88/medved.

3.5.2 Децентрализованные сканеры

Так как потребность в простом и надежном хранилище находок для всего нетсталкерского сообщества сохранялась всегда, команда Blacknode Research решила создать проект **Otklik**, который бы использовал технологии блокчейна, нейронных сетей и распределенного хранения данных. Основные отличия от всех предыдущих сканеров можно найти в их официальном канале: https://t.me/blacknode_research.
Исходный код одной из версий: https://github.com/v696973/otklik-dev-legacy.
Обсудить дальнейшую судьбу проекта можно в чате: https://t.me/otklik_dev

[207] https://t.me/camshift

3.5.3 Методы машинного обучения

Командой Blacknode Research был реализован проект по кластеризации миллиона скриншотов со стримов веб-камер: https://t.me/netstalking_webcameras. Для более подробного рассмотрения проекта можно посмотреть https://t.me/blacknode_research и попросить у нетсталкеров Jupiter Notebook **notebook.zip**. Кроме кластеризации в нетсталкинге есть множество проблем, которые могут быть решены с помощью машинного обучения. Для поиска подобных проектов можно обратиться к Istitoq[208].

3.6 Анонимные оверлейные сети

Прежде, чем перейти к понятию «оверлейные сети», раскроем понятия «туннелирование», «VPN» и «прокси» для упорядоченности и разделения терминов.
Туннелирование — в широком смысле это установка логической связи между двумя сетевыми устройствами (в т.ч. оконечные машины, маршрутизаторы и проч.) путем инкапсуляции («вкладывания») дейтаграммы данных одного уровня сетевой модели (OSI, TCP/IP) в дейтаграмму данных любого другого уровня сетевой модели, не обязательно в строгом иерархическом следовании модели. Протокол, в дейтаграммы которого вкладываются туннельные дейтаграммы, называется транспортным, т.е обеспечивающий непосредственную связь между точками для переноса туннельных дейтаграмм. Промежуточный протокол между транспортом и тоннелем, поддерживающий логическую связь, может называться протоколом инкапсуляции. Пример — в IP-пакеты с «белыми» адресами сети Интернет (транспорт) вкладываются дейтаграммы протокола GRE (протокол инкапсуляции), уже внутри которого вкладываются снова IP-пакеты (туннельный пакет) с адресами из частного диапазона. Более простой пример — туннельный протокол IP/IP, где прямо в транспортный IP пакет, без каких-либо промежуточных заголовков, вкладывается туннельный IP-пакет. Тут важно заметить, что туннелирование в широком смысле не предполагает шифрования данных, а только обеспечивает логическую сетевую связь поверх транспортных сетей. Причем, чаще всего, ничто не мешает уже установленную логическую туннельную связь использовать как транспортную для другого тоннеля, т.е. «наслаивать» тоннель поверх еще одного тоннеля.
VPN - Virtual Private Network, виртуальная приватная сеть. Это некоторая виртуальная сеть, виртуальность которой обеспечивается туннелированием, закрытая по отношению к транспортной сети, поверх которой она строится. Как раз термин VPN уже предполагает шифрование данных для обеспечения приватности, закрытости, т.е. невозможности прочтения вложенных данных с точки зрения транспортной сети. Чаще всего под VPN понимают сеть многих промежуточных и оконечных точек, построенную по одной технологии (туннелирования), которая используется только для обеспечения связи на некотором одном уровне сетевой модели (чаще всего — для IP-связности, реже L2-связности, см. виртуальный коммутатор). Т.е. по VPN ходят

[208] https://t.me/Istitoq

туннельные пакеты, которые уже переносят данные того же и более высоких уровней. Это часто используют организации (для соединения сети офисов/филиалов/кампусов) и частные лица. Стоит отличать site-to-site VPN — т.е. соединение подсетей, и client-to-site VPN, т.е. подключение оконечного пользователя к сети. Решения могут быть как открытые и общедоступные (PptP, OpenVPN, IPSec и прочие), так и закрытые и/или сертифицированные для специального назначения. Насчет последнего, в РФ для защиты персональных данных граждан должны использоваться разработки, сертифицированные ФСБ (СКЗИ с алгоритмами ГОСТ 28147-89 / ГОСТ Р 34.12-2015).
Другое понятние, требующее пояснения — это «**прокси**» (прокси-сервер, Proxy-server). Прокси (proxy - в данном случае наиболее уместный перевод - «посредник») — это некоторое устройство/сервер, который в модели «клиент-сервер» устанавливается посередине и становится посредником соединения. Разберем частный случай. Клиент обращается к целевому ресурсу и при этом хочет воспользоваться прокси-сервером. Соответственно, он обращается с прокси-серверу с вложенным запросом на целевой ресурс. Прокси-сервер замыкает соединение «клиент-прокси», и открывает соединение от своего имени «прокси-сервер» (в данном случае сам прокси является клиентом). Целевому серверу он адресует запрос клиента от своего имени. Сервер отдает запрашиваемую информацию прокси (в рамках соединения «прокси-сервер»), а тот в свою очередь переадресует эту информацию клиенту (в рамках соединения «клиент-прокси»). Таким образом, со стороны сервера будут видны только запросы от прокси, при этом изначального «настоящего» клиента сервер (в идеальном случае) идентифицировать не может. Со стороны канала связи, который обеспечивает соединение «клиент-прокси», также не видно (в идеальном случае), к какому серверу на самом деле обращается клиент. Количество соединений возможно наращивать, создавая «прокси-цепочку» (proxychain), что усиливает анонимность соединения «клиент-сервер», а также задействовать шифрование вложенных данных. Наиболее часто используемые протоколы прокси для веб-трафика: HTTP-прокси, SSL-прокси, SOCKS v4/v5. Из-за присутствия принципа вложенности, эту технологию некоторые относят к туннелированию. Следует отметить, что принцип прокси может использоваться не только для обеспечения анонимности или обхода блокировок. Применений в компьютерных сетях множество: например ARP-proxy, DHCP-proxy, DNS-proxy, балансировка нагрузки, кэширование данных, информационная безопасность и т.п.
Теперь перейдем к понятию **оверлейных сетей** (overlay - надлежащая, «поверхностная»). Это наиболее широкий термин из рассмотренных выше. Под оверлейной можно понимать некоторую логическую сеть, работающую поверх другой; эта другая считается транспортной для оверлея. Проще говоря, это сеть, «наслоенная» на другую сеть. VPN — случай оверлейной сети. IP-сеть, работающая поверх Ethernet-сети, или поверх любой другой сети канального уровня — тоже по сути своей оверлейная сеть. Часто в это понятие вкладывают более узкое значение. Тогда оверлейная сеть — это некоторая логическая сеть передачи данных, работающая поверх сети Интернет, но сервисы которой (серверные или распределенные) недоступны средствами традиционной сети Интернет, такими как структура IP+DNS+BGP и стек IP/TCP/HTTP(S). Получить

доступ можно лишь через специальные приложения, протоколы и логику работы. Другими словами, оверлей использует сеть Интернет сугубо как транспорт, но логически не как место размещения сервисов. Часто это позволяет обеспечить свойства, недоступные в Интернете, такие как анонимность передачи и размещения данных (Tor, I2P) и распределенное хранение файлов (P2P-сети, torrent, DC). Также оверлейными сетями называют и те, что дублируют сеть Интернет в структурном плане, но работают поверх нее с помощью протоколов туннелирования трафика (anonet, dn42).

3.7 Tor

Наиболее популярной оверлейной сетью, несоменно, является TOR[209]. Часто её связывают с криминалом, «волшебной палочкой» обеспечения анонимного хождения по сети. Считается, что Tor обеспечивает высокую степень защиты от таких программ шпионажа, как PRISM[210].

Принцип работы Tor хорошо описан в рунете и на английской вики-статье, также наглядное описание можно увидеть на youtube-канале Computerphile[211]. Вкратце, до подключения к оконечному серверу в Интернете, мы проходим цепочку из минимум трёх случайно выбранных прокси-серверов, тем самым обеспечивая анонимность пересылаемых данных (см. рис. [5]). Соединения зашифрованы по «луковичному» принципу таким образом, что:

- входной прокси-узел не видит, какому оконечному серверу или выходному прокси предоставлены данные, а лишь знает, какому промежуточному прокси-узлу переслать данные и какому клиенту вернуть данные;
- промежуточный прокси-узел не видит, от какого клиента или какому оконечному серверу предоставлены данные, а лишь видит, какому выходному прокси-узлу переслать данные и какому входному узлу вернуть данные;
- выходной прокси-узел не видит, от какого входного прокси-узла и клиента идут данные, а лишь знает, какому оконечному серверу переслать данные и какому промежуточному узлу вернуть данные.

Чтобы осуществить отправку сообщения по вышеописанной цепочке TCP-соединений в сети Tor (подробнее про TCP и запрет использования UDP в Tor будут описаны в следующих главах), каждый узел генерирует свою пару открытый/закрытый ключ[212] и знает все открытые ключи остальных узлов в цепи. Пример последовательности сообщений в такой цепи от пользователя S до сервера R показан на рисунке [5], где OS — входной узел в сеть Tor, OR — выходной узел, m — сообщение.

[209] https://ru.wikipedia.org/wiki/Tor
[210] https://ru.wikipedia.org/wiki/PRISM_(программа разведки)
[211] https://www.youtube.com/watch?v=QRYzre4bf7I&vl=tr
[212] https://ru.wikipedia.org/wiki/Криптосистема_с_открытым_ключом

Fig. 5. Принцип работы Tor

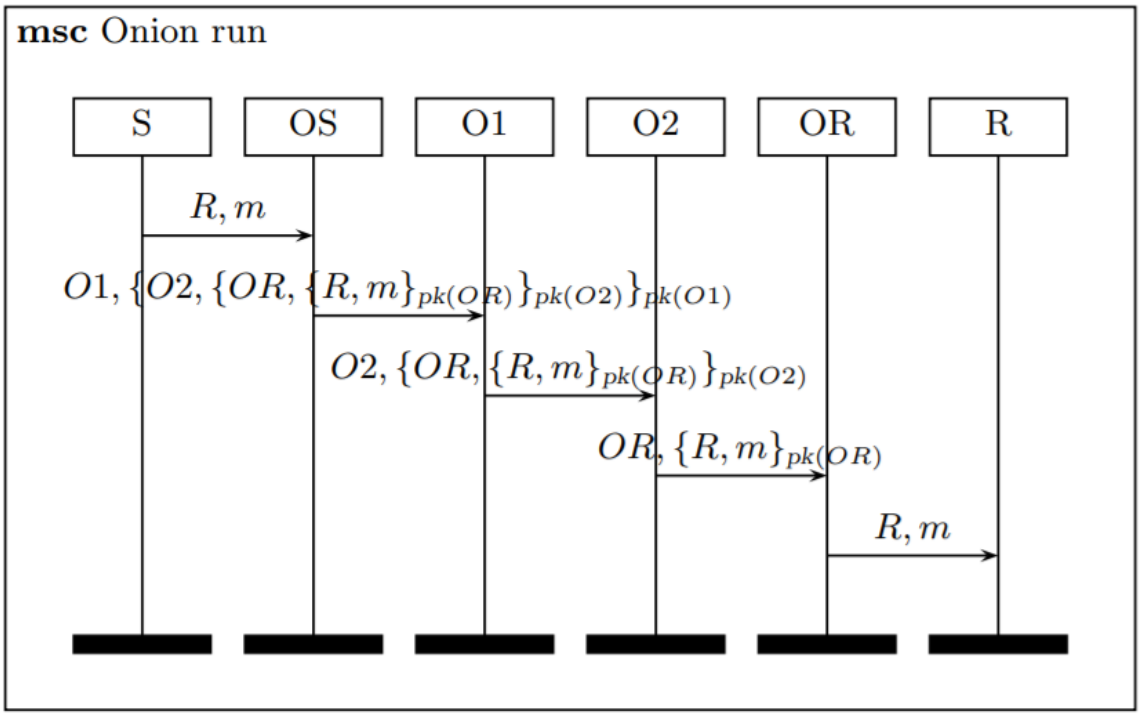


Fig. 6. Пример отправки сообщения в цепи Tor

Предположим, что выбранный путь отправки сообщения — OS; O1; O2; OR, тогда сообщение, отправляемое до O1, зашифровано следующим образом:
$message_{toO1} = \{O1, \{O2, \{OR, \{R, m\}_{pk_{OR}}\}_{pk_{O2}}\}_{pk_{O1}}\}$, т.е. заголовок, идентифицирующий предполагаемого промежуточного получателя O1 и полезную нагрузку зашифрованный открытым ключом O1. Так как мы ожидаем, что только O1 знает свой собственный секретный ключ, то O1 может очистить только внешний слой этого составного сообщения. Следовательно, O1 получает сообщение
$message_{toO2} = \{O2, \{OR, \{R, m\}_{pk_{OR}}\}_{pk_{O2}}\}$ и узнает, что это сообщение должно быть передано на маршрутизатор O2. Аналогично O2 и OR снимают слой с «лука» и, наконец, OR знает, что он должен отправить сообщение m своему пользователю R.
Причина, по которой этот протокол устанавливает конфиденциальность сообщения отправителя и получателя, заключается в том, что сообщения, покидающие узел, не могут быть связаны с сообщением, которые поступили в другой узел. Эта несвязанность входящих и исходящих сообщений требует, чтобы злоумышленник не смог отследить пользователей S и R, просто подобрав открытые ключи всех маршрутизаторов в цепи. Поэтому нам требуется рандомизированное шифрование, что означает, что одно и то же сообщение зашифрованный одним и тем же ключом каждый раз выдает другое зашифрованное сообщение. Это может быть получено, например, с помощью добавления «соли»[213] в сообщение.
Конкретные алгоритмы шифрования, применяемые для отправки сообщений в Tor, описаны в следующей спецификации:
https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt.
Более подробную информацию об устройстве анонимных оверлейных сетей можно найти на сайте:
https://www.freehaven.net/anonbib/topic.html#Anonymous_20communication
Помимо этого, сеть Tor также обеспечивает анонимность не только клиентов, но и серверов – средствами т.н. «tor hidden services»[214]. «Hidden services» позволяет подключаться к серверам не по их доменным именам в Интернете (следовательно, по IP-адресам), а исключительно через сеть TOR по доменным именам .onion (бывают 16-тизначные и более новые – 56-значные, отличаются возможностями отслеживания адресов), скрывая при этом настоящий адрес сервера. В основе алгоритма поиска доменных имен .onion являются так называемые рандеву-узлы[215]. Анонимность клиента при этом не нарушается, а сам сервис зачастую (если того не пожелал администратор) из обычного Интернета недоступен. Проще говоря, сайты в Tope зовутся скрытыми сервисами[216]. Таким образом, условно Tor можно разделить на 2 типа пользования – это выход в сеть Интернет через Tor и подключение к hidden services внутри сети Tor.

Наиболее простой способ выхода в сеть Tor – использование Tor-browser. Версии

[213] https://ru.wikipedia.org/wiki/Соль_(криптография)
[214] https://www.youtube.com/watch?v=lVcbq_a5N9I
[215] en.wikipedia.org/wiki/Rendezvous_protocol
[216] https://2019.www.torproject.org/docs/onion-services.html.en

есть под множество ОС – Windows, Linux, Androd. Tor-browser – по сути модернизированный Firefox с плагинами, такими как torbutton, noscript и https-everywhere.

Существуют альтернативные экспериментальные проекты, построенные по аналогии с сетью Tor, один из таких проектов — HORNET[217]. Его отличительная особенность в том, что он позволяет ускорить прохождения трафика через узел до 93 Gbit/s.

Интерфейс Tor-browser.
Достаточно запустить браузер – и вы в сети Tor. Чтобы проверить, что все в порядке и браузер настроен правильно, есть собственный специальный сервис check.torproject.org. Чтобы еще больше убедиться, можете проверить свой «видимый» IP по разным другим сервисам проверки адреса: 2ip.ru, Яндекс.Интернетометр, ifconfig.co, whoer.net.
Так же стоит установить максимальные настройки безопасности, отключить javascript или же включать js только на доверенных сайтах, не открывать Tor браузер на полный экран, так как по параметрам открытого окна, уровню заряда аккумулятора в ноутбуке (если работает HTML5) и другим настройкам браузера можно деанонимизировать пользователя с большой вероятностью. Такая техника деанонимизации известна под названием фингерпринтинг.
Небольшая памятка по сохранению анонимности в сети Tor:

- Не устанавливать в Tor браузер расширения.
- Не отключать дополнение NoScript.
- Часто обновлять цепочку нодов.
- Не открывать браузер Tor на весь экран.
- Не работать с браузером Tor с админ правами.
- Никогда не заходить используя свой логин и пароль на свою главную почту или свои реальные аккаунты социальных сетей, в которых имеется какая-та информация о вас или которые как-то связаны с вашими настоящими аккаунтами. Исключение только формы авторизации Onion сайтов и форумов. И конечно для таких сайтов желательно использовать отдельный почтовый ящик, который также не связан с вашей настоящей почтой. Причем почтовый ящик следует поднимать в сети Tor или хотя бы использовать https://protonmail.com/.
- Все скаченные файлы проверяйте на вирусы. Например, для этого можно использовать https://www.virustotal.com/
- Своевременно обновлять браузер Tor.

[217] https://habr.com/ru/post/356818/

- Не устанавливать протекающую капчу на свой onion-сайт[218].

Вбив в адресную строку адрес .onion ресурса, вы попадаете на hidden service. Следует отметить, что использование Tor не обеспечивает абсолютную анонимность. Более подробный гайд можно найти на Хабрахабре, где опубликовали перевод[219] списка советов о поведении в Торе.

Помимо прочего, в сеть Tor по сути можно выйти не только с помощью специального браузера. Сам браузер обращается к SOCKS5-прокси, «поднятом» на лупбэк-сокете 127.0.0.1:9150 (иногда может быть 127.0.0.1:9050). Поднимается этот прокси в тот момент, когда запускается браузер, и продолжает работать, пока он открыт. Этот локальный SOCKS5-прокси — и есть сама входная точка в Tor, за которой уже идет программная прошивка для подключения к сети. На Linux-машинах возможно установить Tor без специализированного браузера отдельно. Так как поднимается SOCKS5-прокси на локальном сокете 127.0.0.1:9150, а следовательно, можно проксировать на него любые протоколы, клиенты которых поддерживают SOCKS5. В результате через сеть Tor можно подключаться к внешним или hidden service серверам по ssh, telnet, ftp, gopher и прочим протоколам. Нужно только указать клиентскому приложению SOCKS5-proxy с IP-адресом 127.0.0.1 и портом 9150 при запущенном браузере. И вы можете подключиться, например, к FTP более-менее анонимно, либо зайти на hidden service не только по HTTP(S).

Пример альтернативного подключения к hidden service — подключение к BBS, размещенным на на нём. Есть также софт, позволяющий запроксировать какие-либо сетевые программы вне зависимости от того, предусмотрено ли это изначально. Например, некоторые пользователи используют onioncat для подключения к торрентам в клирнете через Tor, однако не следует использовать данный способ с *µTorrent*, который записывает ваш настоящий ip в пакете, который пересылается через Tor. Почему использование торрентов через Tor является плохой идеей подробнее описано на этой странице:https://blog.torproject.org/bittorrent-over-tor-isnt-good-idea.
Также на Linux есть специализированный torsocks[220] — им довольно удобно пробрасывать telnet или ssh. Для более общего пользования — proxychains.

3.7.1 Навигация в Tor

Для посещения «скрытых сервисов» в первую очередь используются каталоги — привет из прошлого Интернета до эры поисковиков, так как поисковики по Tor работают не очень хорошо из-за технических ограничений.

[218] https://habr.com/ru/post/235841/
[219] https://habr.com/ru/post/329756/
[220] https://github.com/dgoulet/torsocks

Популярный пример каталога в Интернете есть на википедии, но существуют они и на самих hidden service, что представляет обычно больший интерес.
Из инструментов можно отметить:

- Поисковики (Google, Yandex, Duckduckgo). Существует много каталогов и упоминаний интересных скрытосервисов в обычном Интернете, к примеру, в Reddit и частных блогах;
- Daniel's Hosting[221] — бесплатный хостинг скрытосервисов с перечнем большинства размещённых ресурсов, почтой и чатом. Неактивные сайты вычищаются раз в месяц;
- DeepLink[222] — индекс .onion ссылок. Позволяет искать .onion ссылки по части доменного имени, заголовку, описанию;
- DeepLink Random[223] — генератор случайных .onion имен (рандомайзер);
- Hyperion[224] — карта hidden service. Имена представлены не полностью. Достраивать их можно, воспользовавшить инструментом из п. 2 выше, или пробивая по обычным поисковикам;
- Fresh Onions[225] — краулер и каталог новых сервисов. Собирает и проверяет новые ссылки как на самих .onion-сайтах, так и на множестве других источников: pastebin, reddit, поисковики в Top, бесплатные хостинги скрытосервисов, сторонние каталоги;
- UnderDir[226] — каталогизированные сайты разделены по категориям, в том числе по языку;
- Tor2Web[227] — гейт из Интернета на внутренние сервисы Tor. Как пользоваться написано на самом сайте. Есть и другие подобные гейты;
- TORCH[228] — Поисковик по Tor'у;
- TorLinks[229] — каталог ссылок;
- The Hidden Wiki[230] — каталог ссылок;

[221] https://danwin1210.me/
[222] http://deeplinkdeatbml7.onion/index.php
[223] http://deeplinkdeatbml7.onion/random.php
[224] https://www.hyperiongray.com/dark-web-map/
[225] https://www.freshonions.net/
[226] http://underdj5ziov3ic7.onion/
[227] https://www.tor2web.org/
[228] http://xmh57jrzrnw6insl.onion/
[229] http://torlinkbgs6aabns.onion/
[230] http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page

- Abikogail[231] — поисковик по Tor.
- Lookonion[232] — поиск по умолчанию в Tor-браузере, доступный из обычного интернета.
- ahmia.fi[233] — поисковик по Tor.
- Tor-YaCy[234] — YaCy, децентрализованная поисковая машина, работающая в рамках одноранговой сети. Подробные гайды по поднятию сервера YaCy для индексации .onion можно найти на вики: http://wiki.yacy.net/index.php/En:YaCy-Tor.
- OnionTube[235] — аналог YouTube в даркнете. Есть различные жанры видео, поиск, последнее и популярные каналы. Можно загрузить что-то своё, либо что-то скачать (для этого необходима регистрация).
- http://j7zbybfl5ho2rta3.onion — RetroBBS с популярными в наше время обсуждениями линукса, хакинга, i2p и т.п., и чуть менее популярным интерфейсом. По сути здесь развернуто два безопасных узла: rocksolid и dove-net. Обсуждение самих узлов также внутри BBS. Ссылка в клирнете http://rocksolidbbs.com/.

Также существуют различные индексаторы .onion:
https://github.com/iomintz/onion-service-index
http://zlaehcuajft45pvy.onion
http://jld3zkuo4b5mbios.onion/
Кроме традиционных http-onion ссылок, существуют ещё Gopher подключения. Инструкция по исследованию этого явления можно прочитать по этой ссылке:
https://gopherproxy.meulie.net/bitreich.org/1/onion
Примеры gopher-ссылок:
gopher://hg6vgqziawt5s4dj.onion
gopher://par7qdjbxvve57ts.onion/
gopher://xopo4w4zpyw2u43n.onion/1/darknet-access/

3.7.2 Сканирование Tor

Сканирование портов hidden-service — нетривиальная задача. «Натравить» nmap с помощью torsocks или proxychains на .onion-хост с ходу не получается. Для данной задачи у nmap есть инструкции (раз), но тут все довольно непросто в реализации, и похоже, не во всех случаях работоспособно. Более удобное решение есть на github — hsportscanner[236]. Кратко о пользовании:

[231] https://abikogailmonxlzl.onion.casa/
[232] http://lookonion.com/
[233] https://ahmia.fi/search/
[234] http://63px7zirpd7npu3j.onion
[235] http://tubef7zilcjhme2g.onion
[236] https://github.com/ivanpustogarov/hsportscanner

1. Скачиваете скрипт с git

2. При необходимости в главном скрипте hsportscanner.py можете поменять адрес и порт Tor-прокси:
   TOR_SOCKS_IP_ADDRESS = "127.0.0.1"
   TOR_SOCKS_PORT = 9150

3. Запускается следующим синтаксисом:
   ./hsportscanner.py -h [.onion-адрес] -p [номера портов в формате nmap]
   Например:
   $ ./hsportscanner.py -h gnosisbbs43ppu7h.onion -p 23

Другим инструментом является docker-onion-nmap[237] – docker-контейнер, в котором собран nmap+dnsmasq+tor+proxychains. Использование крайне простое, достаточно установить docker. Вам нужно указать порты в формате nmap и .onion-адрес:
$ docker run –rm -it milesrichardson/onion-nmap -p 80,443
facebookcorewwwi.onion
...
PORT STATE SERVICE
80/tcp open http
443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 3.58 seconds

Более сложный инструмент – onionscan[238]. Он делает комплексное сканирование hidden service сервера – проверяет некоторые популярные порты на доступность, ищет утечки информации в веб-директориях, граббит файлы и прочее. Полный список возможностей есть тут[239]. Для запуска нужно установить язык Go, инструкция по пользованию есть на странице github. Опять же, должен быть запущен Tor, и, скорее всего, придется указать сокет прокси самостоятельно. В итоге полная команда может иметь вид:
$ ./onionscan –verbose –torProxyAddress 127.0.0.1:9150 *.onion* –

Создание узлов сети: Tor Relay за пять минут[240]

[237] https://github.com/milesrichardson/docker-onion-nmap
[238] http://www.automatingosint.com/blog/2016/07/dark-web-osint-with-python-and-onionscan-part-one/
[239] https://github.com/s-rah/onionscan/blob/master/doc/correlation-lab.md
[240] https://habr.com/ru/post/228971/

3.7.3 Поднятие Tor hidden service

Tor позволяет пользователям и узлам создавать .onion ссылки. То есть вы можете открыть веб-сервер, SSH-сервер и т. д. для сети Tor, не раскрывая свой IP-адрес. Поскольку вы не используете публичный адрес, вы можете запустить службу onion за брандмауэром. Шаги поднятия onion сайта:

1. Запустите Tor.

2. Установите веб-сервер. Например, можно воспользоваться nginx или lighttpd (apache вряд ли пригоден для анонимности).
   Примерный набор команд для настройки веб-сервера:
   (sudo apt-get install nginx)
   В /etc/nginx/nginx.conf поменять следующие значения:
   http {

   . . .
   # не предоставляем версию используемого софта
   server_tokens off;
   # отключаем ведение логов
   #access_log /var/log/nginx/access.log;
   #error_log /var/log/nginx/error.log;
   error_log /dev/null crit;
   . . .

   Далее создаём файл нового виртуалхоста.
   Включаем его.

3. Введите настройки в torrc и перезапустите Tor. Для этого введите в /etc/tor/torrc:
   HiddenServiceDir /var/lib/tor/yoursite1 # каталог создаётся автоматически
   HiddenServicePort 80 127.0.0.1:80
   Первая строчка в конфиге указывает путь к закрытому ключу, который создаётся автоматически Tor'ом при первом запуске после модификации конфига и играет роль onion-домена.
   $ sudo ls /var/lib/tor/yoursite1
   hostname private_key
   Файл **hostname** содержит адрес домена сгенерированного на базе хеша ключа **private_key**, который в свою очередь сгенерировался случайным образом при первом запуске.
   Удаление/модификация файла **hostname** не влечёт никаких последствий, при следующем перезапуске Tor он вновь создаётся на основе ключа. Это скорее файл-подсказка для вас.

А вот ключ **private_key** необходимо держать в секрете. До тех пор пока вы являетесь единственным владельцем этого файла - ваш домен никто и никогда не украдёт.
Вторая строчка *HiddenServicePort 80 127.0.0.1:80* задаёт какой порт будет у onion-ресурса и какой адрес и порт будем форвардить на него. Например, берём адрес/порт 127.0.0.1:80 и форвардим его на *.onion:80.
Если сайтов несколько, то нужно прописать ещё одну пару строчек, которые будут соответствовать сайту на веб-сереверe. Как сгенерировать более защищенный 56-тизначный onion адрес можно прочитать в официальной документации: https://2019.www.torproject.org/docs/tor-onion-service.html.en#four Также несмотря на то, что адреса генерируются случайным образом, их можно подбирать. Подробнее об этом написано в статье:
https://cryptopunks.org/article/generate+custom+onion+address/.

3.7.4 Мессенджеры

Tor-браузер не является универсальным решением всех задач, связанных с передачей информации, поэтому для усиления устойчивости шифрования и удобства работы с конкретными приложениями используются специализированные протоколы поверх луковичной маршрутизации. Для переписок используется протокол bitmessage, реализованный в приложении PyBitmessage[241]. Самым ближайшим аналогом BitMessage в привычном многим интернет мире является электронная почта. Главное отличие от существующих мессенджеров в том, что у него отсутствует центральный сервер, сообщения передаются по p2p-сети bitmessage[242]. Аналогом такого подхода можно назвать протокол Tox. Судя по опыту использования, bitmessage работает стабильнее, но несмотря на это решения децентрализованных мессенджеров всё ещё требуют значительной доработки, поэтому для более стабильного соединения и приватности используют проверенный временем протокол XMPP, другое название – jabber. Настройка onion-jabber сервера аналогична поднятию .onion сайта:
https://cryptopunks.org/article/jabber_over_tor_on_raspberrypi/.
Для подключения через смартфон можно использовать приложения Tor messenger, либо популярный xmpp-клиент Conversations. Инструкцию можно найти на сайте https://creep.im/xmpp_tor/

3.7.5 Файлообмен

Из-за отсутствия встроенного UDP в Tor затруднительно использовать протокол BitTorrent, Kademlia и другие способы для быстрой передачи файлов в p2p-сетях[243]. Вместо этого используются onion-сервисы, которые выполняют роль файлового храни-

[241] https://github.com/Bitmessage/PyBitmessage
[242] https://bitmessage.org/bitmessage.pdf
[243] A Survey on Distributed Hash Table (DHT): Theory, Platforms, and Applications

лица. По такому же принципу работает OnionShare[244], позволяющая безопасно и анонимно передавать и получать файлы, а также организовать работу публичного сервиса для обмена файлами. В принципе, возможно реализовать быстрый файлообмен по аналогии с DC++ в сети Tor, одна из таких попыток: https://ru.wikipedia.org/wiki/WASTE. Проект закрыт 14 января 2004 года. Надеюсь, в будущем получится разработать программу, релизующая вариант протокола Kademlia в сети Tor, для этого можно использовать OpenKAD[245]

3.7.6 Интернет-легенды из Tor

В интернете можно найти множество статей и видеороликов, пересказывающих мифы и легенды относительно содержания «Даркнета». Авторы этих материалов пытаются превратить его в кладовую сакральных знаний с доступом к любым запрещенным товарам и услугам. На деле же большинство экзотических предложений — просто разновидность мошенничества с целью заработать на доверчивых людях.
Классическими примерами такого обмана можно назвать «редрумы», торговля людьми, продажа хакерского ПО, которое способно устанавливать radmin, отправив голосовое сообщение в мессенджере, торговля паспортами, банковские карты с балансом. Зайти на такие сайты можно по ссылкам:

1. http://redroomfing27toi.onion/
2. http://zxjfjm5iinmgezyj.onion/
3. http://xhackergnluw32xz.onion/

Однако в сети Tor можно найти настоящие материалы с преступлениями. Например, Doll Maker, Daisy Destruction, на одном из этих видео изображена мучительная смерть младенца. К счастью, авторов такого контента смогли деанонимизировать[246].
Продажа запрещенных веществ, оружия также является проблемой, которую используют для обоснования создания новых ограничений и контроля Интернета со стороны государства. В связи с этим формируются военные организации, научно-производственные объединения[247] с целью написания софта для осуществления атаки на анонимные сети.
На деле же большинство вещей происходящих в сети Tor это обычный серфинг, использование технологии для защиты приватности своих данных и свободы слова.

3.8 I2P

I2P — анонимная оверлейная сеть. От Tor отличается техническими особенностями и тем, что в основном используется не для анонимизации выхода в сеть

[244] https://onionshare.org/
[245] https://github.com/CCOrg/OpenKAD
[246] https://ru.wikipedia.org/wiki/Скалли, Питер
[247] Взлом SyTech: https://rex-net.livejournal.com/2006746.html

Интернет, а для пользования внутрисетевыми ресурсами. Анонимны как пользователи, так и сервера.
Используется псевдо-доменная дона .i2p. Однозначно узлы идентифицируются большими именами в формате Base32, например:
xxu3lso4h2rh6wmrxiou3ax7r7la7x6dhoepnku3jvrlwp35pefq.b32.i2p
Но в сети есть свой аналог DNS, который ставит в сопоставление более короткие и читаемые имена, такие как 102chan.i2p. Т.е. адрес узла 102chan.i2p, аналог доменного имени в сети Интернет, соответствует однозначному адресу
xxu3lso4h2rh6wmrxiou3ax7r7la7x6dhoepnku3jvrlwp35pefq.b32.i2p, аналог IP-адреса в сети Интернет.
Основная страница загрузки предлагает I2P на множество ОС. В отличии от Tor тут нет готового браузера, что требует некоторой настройки. Рассмотрим порядок установки на Windows:

1. Скачиваем i2p на Win с сайта. На момент написания почти все ссылки были битые и только одна живая. Устанавливаем. «Windows Service» на первых порах не пригодится — это нужно, чтобы запустить i2p как виндового демона, т.е. в фоне, удобно если держать постоянно работающую ноду.

2. После установки запускаем i2p (тот который «restartable») из меню «Пуск» — пусть прогревается. Пока что это происходит устанавливаем (если такогово нет) браузер Firefox. Firefox не обязателен, но рекомендуется, так как в нем удобно создать отдельный профиль браузера. Запускаем Firefox, в строке вводим «about:profiles» - заходим в настройки профилей. Нажимаем «Создать новый профиль», создаем профиль под именем, например, «i2p».После создания профиля устанавливаем его по умолчанию («Установить как профиль по умолчанию»), после чего нажимаем «Перезапустить в обычном режиме».Профиль создан – теперь, все что касается i2p, будет хранится в этом профиле, включая настройки браузера, плагины, закладки.

3. После того, как браузер запустился, заходим в настройки («about:preferences»), находим настройки прокси-сервера:
   Нажимаем «Настроить». Настраиваем прокси как на скриншоте. HTTP-прокси, адрес 127.0.0.1, порт 4444. Нажимаем ОК, сохраняем настройки.

4. Заходим в консоль маршрутизатора i2p – вбиваем в строку адрес 127.0.0.1:7657

5. Первым делом заходим в «Адресная книга» (должна быть на главной панели) → «Подписки». Там будет всего один дефолтный адрес. Как уже было сказано ранее, в i2p действует свой аналог DNS. Разрешение имен происходит с помощью адресных книг, или подписок. Это файлы, содержащиеся на внутренних узлах сети, в которых содержатся соответствия читаемым именам узлов реальных имен. Дефолтная подписка довольно скудна, поэтому добавим сюда еще

несколько:
http://joajgazyztfssty4w2on5oaqksz6tqoxbduy553y34mf4byv6gpq.b32.i2p/export/alive-hosts.txt
http://inr.i2p/export/alive-hosts.txt
http://stats.i2p/cgi-bin/newhosts.txt
http://rus.i2p/hosts.txt
http://no.i2p/export/alive-hosts.txt
http://reg.rus.i2p/public/a-hosts.txt
http://stats.i2p/cgi-bin/newhosts.txt
После добавления сохраняем настройки. Также рекомендуется подкрутить скорость (на главной - «Настройки скорости»).

6. Для проверки работоспособности можно зайти на exchanged.i2p или 102chan.i2p Выше рассмотрена самая простая настройка. Для более удобного проксирования на i2p можно воспользоваться раширением foxyproxy. Устанавливаете расширение, заходите в настройки, слева вверху нажимаете «Add», создаете новый прокси верхним в списке с настройками: *Proxy Type: HTTP; Title: как вам угодно; IP-addess: 127.0.0.1; Port: 4444* Нажимаете Save. После сохранения открываете «Patterns» в строке с прокси Создайте паттерн. Из «White patterns» удаляете старый паттерн, нажимайте «New White» и создаете новый с содержанием: Name: как вам угодно; Pattern: *.i2p ; Type: wildcard; http(s): both; On/Off: On Сохраняете все настройки. Нажимаете на значок FoxyProxy и выбираете «Use Enabled Proxies by Patterns and Priotity»

Таким образом можно использовать firefox параллельно с выходом в Интернет – все обращения на .i2p-имена будут идти через i2p-прокси, остальные – в Интернет.Чтобы сделать хождение по i2p более безопасным, можете установить расширения из Tor Browser. Наиболее нужное из них - это NoScript для отключения JavaScript на страницах. Не стоит забывать и про другие сервисы, предоставляемые i2p – это почтовый шлюз, IRC-шлюз, bittorrent-шлюз. Со списком сервисов можно ознакомится здесь: https://geti2p.net/ru/docs/applications/supported#email Если есть желание поднять свой шлюз в сеть i2p на отдельной машине, можете рассмотреть варианты на Linux - JAVA-приложение или deb-пакет на Ubuntu/Debian, установить как сервис Windows, или посмотреть в сторону i2pd – полноценный узел i2p, написанный на C++. Также существует и проект по сборке i2p в браузер, как для Tor.

3.8.1 Сканирование I2P

В 2015 году провели первую масштабную «перепись» пользователей сети с помощью нескольких поднятых нод. Крис Барри воспользовался тем, что I2P не скрывает, что тот или иной узел использует её. Обнаружилось около 50 тысяч пользовательских маршрутизаторов, из которых половина — в России.
Ресурсы i2p:
http://anch.i2p/— имиджборда анархистов

http://angallery.i2p/— коллекция аниме-арта
http://freezone.i2p/— социальная сеть по типу хабра
http://hiddenchan.i2p/— имиджборда (сейчас закрыта, но можно скачать дамп), убежище для ушедших с сосача, двача и др.
http://lenta.i2p/— новостная лента создаваемая посетителями
http://rus.i2p/— главная русская вики
http://progromore.i2p/— вики программистов
http://deepweb.i2p/— имиджборда и вики (зеркало в .onion)
http://anotube.i2p/— видеохостинг по типу ютуба

3.8.2 Ускорение получения данных из I2P

Для ускорения доступа к ресурсам i2p можно настроить выходную ноду на сервере, которая будет устанавливать как можно больше туннелей, подробный гайд описан по ссылке:
http://netwhood.online/2018/09/14/overlay-node/

3.9 Freenet

Freenet — одноранговая сеть, предназначенная для децентрализованного распределённого хранения данных без возможности их цензуры, созданная с целью предоставить пользователям электронную свободу слова путём обеспечения их строгой анонимности. Технология работает за счёт объединения предоставленной пользователями (членами сети) полосы пропускания и дискового пространства своих компьютеров в общий фонд для публикации или получения информации. Это называется пулингом. Freenet использует разновидность маршрутизации по ключам, похожую на распределённую хеш-таблицу, для определения местонахождения пользовательских данных[248]. Упрощенно, Freenet – это распределенное хранилище информации, ориентированное на анонимность и обход цензуры. Каждый компьютер, подключенный к сети («узел») хранит у себя на диске какую-то часть информации, которую запросил пользователь. Недостающая часть этой информации запрашивается с другого узла. Такая организация доставки контента не позволяет использовать веб-страницы с динамическим содержимым и это накладывает[249] определенный отпечаток на контент, который располагается в сети.

Пользователь волен сам выбирать уровень защиты/быстродействия, который предоставляет ему сеть. Так, существуют возможность подключаться к любым узлам сети («уровень опеннета») или ограничить собственные подключения только доверенными узлами («уровень даркнета»). Также существует несколько уровней защиты самого хранилища на узле: постоянным ключом или же временным, который хранится лишь в оперативной памяти. На уровне опеннета наблюдается достаточно высокая

[248] https://ru.wikipedia.org/wiki/Freenet
[249] https://urbanculture.in/Freenet

скорость работы – страницы-каталоги открываются не более, чем за минуту.

Доступ к сайтам также производится с помощью страниц-каталогов, поддерживающихся добровольцами. К сожалению, не все каталоги обновляются своевременно. Также существует экспериментальный поиск по ключевым словам, но на момент написания руководства он находится в нерабочем состоянии, поскольку не находит даже распространенные слова и словосочетания.

Попадание во Freenet производится с помощью несложно инсталлируемого клиента, встраивающего необходимые компоненты в браузер. Работа с клиентом производится через веб-интерфейс, аналогично I2P.

Преимущества:

- Не имея ключа, невозможно получить доступ к данным.
- За счёт полной анонимности и децентрализованности невозможно установить местонахождение пользователя или уничтожить находящуюся в сети информацию.
- При работе в режиме F2F соединение будет устанавливаться только с узлами из списка доверенных.
- Даже если часть сегментов данных потеряны, их всё равно можно восстановить.
- Доступ к данным возможен даже в том случае, если отправитель в данный момент отключен от сети.
- Дружелюбность среды — пользователю предлагается список возможных действий с подробными инструкциями, понятными даже тем, кто прежде использовал компьютер только в качестве печатной машинки.

Недостатки:

- Отсутствие поисковых систем — имеются только довольно многочисленные и не претендующие на полноту страницы-индексы, на которых собраны ссылки на понравившиеся их создателям ресурсы.
- Достаточно низкая скорость передачи данных — одна страница с большой фотогалереей может грузиться полчаса. По этой причине
  - наиболее распространённой формой информации является текстовая — выбор фильмов, ПО и музыки крайне невелик;
  - большинство сайтов выглядят откровенно аскетично;
  - отсутствуют сервисы, работающие в режиме реального времени.
- В отличие от Tor и I2P, Freenet не имеет шлюза для выхода в обычный Интернет.
- Контент, не пользующийся спросом, очень быстро удаляется[250].

[250] https://urbanculture.in/Freenet

3.10 Пиринговые сети

Они же P2P. В обзоре оверлеев мы упоминали, что существуют сетевые технологии, дающие транспорт для передачи данных (собственно оверлейные) и которые сами осуществляют эту передачу. О вторых и пойдёт речь. Изначально под пиринговыми сетями понимаются файлообменные, и лишь впоследствии концепция одноранговости, то есть равноправия узлов развилась в меш-сетях (далее) и уже упомянутых оверлейных. Таким образом, концепт P2P на сегодня не ограничивается пирингами. Он разрастается до идеи «альтернативного интернета» и включает создание собственных сервисов общения и распространения контента — аналогов популярных глобальных ресурсов. Так, Mastodon является аналогом Twitter. Контент может включать в себя редкую музыку, видеозаписи, архивы журналов и книг, авторские тексты, подборки изображений. Зачастую файлообменные сети основываются на обмене материалами: чтобы что-то получить, нужно что-нибудь отдать. Это известно пользователям закрытых торрент-трекеров, которые зарабатывают очки, становясь сидами, то есть раздающими, а затем меняют их на скачивание объёмов в роли пиров. Дальше перечислим значимые файлообменные сети.

- DC++ (DirectConnect) – локальная файлообменная сеть, построенная на хабах — серверах, где вы можете искать среди расшаренных папок других юзеров, предварительно также поделившись заданным объёмом своего диска. В чатах этих узлов можно ознакомиться с местными правилами, а кроме того там кипит своя жизнь.

- eDonkey и eMule, также «осёл» - хорошее подспорье для выкачивания редкого контента, в том числе зарубежного, но следует проверять details файла после добавления в список закачки, чтобы не нахвататься вирусов. Не скачивайте архивы и исполняемые файлы малого размера. Помимо внутреннего поиска, ed2k-ссылку на нужный файл можно обнаружить в поверхностной сети, в том числе на тематических ресурсах.

- Perfect Dark — японская сеть с соответствующим уклоном содержимого.

3.10.1 Soulseek

Рассмотрим скачивание и расшаривание на примере Soulseek – сети, профилирующейся в основном на распространении музыки. Некоторые авторы выкладывают релизы сразу сюда, а коллекционеры меняются редкими качественными записями, блокируя их для тех, кто не раздаёт им ничего полезного.

При первой установке клиент предложит вам регистрацию. Интерфейс самой программы состоит из двух слоёв вкладок и верхних кнопок для работы с ними.

Большинство действий с объектами внутри вкладки происходит через меню, вызываемое правой кнопкой мыши. Поиск через вкладку Search позволяет искать по части названия, включая расширение. Если ничего не найдено, что может быть связано с отсутствием владельца искомого в сети, отложите запрос на будущее кнопкой

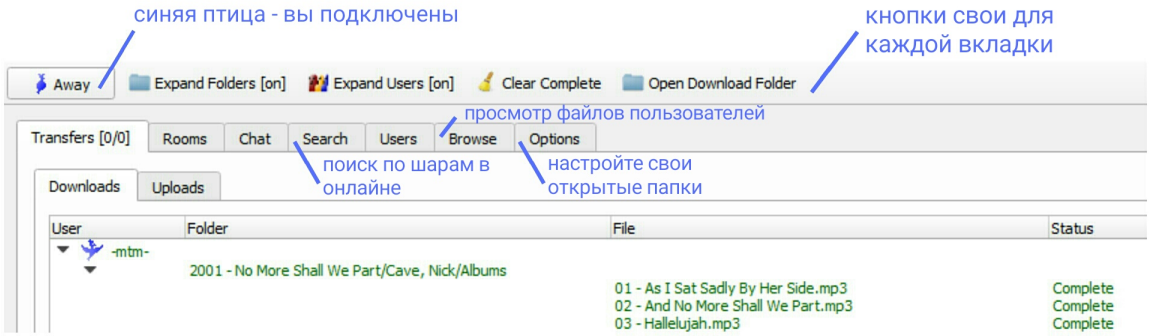


Fig. 7. Фрагмент интерфейса Soulseek

Add to Wishlist. Можно также сортировать выдачу. Заметив интригующий путь до файла, попробуйте зайти в архив пользователя и осмотреть его на предмет чего-то подходящего для вас, о чём вы пока не знаете. В меню по правой кнопке выберите Browse folder либо User's file list. Если нужно сохранить интересного человека, выберите там Add user to list и запишите причину добавления в Add user note. Другой способ: войдите во вкладку User. Кнопка Add User позволит вписать его имя в список.

Чтобы расшарить собственные ресурсы и получить возможность скачивать без ограничений, зайдите в Options, вкладка File Sharing. Нажмите кнопку Share Folder и выберите нужную директорию. Здесь также можно настроить, куда будут сохраняться загруженные материалы.

3.10.2 ZeroNet

Несложная в установке клиента децентрализованная сеть[251], основанная в том числе на блокчейн-технологиях и BitTorrent, что и делает её самым современным воплощением P2P-технологий. Доступ к сайтам происходит по hash-адресу или .bit-доменному адресу. После его получения происходит подключение к трекеру, откуда сайт скачается на ваш диск при наличии в сети пиров. Сеть нецензурируема по своему дизайну, а потому вы можете столкнуться с нежелательным контентом (см. главу 6.5). Некоторые ресурсы сети:

- Торрент Play:
  http://127.0.0.1:43110/1PLAYgDQboKojowD3kwdb3CtWmWaokXvfp
- ZeroTalk — крупный форум: http://127.0.0.1:43110/Talk.ZeroNetwork.bit
- Отечественный рускоговорящий аналог большого форума:
  http://127.0.0.1:43110/1Apr5ba6u9Nz6eFASmFrefGvyBKkM76QgE

[251] https://zeronet.io/

- Имиджборда: http://127.0.0.1:43110/0chan.bit
- Поисковик, который ищет только по названиям сайтов: http://127.0.0.1:43110/kaffiene.bit
- Файлообменник: http://127.0.0.1:43110/1GrtBsG57kjU2Z3iAQebG9D5c8CRDRLoPj

3.11 Меш-сети

Сюда относятся проекты полностью децентрализованных одноранговых сетей (см. также главу 6.3). В основном они строятся на wi-fi-роутерах, общающихся друг с другом по тому или иному разработанному протоколу и работающих как ретрансляторы. Сетки быстро разворачиваются, принципиально децентрализованы и приватны, но не всегда анонимны. Mesh в названии означает, что соединение происходит по принципу «каждый с каждым». Неуправляемость сети и другие преимущества концепта, включая дешевизну, привели к появлению множества локальных и глобальных разработок. Одной из первых стала Guifi[252], объединившая в 2004 году ряд каталонских деревень, лишённых интернета, и развившаяся с годами по всей Испании. Задействованной в ней прошивкой для роутеров LibreMesh[253] пользуются итальянская сеть Ninux, немецкая Freifunk[254], австрийская FunkFeuer, аргентинская AlterMundi. Проекты African WUG и One Laptop Per Child также стремились подарить возможность коммуникации жителям удалённых регионов. Так как всё это основано на Wi-Fi-сигналах, то подключение зависит от наличия роутера-участника сети поблизости, из-за чего и получается ограниченность локальных мешей по странам. Границы можно переходить воздушными шарами, как сделал Google Loon[255]. Помимо собственно прошивки, для организации мешей разрабатывалось несколько протоколов, замерших на разных этапах воплощения. Наиболее известен — cjdns, основа для Hyperboria, по которой даже есть онлайн-карта, имеются свои аналоги соцсетей и региональные узлы некоторых стран. На сегодня самым развитым решением считается Yggdrasil. Он опирается на древовидную связь между узлами, что, строго говоря, уходит от концепта Mesh. Однако это решает ряд проблем реализации, так что можно предсказать этому мифическому древу большое будущее. Иггдрасиль — полностью зашифрованная сеть на основе IPv6. Внутри поднят форум, вики и множество IRC, торрент-трекер и несколько игровых серверов. На момент написания жива и активна нетсталкерская нода: https://netwhood.online/yggdrasil_public/

[252] http://guifi.net/
[253] https://libremesh.org
[254] https://freifunk.net
[255] http://www.patentlymobile.com/2013/11/googles-high-altitude-balloon-network-called-project-loon-is-revealed-in-new-patent.html

3.12 Другие сети

В этой главе будут рассмотрены редко используемые, устаревшие и правительственные сети узкого назначения.

3.12.1 Gopher

Gopher — устаревший протокол передачи и хранения файлов, источник редкого контента, который был популярен до 1995 года. Gopher был разработан Миннесотским университетом в 1991 году как менее сложная и более быстрая альтернатива FTP с подобной иерархической структурой, о чём сказано в FAQ Floodgap[256], крупнейшего узла сети. 30.07.1993 была опубликована нереализованная спецификация[257] Gopher+, в которой обсуждалась поддержка метаданных и свойств файлов. В 1995 году на базе Gopher+ была выпущена программа GopherVR[258] для 3D визуализации сети, с навигацией от первого лица. Впоследствии она обновлялась, последняя версия датируется 2015 годом и поддерживается на ОС-ах Mac и Linux.

В наши дни новые сервера появляются редко. Судя по статистике[259], по состоянию на 02.06.2017 активны 138 серверов, 89 из которых появились позднее 1999 года. По сравнению с 2012 годом, когда работали 160 узлов, их число ощутимо снизилось, поэтому следует архивировать их. Гоферу соответствует открытый 70 TCP порт, поэтому для поиска неиндексируемых серверов вы можете воспользоваться IP-сканерами: masscan или nmap. Для краулинга существует инструмент, умеющий отображать результаты на карте. Последнюю созданную нами карту можно видеть здесь[260]. Рекомендуется запускать его из коммандной строки с параметром «grawler-master.exe -crawlers 50», чтобы увеличить количество потоков (по умолчанию их 8).

В современных браузерах ссылки с префиксом gopher:// открываются с помощью специального гейта[261] или его аналога[262]. Переход по внутренним ссылкам обрабатывается автоматически. Если вы пользуетесь Mozilla Firefox или SeaMonkey, то можете установить плагин[263] для посещения сайтов Гофера напрямую. В бета-версии находится приложение[264] для телефонов на базе Android. Любителям CLI понравится текстовый браузер Lynx[265] со встроенной поддержкой протокола.

---

[256] gopher://gopher.floodgap.com:70/0/gopher/welcome
[257] gopher://gopher.floodgap.com/0/gopher/tech/gopherplus.txt
[258] gopher://gopher.floodgap.com/1/gophervr
[259] gopher://gopher.floodgap.com/0/v2/vstat
[260] https://ibb.co/m877td
[261] https://gopher.floodgap.com/gopher/gw
[262] https://gopherproxy.meulie.net/
[263] http://gopher.floodgap.com/overbite/files/overbiteff.xpi
[264] http://gopher.floodgap.com/overbite/d?android
[265] http://lynx.browser.org/

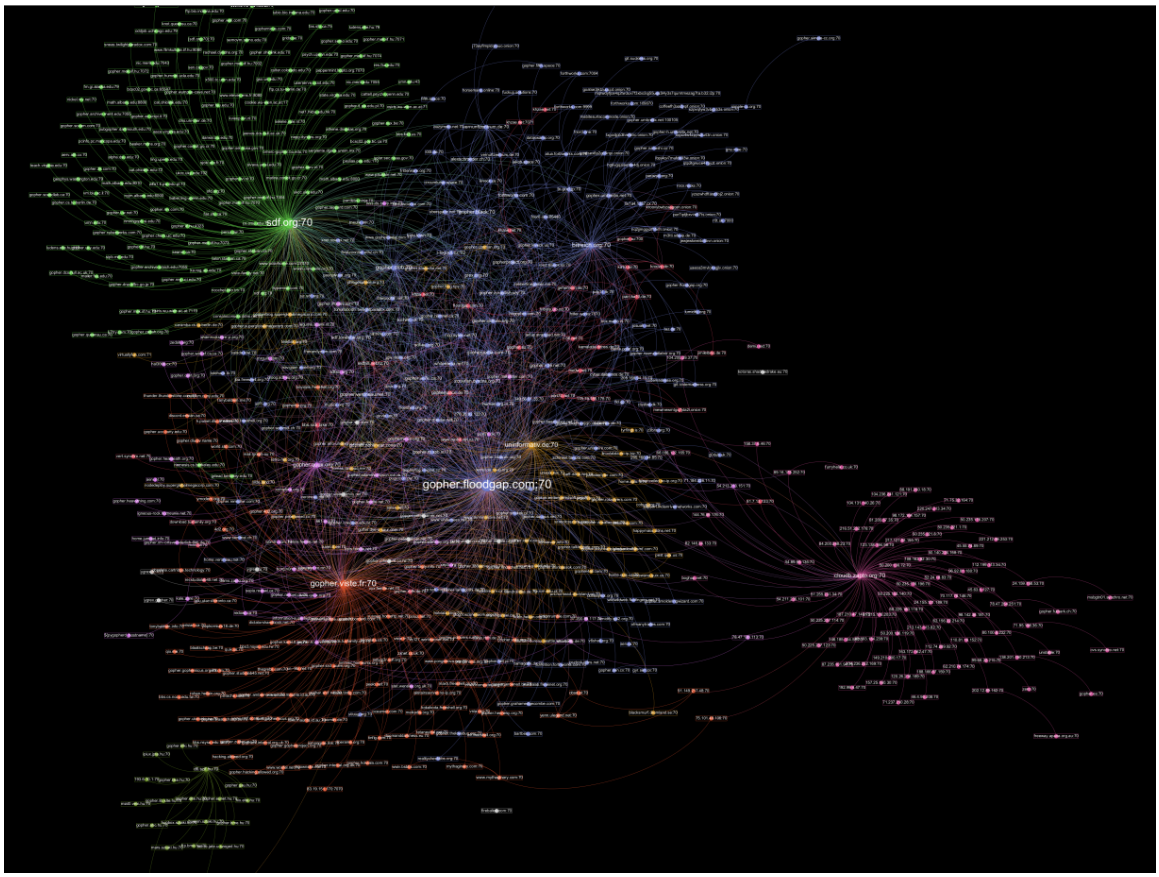


Fig. 8. Другой вариант карты, отображённый Gephi. Видно, как сайты группируются вокруг наиболее крупных серверов

Отправная точка новичка — сервер Floodgap[266], где находятся обновляемый список[267] всех проиндексированных серверов и поисковик[268] Veronica-2 с гайдом[269] по работе с ним. Вы также можете посмотреть архивные скриншоты серверов и некоторые файлы в каталоге, если вам не хочется проверять их вручную. Кроме прочего, в Гофере даже есть рабочая имиджборда[270] и свои пофайловые блоги[271] — phlogs, где можно узнать новости сети или отдельных узлов.

Владельцы серверов – сетевые энтузиасты, поэтому неудивительно, что небольшая часть их уже перешла на IPv6.

[266] gopher://gopher.floodgap.com/1
[267] gopher://gopher.floodgap.com:70/1/world
[268] gopher://gopher.floodgap.com/0/v2
[269] gopher://gopher.floodgap.com/1/v2/help
[270] gopher://port70.net/1chan
[271] gopher://sdf.org/1/phlogs

3.12.2 Fidonet

Fidonet — сеть, созданная для передачи сообщений, в которой соединение проводится через телефонную линию. Помимо «официального» фидо существуют ответвления на основе того же софта и протоколов — так называемые левонеты или FTN (Fido Technology Network). Из-за технических отличий терминология[272], да и стиль общения в сети сильно отличаются от глобального веба. Основной единицей является «нода», т.е. узел — компьютер с необходимым ПО, допущенный до участия. Её оператор выдаёт возможность переписываться обычным участникам - «поинтам», то есть точкам доступа, и несёт ответственность за их действия в сети. Узлы, чьи рядовые юзеры мешают общаться другим, могут даже быть отключены. Высшей модерацией занимаются крупнейшие ноды, или хабы, опирающиеся на общий устав сети (полиси)[273]. Политика эта запрещает коммерческую деятельность и агрессивные действия. Ресурс[274] одного из активных сисопов, через которого можно попасть в Fidonet, рекомендует:

Ни при каких обстоятельствах не раздражайся сам и не раздражай других. . . Если тебя кто обидел, забей, если позволит ситуация - интеллигентно пошли в любое удобное место или зови меня.

Вся переписка сводится к получению и пересылке сообщений, напоминающих почтовые. Письмами же рассылаются управляющие команды. Для коллективного обмена мнениями существуют тематические эхоконференции или эхи. Например, эха RU.FIDONET.TODAY - Обсуждение сети Фидо и её жизни в натоящее время.

При разработке сети анонимность не закладывалась, что некоторые считают плюсом, так как общаются с очевидно реальными людьми. При работе в Фидо каждый поинт знает, через какие компьютеры проходят его письма. Хотя это делает переписку полностью открытой, но также даёт полное представление о том, где оседает контент. Также здесь достаточно одного клиента для сбора желаемой информации со всех площадок, что напоминает умирающие RSS-подписки в их лучшие дни. Эта идея вдохновила на создание протокола ii / IDEC[275] с подобным Фидо принципом, и даже интерфейс клиента напоминает GoldEd.

Большинство пользователей здесь — люди среднего возраста. Сеть обладает своей характерной культурой и считается памятником раннего сетевого периода СНГ.

[272] http://lurkmore.to/Фидо/Термины
[273] https://telegra.ph/Fidonet-segodnya-09-14
[274] https://723.neocities.org/
[275] http://netwhood.online/2018/09/01/ii-idec-by-abtelegramuser/

3.12.3 USENET

История этой сети начинается в 1979, когда двое студентов придумали несложную программу для обмена сообщениями через телефонные линии. Пока Интернет оставался дорогим и подчинённым ARPA, эта альтернатива развилась до более чем 120 000 новостных групп[276]. Принципы работы USENET напоминает Фидо: сообщения рассылаются по узлам и запрашиваются с них, для чего имеется протокол Интернета NNTP. С ним связано две URI-схемы: «nntp://» указывает на статью в новостной группе на определённом сервере, а «news:» адресует её по глобальному уникальному номеру. Таким образом, это не полноценная отдельная сеть.

Названия групп характеризуют иерархию, в которой они находятся: например, sci.math и sci.physics находятся внутри иерархии sci. Помимо «большой восьмёрки» наиболее развитых иерархий, существуют конференции alt.*, появившиеся как ответ на отказы в создании рассылок на некоторые темы в основном костяке [277]. В alt не были введены те жёсткие правила, по которым живут остальные. В частности, именно здесь распространяется программное обеспечение и незаконный контент, хотя администрация начала банить ДП. На сегодня доступ к USENET предоставляют специальные провайдеры, лишь некоторые из которых позволяют скачивать файлы - некоторые пользуются этим вместо торрентов. В поверхностной сети распространяются и дублируются большие объёмы архивов, хранящих подчас очень содержательные дискуссии олдфагов зарубежья, для многих из которых именно здесь началось онлайн-общение. Есть и проект поисковой машины[278].

3.12.4 AnoNET

AnoNET — продолжатель ныне мёртвой сети MetaNet. Технически является частью оверлейной сети обмена трафиком UCIS IX. Используются внутренние DNS и BGP-пиринги,внутри сети есть свои AS, но нумерация используется не из частного диапазона. В настоящее время малонаселена, основным владельцем является Ivo Smits.

Заход в сеть производится посредством подключения через OpenVPN к серверу anocp.ucis.nl (178.33.23.196). Сеть состоит из трёх адресных пространств:

- 21.0.0.0/8 — сама сеть AnoNET из диапазона маршрутизируемых адресов Интернет. Забронирована за DoD, но, так как считается, что сейчас Мин. обороны США не использует эту сеть, поэтому AnoNET взяли ее себе с целью не допустить перекрытия с частными диапазонами внутренних ЛВС пользователей.

[276] https://www.thundernews.com/blog/what-is-the-difference-between-usenet-the-internet-and-the-world-wide-web/
[277] https://www.giganews.com/usenet-history/alt.html
[278] https://nzedb.github.io/

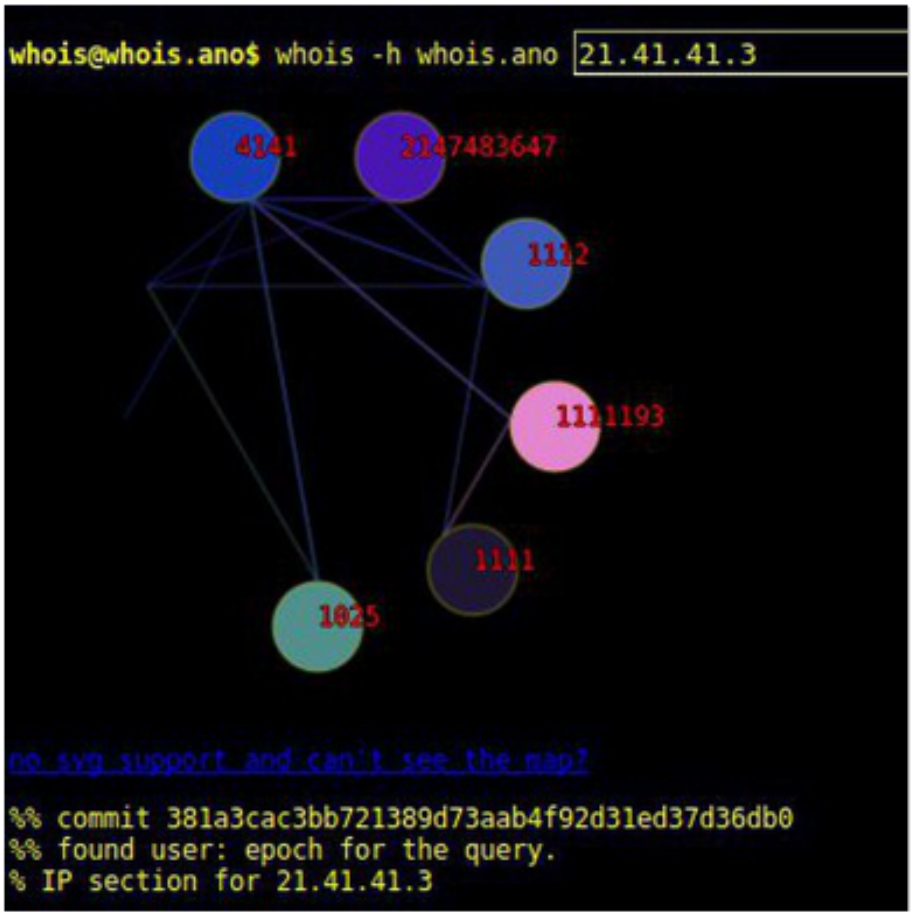


Fig. 9. структура Анонета

- 172.22.0.0/15 — из частного диапазона 172.16.0.0/12, и это пиринг с другой оверлейной сетью https://www.dn42.net/Home
- 198.18.0.0/15 — зарезервирована как частный диапазон для тестирований, владелец не выяснен.

Старт в прогулке можно взять от http://anonet.org/ в разделе Activities. На момент написания живо несколько сайтов и сервисов:

- http://www.ucis.ano/ — .ano сайт проекта UCIS, по сути, это центральная точка AnoNET. Тут есть небольшой каталог ссылок и сервисов, все контакты ведут на Ivo.
- http://ix.ucis.ano/ — UCIS Internetwork Exchange. Выше было указано, что есть пиринг с сетью dn42 и был пиринг с сетью VAnet. Вот тут указано, какие сети подключены к IX (всего две, да). Есть местный Looking Glass, отсюда можно

брать более точные сети AnoNET и dn42, однако интенсивный скан настоятельно не рекомендуется.

- http://wiki.ucis.ano/Anonet — местная вики, также есть маленький каталог ресурсов.
- http://www.ucis.ano/dump/ — файлопомойка Ivo.
- http://cablegate.ucis.ano/ — зеркало WikiLeaks.

Есть местный IRC[279], который одной ногой стоит в Интернет — IRC.Kwaaknet.Org. Основной канал, где есть отвечающие — #anonet. Также прямо в irc средствами DCC проводится файлообмен, например, канал #software.

AnoNET еще стоит исследовать в плане обнаружения внутренних сервисов, причем делать это нужно как внутри сети, так и снаружи. Жизни в проекте мало, объемных каталогов нет. Возможно, стоит регулярно искать новые упоминания в Интернете или проводить глобальное сканирование с очень низкой скоростью.

3.12.5 Closed Shell System

Closed Shell System — мифические сети, по описаниям напоминающие интрасеть, о которой мы говорили ранее. Название, вероятно, происходит от сети Клоза (Clos Network) - разновидности коммутационных сетей (circuit networks). Им приписывают содержимое вроде архивов секретов Теслы или пришельцев. С ними же связана легенда о «марианской сети»[280] , то есть глубочайшем слое коммуникаций, недоступном простым смертным. Именно она, видимо, легла в основу нетсталкерской «схемы уровней».

В основном они пришли из испанского и португальского сегмента, как видно в этой подборке паст. Представление о «содержимом» таких тайных сетей можно получить тут. С тех пор англоязычная сеть любит истории про странные домены верхнего уровня (.clos и т.п), где хранятся ценнейшие материалы.

Друг за другом появились такие имена доменов и названия сетей:

- Closys, Closed Shell Systems или ClosNet (.clos),
- Lokynet (.loky),
- ChaosVPN (.hack),
- DarkFantasy network (.dafy) и прочие.

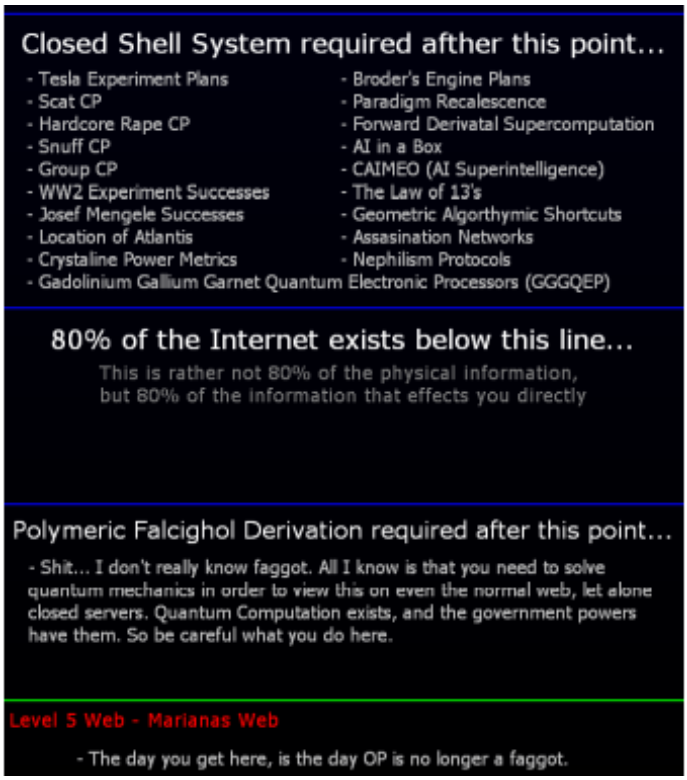


Fig. 10. Одна из вариаций схем

Вместе с желающими попасть внутрь возникли и те, кто сумел нагреть на этом руки. Масса видео на ютубе, повторяющих легенду или пасты, обещающие доступ через IPv7 (несуществующий), выглядят невинно. Но часты случаи продаж способов проникновения, о чём предупреждает Хостинг Даниэля. Есть даже русскоязычный мануал по нагреву западных «мамонтов» жаждущих познакомиться с .clos. В связке с «марианскими сетями» упоминается установка сети Polaris[281]. На самом деле это небольшая исследовательская сеть NASA, развёрнутая в одном из научных центров и обрабатывающая данные об озоновом слое. Инструкции по ссылке нужны были для их внутреннего использования.

Оказалось[282] [283], что часть легенд запущена латиноамериканскими хакерскими командами. Впоследствии они не раз пытались опровергнуть их, но тщетно. В частности, .clos являлось доменом внутренней сети администраторши одного из таких «караванов» взломщиков. Интересно, что она запускалась по предварительной договорённости в заданное время.

[279] irc://irc.ucis.ano
[280] https://pastebin.com/hGUiqa3X
[281] https://cloud1.arc.nasa.gov/polaris/comm/linux.html
[282] https://pastebin.com/hGUiqa3X
[283] http://kruegernyuewww3c.onion/

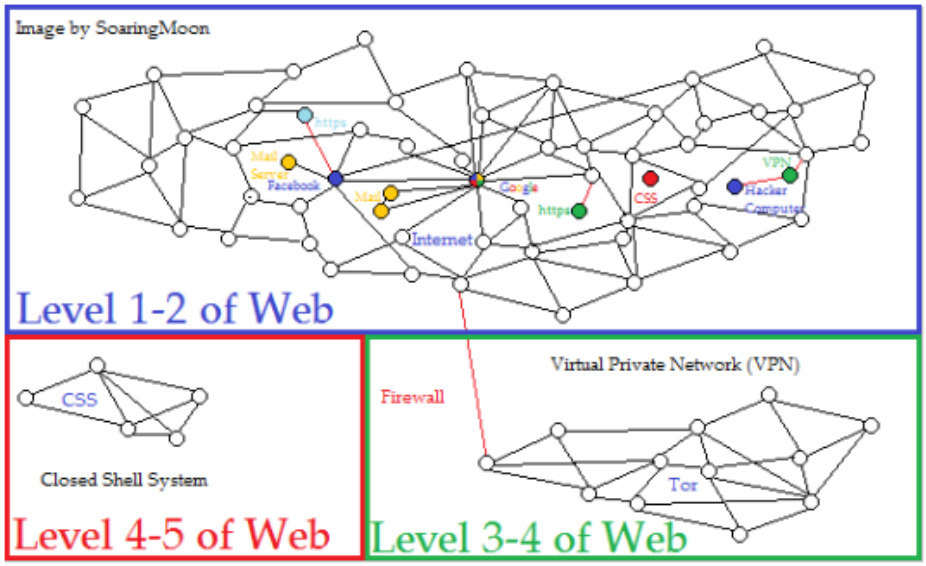


Fig. 11. Более близкий к реальности вариант схемы

ChaosVPN также оказался небольшой любительской надсетью, куда проник через другие протоколы пользователь abslimit. Эта надсеть ранее была доступна по инвайтам, нынешнее положение дел и порядок подключения можно узнать на официальной вики[284].

Технически псевдо-доменные имена возможно создать на собственном VPS, в закрытой оверлейной сети. Сделать это может любой желающий, а не только владелец тайных технологий.

Конечно, это не значит, что интрасети организаций не существуют или не содержат ценных данных, способных перевернуть мнение о мире. Содержимое подобной сетевой структуры рассекречивал Эдвард Сноуден, загрузив его на USB-носитель физически, а не путём хитрого доступа из интернета. Однако следует отличать их от просто альтернативных конфигураций, настроенных любителями для себя.

3.13 Карты

В 2007 г. корпорация Google в рамках открытия сервиса Google Steet View[285] отправила в путешествие по миру сотрудников на машинах. С их крыш, на высоте 2,5 метров, камера снимает панораму в 360° по горизонтали и 290° по вертикали. Впоследствии средства перемещения расширились до трициклов, снегоходов, лодок

[284] https://wiki.hamburg.ccc.de/ChaosVPN
[285] google.com/streetview

и подводных агрегатов. Сейчас хранилище охватывает 2 петабайта данных, 39 стран, 3000 городов и 8000000 км дорог. Алгоритмы обрабатывают изображения наложением водяных знаков и размытием лиц, номеров авто и телефонов, некоторых вывесок или указателей. Любой может подать жалобу[286] для блюра имущества, объектов личной жизни и «неподобающего контента». К нему относят сцены насилия, чудаковатое поведение людей, графические баги и находки типа статуи[287] во Франции, которые коллекционируют в сообществе /r/creepy[288] и упоминают в новостях[289]. Позируя ради славы, фрики разыгрывают[290] убийства.

Разросшиеся вслед за Гуглом инструменты[291] вдохновили богему и нетсталкеров. Первым идею подхватил канадский художник Джон Рафман[292], воплотивший её в проекте «9 eyes» — блоге об уличной фотографии *решающего момента* (по Картье-Брессону) в Сети. Он также изучал заброшенные онлайн-игры и 3D чат-клиенты навроде worlds.com, популярные на /x/ и /sn/, и удостоился эссе[293] с интервью[294]. Иной искусствовед, Мишка Хеннер[295], печатал девушек из эскорт-услуг, военные базы, поля под фермы и фабрики в глянцевых журналах. Интерес к виртуальным странствиям возрос, когда открылись **рандомайзеры**: mapcrunch.com предложил персональные галереи и регулярный топ, а Random Ize[296], randomstreetview.com и python-скрипты[297] — эргономичность. Вскоре анонимы и geoguessr.com придумали игры на отгадывание названий случайных государств и местоположения ближайшего аэропорта.

Однако применение карт не ограничено нетрандомом. Можно целенаправленно изучать предположительно загадочные места, комбинируя сервисы, так как каждый спутник снимает по-своему. Помимо Гугла, картографией с помощью спутниковых снимков занимаются и другие компании: Bing[298], Яндекс. Для поиска необычных мест на картах и прояснения свойств уже найденных стоит обратиться к инструментам вики-картографирования, наполняемым заинтересованным сообществом: http://wikimapia.org/ , https://www.openstreetmap.org/ , просмотрщикам топографических карт: https://www.marshruty.ru/Maps/Maps.aspx , ретрокартам http://www.etomesto.ru/ и http://www.retromap.ru/, а для адресов пользоваться кадаст-

[286] express.co.uk/life-style/property/761003/google-maps-remove-house
[287] https://imgur.com/a/BBf7Q
[288] https://www.reddit.com/r/creepy/search?q=google+maps&restrict_sr=on&sort=relevance&t=all
[289] http://www.viralnova.com/creepiest-things-on-google-maps/
[290] http://www.bbc.com/news/uk-scotland-edinburgh-east-fife-27670099
[291] https://en.wikipedia.org/wiki/List_of_street_view_services
[292] http://telegra.ph/Dzhon-Rafman-08-27
[293] http://artfcity.com/2009/08/12/img-mgmt-the-nine-eyes-of-google-street-view/
[294] http://web.archive.org/web/20180321032512/https://interviewrussia.ru/art/hudozhnik-dzhon-rafman-dlya-hudozhnikov-internet-segodnya-eto-parizh-nachala-xx-veka
[295] https://en.wikipedia.org/wiki/Mishka_Henner
[296] https://random-ize.com/random-map/
[297] https://github.com/hugovk/random-street-view
[298] https://www.bing.com/maps

рами, для России это http://pkk5.rosreestr.ru/ . Фотографии из определенных географических мест также можно искать с помощью Panoramio. Этот сервис использует EXIF-данные для публикации фотографий на карте. Более продвинута kamerka, требующая, впрочем, платного аккаунта Shodan: она собирает материалы из соцсетей, соответствующие заданной координатами локации. Некоторые сервисы строго тематичны: отмечают только радары ГИБДД или IoT-устройства.

В анализе карт ключевую роль играет опыт. Нет мистики в разноцветных овалах, это могут быть поля нетипичной формы или другие зоны деятельности людей. Следы ветра и различные отложения могут давать необычную картину. Разница в разрешении снимков и швы их склейки, а также, по-видимому, вырубка леса под линии связи создали иллюзию геоглифа в этом исследовании[299]. Изучите предмет прежде, чем делать выводы.

3.13.1 Игровые пространства

Нетсталкеры занимаются изучением заброшенных онлайн-игр, конференций и 3D чат-клиентов. В немодерируемой сетевой среде часто собираются маргинальные личности. Возможность мощного визуального творчества параллельно с системой общения позволяет им не только самовыражаться, но и устраивать собрания чего-то похожего на культы, и оставлять загадки.

Fig. 12. Встреча участников «Миров»

[299]https://cont.ws/@valentindeg/694839

Наиболее известны в этом смысле Worlds.com, Second Life и Minecraft. Поиск для «Миров» сводится к изучению внутриигрового пространства. Также, поскольку каждый «мир» является опубликованным в произвольном месте сети текстовым файлом специального формата, возможно искать их дорками. Сервера Майнкрафта можно сканировать по порту 25565 или ориентируясь на баннеры его протокола на других портах.

Я как-то решил просканить один диапазон по порту 25565 и набрёл на покинутый сервер, где было просто огромное количество всяких построек. Это были целые города, соединённые между собой магистралями из рельс, протянутыми на много тысяч блоков. Видно было, что это было создано игроками, в сундуках лежали чьи-то вещи, на домах были таблички с никами владельцев. Я бродил в полном одиночестве по этому гигантскому заброшенному миру. Кто тут играл? Как давно? Почему сюда больше не заходят? Эти вопросы так и остались прекрасной загадкой. На следующий день сервер был отключён.
— Zerogoki

Пример отдельного «Мира» можно получить на angeleyesesprit.sytes.net, есть и коллекции скриншотов.

3.13.2 Изображения

Поиск графических объектов возможен в двух видах: под некий запрос и по самому изображению. Первый вариант касается случаев, когда вам нужно подобрать визуализацию какой-то идеи. Для этого вы можете обратиться к традиционным поисковикам, но больше выхлопа получится из специальных ресурсов для художников и фотографов. Можно начать со сверхпопулярных Instagram, Tumblr с его неразвитым теговым поиском и агрегатора Pinterest. Но огромные залежи любительского и профессонального искусства хранятся на Deviantart, Pixiv, ArtStation, VIRINK и меньших площадках для арта, где и встроенный поисковик часто содержит больше настроек. Ресурсы по продаже стоковой графики, такие как Shutterstock, https://ru.depositphotos.com/, https://www.bigstockphoto.com/ru, снабжают контент водяными знаками, но в некоторых случаях можно получить исходный платный файл (не используйте его в коммерческих целях): взять ссылку на проштампованную версию и перебором создать прямую ссылку на чистую версию. Отличный источник старинных изображений — различные библиотеки с отсканированными книгами, каталоги эфемер на продажу и онлайн-площадки торговли подержанными вещами, от ebay.com до коллекционерских платформ из разных стран вроде StampWorld, Delcampe, и Numista. Изображения интернациональны, а потому текстовые запросы составляйте на разных языках, если не нашли на русском и английском.

Если же конкретизировать запрос невозможно, сёрфинг-фланирование по вышеперечисленным ресурсам дополнят рандомайзеры по imgur.com, например, этот (см.

также 3.3). Будьте осторожны с этим способом — он не фильтрует NSFW-контент. Вы можете создать собственный рандомайзер по любому источнику графики, в том числе выбирать её с файлообменников и открытых серверов.

Много фотографий техники, семейной жизни, различных мест, сканов документов можно найти на FTP и SMB-серверах, а чужие просмотры отловить с помощью спутниковой рыбалки.

Поиск по изображению пригождается, когда необходимо получить первоисточник картинки, более крупную версию, варианты ракурсов фото и т. п. Он часто становится частью делисёрча или расследования. Воспользуйтесь реверсивными поисковиками общего характера[300] и специализированными сайтами вроде Karmdecay[301] для Реддита. Специализированный поисковик tineye, бывший первопроходцем[302], уступил инструменту Google. Тот, в свою очередь, слабее Яндекс.Картинок с их технологией CBIR в распознавании лиц[303].
Опенсорсный w/a/ifu2x34[304] увеличивает фотографии и устраняет артефакты. С аудиозаписями поможет распознавание музыки: AudioTag (браузерная утилита, проверяющая по отпечаткам более миллиона треков), MooMa.sh (извлекает мелодии из роликов YouTube, Vimeo и Dailymotion и анализирует их) и Shazam[305] (приложение на IOS и Android, записывающее звук с микрофона), или реквесты в сообществах социальных сетей: vk.com/melodyhelp и watzatsong.com. Для видеозаписей эти стратегии реализованы либо закрытыми системами в духе Content ID[306], защищающей авторские права, либо комплексными методами дорогущего Spotter[307](месячная подписка на 10 запросов стоит 25000 руб, добывает итог по образцу, названию и ключевым словам) и покадрового поиска, когда вы берёте 6-7 скринов ключевых моментов видеоряда и реверсите их.

Литература

[1] Проект «CASCA», Расширенное руководство по онлайн-камерам v0.3.1, 2018 г.
[2] Проект «L0cation Unindentified», https://github.com/lm0vel/L0cation_Undefined-maps/wiki

[300] https://en.wikipedia.org/wiki/List_of_CBIR_engines
[301] http://karmadecay.com/t
[302] https://www.tineye.com/
[303] https://staurus.net/google-vs-yandex-poisk-po-kartinkam
[304] http://waifu2x.udp.jp/
[305] https://www.shazam.com/ru
[306] https://support.google.com/youtube/answer/2797370?hl=ru
[307] http://spotter.tech

4. АНАЛИЗ НАХОДОК

Нередко нетсталкеры сталкиваются с непонятными сетевыми объектами. Их странность может заключаться как в смысловом наполнении, так и в технических особенностях. Из-за малого опыта они часто не понимают, что именно содержит их находка, ценна ли она, и насколько серьёзно её следует воспринимать. Вопреки заблуждению, необычные явления встречаются в поверхностной сети точно так же, как и в дипвебе, что подтверждает Эльзагейт и некоторые примеры далее. Анализ нужен даже в повседневной сетевой деятельности из-за обилия в вебе маркетинга, кликбейтов, мошенничества и фейковых новостей. Для защиты от последних гуглите прямые цитаты обсуждаемых лиц и учитесь отсеивать неавторитетные источники, как гласит[308] этика Википедии. Помните, что восприятие ложных сведений напрямую влияет на ваши жизненные выборы.

Смысловой анализ

Большинство начинающих нетсталкеров желают находить странные сайты или какой-то другой загадочный контент. Есть две вещи, которые надо сразу уяснить.

1. Все сетевые объекты размещаются в интернете людьми. Контент могла сгенерировать машина, но опять же по заданию человека, на хостинге, развёрнутом человеком. Если кто-то разместил контент - значит, его на это что-то сподвигло. Ваша нетсталкерская задача - постараться понять, что именно. Автор хотел восхитить посетителей, донести до них сообщение, поиграть с ними, обмануть их?

2. Загадочность и труднодоступность находки, убедительность тона автора и внешний антураж не делают информацию или контент более ценными. Субъективное остаётся субъективным, бредовое - бредовым, ложное — ложным. Помните, что в интернете может постить каждый, равно как и создать себе сайт. Руководствуйтесь рекомендациями по реверсингу смысла.

Цель — определить смысл находки, мотив автора и, как следствие, ценность объекта. Последняя может быть субъективной (вам очень понравилось или дало пищу для ума) и общественной (в сети не упоминалось, другие нетсталкеры не находили).

Как ни банально, но начните с того, чтобы вчитаться в текст и последовательно пройти по всем ссылкам, которые видите. Не игнорируйте внешние ссылки и счётчики просмотров, поскольку они могут сдеанонить ник владельца. Чтобы не держать в краткосрочной памяти, делайте короткие заметки, как в этом посте, или выписывайте на майндкарту, отображая свой путь вглубь. Пока графическое отображение истории браузера остаётся мечтой, попробуйте этот аддон для Chrome. Он отражает связи

[308] https://ru.wikipedia.org/wiki/Википедия:Авторитетные_источники

между пройденными вами страницами. Есть ещё интересные решения для Firefox: раз, два.

Не забывайте искать по всем ключевым словам, какие заметите.

Скользнув глазами по странице, можно не увидеть большую часть ее свойств. Из-за этого можно пропустить важный объект, приняв его за нечто скучное или тривиальное. Поэтому простой просмотр ресурса следует дополнять техническим анализом.

Технический анализ служит смысловому и не всегда может быть отделён от него: изучение технических особенностей объекта раскрывает его назначение. Иногда эти подробности становятся единственным источником понимания сути находки. В других случаях базовые знания сетевых протоколов позволяют дополнить расследование[309] [310] или найти владельца простейшим whois. Чтение с помощью Wireshark пакетов, полученных, к примеру, из потока данных со спутника, расскажет о сайтах и протоколах. Нехватка навыков в техническом анализе приводит к ложным впечатлениям и распространению легенд о невозможных явлениях или об искажённых образах реально существующих сетей (см. главу 3.12.5 о Closed Shell Systems).

Разбирать методы начнём с работы над **результатами сканирования**, так как это обычно источник наиболее сложных в анализе и необычных находок. Сайты и файловые архивы альтернативных и оверлейных сетей, полученные другими способами поиска, обрабатываются аналогично.

4.1 Анализ сетевых узлов

Ранее мы говорили о сканировании сети как об одном из основных способов поиска нетсталкерами новых объектов.

Из **IP-адреса** можно получить следующую информацию:

- Приблизительное местоположение сервера и, возможно, имя владельца или название организации - с помощью whois. Чаще всего так можно получить лишь информацию о провайдере.
- Поднятые сервисы - с помощью nmap. Сканирование всех портов выдаст отчёт не только об открытых портах, но и о предполагаемых сервисах, различаемых по т.н. фингерпринту (отпечатку). Кроме того, существуют таблицы соответствия, например, на Википедии. Обычный запрос к поисковику вида «port xxxx» также может помочь прояснить ситуацию. Иногда владельцы серверов защищаются,

[309] https://telegra.ph/INTERNET-PROTOCOL-CRYPTO-GAME-03-24
[310] https://telegra.ph/INTERNET-PROTOCOL-CRYPTO-GAME-chast-2-04-03

открывая «вхолостую» огромное множество портов, что затрудняет и работу nmap, и просмотр результатов.

- Привязанное доменное имя, если имеется - с помощью reverse DNS lookup.
- Историю смены сервером адресов, если имеется.
- Более точную геолокацию - с помощью карты, основанной на результатах RouterScan.
- Информацию, найденную до вас – вбивая IP или выявленное на одном из предыдущих шагов доменное имя в обычные поисковики или Shodan и подобные. К примеру, ftp-сервера NASA упомянуты на сайтах подразделений данного агентства, что позволяет быстро разобраться с научной темой их содержимого.

На одном IP-адресе может быть открыто множество портов. Камеры нередко соседствуют с ftp-серверами, хранящими записи с них[311], а также с роутерами. Простые веб-странички на порту 80 окружены на других портах произвольными протоколами, к примеру, для обмена текстовыми или голосовыми сообщениями. Яркие примеры можно встретить на отдельных Tor-нодах[312]

4.1.1 Возможные результаты на http(s)

Первый шаг анализа - понять, что за объект перед вами, ознакомившись с ним. На http(s) живут такие ресурсы:
1. Пустышки. В браузере открывается белый лист. Анализ сводится к проверке исходного кода на наличие неотображаемой информации.
2. Заглушки. Это страницы, создаваемые при установке серверного ПО одновременно с открытием портов. Они стандартны, у каждого из вендоров серверов своя. При необходимости администратор заменяет такую страницу на собственную (см. далее) либо закрывает порт, отвечающий по http(s), чтобы она не отображалась вовсе. Обычно живут на порту 80.
3. Страницы с кодами ошибок[313]. Иногда администраторы подменяют отображаемое по ошибочному запросу, создавая кастомные ответы чаще всего на такие ошибки, как 403 и 404, а также шуточную 418: она сообщает, что сервер не умеет варить кофе, потому что на нём чайный заварник.

4. Веб-интерфейсы сервисов, или т.н. «веб-морды». Это веб-интерфейсы для развёрнутых на сервере приложений. К примеру, «мордой» IP-камеры считается её онлайн-плеер, у роутера это страница настроек. Порт произвольный, зависит от сервиса. Анализ сводится к определению названия и предназначения сервиса или модели устройства, для чего иногда придётся выявить и местоположение. Пробейте все

[311] http://telegra.ph/Kamery-na-korejskih-FTP-12-01
[312] http://telegra.ph/Tor-nody-rkfgme-03-16
[313] https://ru.wikipedia.org/wiki/Список_кодов_состояния_HTTP

Fig. 13. Вариант страницы с кодом 418, найденный на http://82.64.25.212/

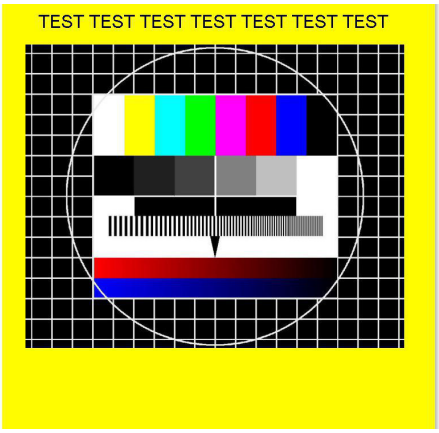
ключевые слова, присутствующие на странице. Более глубинный способ - прочесть HTTP-баннер с помощью nmap, о чём подробнее в 4.6.1:

nmap -Pn -p 80 -sV –script=banner 192.168.1.106

5. Сайты. Будем считать таковыми любые веб-страницы, наполнение которых определяется лишь самим владельцем. Самая разнообразная и интересная категория. Проанализировать сайт - значит, понять, с какой целью его завели и что именно на нём содержится.

Из сайтов отдельно выделим:

- Нестандартные заглушки. Характерная для установленного сервера страница заменяется произвольной. Других страниц нет (но это не значит, что нет других веб-сервисов на других портах).



- Эксперименты. Владелец тренируется в веб-дизайне, работе скриптов, кодин-

ге. Характерны отдельные бессвязные элементы дизайна, или наоборот - минимум оформления, зато интерактив из одной-двух функций, или даже отдельный неоконченный сервис.
- Домашние. Это личные сетевые площадки, рассказывающие обычно о жизни владельца, его увлечениях. В эпоху до соцсетей и блогов являлись основным способом показать себя другим пользователям сети. Ранее назывались «хомяками» (от англ. home site).
- Официальные. Площадки, принадлежащие организациям, коммерческим, государственным и другим структурам.
- Нет-арт. Основная цель создания образца «сетевого искусства» - это вызвать у посетителя какие-либо переживания или воздействовать на его эстетическое чувство. Для этого автор старается задействовать смесь дизайнерских средств и техник, гипертекстовой парадигмы, программных средств. Нет-арт может быть интерактивным, а может представлять собой одностраничник с парой картинок: главное здесь не объём, а создание эффекта.
- Сетевой квест либо АРГ. Первая (или любая другая) страница сайта оказывается началом в цепочке загадок.

Анализ. Получите всю возможную информацию из ip-адреса и домена, как указано выше. Это важный момент, иногда даже негативные результаты данного этапа включают в отчёты.
1. Осмотрите исходный код страницы. В нем может быть неочевидная ссылка: другая страница или директория, чаще всего лишь с библиотеками скриптов. Это может выглядеть, например, так: <a href="page.html». Другая типичная зацепка - это закомментированные (отображаются зелёным) строки с дополнительной информацией. К примеру, описание сайта, ник, почта или имя владельца, ASCII-арт и пр. Иногда можно найти ссылку на аудио- или видеофайл. Просмотр текста файлов-скриптов позволяет точнее узнать, что происходит на сайте, особенно интерактивном. Это экономит время, как в случае с данным нет-артом, заполненным бесконечными фигурами. Также повторное использование одних и тех же js-файлов - традиционный деанонящий фактор, по которому можно найти другие работы автора.

2. Поищите **поддомены и директории**. Для этого есть готовые пентестерские утилиты. Sublist3r[314] ищет поддомены, перебирая закешированное в поисковиках. DirBuster[315] брутфорсит возможные названия директорий и файлов, используя собственные словари.
3. Посмотрите, как выглядел ресурс в **архивах** web.archive.org и archive.is. Иногда почти пустые страницы оказываются в прошлом насыщенными. Или же на них поначалу лежали личные данные, дополнительная информация, внешние ссылки, как на сайте-квесте ELITEROOT[316].
4. Навестите robots.txt и sitemap, что даст шанс получить скрытые ссылки.

[314]https://github.com/aboul3la/Sublist3r
[315]https://sourceforge.net/projects/dirbuster/
[316]https://telegra.ph/ELITEROOT-07-15

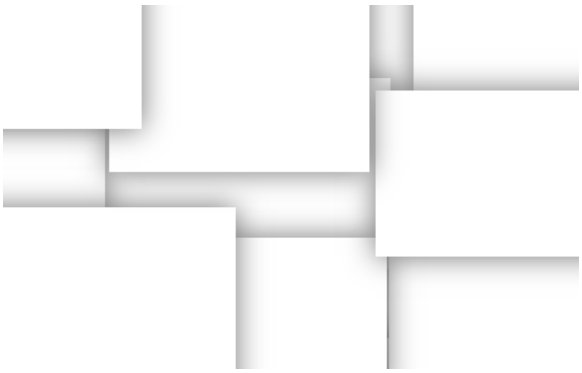


Fig. 14. Судя по коду javascript, вытаскивать эти прямоугольники друг из-под друга можно бесконечно. Они генерируются заново.

5. В случае с https, вы можете проверить сертификат сайта. Он может содержать некоторую информацию о владельце. Для поиска по сертификатам можно взять, например, https://censys.io/certificates или его шодановский аналог. Например, вбейте туда серийный номер, и поисковик выдаст другие сайты или альтернативные домены.
Параметры, которые можно использовать в запросах к Censys:

parsed.serial_number: поиск по номеру
parsed.fingerprint_sha256: поиск по фингерпринту
parsed.subject.locality: где выдан сертификат

Дополнительные инструменты:

DomEye - анализирует фрагменты публичной информации о сайте и ищет ресурсы, где они также встречаются. Сюда входят различные трекинговые коды рекламных площадок, ID партнёрской программы Amazon, email и другие мелочи. А ещё у него есть расширение для Chrome, чтоб всегда носить с собой в походы по сети. Если вашего сайта не нашлось в базе, тулза обещает обыскать его в ближайшие несколько минут, поэтому в случае неудачи повторите поиск позже.
DNSlytics - небольшой агрегатор инструментов. Есть ряд фич, присутствующих и в Maltego, типа указания DNS-сервера, в зоне которого находится сайт. Интересна функция поиска доменов с таким же именем, но на другом домене верхнего уровня (TLD):

4.2 Игры в Альтернативной Реальности

Alternate Reality Game (ARG) — это интерактивное трансмедийное[317] повествование на базе реальности, которое развивается в реальном времени и изменяется в зависимости от действий игроков. Влияние его аудитории так высоко, что ARG может пойти по непредвиденному сценарию, завершиться раньше времени или остановиться на середине.

[317] https://ru.wikipedia.org/wiki/Трансмедийное_повествование

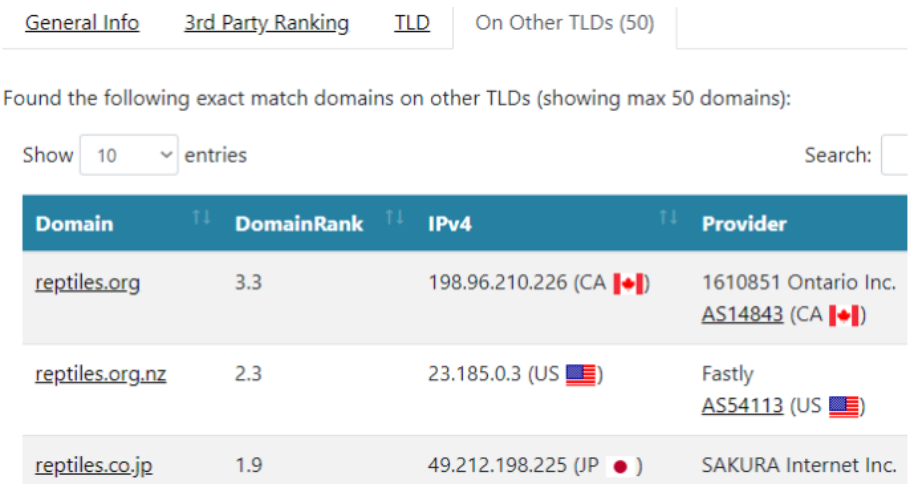


Fig. 15. Вкладка поиска доменов

Игры создаются и, насколько это возможно, контролируются одним или несколькими кукловодами (puppet-master/PM). Во время ARG их личности неизвестны игрокам, но могут быть раскрыты в конце, т.е. находятся за занавесом (curtain) — условным обозначением границы, из-за которой кукловоды не связываются с участниками напрямую, но контактируют через персонажей и внутриигровой дизайн.

ARG начинается с «кроличьей норы» (rabbit hole, trailhead) — первого общественного упоминания, которое нелинейно завлекает посетителей. Нор может быть несколько: чем больше, тем проще найти игру. Во время прохождения игроки совместно решают головоломки, беседуют с протагонистами и раскрывают сюжет благодаря мультимедийным средствам связи: телефонам, почте и интернету. Иногда они путешествуют по GPS-координатам в поисках новых зацепок — например, чтобы забрать флешку или диск. На это опирается принцип TINAG (This Is Not A Game): в идеале участники не знают, что события игры вымышлены. Неопределенность может сохраниться и по её окончанию, если авторы не подтвердят вымысел. Старайтесь не путать криптографические соревнования типа Цикада 3301[318] с ARG, т.к. первые не имеют сеттинга и/или сюжета и обычно являются вербовкой в сообщества или развлечением.

ARG — мощное средство пиара. Например, в 2001 г., для рекламы фильма A.I, Microsoft провела одну из первых сетевых ARG — The Beast[319]. Работавшие над ней люди позднее основали компанию 42 Entertainment[320], ответственную за такие из-

[318]https://en.wikipedia.org/wiki/Cicada_3301
[319]en.wikipedia.org/wiki/The_Beast_(game)
[320]http://www.42entertainment.com/

вестные игры, как I Love Bees[321], Year Zero[322] и Why So Serious?[323]. В 2010 г. Valve и команда разработчиков Portal 2 создала Portal ARG[324] для анонса сиквела. ARG также могут быть постоянными и самостоятельными. В 2015 г. была выпущена видеоигра Black Watchmen[325], в которой нужно расшифровывать коды, искать информацию и пользоваться картами. Прототипом такой механики была французская игра 2004 г. In Memoriam[326], передававшая игрокам файлы с закрытого вебсайта.

Согласно данным крупнейшего тематического форума Unfiction[327], ежегодно выходят до 10 «коммерчески» ARG и несколько сотен любительских. На их почве формируются новые жанры и сеттинги: так в веб-сериалах развивалась мифология[328] о Слендермене[329]. В России такие игры как явление настолько малоизвестны, что статью о них даже хотели удалить[330] с Википедии. Ниже приведены примеры прошедших российских ARG и их хронологий.

4.2.1 Примеры ARG Рунета

Девушка с таймером

29.05.2017 на Дваче появилась серия тредов[331] о YouTube-трансляции с привязанной к стулу молчащей девушкой с планшетом, на котором шёл обратный десятичасовой отсчёт. На фоне играло радио «Говорит Москва». С 13:00 по 20:00 передача удалялась модерацией и пересоздавалась под случайными названиями. В 20:30 она перекочевала на Periscope, где отключалась каждые 15 минут, но всё-таки продержалась до конца таймера. В это время мимо проезжали автомобили, доносились голоса и шаги и несколько раз мигал свет.

За час до финала с радиостанцией связался Adolf, администратор peka2.tv, и ведущие провели экстренный ночной [332]эфир[333]. Они напрямую обращались к девушке, задавали ей вопросы, получали противоречивые показания и почти узнали её номер телефона. Без 9 минут полночь послышался звон стекла, трансляция деактивировалась, и вскоре эфир закончили. На следующий день сообщество Black Elephant опубли-

[321] https://en.wikipedia.org/wiki/I_Love_Bees
[322] https://en.wikipedia.org/wiki/Year_Zero_(video_game)
[323] https://en.wikipedia.org/wiki/The_Dark_Knight_(film)#Marketing
[324] https://half-life.wikia.com/wiki/Portal_ARG
[325] https://www.blackwatchmen.com
[326] https://en.wikipedia.org/wiki/In_Memoriam_(video_game)
[327] https://forums.unfiction.com/forums/
[328] http://forums.unfiction.com/forums/index.php?f=264
[329] https://ru.wikipedia.org/wiki/Слендермен
[330] https://ru.wikipedia.org/wiki/Википедия:К_удалению/25_августа_2009#Игра_в_альтернативной_реальности
[331] http://arhivach.ng/thread/265329
[332] href
[333] https://www.youtube.com/watch?v=A4mqEWDbpog

ковало разгадку[334] инцидента, который осветили авторитетные новостные журналы: TJournal[335], The Question[336] и Лента[337]. Негуманность социального эксперимента возмутила Алексея Гудошникова на тематическом эфире[338].

Русин

Пример того, как трудно различить между собой загадочное явление и бред сумасшедшего. Трактуется некоторыми как ARG из-за косвенной связи автора со спецслужбами, доказанной его навыками и интересами.

Павел Русин с 2014 года регулярно выкладывал на своей странице ВКонтакте[339] несвязные тексты, регулярно их зачищая. По ним он является наследным принцем княжеского рода Стародуб, Князем Сибири и незаконнорожденным отпрыском короля Испании Хуана Карлоса I. Также именует себя выходцем из Дома Лео Толстой, морским пехотинцем и т.п. Много пишет о взятых у него в долг деньгах. Установлено, что настоящее имя Русина - **Кривоногов Павел Александрович**, 02.07.1974 года рождения, и у него имеется огромный долг перед банком. Подтверждён его опыт работы с военным делом, айкидо, информатикой.

Всё это заставило анонимов /sn/, где постоянно держался тематический тред, заподозрить аккаунт в связях со спецслужбами и передаче шифровок, замаскированных под шизофазию. В пользу этого приводились, например, такие доказательства:

- После подключения логгера к стене Павла админ этой программы опубликовал случай редактирования падежей в записях с правильных на неправильные, «шизофреничные». Логгер впоследствии был якобы удалён гитхабом, ныне расположен на bitbucket.

- Один из пойманных этим софтом постов содержал в себе шифровку, указывающую на сходку поклонников Кастанеды, которым увлекался Русин.

- По телефону общался без признаков разрушения речи. Звонил человек из круга владельца логгера.

Впоследствии программиста обвинили во множественных **фальсификациях**, из-за чего он мгновенно же удалил сайт с логами, подтвердив подозрения. Большая

[334] https://vk.com/blackphant?w=wall-143150516_1710
[335] https://tjournal.ru/flood/44824-devushka-s-taymerom
[336] https://thequestion.ru/questions/269982/chto-za-translyaciya-v-periskope-so-svyazannoi-devushkoi-i-taimerom-na-grudi
[337] https://lenta.ru/news/2017/05/30/fearstream/
[338] https://www.youtube.com/watch?v=SxlBTctkpig
[339] http://web.archive.org/web/20140120212253/https://vk.com/kupurizeya

часть расследования свелась таким образом к противостоянию нескольких «детективов», один из которых боролся за внимание и создавал вышеприведенные «доказательства», ложность которых доказана многократно в тредах. Так что ход исследования любого странного контента или АРГ может зайти не туда не только по вине «кукловода», но и ваших союзников.

Ростовские шифровки

16.11.2016 года в разделе /b/ на дваче появился кадр лесополосы в Ростове вместе с напоминающим шизофазию текстом. Спустя 5 тредов, 7.12.2016 появился аккаунт[340] на Facebook под именем Гарри Тарантул. С тех пор новые материалы публиковались там. Тексты легко расшифровывались[341] и содержали указания на закопанные в разных местах Ростова фрагменты человеческих тел и одежды. Несколько анонимов выезжало на данные точки, обнаруживали одежду. АРГ известна также как « Марширующий» - по имени члена банды убийц, или «Триумфально» - по одному из слов, часто используемых в постах для эффекта шизофазии.

Omegaproject

1 декабря на доске /b/ имиджборды Двач был создан тред, в котором ОП решил поделиться странным сообщением, которое его другу прислали с фейкового аккаунта:

«Hello, my friend We're looking for people interested in helping out
Maybe it's you»

К сообщению прилагался двоичный код, давший при расшифровке: «В тебе есть потенциал, следуй по пути - omegaproject.xyz». Сайт имитировал консоль с несколькими командами, а также принимал пароль. Паролем оказалась расшифровка закреплённого QR-кода. В ответ на него сайт выдал страницу, где в исходном коде было название ещё одной: iiiiiiiiiiiiiiiiiiiiiiiii.php Далее, чередуя анализ исходного кода и простые шифры игроки получили ещё несколько страниц, остановившись на строке «EE36-3A5C-619A-483B». После этого шифровки стали сложнее, они включали запароленные хэши, для получения которых нужно было вскрывать исполняемые файлы и картинки. Примечательно изображение шахматного поля, внутри которого была позиция a18a, то есть координаты ладьи. Если прохешировать слово «ладья» (rook), потом буквы и цифры хеша посчитать координатами на доске и отметить, то получается узор, подобный QR-коду, а если убрать чёрные клетки, то виден двоичный шифр. Ещё **пример** цепочки заданий: есть страница с паролем: https://omegaproject.xyz/noway/vikvikviking.php. Есть декодер. И есть текст из раржпега: «7267aa2f3d5220575569848f460dcb94192:278:279:277:288:317:214:289:276:324:276:278:213:235:271:296:275:26557461b4d1421f4a362b02807a063d170». Судя по названию файла psd.txt, там зашифрован пароль для vikvikviking.php. Осталось найти ключ для расшифровки. «Grav< 1973» не подходит, но может на что-то указывать.

[340] https://facebook.com/readit973
[341] https://bitbucket.org/rusinthread/triumfalno/src/e0e46f284b6958c32f577f26f0b6eb66d097c151/data.md

Если считать < за стрелку, то нужно прочесть слово задом наперёд. Grav = Varg = Варг Викернес (1973 года рождения) = Burzum. Бурзум являлся кейвордом для той длинной строки. На выходе получался пароль «GoodJobFofjwaFhwig».
Касаемо задействованных страниц во ВКонтакте: команда в терминале «/nav connect», вывела на профиль ВК «Hrógeirr Björg»[342], где среди изображений имеется масса различных QR-кодов. Они скрывали различные слова и адреса страниц, а также записку privnote, уже просмотренную на момент обнаружения.

Квест не был решён до конца, а конференция в Telegram, занятая им, закончила существования на поисках «крысы», сливавшей результаты на двач, что давало анонам шансы добраться до разгадки раньше. Это было важным по той причине, что ряд квестов и ARG раскрывают свой финал лишь первому победившему или нескольким.

RT-2472 (Чёрный Опал)

22 марта 2015 был начат постинг в группе ВК RT-2472[343]. Записи имитировали диалоги о паранормальном, полученные по телефонной связи, по радио, по SMS. Затем стали попадаться «Космические сигналы» со строками в base64, «Видеозаписи» в виде описаний происходящего на выдуманном для сюжета видео, треки с названиями в виде букв и цифр. Люди стали отмечаться в комментариях с разгадками. В 2019 году была создана конференция для тех, кто был замечен в такой активности. Администратором выступил женский аккаунт «Солнечный Удар» .

Вскоре она начала проводить голосования за исключение тех или иных участников, в которых то и дело отмечались не разобравшиеся в деле новые зашедшие в чат. Проект был объявлен социальным экспериментом. Игроки принялись разбираться не только в шифрах и загадках, но и в истинных мотивах организаторов, подкидывавших в беседку всё новые события и сомнения, что и размыло границу между просто продуманным квестом и ARG. На момент написания игра в разгаре.

В основном, использовались:

- b64, rot, другие шифры и кодировки, их наслоения;
- спектрограммы;
- координаты гугл-карт, где на местности и панорамах обнаруживали подсказки;
- QR-коды или их фрагменты;
- ввод числовых кодов через ALT, чтоб получилась Unicode-строка.

Одним из шагов была шахматная партия с Солнечным Ударом.

[342] https://vk.com/id452358855
[343] https://vk.com/rt2472

4.2.2 Способы анализа АРГ

Анализ АРГ сводится к определению ресурса как игрового и разгадыванию сюжетного хода. В этом понадобится не только знание традиционных шифров, но и культурный багаж, в частности, умение ориентироваться в символах и аллегориях[344]. Как вы убедились из примеров, несложно спутать «кроличью нору» с неигровыми объектами.
Записывайте ход игры, а лучше отображайте схематически или в виде майндкарт, как на этой схеме по nino, или этой и этой.

Что можно принять за АРГ:

- Страницы безумцев, отличающиеся искренними фантастическими убеждениями, не совпадающими с реальностью.
- Нет-арты, поскольку эти лишены загадок и сильно зависящих от посетителя сюжетов.
- Сетевые квесты или сетевые загадки (riddles), где нет tinag-фактора. Впрочем, в последние годы их смешивают.

Работы сумасшедших отстоят от ARG за счёт нарушения логики. Общее правило: сверяйте написанное с известными вам психиатрическими синдромами. Самые яркие признаки, связанные с распадом личности:

- Много повторов одной и той же мысли или образа, выделений по смыслу или дизайном (в т.ч. много заглавных букв), акцентирование внимания.
- Пафос подачи. Информация на сайте повествует о некоем абсолюте, о глобальном или радикально новом. Могут присутствовать псевдонаучные термины. Их вы можете отличить от научных с помощью того же поисковика, но обычно они бросаются в глаза, особенно когда есть эзотерический окрас.
- В качестве «доказательств» приводятся домыслы или не связанные явно с материалом сайта события. В открытом письме некоего Петрова Совбезу России говорится, что президента убьют, ссылаясь на обычные статьи в СМИ о президенте США. То есть автор живёт своей альтернативной логикой.

Под влиянием сверхценных идей или голосов в голове люди создают целые послания незримым читателям в надежде, что на них кто-то наткнётся. Так было с хакером Michael Guidry, рассылавшем отчёт о палачах из ФСБ по открытым FTP-серверам. С другой стороны, то же самое может создать обычный здоровый человек, желающий выразить что-то глубоко значимое для себя. Скажем, философскую идею, рассказ о важном воспоминании, призыв выровнять спину, а может, просто попытку

[344] https://ru.wikipedia.org/wiki/Список_аллегорических_фигур

выговориться - так было с закодированным в base64 сайтом C. Rubin-a. Такое можно найти и на домашних сайтах, если внимательно их осматривать.

Некоторые «послания», пожалуй, невозможно отличить от действительно хорошей кроличьей норы в АРГ. Мы видели пример этого в «Ростовских шифровках». Но если оно:

- эмоционально цепляет и побуждает действовать;
- намекает на присутствие на сайте или где-то ещё в сети дополнительных материалов, которые нужно искать; содержит в коде непонятные слова и названия, фрагменты шифра;
- содержит в самом тексте оригинальные названия или имена, поиск по которым явно не будет забит спамом...

...то можете уже предполагать ARG. Это сохранит от разочарований, когда окажется, что интригующая тайна была частью сюжета.

Иногда можно вычислить и ведущего игру. Например, кто-то из участников разгадывает очередной фрагмент, но не может объяснить, где он взял ключ, как это сделал с шифром Виженера пользователь MurdocLoch в «Trials Evolution».

4.2.3 Виды шифров

Шифровки и их комбинации хорошо описаны любителями CTF (Capture The Flag) - челленджей на сетевые расследования, напоминающих квесты. «Флагом» называется строка-ключ, обнаружение которой среди зашифрованной или труднонаходимой информации является целью игры. Подробно можете ознакомиться здесь[345]. Не путайте с литспиком, где буквы заменяются напоминающими их спецсимволами[346].

1. Сетевые шифры (кодировки)
   Большая часть кодов поддаётся расшифровке через онлайн-сервисы. Общий смысл — символы алфавита заменяются другими символами или их комбинацией, однако есть и более сложные случаи.

   - ASCII-код — десятичные числа кодируют символы алфавита, цифры и некоторые другие. Это традиционный способ кодирования текста для нужд операционных систем, программной обработки. Общего с ASCII-артом у него только то, что в этом арте используются любые символы, описанные одноименной кодовой таблицей — но не более.

[345] http://itsecwiki.org/index.php/String_crypto
[346] https://en.wikipedia.org/wiki/Leet

- Двоичная кодировка — ASCII-код символа переводится в двоичный алфавит, то есть комбинацию 0 и 1. Строка может быть разделена на октеты или быть сплошной, тогда длина её будет делиться на 8, 7 или 6.
- Base 64. Этот код легко узнать на глаз по комбинации из строчных и заглавных букв и цифр, часто в конце есть == или =. Пример: MTIzOjtmbGFnMQ==
- Его стоит отличать от base32, у которого все буквы одного типа, например, строчные. На конце 1-6 знаков «=»
- Base85/Ascii85 Пример: < BlnE-@s;X&BeF=EB.ktp1Gg7?,:”RA-7UDm?N >
- Punycode. Кодирует, в частности, кириллические домены. Не переводит латинский алфавит, цифры и символы.

2. Традиционные шифры

- Шифр Цезаря - исходный текст заменяется текстом из символов, сдвинутых по алфавиту на заданное расстояние. Его вариация ROT13 (со сдвигом 13) используется настолько часто, что стала мемом USENET[347]. Он является обратным, т.е. для дешифрования применяется тот же алгоритм, что и для шифрования.
- Шифр Виженера - состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Расшифровка здесь требует предварительной отгадки ключевого слова, исходя из которого и выбирается смещение.

Простые шифры и кодировки могут встретиться вам в комбинированном виде. Например, сообщение пропущено через шифр, а только потом перекодировано в base64. Существует специальная программа для создания и расшифровки таких цепочек из шифров: CyberChef[348], добавленная в сборку «Перевал»[349].

4.2.4 Стеганография

Стеганография - это процесс встраивания любого файла или их набора внутрь объекта-прикрытия, называемого контейнером. Передаваемые данные «размазывает» по нему, что делает их необнаружимыми. Результат - объединение неприглядного контейнера и важного сообщения - называется **стего**. В простейшем случае это может быть дописывание информации в конец файла. Иначе изъять спрятанный месседж можно той же программой, которая его туда заложила, наиболее частым выбором является steghide. Есть и другие приёмы.

[347] https://en.wikipedia.org/wiki/ROT13#Letter_games_and_net_culture
[348] https://gchq.github.io/CyberChef/
[349] https://github.com/wegwarte/pereval-server

- Для изображений. **Затемнение**, которому нужно выкрутить яркость или убрать часть спектра. **Датамош** (datamosh), когда в изображении, открытом как текст в NotePad++ или другом подходящем редакторе, заменена часть символов на кодовые. Сопоставив искажённую картинку с исходником, получаем сообщение.

- Для аудио. Картинка на **спектрограмме**, подобно творчеству Apex Twin. Соответствие частот **двоичному коду**, который затем расшифровывается. Софт: для mp3, для любого аудио.

- В Telegram можно в круглом **видеосообщении** спрятать информацию по углам. Бот для преобразования @TelescopyBot.

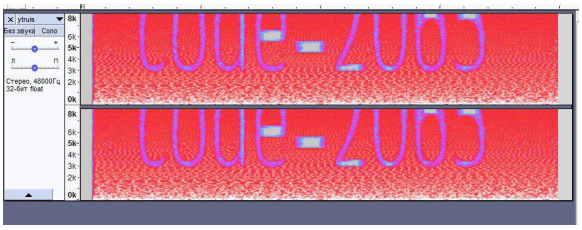


Fig. 16. На спектрограмме виден код

Наконец, хранилищем стеганографического сообщения могут быть метаданные, о которых подробнее смотрите в 4.8.

4.3 Нет-арт

Нетсталкеры зачастую определяют нет-арт как сайт, в рамках которого средствами веб-кодинга создано некое произведение: эстетичное, интерактивное, передающее какой-либо посыл или атмосферу. Однако первоначальные взгляды на это явление несколько иные.
В 2002 году уже чётко отделяли арт, распространяемый по сети и арт, созданный с помощью сети. Однако первоначально, на заре интернета, представления о «сетевом искусстве» были куда шире. «Введение в нет-арт», 1994-1999, выделяет такие жанры:

1. Подрыв власти
2. Сеть как объект
3. Интерактив
4. Стриминг (?)
5. Дневник путешествий
6. Коллаборация по сети

7. На основе поисковиков
8. Тема секса
9. Повествование
10. Пранки и конструирование фальшивой персоналии
11. ASCII-арт
12. Браузерный арт, арт на основе программных онлайн-сервисов
13. Арт на основе форм
14. Многопользовательские интерактивные среды
15. Арт на основе IRC, электронной почты, ICQ, CUSeeMe, почтовых рассылок.

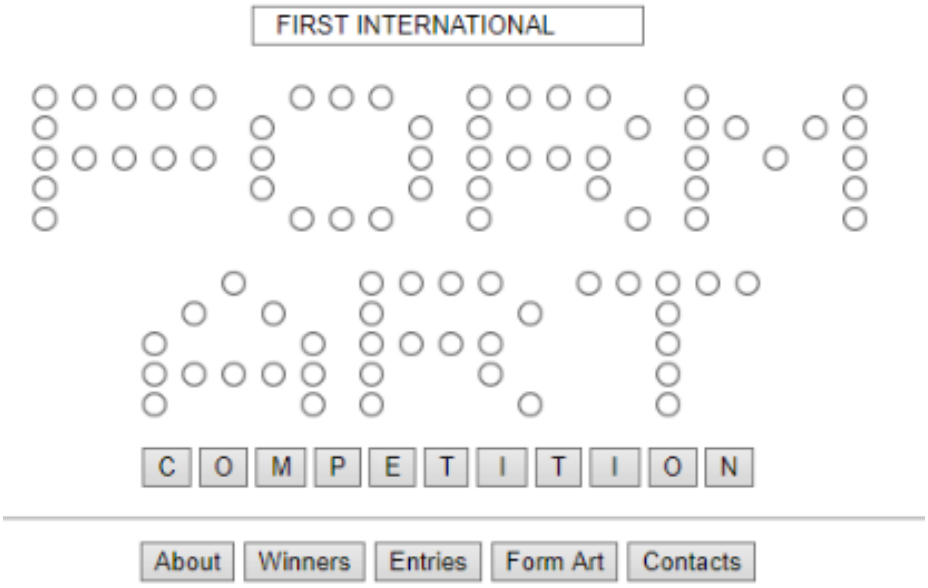


Fig. 17. Конкурс нет-артов на основе форм

Следствием развития этих жанров текст называет превращение интернета в «магазин, порно-лавочку и музей», а сетевого художника определяет как «того, кто свободно работает с полностью новыми формами [искусства] вместе со старыми, более традиционными формами; того, кто понимает растущую необходимость свободного двустороннего и многостороннего общения вокруг репрезентации». Таким образом, то, что ранее видели как единичные образцы искусства, стало неотъемлемой частью Web 2.0. Интересно, что один из идеологов нет-арта — наш соотечественник, Алексей

Шульгин. Его сайт[350] содержит примеры классических работ в некоторых из упомянутых жанров.

На сегодня некоторые виды нет-арта отжили по техническим причинам, некоторые, как онлайновые арт-площадки — стали частью обыденности. С развитием технологий появились и новые. Профиль в соцсети вполне может быть оформлен как произведение со своим посылом, и даже дезинформация становится формой творческого выражения[351] [352] [353], пародирующей теории заговора.

Сайты художников и личные странички, заглушки не называются нет-артами, равно как и красиво оформленные бизнес-проекты: их основная цель утилитарна. Это не значит, что нет-арт полностью иррационален. Cameron's world[354] служит подборкой важных для его автора объектов с Geocities, а проекты типа Mouchette[355] обладают развитым нарративом, осознать который можно лишь опытом, обойдя лабиринт страниц. Многие же работы выглядят лишь хаотичным нагромождением объектов, особенно если дают возможность приобщиться самим посетителям, как Floodnet[356] или mebius.co.uk[357].

Сетевые артисты используют в качестве художественных приёмов:

- неожиданные сочетания графики, текста, видеозаписей, а также их многократное повторение;
- гиперссылки, вовлекающие пользователя в путешествие и добавляющие минимальный интерактив, иногда нелинейный;
- скрипты, дополняющие и усиливающие этот опыт;
- скрытые элементы, из-за чего некоторые нет-арты можно спутать с квестом и наоборот;
- эффекты вёрстки, шрифтов;
- трёхмерные модели и пространства.

Таким образом, **анализ** здесь сводится к отличению нет-арта от обычных учебных проектов программистов и веб-дизайнеров, определению новизны находки поиском её упоминаний и, наконец, к попытке понять общий посыл и приёмы для его

[350] http://www.easylife.org
[351] https://telegra.ph/sub-rosa-07-20
[352] https://www.thedailybeast.com/birds-arent-real-is-the-conspiracy-theory-mocking-qanon
[353] http://fov2uy7x37f5u3w2huscgk3gqlvvixrvww5v3dqaqcidla6c3wlyogqd.onion/
[354] https://www.cameronsworld.net
[355] https://anthology.rhizome.org/mouchette
[356] https://anthology.rhizome.org/floodnet
[357] https://web.archive.org/web/20121015160543/http://mebious.co.uk/

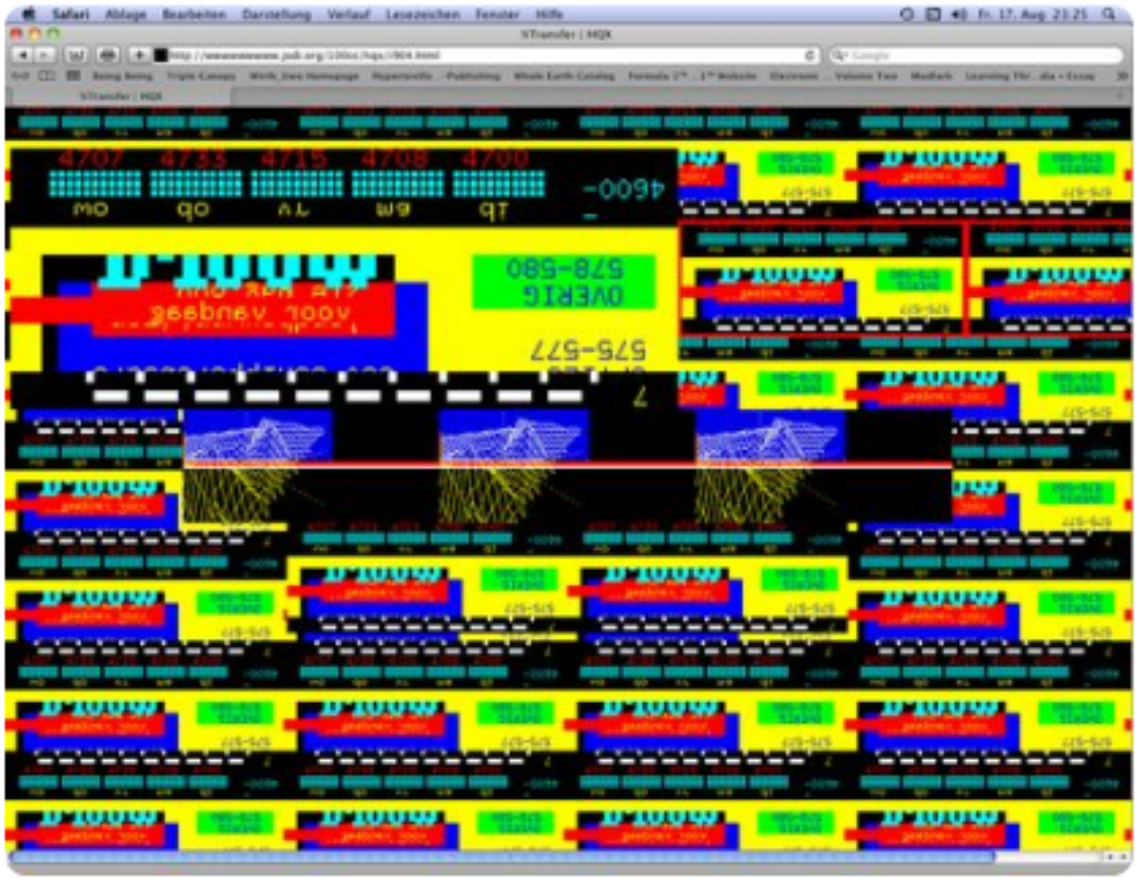


Fig. 18. Одна из страниц известнейшего нет-арта jodi.org

выражения.

4.3.1 ASCII и ANSI-графика

Во времена, когда у компьютеров не было возможности отображать графику, её выводили символьными рисунками - наследниками каллиграмм и картинок, выполненных на печатной машинке. ASCII-арт - это картинки, составленные из символов стандарта ASCII. Их до сих пор можно встретить в консольных приложениях и файлах Readme, FILE_ID.DIZ и .nfo, куда они помещаются как дополнение к описанию материала или как отдельные «артпаки», своего рода галереи. ANSI-графика отличается расширением символьной таблицы и наличием цветов, что обеспечивалось отдельным драйвером ANSI.SYS, доступным в MS-DOS. Использовалась в BBS. Может распространяться в виде .ans-файлов.

Рисование в текстовом режиме сформировало свою культуру, или «сцену» , включающую творчество цифровых пиратов, но известно и обычному пользователю:

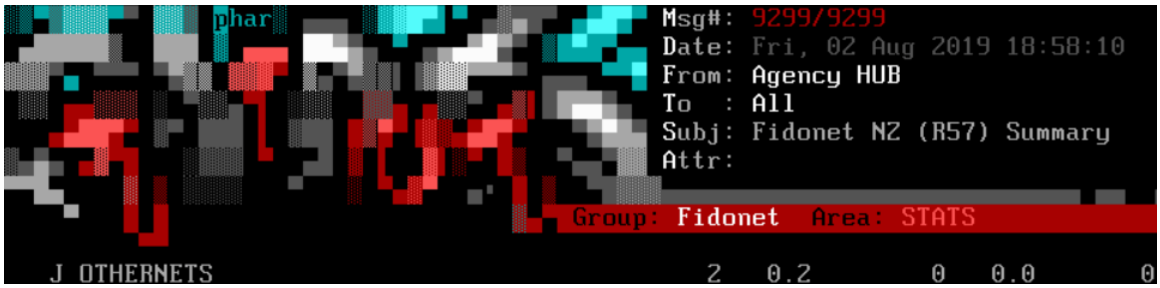


Fig. 19. ANSI-арт

«смайлик» - простейший образец. Широко распространён ASCII-рисунок коровы или другого животного с небольшим сообщением – т.н. cowsay. Его можно встретить, к примеру, в исходниках сайтов или различном ПО, работающем с командной строкой. Многие message of the days в IRC-каналах сдобрены надписями или картинками в ASCII, ознакомьтесь с их подборкой.

4.4 IP-камеры

Зрение является основным способом восприятия человека и формирует более привлекательную картину окружающего мира, нежели текст или звук. Нетсталкеры порой наблюдают за выращиванием психоактивных веществ, показаниями приборов заводов и НИИ, совершением преступлений и даже воплощением крипипаст[358] (пока одни снимают «паранормальное», другие его вещают), а вуайеристы торгуют видео из семейных спален и салонов проституток. Хакеры проводят DDoS-атаки не только роутерами, но и камерами: как-то всплыл ботнет[359] с 25000 заражённых девайсов. Знающий местоположение применяет их для деанонимизации людей или расследования инцидентов типа смерти Элизы Лэм[360]. Детективы просматривали 800 часов архивных записей, и такой ручной подход, увы, остался до сих пор: детекция движения или изменений на камерах (по исходникам статичной картинки) мало где есть.

Помимо проверки статуса распространённых портов (80-83, 8080-8083, 8888, 8000, 8001, 9000, 88, 85, 8008) обычными IP-сканерами или специализированными утилитами вроде Verda[361], самописной надстройки над nmap, определяющей камеры по шаблонам HTTP-баннеров, адресов и ответов серверов, трансляции ищутся дорками[362] поисковиков, чья нотация операторами меняется с синтаксисом. Не забывайте, что сервисы типа Google или Яндекса индексируют сайты по упоминаниям, отображая малую часть от их общего числа, в отличие от Shodan, Censys и

[358] https://mrakopedia.net/wiki/Веб-трансляции
[359] https://threatpost.com/botnet-powered-by-25000-cctv-devices-uncovered/118948/
[360] http://murders.ru/elise_l_1.html
[361] https://github.com/wegwarte/verda-v1
[362] https://telegra.ph/Dorki-IP-kamer-08-18

PunkSPIDER, не сужающих поиск уточнением запроса. По тэгам можно найти обсуждения[363], списки[364] и библиотеки, которые чаще носят развлекательный характер, как EarthCam[365], ip-24.net и goandroam.com, нежели серьёзные проекты: AMOS[366], insecam.org и opentopia.com.

Если камера защищена, и заводские логины-пароли из списков ipvm[367].com и open-sez.me[368] не подходят, попробуйте проникнуть по URL[369] (потоковое изображение; панель управления) или добавить словари репозитория SecLists[370] для брут-форса, в базы утилит Hydra[371] и Burp Suite[372]. Формы входа продуктов Hikvision по дефолтной авторизации обходит hikka[373], экспортирующий результаты скриншотами и .csv-форматом для удобного просмотра в iVMS[374]. Присутствуя на показе, не выполняйте действий, в последствиях которых вы не уверены, т.к. очищаемые журналы активности видит владелец. Лучше не создавать и не изменять учётные записи: когда действия заметит админ, камера переедет на свободный IP-адрес. Обычно она оснащена PTZ-панелью для панорамирования, наклона и зума, доступной только пользователям выше гостевых привилегий. Иные модели имеют микрофон и динамик, транслирующие звуки помещения или голос (в т.ч. микшер) наблюдателя, что привлекает пранкеров[375], раздражающих рабочих и жильцов.

Утилиты управления DVR и NVR, цифровыми и сетевыми видеорегистраторами, гуглятся как «dvr/nvr software» и поставляются производителями, как делают Canon[376] и Dahua[377]. Почти каждая марка навязывает свой софт для просмотра и подключения камер, и без единой политики многие из них работают на устарелом ПО. ActiveX, фреймворк воспроизведения программных компонентов на IE (успешно эмулируется Chrome[378] и Firefox[379]), скачивает и распаковывает .cab-архив в систему, впоследствии обращась к его содержимому. Для запуска Java-апплетов, написанных

[363] http://archive.4plebs.org/x/search/text/anony%2Fmjpg.cgi/page/1/
[364] https://pastebin.com/search?q=anony%2Fmjpg.cgi
[365] https://www.earthcam.com/
[366] http://amos.cse.wustl.edu/
[367] https://ipvm.com/reports/ip-cameras-default-passwords-directory
[368] http://web.archive.org/web/20180106023956/http://open-sez.me/
[369] https://www.ispyconnect.com/sources.aspx
[370] https://github.com/danielmiessler/SecLists
[371] https://github.com/vanhauser-thc/thc-hydra
[372] https://portswigger.net/burp
[373] https://github.com/superhacker777/hikka
[374] http://ftp.hikvision.ru/09. Утилиты/1.%20IVMS-4200/
[375] https://www.youtube.com/playlist?list=PL8jkwhXa3jRKRywyDV5BjWJ6tsFI-KIm4
[376] http://softpedia.com/get/Internet/WebCam/WebView-Livescope-Viewer.shtml
[377] http://dahuasecurity.com/download_2.html
[378] https://chrome.google.com/webstore/detail/ie-tab/hehijbfgiekmjfkfjpbkbammjbdenadd
[379] https://addons.mozilla.org/ru/firefox/addon/ie-tab-2-ff-36/

на ЯП Java плагинов, должна быть установлена 6-ая среда JRE[380], конфликтующая с более поздними версиями. Проблема разрешается их удалением или отключением в настройках вместе с понижением уровня защиты до «Medium» или «Low». Чуть реже попадаются камеры на Apple'овской технологии QuickTime[381] в качестве основного или побочного режима. Перечисленные средства проверены на Internet Explorer 5.5, Google Chrome 40 и Mozilla Firefox 43. Удручает, что на кастомные расширения порой ведут битые ссылки, а по названиям установочные файлы найти трудно: к примеру, RmtViewerV2.cab совсем не гуглится, хотя он существует[382].

К счастью, ради стандартизации компании уходят с отживших расширений на отображение беззвучной обновляющейся картинки с опцией указания кадровой частоты. При её высоких значениях скорость передачи изображения неотличима от фильма. Популярно и потоковое вещание, чьи mjpeg/h.264 форматы поддерживают последние браузеры, а URL по HTTP/RTSP протоколу хорошо открывается в VLC-проигрывателе[383] хоткеем Ctrl+N. Порой так удаётся обойти авторизацию: у AXIS корень сайта требует входа, но переход по пути /mjpg/video.mjpg не препятствует показу потока. VLC-плеер также умеет записывать трансляцию в видеофайл с аудиодорожкой, что полезно на особо интересных находках.

Старайтесь не разглашать камеры, которые ещё не известны публике, т.к. несведущий сменит пароль, и вы лишитесь находки.

Анализ камер сочетает работу с IP и с изображениями.

4.5 Файловые сервера

Анализ сводится к определению содержимого и выявлению каких-либо нестандартных материалов. Бывает интересно составить «портрет» владельца. Назначение многих серверов можно быстро определить по размещённым в них папкам. Внешние накопители с системой бекапа, а также серверное ПО создаёт стандартную систему директорий. Зная об этом, можно прицельно искать жёсткие диски или, наоборот, избегать их.

Немало открытых FTP принадлежат научным и образовательным учреждениям, которые специально делятся данными. Пример:
ftp://196.24.44.52/ Один из серверов Южноафриканского Centre for High Performance Computing. Им, кстати, принадлежит весь блок /24. На сервере присутствуют

[380] https://www.oracle.com/java/technologies/javase-java-archive-javase6-downloads.html
[381] https://support.apple.com/kb/DL837?locale=ru_RU
[382] https://goo-gl.su/qLlqy
[383] http://www.videolan.org/vlc/index.ru.html

Fig. 20. Содержимое FTP-сервера, сгенерированное прошивкой подключенной камеры

спутниковые снимки различных областей страны проекта EONEMP - сбор информации про цианобактерии в экваториальных водах. Кроме всего прочего, большой архив спутниковых снимков спектрометра MODIS .

— Проект Random Open Science

На многих серверах включены не только права на чтение, но и на запись. Это превращает их в площадку для рассылки вредоносных скриптов (Photo.scr, IMG001.exe и неясный george.php[384]) или своих посланий человечеству. Хакер Майкл Гуидри массово заливал свои изобличения спецслужб, якобы подмешивающих ему наркотики.

Вскрывая незнакомые файлы в Notepad++ или другом текстовом редакторе, можно ознакомиться с их внутренним устройством (или форматом) и определить назначение, даже если по расширению ничего в поисковиках не нашлось. Научные данные могут храниться в виде, обрабатываемом лишь локальными программами - иногда на сервере или странице на порту 80 можно найти сам софт, написанный, к примеру, инженерами NASA.

[384]https://telegra.ph/Netstalker-0x1-anomalii-FTP-05-16

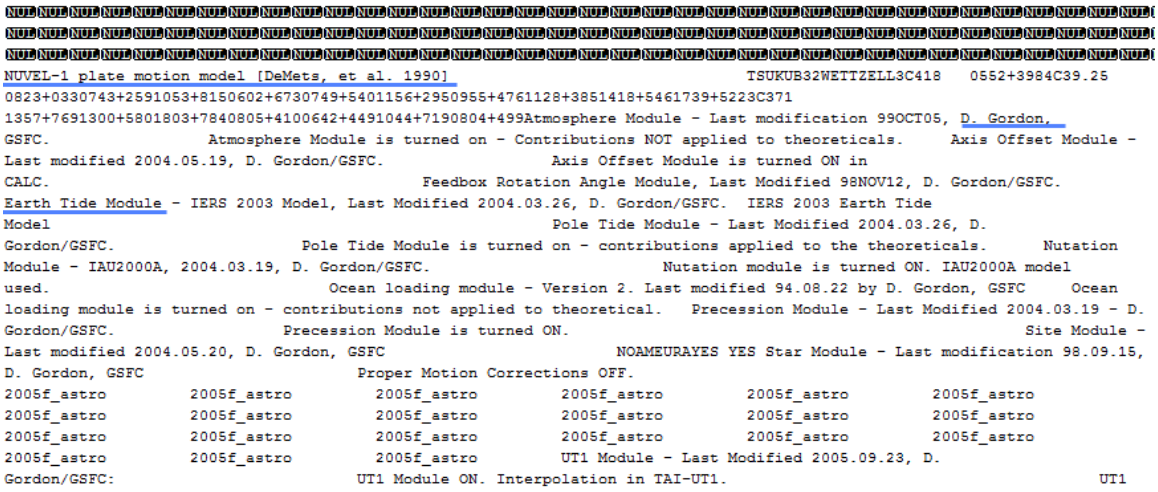


Fig. 21. Назначение файла и фамилия владельца при открытии в текстовом виде

4.6 Другие устройства

По содержимому интерфейса и его исходного кода можно определить, к какому конкретно устройству вы через него подключаетесь. Стандартные порты отличаются не только для разных производителей, но и для разных моделей одного и того же девайса. С развитием Internet of things можно встретить в сети как бытовые устройства, более или менее сложные (вплоть до интерфейсов «умных домов»), так и промышленные или относящиеся к городскому пространству, общественной безопасности. Так, в апреле 2018 была обнаружена открытая панель управления гондолой подъёмника в Австрии. Допустимость какого-либо взаимодействия с подобными IoT-объектами является одним из предметов этической дискуссии в среде нетсталкеров. Очевидно, что действия над интерфейсом без предварительного его анализа могут привести к последствиям, которых не желали бы не только владельцы, но и вы сами.

4.6.1 Анализ баннеров

Подразумеваются специальные заголовки, выдаваемые, например, при сканировании утилитой nmap. Расположенный на сервере протокол отвечает соответственно своим настройкам. Иногда это позволяет распознать конкретное устройство или сервис, но встречаются и неизвестные ответы. Они требуют пристального анализа, так как могут свидетельствовать о работе чего-то неизвестного. nmap выдаст сырой выхлоп, если не сможет определить его владельца самостоятельно: так называемый отпечаток (fingerprint), содержащий фрагмент сырого ответа сервера[385].

Баннер-граббинг - техника получения информации о хосте, позволяющая иден-

[385]https://isc.sans.edu/forums/diary/nmap+Service+Fingerprint/24972/

тифицировать [386] сервисы на портах для дальнейшего взаимодействия. Собранное затем используется для фильтрации результатов, то есть предварительной каталогизации выдачи. Условно делится на активный и пассивный.

Активный баннер-граббинг подразумевает отправку TCP (и не только) пакетов, подразумевая прямое взаимодействие исследователя с хостом, а значит и возможность установить IP-адрес, с которого происходит отправка. IDS заточены под обнаружение таких действий, так что если вы не уверены в том, что вам нужно просто забрать баннер сервиса - лучше проксировать трафик или использовать пассивный баннер граббинг. Для активного баннер-граббинга можно использовать как простые утилиты вроде telnet, nc, curl и wget, так и сканеры вроде masscan и zmap. Однако лучшим решением признанно считается nmap из-за его флагов -A и -sV и базы отпечатков, способых идентифицировать службы и сервисы в зависимости от порта.

Пассивный баннер-граббинг предполагает использование сервисов третьих лиц для извлечения баннера из хоста. Для таких целей отлично подходят дорки поисковиков, Shodan[387], Censys[388] и Zoomeye[389].

Напомним, что владелец сервера может поместить любой сервис на абсолютно любой порт, что делает угадывание сервиса по номеру порта бесполезным. Также следует упомянуть, что без баннер-граббинга нельзя узнать точную версию сервиса, а иногда на одном порту могут располагаться несколько сервисов. Таким образом, баннер-граббинг незаменим для изучения сетевых находок.

4.7 Файлы

Вы могли получить их с файлового сервера, обменника, соцсети, сайта-коллекции или спутника. Анализ, помимо очевидного смыслового, часто сводится к выявлению первоисточника, а иногда и проверке достоверности. Кроме того, в виде архивов, аудио- и видеофайлов, имитаций документов могут вбрасываться загадки или «послания в никуда». Ознакомьтесь с главой «Стеганография», а также с понятием **метаданных**: многие форматы подразумевают встраивание дополнительной информации про обстоятельства создания файла. Большинство пользователей оставляют её нетронутой, что позволяет узнать больше. Сравнительно унифицированный список параметров, полезный и для автоматизации анализа, называется Дублинским ядром[390]. Мета может быть удалена либо изменена, и создатели квестов пользуются этим, вставляя подсказки. Помните, что ушлые творцы фейков могут поменять время в своей ОС,

[386] https://nmap.org/man/ru/man-version-detection.html
[387] https://www.shodan.io
[388] https://censys.io/ipv4
[389] https://www.zoomeye.org
[390] https://ru.wikipedia.org/wiki/Дублинское_ядро

чтобы имитировать древность или сверхъестественное происхождение документа.

4.8 Изображения

Фотографии и картинки стоят особняком в анализе. Метаданные EXIF могут выдать если не место, где щёлкнул затвор фотоаппарата или телефона, снабжённого GPS, то хотя бы его модель и другие параметры. Для просмотра можно использовать онлайн-сервисы, вроде Jeffrey's Exif Viewer. Также этот вид метаданных может порождаться сканерами и некоторыми графическими редакторами. Даты на исходном устройстве могли быть настроены неверно, отсюда может появиться неествественный год или время суток. Кроме того, ложные данные могут быть вписаны вручную, поскольку никак не шифруются. Помимо геолокации можно, например, оценить реальные размеры объекта, если заполнен параметр Subject Distance. IPTC (International Press Telecommunications Council) может хранить копирайт, теги и другие сведения, важные для лицензирования. XMP (Extensible Metadata Platform) – порождаются Adobe Lightroom, создавая дополнительный файл.

На сегодня ряд соцсетей, включая ВК, удаляет метаданные залитых снимков. Но определить локацию можно и приёмами OSINT, как показано в этой статье[391]. Рекомендуется сначала выявить «глобальные» подсказки, то есть те объекты, которые укажут на общее местоположение. Затем «местные» детали позволят узнать конкретику. Форматы дорожных знаков, номеров транспорта, вывесок могут указать страну или хотя бы часть света. То же касается архитектуры зданий, а самые высокие из них, что видны на снимке, могут примерно указать место. Угол наклона поможет определить этажность, если фото сделано с высоты.

Те же приёмы работают и для видеороликов.

Для анализа достоверности фото также есть много приёмов. Сервис FotoForensics[392] анализирует ELA (Error Level Analysis), степень пережатия для JPEG, скрытые пиксели. Если при ELA какая-то область изображения светлее другой того же цвета, то ее могли редактировать. Многократно пересохранённое изображение будет содержать характерные шумы. На смонтированном изображении вставленный объект при ELA будет значительно ярче, чем другие области. Также ярче будут области с высоким контрастом (текст, линия, контур). Наконец, помимо стеганографических сообщений, картинка может содержать RARJPEG, или встроенный в изображение архив. Он открывается простым переименованием расширения в .rar. Не обязательно проверять большие массивы картинок вручную: можно создать скрипт, проверяющий наличие соответствующей сигнатуры, как, например, вот этот фильтр в Rghost-граббере.

[391] https://telegra.ph/Quiztime-12092019-Gde-ehto-mesto-Globalnye-i-mestnye-identifikatory-09-28
[392] https://fotoforensics.com/

Fig. 22. Форматы номерных знаков

Так называемые наноборды используют картинки, загружаемые на обычные имиджборды, как транспорт своих постов.

4.9 Анализ документов

Цель - определить степень достоверности и важности документа и его содержимого. Рассекреченные и слитые документы о различных аномальных или малоизвестных явлениях становятся предметом спекуляций и фальсификаций. При анализе нужно обращать внимание на соблюдение всех норм и другие детали, например, анахронизмы. Так, в документах, якобы принадлежащих КГБ и датированных 1983-м обнаружились упоминания процессора Pentium 286 и «оператора ПК», а также нефор-

матные отступы на страницах.

Грифы и особенности по России и СССР[393]:

- ДСП (для служебного пользования). Несекретные сведения регулируются так же, как и U//FOUO в США. Стандартно пометка ставится в верхнем правом углу, с проставлением номера экземпляра. Простейший запрос по поиску: Для служебного пользования "Экз №". Если ограничение наложено только на приложение, то пометка дополняется словами "при наличии приложения N".

Fig. 23. Пример содержащего пометку документа

- КТ (коммерческая тайна) - такая информация, которая может при раскрытии дать кому-то коммерческую выгоду при использовании. Должно быть обязательное указание юридического лица, которому она принадлежит. Можно составлять запросы, указывая название организации: Коммерческая тайна ООО такого-то.
- Конфиденциально - Формально, к конфиденциальной информации относятся персональные данные и многие другие сведения, разглашение которых должно

[393]https://telegra.ph/O-sekretnyh-dokumentah-Rossiya-02-27

регулироваться. На деле, он используется довольно свободно: простым запросом *конфиденциально "экз №"filetype:pdf* можно найти множество интересных примеров.

- Секретные документы. настоящее время в России имеется три грифа: Секретно - третья форма допуска, можно выезжать за границу; совершенно секретно - вторая форма допуска; особой важности - первая форма допуска.

Грифы и особенности по США[394]:

Классификация секретной информации и её регулирование в данной стране сложны за счёт наличия множества очень разных спецслужб с богатой и запутанной историей.

Отличительные особенности, без которых достоверность не подтверждается:

- общая степень секретности означается сверху и снизу первой страницы;

- если имеется больше одной страницы, отметка о секретности должна быть сверху и снизу на: передней и задней обложке снаружи, на титульном листе, на первой странице;

- внутренние листы промаркированы сверху и снизу;

- на каждом из них степень секретности должна быть равна общей или соответствовать наивысшей секретности параграфа на этой странице;

- каждый параграф отмечен своим грифом секретности.

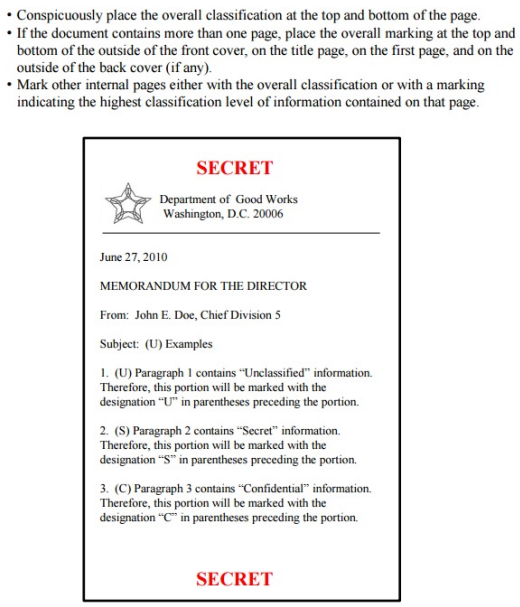
Общий перечень ссылок и важных маркеров с примерами вы найдёте здесь, далее несколько важнейших.

- **TOP SECRET** - совершенно секретно, особой важности (все четыре слова имеют значение): высший уровень секретности, в случае раскрытия данная информация может представлять угрозу национальной безопасности. В качестве маркировки параграфа сокращается до TS Ниже по уровню располагается **Secret** - совершенно секретно (именно два слова) и **Confidential** - секретно.

- **FVEY** - группа Five Eyes («Пять глаз»), включает в себя 5 англоговорящих стран: Австралию, Канаду, Великобританию, Новую Зеландию и США, между которыми подписано «Соглашение о радиотехнической разведывательной деятельности Великобритания – США»

- **Declassified in Part** - Sanitized Cope Approved for Release. Размещается сверху и снизу. Это означает, что часть документа изъята. Рядом с белыми четырёхугольниками цензуры должна стоять маркировка причины. Например, 50X1 - изъятие сроком на 50 лет по причине 1 - конфиденциальность личности источника и упоминаемых людей. 50X1-HUM - на 50 лет по причине №1 «конфиденциальности личности источника» (HUM - от Human).

[394]https://telegra.ph/O-sekretnyh-dokumentah-01-13


• Conspicuously place the overall classification at the top and bottom of the page.
• If the document contains more than one page, place the overall marking at the top and bottom of the outside of the front cover, on the title page, on the first page, and on the outside of the back cover (if any).
• Mark other internal pages either with the overall classification or with a marking indicating the highest classification level of information contained on that page.

SECRET

Department of Good Works
Washington, D.C. 20006

June 27, 2010

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

Subject: (U) Examples

1. (U) Paragraph 1 contains "Unclassified" information. Therefore, this portion will be marked with the designation "U" in parentheses preceding the portion.

2. (S) Paragraph 2 contains "Secret" information. Therefore, this portion will be marked with the designation "S" in parentheses preceding the portion.

3. (C) Paragraph 3 contains "Confidential" information. Therefore, this portion will be marked with the designation "C" in parentheses preceding the portion.

SECRET

Fig. 24. Скриншот из руководства АНБ по маркировке секретных документов

- **Distribution Statement** - пометка об ограничении распространении (не секретность), используется Министерством Обороны США (DoD, Department of Defense) для контроля доступа к документам. Используются литеры от A до F, также ранее использовалась X, заменённая сейчас на C.

Раскрытие документов по давности обнуляет пометки о секретности типа TOP SECRET, DESTRUCTION NOTICE - обращайте внимание на даты. Что до источников секретных документов, то достаточно воспользоваться ссылками из этой статьи или просто использовать в Google дорк вида *site:nsa.gov "SECRET "Distribution statement E"inurl:mil* и так далее. И одно из простых правил: если не можете понять предназначение/смысл термина - гуглите не только его, но и все соседние термины, находите похожие документы и анализируйте их.

Литература

[1] Проект «CASCA», Расширенное руководство по онлайн-камерам v0.3.1, 2018 г.

5. ХРАНЕНИЕ И СИСТЕМАТИЗАЦИЯ

По мере поступления новой информации приходится возвращаться к старой, но время идёт, и она теряется или изменяется. Настройки приватности меняются, видео удаляются, сайты блокируют, ваша цель тонет в море результатов поиска, а очевидцы не хотят больше с вами говорить. Эти потери между полным объёмом материалов и

тем, что попадёт в отчёт, называются **эрозией информации**, а потеря объекта, на который ведёт гиперссылка - разложением ссылки[395]. Опыт архивариусов[396] показывает, что вебсайт в среднем действует от 44 до 100 дней. Важно уметь резервно копировать полезные динамические страницы, т.к. профили в соцсетях, свежие новости и файлы с файлообменников удаляются регулярно. Далее приведены наиболее эффективные техники архивации — структуризации прежде разрозненных данных в целях упрощения поиска, сбора статистики и выявления закономерностей.

5.1 Методы архивации в целом

Зачастую веб-страницы закачиваются горячими клавишами Ctrl+S или пунктом «Сохранить как» в выпадающем меню ПКМ. Люди выбирают меж компактным .html-файлом без внешних ресурсов и «полным сохранением» .htm(l)-документа и папки со всем, на что ссылается исходный код. Оба способа по-своему неудобны и давно заменены MHTML, пакующим изображения, flash-анимации, мультимедиа и скрипты (JS, PHP, Java) в один .mht-файл. В более старых версиях Chrome он скрыт среди настроек (chrome://flags), аналогично в Opera, перешедшей на движок Chromium:

opera://flags/
далее включить
#save-page-as-mhtml

Firefox требует установки плагина[397]. Кроме того, «Огнелису» характерен MAFF[398] — единственный формат, хранящий метаданные (масштаб, полосу прокрутки, дату сохранения и адрес первоисточника) и прочие ресурсы в обычном zip-архиве. Вы также можете скринить страницы ShareX[399] или конвертировать в .pdf расширениями на Firefox[400] и Chrome[401] или в онлайне[402]. Ещё дальше идёт программа wallabag[403], записывающая ход просмотра страниц, что может быть полезно для архивации прохождения ARG или демонстрации нет-арта.

Если вы не сортируете бэкапы, и они актуальны лишь во время просмотра без интернета, то лучше включить оффлайновый режим, подгружающий уже посещённые страницы из очищаемого браузерного кэша, который есть и у Chrome[404], и у

[395] https://en.wikipedia.org/wiki/Link_rot
[396] http://www.digitalpreservation.gov/personalarchiving/
[397] https://addons.mozilla.org/en-US/firefox/addon/mozilla-archive-format
[398] https://addons.mozilla.org/ru/firefox/addon/mozilla-archive-format/
[399] https://getsharex.com
[400] https://addons.mozilla.org/en-US/firefox/addon/webtopdf/
[401] https://chrome.google.com/webstore/detail/save-as-pdf/kpdjmbiefanbdgnkcikhllpmjnnllbbc
[402] https://www.web2pdfconvert.com/
[403] https://wallabag.org/en
[404] http://web.archive.org/web/20160729200243/http://www.howtogeek.com/263577/how-to-enable-offline-browsing-in-chrome/

Firefox[405]. Вы можете загружать savefrom.net-помощником медиафайлы (аудио, видео и фото; их альбомы и плейлисты) с популярных хостингов: ВКонтакте, YouTube, Vimeo и т.д. Перечисленные средства непрактичны для создания локальных копий вебсайтов (зеркалирования) и полного или выборочного древа их файловой иерархии с помощью портативных веб-краулеров. Эту задачу решают менеджеры закачек типа бесплатных HTTrack[406] и BackStreet Browser[407] или проприетарных WebCloner[408] и Offline Explorer[409], рецензированных путеводителем[410] в 2008. Пользователи Linux уже владеют консольным инструментом wget[411] и многофункциональным cURL[412], чей трафик можно торифицировать для сохранения .onion вебсайтов.

HTTrack способен не только на зеркалирование сайтов в сети Интернено и в сетях Tor и I2P, для чего следуйте мануалу[413].

Однако собранное мигом исчезнет, когда выйдет из строя носитель информации. Читаемые кардридером карты памяти (форматов Secure Digital, Memory Stick и XQD), встраиваемые не только в ПК, но и в фотоаппараты, приставки и телефоны, совместно с USB-накопителями средней стоимости (производителей Kingston, SanDisk и Transcend) вытеснили CD/DVD компакт-диски, наименее надежные в эксплуатации и страдавшие даже от прикосновения пальцев. Выдерживая до 1500 подключений и 5000 циклов перезаписи, флешки служат 7-8 лет в крайне хороших условиях хранения: в сухости, при температуре 10-43 °C и подальше от магнитных полей, механических повреждений и электростатического разряда, что обычно невыполнимо. Согласно сравнению[414] с SSD, те же советы относятся к HDD дискам, менее стойким из-за подвижных элементов конструкции, но в 3-4 раза более выгодным по соотношению цены и объёма. Они лидируют в записи тяжёлых файлов (архивов, фильмов, игр...) на 1gb, а SSD — в быстром запуске ОС, приложений и всего мелкого.

Не пугайтесь логических неисправностей служебных таблиц, когда с преждевременным извлечением устройства из разъёма данные остаются в целости, но накопитель распознаётся пустым. Это лечится массой программ[415]. Опаснее поломка контроллера, исправляемая прочтением данных с чипа в сервис-центре или перепро-

[405] http://web.archive.org/web/20161004104501/http://www.howtogeek.com/263854/how-to-enable-offline-browsing-in-firefox/
[406] http://www.httrack.com/
[407] http://www.spadixbd.com/backstreet/index.htm
[408] https://download.cnet.com/s/webcloner/
[409] https://metaproducts.com/products/offline-explorer-enterprise
[410] https://www.ixbt.com/soft/offline-browsers-6.shtml
[411] https://ru.wikipedia.org/wiki/Wget
[412] http://osxh.ru/terminal/command/curl
[413] http://netwhood.online/2018/10/10/site-mirroring/
[414] https://www.iphones.ru/iNotes/599758
[415] https://www.lifewire.com/free-data-recovery-software-tools-2622893

шивкой (файлы уничтожаются) на дому. Для повышения производительности или отказоустойчивости вы можете объединить[416] жёсткие диски (желательно идентичные по размеру, фирме и серии) в RAID-массив одного из двух типов (больше — реже), выполняющих разные функции. RAID 0 (Striping) содержит 2-4 диска, которые быстрее обрабатывают записываемую по блокам информацию, в результате чего байты файлов распределяются по нескольким дискам, и при смерти одного из них сведения сотрутся. RAID 1 (Mirroring) отличается стабильностью в ущерб объёму и скорости: второй диск не редактируется, но заполняется полной копией содержимого первого, и если оба не выйдут из строя, то данные не исчезнут.

Проблему недолговечности предвидели и активисты из Internet Archive[417], электронной библиотеки, сохраняющей цифровые культурно-исторические ценности. Её пополняемая посетителями и ботами база содержит 15 петабайт данных и индексирует всё, что не ограничено правообладателями или robots.txt, а подпроект WaybackMachine[418] архивирует вебсайты по датам. Вы можете предлагать туда ресурсы, и если какой-то сервис с прежним видом недоступен, проверьте его адрес в веб-архиве или на похожих «временных капсулах». Например, archive.is по запросу захватывает состояние любых, в т.ч. динамических (Google Maps, Twitter...) страниц, учитывая оформление и скрипты. WebCite[419] предназначен для академического цитирования и сохраняет весь контент, в т.ч. документы и картинки полного разрешения, сокращая ссылки. Peeep.us подходит только для личного пользования, умеет бэкапить ресурсы с базовой авторизацией, требует гугл-входа и добавляет заархивированное вами в удобный приватный список. Эти сервисы, как и некоторые переводчики, позволяют обходить интернет-блокировки. Если вам не удается восстановить копии через веб-архивы, поищите их в кэше поисковиков[420] или на узконаправленных хранилищах типа Архивача[421] и a2ch.ru под имиджборды, которые я проверял, работая над /sn/ archives[422].

Вслед за архивацией сортируют находки по папкам. Бездумное их нагромождение усложняет навигацию. Желательно заготовить каталоги по интересующим темам заранее, пополняя их в процессе загрузки файлов с неизменяемыми именами, полезными при определении источников. Вы можете добавить к названиям короткие префиксы, упрощающие опознание, т.к. тэгов нет в стандартных проводниках, заменяемых, впрочем, бесплатным Total Commander[423] или платным XYplorer[424]. Полезны и органайзеры рабочего пространства: tagspaces.org создаёт текстовые заметки,

[416] https://compress.ru/article.aspx?id=21065
[417] http://archive.org/
[418] http://web.archive.org/
[419] https://webcitation.org/
[420] http://www.thesearchenginelist.com/
[421] https://arhivach.ng/
[422] https://mrakopedia.org/wiki/Каталог_тредов
[423] https://www.ghisler.com/
[424] https://www.xyplorer.com/

помечает файлы для гибкого поиска и менеджит веб-страницы; trello.com помогает кооперироваться и управлять задачами, проектами и расследованиями; а вики-движок tiddlywiki.com поднимает энциклопедию на сервере или локалке. Ссылки же можно держать как привычными закладками браузера, так и расширениями типа diigo.com и evernote.com, или социальной площадкой обмена: Delicious и checkitlink.com. Обсуждением оптимальных стратегий именования и размещения накоплений занимается сообщество datahoarder'ов[425].

Когда от анализа зацепок распухает голова, мысли упорядочивают mindmaps — визуальные схемы связей от общего к частному меж объектами и идеями, представленными звеньями концептуального веера[426] или паутины. Она знакома вам по детективным фильмам и их «evidence boards», доскам, на которых полицейские соединяют перекрещивающимися линиями доказательства по делу. Карты мыслей применяются в областях конспектирования, записи заметок, мозгового штурма, планирования, разработки, обучения, и, важнее всего, при структуризации знания. Отображая ход мышления стимуляцией ассоциаций, они позволяют осознать незамеченную закономерность, деталь или связь, и избежать[427] статистических ошибок. Их можно не только создавать решениями студентов[428] и компаний[429] (или графическими редакторами), но и нетсталкерить: так, результаты парсинга публичных диаграмм wisemapping.com залиты в канал[430] телеграма.

Когда нужно сэкономить ресурсы, минимизируйте занимаемое ими на носителе место. Не бойтесь сжатия с потерями, если вы не сужаете компоненты программ или текстовые документы: без ненужного изменения размеров дефекты будут незаметны глазу. Сравните картинку в двух форматах экспорта GIMP: .png с максимальной степенью компрессии весит целых 2мб, а .jpg с качеством в 100% — лишь 900кб, и чем ниже, тем меньше: вплоть до 300кб при 90% без видимых искажений. Объёмные папки и файлы хорошо архивирует 7-zip[431], имеющий 24 позицию в общем рейтинге[432], уступая консольному PAQ8[433] и проприетарному WinRK[434]. Реализованный им .7z предлагает на 4-25% лучшее сжатие, чем .zip, и столь же долгую упаковку, за 10 минут вдвое уменьшая папку весом в 1 ГБ. Обычные аудиозаписи, не требующие опознания и дешифровки, в отличие от телеметрии или сигналов спутников и радиочастот, стоит содержать не на .wav, а в .mp3, значительно сокращающем трек: например,

[425] https://www.reddit.com/r/DataHoarder/
[426] http://prismotrov.com/idea-generation-method-conceptual-fan/
[427] http://best-stat.ru/oshibki-v-statistike-i-v-zhizni.html
[428] https://www.lifehack.org/articles/featured/11-free-mind-mapping-applications-web-services.html
[429] https://stratabeat.com/10-effective-mind-mapping-software-tools/
[430] https://t.me/testwise
[431] https://www.7-zip.org/
[432] https://maximumcompression.com/data/summary_sf.php
[433] http://mattmahoney.net/dc/
[434] http://winrk.co.uk/

с 34 мб формата .m4a до 5 мб при неизменном 320-ом битрейте. Экспериментируйте, выбирая подходящие соотношения режимов вручную или онлайн-конвертерами.

5.2 Архивация FTP-серверов

Сохранение с помощью FileZilla возможно простым перетаскиванием всего или только выбранного содержимого сервера в окошко локального диска. Но сначала создайте у себя папку под этот материал, нажав правой кнопкой и выбрав «Создать каталог и открыть его». Совет по наименованию: вставьте в название адрес фтпшника и добавьте пару слов, по которым вы примерно вспомните содержимое.

Хранить адреса и быстро подключаться к ним помогает ещё одно окно Файлзиллы: Менеджер Сайтов (Ctrl+S для вызова). Помимо IP и вашего названия он сбережёт тип входа и шифрования, что важно для подключения к узлам без TLS. Группировать записи позволят каталоги.

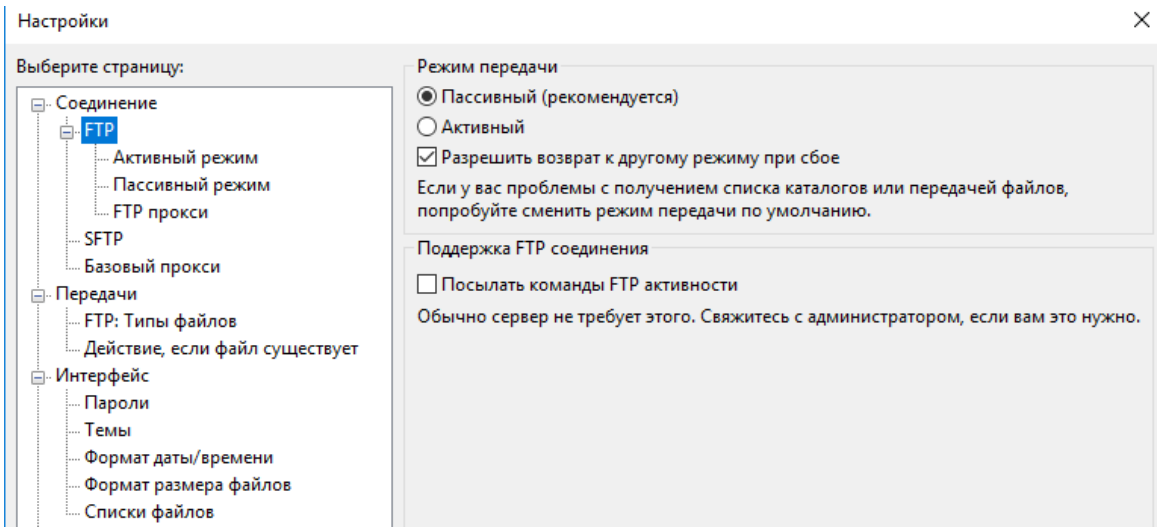


Fig. 25. Работа с Менеджером сайтов

Некоторые сервера обновляют содержимое, поэтому важные для вас узлы стоит мониторить регулярно. Вы можете выкачивать только недостающие в текущем бекапе файлы, для чего есть галочка (название). Не обязательно вытаскивать всё за один раз, так как прерванную задачу можно завершить после следующего запуска Filezilla, запустив её вручную из списка под навигатором.

5.3 Архивация камер

Как вы уже знаете, существует множество производителей и прошивок камер. Также есть разные форматы стримов, что затрудняет перехват и запись разработчикам вроде Проекта Casca. Таким образом, остаётся два способа сохранять видео: скачать его из архивов самой камеры или захватить с экрана во время трансляции с помощью Bandicam. Программы просмотра, такие, как SmartPSS для вендора Dahua и iVMS для Hikvision, дают доступ к хранилищу записей. В ряде случаев это возможно и через веб-интерфейс.

5.3.1 Скачивание в SmartPSS

Видеозаписи с камер хранятся в непережатом виде и занимают огромное место. Выкачка даже часового ролика может занять полдня. Поэтому обычно приходится вытаскивать только избранные отрезки. Кроме того, вы можете брать скриншоты.
Предполагается, что цель уже добавлена в Devices. Войдите в раздел Playback. Отметьте галочкой нужную вам камеру из левого меню и перетащите её в окошко просмотра. Когда процесс поиска (Searching) в нижнем левом углу остановится, вам станет доступна полоса перемещения по видео. Найдя интересный фрагмент, подвигайтесь по полосе и определите его начало и завершение. Затем отметьте эти точки с помощью инструмента «ножниц». Выбрав диапазон, нажмите «ножинцы» ещё раз. Программа предложит выбрать путь сохранения и формат. Затем нажмите пиктограмму скачивания слева от ножниц.

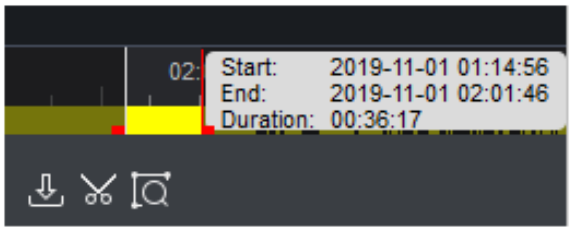


Fig. 26. Выделение фрагмента видео для скачивания

Полученное видео можно пережимать и конвертировать в другие форматы ради экономии места и быстрой удобной передачи по сети.
Скриншоты в этом режиме берутся так же, как при просмотре камеры в реальном времени: кнопкой «фотоаппарат», появляющейся при наведении на экран просмотра.

5.4 Написание отчётов

Завершая рассмотрение своего сетевого улова, стоит оставить после себя и описание наиболее интересных образцов, рассказав, чем они ценны или необычны, что

раскрывают и куда приводят. Либо, если вы занимаетесь нетсталкингом в команде, наоборот – короткие отписки о бесполезности найденного. При коллективном разборе материалов важно отмечать все пройденные объекты, чтобы другие уже не заглядывали в них. Отчёты служат для как можно более полной и понятной фиксации трудов по анализу и архивированию. Нет и не должно быть единого для всего нетсталкинга формата их написания, поэтому далее приведены лишь некоторые идеи по качественному наполнению. Отдельные команды могут вводить свои шаблоны, которым должны следовать участники: например, требовать указание категории находки в соответствии со внутренней классификацией.

Простейший вид отчёта – описание своими словами просмотренной находки. Всегда следует включать адрес или способ доступа, название или заголовок (если есть). Дальнейший текст будет варьироваться в зависимости от типа ресурса. При наличии в ней визуальных материалов или медиа логично вставить значимые скриншоты или указания на файлы, заблаговременно внесённые в ваш архив. Прямые ссылки часто бесполезны по указанным ранее причинам.

Структура текста может соответствовать шагам вашего сёрфинга и анализа. Не пренебрегайте как технической информацией (найденные на узле протоколы, какие-либо сложности при доступе к ресурсу или при прочтении медиаконтента), так и выкладкой своих выводов. Фиксируйте промежуточные переходы и пути получения данных, а также ничего не давшие попытки. Это поможет другим научиться у вас или же найти пропущенное звено и дополнить ваше расследование. Удобно делать это по мере продвижения в поисках: пройти шаг, записать его результат, перейти к следующему. Другой вариант: последовательное описание элементов (разделов сайта, директорий сервера, элементов меню программы, секций файла и т.п.).

Итак, хороший отчёт содержит:

- Информацию о координатах находки, чтобы можно было её посетить, или источник обнаружения (видеохостинг, соцсеть, файлообменник, f2f-сеть и т.п.)
- Скриншот на случай, если находка окажется недоступна
- Описание того, что содержит или делает находка
- Перечень дополнительной информации, полученной анализом. Другие открытые порты и их содержимое, если это веб-узел;
- Вывод о целях создания. Можете добавить своё мнение или эмоции.

Памятуя об эстетическом факторе, нетсталкеры создают и **художественные описания** своих находок. Особенно это распространено относительно камер и частных файловых архивов, поскольку они чаще всего становятся источником разнообразных впечатлений.

Майндкарта сама по себе может стать одним из вариантов отчёта, если не требует

дополнительных пояснений. Это особенно актуально для отображения хода игр в альтернативной реальности.
В случае обнаружения ценного текста на иностранном языке отчёт заменяется или дополняется переводом. Не пользуйтесь услугами Google Translate или его аналогов для прогонки всего материала. Странно звучащие при дословном переводе фразы ищите в сети: это может быть сленг или устойчивое выражение, уже имеющее корректный русскоязычный аналог или хотя бы смысловое пояснение.
В заключение скажем, что в случае ценной находки неполный, с прорехами, со стилистическими или грамматическими ошибками отчёт предпочтительнее его полного отсутствия.

5.4.1 Отчёты об IP-камерах

Порой утверждают, будто при просмотре прозвучал голос, хотя аппарат был без микрофона. Избегая заблуждений, изучите подробности о «железе» и соотнесите функционал модели с показаниями. Сперва укажите вендора, т.е. производящую и распространяющую продукцию компанию: AXIS, Panasonic, MOBOTIX и т.п, а затем ID серии: WVC54G, SNC-RZ25, TV-IP201. Эти сведения находятся на странице просмотра или строке состояния, куда выводится время: зачастую ошибочое, т.к. не всякий владелец синхронизирует NTP-серверы. В последний черёд перечислите функции: поддержку Audio I/O, PTZ, Presets (предустановленные значения параметров PTZ), Stream, Backup, Sensors (датчики движения, звука и тепла).

Сориентировавшись, соберите материалы: по 2 снимка ночью и днём, пятиминутный образец видео и, в случае поддержки, звука. Определите страну и город по whois, узнайте[435] часовой пояс и разметьте по нему лучшее время для документирования. Выделите место под круглосуточное наблюдение, если камера того стоит или вызывает вопросы. Убирая её в долгий ящик, прикрепите дату последней проверки, т.к. статус трансляций меняется. Они могут быть: активны (доступны для просмотра в том же виде), неактивны (отключены, защищены или сбоят; причину лучше уточнить) и заменены (технически работают, но точка установки отлична от прошлой).

6. БЕЗОПАСНОСТЬ И КРИПТОГРАФИЯ

Порой активность в нетсталкинге привлекает злоумышленников и других исследователей, а неосторожность — ещё и власти. Даже если вам нечего скрывать сейчас, секреты могут появиться со временем. Известно, что нетсталкеры находили анонимные FTP с записями звонков российского аэропорта и переговоров по внутренней связи; результатами криминалистических экспертиз и сканами ордеров на

[435] https://www.timeanddate.com/worldclock/

обыск или арест. Загрузка, хранение и обмен данными требуют защитных мер, т.к. по некомпетентности можно деанонимизировать себя и своих коллег. В этой главе вы познакомитесь с практиками безопасной и анонимной работы в Интернете, но знайте, что они не универсальны и не ультимативны. Даже экспертам по ИБ[436] не удаётся разом исключить все возможные угрозы, поэтому они работают с их моделированием в конкретных условиях и с анализом рисков, задавая себе вопросы о том, что, от кого и зачем нужно защищать.

6.1 Обход блокировок

Во многих государствах, в том числе на территории СНГ, действуют акты о цензуре[437], ограничивающие свободу слова и доступ к «противоправной» информации. Зачастую из-за одной страницы вебсайты блокируются не только по домену, но и по IP-адресу, и если у провайдера нет денег на DPI[438], то другие ресурсы с того же хоста могут быть ограничены за компанию. Недавние законы[439] о регулировании анонимайзеров и мессенджеров зародили сомнения о перспективности существующих средств связи. К счастью, документы имеют лазейки: организатор мессенджера идентифицирует пользователей по номеру телефона, поэтому под определение не попадают протоколы IRC и XMPP и встроенные в приложения чаты. В отличие от Signal[440] и Tox[441], по умолчанию сообщения через них не шифруются, что исправляется установкой PGP/OTR защиты, описанной в главе 6.4. В случае запрета удобных Telegram и Discord ещё останутся надёжные резервные коммуникации.
Сложнее обстоит дело с анонимностью. Роскомнадзор обязуется заносить в реестр[442] средства обхода интернет-блокировок (в т.ч. упоминающие их поисковые системы и другие источники информации), которые откажутся сотрудничать и ограничивать вебсайты чёрного списка. Запрет таких сервисов (VPN, SOCKS4/5 Proxy) возможен двумя путями: по IP-адресу или по типу трафика. Первый случай привычен: блокируются адреса серверов, оформляющих покупку услуг и их регистрацию. Владельцы не приобретут новых клиентов и потеряют долю старых, но технологии продолжат работать и активироваться через третьих лиц. Так, никуда не денутся свежие версии оверлейных сетей. Второй же вариант пока нереализуем, т.к. требует установки дорогостоящего DPI-оборудования от всех операторов связи, как это было с «Золотым щитом»[443] в Китае.
Далее описаны охватываемые законом технологии (Tor и I2P, уже рассмотренные ра-

[436] https://ru.wikipedia.org/wiki/Информационная_безопасность
[437] http://rebrand.ly/ac-arguments
[438] https://ru.wikipedia.org/wiki/Deep_packet_inspection
[439] https://meduza.io/news/2017/07/21/prinyaty-zakony-o-messendzherah-i-zaprete-anonimayzerov
[440] http://whispersystems.org/
[441] https://tox.chat/
[442] https://reestr.rublacklist.net/
[443] https://ru.wikipedia.org/wiki/Золотой_щит

нее, не учитываются) и меры противодействия влиянию на них.
Прежде всего, запрещаются прокси-серверы — посредники, которые перенаправляют соединения пользователя и делятся на 3 категории:

- HTTP: пропускают только веб-трафик и уведомляют адресата о применении прокси; устарели и наименее безопасны.
- SOCKS: передают сетевой трафик всех протоколов (HTTP, FTP, TELNET, SSH...), ничего не сообщая получателю; практичны и скупаются на чёрных рынках.
- CGI: т.н. «анонимайзеры», сервисы типа HideMyAss![444] с формами ввода ресурсов, которые открываются на странице через CGI в адресной строке; наиболее популярны и просты в эксплуатации.

Бесплатные прокси общедоступны: HideMy.name[445] и Free Proxy List[446] суммарно содержат около 400 серверов, а на Пастебин ежемесячно загружаются дампы[447] по 1000 с лишним ссылок. Чтобы не настраивать их для каждого приложения вручную, применяются соксификаторы: Proxifier[448] или другие программы из перечня[449]. Помните, что весь трафик прокси-серверов, если он не передан по https, могут прослушивать сисадмины, и вам придётся довериться им. К счастью, число возможных прокси-адресов так высоко, что РКН не удастся отыскать и внести в чёрный список каждый из них.
Поэтому незачем беспокоиться и за VPN (виртуальные частные сети) — защищённые каналы связи, зашифрованные «туннели», теория[450] и разновидности[451] которых простым языком описаны Лабораторией Касперского. Они так распространены, что функция подключения к ним интегрирована во многие телефоны на базе Android и не требует загрузки ПО. Бесплатным VPN сложно доверять: объём их трафика и интернет-скорость ограничены, а прибыль зачастую добывается обманом пользователей, как это было с Hola[452]. При выборе коммерческого VPN-сервиса и чтении договора узнайте: 1) хранятся ли (если да, то как долго) журналы с соотношением IP-адреса, метки времени и прочих идентификаторов; 2) юрисдикцию компании и условия выдачи персональных данных 3-ей стороне; 3) принимается ли оплата криптовалютами (если нет, то лучше отказаться от услуг). Похожие вопросы были заданы международным VPN-провайдерам в опросе[453] 2014 года. Вы также можете настро-

[444] https://hidemyass.com/ru-ru/proxy
[445] http://hidemy.name/ru/proxy-list
[446] https://free-proxy-list.net/
[447] https://pastebin.com/search?q=proxy+list
[448] http://proxifier.com/
[449] https://en.everybodywiki.com/Comparison_of_proxifiers
[450] https://blog.kaspersky.ru/vpn-explained/10635
[451] https://blog.kaspersky.ru/vpn-implementations/11156
[452] https://www.theverge.com/2015/5/29/8685251/hola-vpn-botnet-selling-users-bandwidth
[453] https://torrentfreak.com/vpn-services-that-take-your-anonymity-seriously-2013-edition/

ить свой VPN, сканируя иностранные роутеры, перебирая заводские пароли и следуя указаниям гайдов[454].

6.2 Ограничение слежки

Пусть за нами и следят с рождения, и все наши личные сведения хранятся органами на бумаге и в цифре, не так просто связать сетевую активность человека с его личностью. Однако из-за наивности люди часто разглашают конфиденциальную информацию третьим лицам, благодаря чему работает доксинг — совокупность методов добычи через социальную инженерию, изучения и публикации персональных данных для шантажа, хакинга и фишинга (например, ответа на «секретные вопросы»), активизма.
Чтобы не стать жертвой злоумышленника:

1. не обсуждайте и не упоминайте реальные имя, возраст, место жительства и прочее личное;
2. не высылайте фотографии незнакомцам, по необходимости зачищайте служебную информацию в фото – EXIF;
3. не пользуйтесь геолокацией на недоверенных сервисах;
4. не публикуйте посты в обычном Интернете из-под прокси;
5. не заходите на одни сайты в одинаковое время (например, после работы или учёбы);
6. платите за сокрытие WHOIS при оплате домена;
7. держите независимые аккаунты на разных сервисах: отдельные почты для заказов в магазинах и платежей, общения, видеоигр, подтверждения регистрации;
8. при использовании социальных сетей открывайте подробности своего профиля только для друзей и не добавляйте в них кого попало;
9. изредка проверяйте свои личные данные в поисковиках и устраняйте утечки.

Многие популярные сайты и поисковики (за исключением некоторых: DuckDuckGo и searX), собирают и продают статистику о всех ваших действиях рекламным агентствам. Если вы сомневаетесь в том, делает ли это ваш поисковик, то просмотрите разрешения по использованию своих данных, уточните модель заработка поисковика на вас (простыми словами, если вы не платите за услуги, то продают вас, а не вам).
Персонализация результатов поиска в поисковиках и других сайтах (например, соцсетях) приводит к появлению пузыря фильтров — явления, когда агрегируемый контент (результаты поиска и ленты новостей, рекламные объявления) фильтруется под

[454] https://www.ixbt.com/live/kirill-kochetkov/vpn-na-domashnem-routere-bystro-i-nadezhno.html

«предпочтения» пользователя. Тем самым отсеивается то, что якобы нерелевантно интересам человека. Ниже перечислены некоторые способы выбраться из пузыря, и лучше сочетать несколько из них.

- Включите режим инкогнито или приватности, в котором не сохраняются история, кэш, куки и введённые пароли. Используйте его только для одноразовых сеансов работы с почтовыми ящиками, банковскими аккаунтами, поисковиками и прочими сайтами, требующими авторизацию. Остерегайтесь социальных сетей, т.к. от них за вами тянется след на ресурсы, где есть кнопки лайка и репоста. ВКонтакте, Facebook и Twitter наблюдают, где и когда вы были, и профилируют вашу личность — доходит до того, что доступ к Pornhub из России требует входа через ВК.

- Измените настройки браузера для минимизации опознания. Отключите приём сторонних файлов cookie и обработку WebRTC IP: с их помощью вас идентифицируют вебсайты. Включите отправку заголовка «Do Not Track», который «просит» ресурсы не собирать статистику. Если браузер не устанавливает защищённое соединение по протоколу HTTPS автоматически, добавьте плагин HTTPS Everywhere[455] — так ваш трафик будет сложнее перехватить.

- Установите расширения, блокирующие большинство т.н. «жучков»: скрытые запросы, рекламные виджеты и отслеживающие модули. Рекомендуется использовать комбинацию из uMatrix (Chrome[456] и Firefox[457]) и uBlock Origin (Chrome[458], Firefox[459] и Opera[460]). Уязвимости также содержат средства Flash и HTML5, воспроизведение которых можно контролировать плагином FlashControl (Chrome[461], Firefox[462]).

Однако и это не всё, что раскрывает вас в Сети. Сравнительно недавно на замену куки были изобретены техники идентификации по **фингерпринтам** (цифровым отпечаткам) — опознавательным сведениям, которые сервисы аналитики скрыто собирают о посетителе. Обычно они привязаны к текущему веб-агенту и стираются с его изменением или спуфингом, но уже активно внедряется способ кроссбраузерного фингерпринтинга, осуществляемый выполнением интегрированных в веб-страницу скриптов и апплетов (JavaScript, Java и Silverlight). Самозащита сводится к запрету обработки HTML-тэгов: audio, video, iframe и frame расширениями ScriptSafe (Chrome, Opera) и NoScript (Firefox). Их ключевые способности рассмотрены далее на примере

[455] https://www.eff.org/https-everywhere
[456] https://chrome.google.com/webstore/detail/umatrix/ogfcmafjalglgifnmanfmnieipoejdcf?hl=ru
[457] addons.mozilla.org/ru/firefox/addon/umatrix
[458] https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=ru
[459] https://addons.mozilla.org/ru/firefox/addon/ublock-origin
[460] https://addons.opera.com/ru/extensions/details/ublock/
[461] https://chrome.google.com/webstore/detail/flashcontrol/mfidmkgnfgnkihnjeklbekckimkipmoe
[462] https://addons.mozilla.org/ru/firefox/addon/flash-control

онлайн-тестов Browser Leaks.
Техника **Canvas Fingerprinting** идентифицирует браузер, видеокарту и операционную систему по HTML-элементу <canvas>. Когда человек посещает страницу, рендерится невидимая строка символов или 3D-модель, которая конвертируется в токен, часто отслеживаемый маркетинговыми компаниями. Аналогично работает **WebGL**, отключаемый NoScript в разделе Embeddings. Вы можете подменить цифровой талон с помощью ScriptSafe в разделе Canvas Fingerprint Protection, где содержатся 3 опции, действующие при каждом обновлении страницы. Random Readout генерирует случайный отпечаток; Blank Readout отправляет «пустой» отпечаток с оригинальным разрешением холста; а Completely Block Readout запрещает любую отправку данных. Третий вариант нежелателен из стеганографических соображений: если администратор заметит отказ сообщать отпечаток, он заподозрит неладное. Нетсталкеры стараются не спуфить таймзону, юзер-агент и референер — когда посланные метаданные противоречат собранному иначе (например, через JS), то обман быстро раскрывается, и вас берут на учёт.
Flash Player определяет версию ОС, текущий язык, разрешение экрана, число системных шрифтов и IP-адрес. Silverlight расширяет этот список до сведений о user-agent и часовом поясе. Значительно больше возможностей у Java, сообщающей страну, язык, поставщика и версию ОС, спефикации JVM и Java и характеристики сетевого адаптера. Все три плагина можно глобально отключить в браузерных настройках контента и во вкладке Embeddings у NoScript, где также запрещаются вообще все дополнения. Если установлен FlashControl, то flash-проигрыватель не запустится без спроса. Определение геолокации через Geolocation API тоже требует подтверждения, после которого передаются широта и долгота, адрес, степень погрешности и дата последней проверки. Если вы не пользуетесь навигацией, стоит полностью заблокировать её в настройках (about: config для Firefox; chrome://settings для Chrome) вместе с микрофоном и веб-камерой, которую и вовсе заклеивают изолентой.
Также не забывайте о чисто аппаратной слежке. Даже если телефон отключен, находящийся в нём baseband-процессор способен общаться с башней сотовой связи или её хакерской имитацией[463], что позволяет установить местоположение[464].

Литература

[1] Доклад Валентина Васильева, Browser Fingerprint – анонимная идентификация браузеров, 2017 г.

6.3 Предупреждение внимания к себе

Технологии отслеживания и протоколирования составляют две категории: активные и пассивные. Первые включаются с наводкой на конкретное лицо в случаях,

[463] https://tech.onliner.by/2013/11/20/smartphones-hacks
[464] https://habr.com/ru/post/112449/

когда он интересен органам (СОРМ[465]), конкурентам или личным врагам. Иначе работают маркетинговые жучки, автоматизированные записи (звонки в техподдержку, логи провайдера и т.д.) и **ханипоты** — серверы с уязвимостями, приманки для злоумышленников, которые прослушивают входящий трафик и определяют по нему специфику поведения хакера, а иногда и атакуют его в ответ. Многие специалисты по ИБ администрируют **ханипоты** для разработки стратегий отражения атак и улучшения внутрикорпоративных систем. Поэтому старайтесь не анализировать хосты с диапазонов[466], не рекомендованных к сканированию, т.к. так вы привлекаете внимание, и как можно чаще анонимизируйте свой трафик через torsocks или подобные утилиты. Учтите, что дальнейшие советы не спасут от **0day** — известных узкому кругу специалистов уязвимостей, против которых ещё не разработаны защитные механизмы.
Современные злоумышленники и спецслужбы способны в сжатые сроки подобрать любой пароль короче 20 знаков, если в нём нет цифр, спецсимволов и двойного регистра. Следует защищать аккаунты длинными и неочевидными паролями с двухфакторной аутентификацией. Запоминаются они трудно, но вы можете хранить и генерировать их в KeePassX[467] — менеджере паролей с открытым исходным кодом. Для доступа к его базе данных потребуется ключ-файл любого формата и/или мастер-пароль, который можно придумать (в т.ч. по первым буквам 6 строк любимого стиха или песни) и записать на бумажку или создать методом **diceware**. Для этого 20-25 раз бросается игральная кость, и каждая выпавшая цифра записывается в цепочку. Далее человек разбивает получившийся ряд на группы пятизначных чисел, выбирает соответствующие им слова из списка[468] и совмещает их. Несмотря на длину, заучить такой пароль легко, т.к. он содержит 5-6 слов и сочетается с мнемотехниками[469], но если вы вдруг забудете его, то уже не восстановите. Полезной считается ежемесячная замена паролей на новые: со временем они устаревают и могут быть скомпрометированы при переборе на слабых мощностях.
Регулярно сканируйте ПК на наличие вирусов и **кейлоггеров** — вредоносных сценариев, регистрирующих движения мыши и нажатия клавиш. Если вы уже инфицированы, и антивирусы не помогают, просто переустановите ОС. Никогда не используйте пароли и логины повторно, т.к. в случае их кражи будут взломаны все ваши профили. Не забывайте элементарные правила безопасности:

1) не запускайте неизвестные вложения в электронных письмах, даже если это документы;

2) отключите автозагрузку внешних носителей USB и CD;

3) настройте межсетевой экран для контроля входящих и исходящих подключений;

[465] ttps://ru.wikipedia.org/wiki/СОРМ
[466] http://www.hacking-tutorial.com/tips-and-trick/do-not-scan-this-ip-address-ranges/
[467] https://www.keepassx.org/
[468] https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt
[469] https://4brain.ru/memory/mnemotehniki.php

4) не переходите по подозрительным и укороченным ссылкам, не проверив их поисковиками или CheckShortURL[470];

5) когда просканировать исполнительный файл не удаётся, загрузите его на virustotal.com или запустите на виртуальной машине;

6) раз в неделю обновляйте всё программное обеспечение и версию ОС и чистите мусор CCleaner[471] или BleachBit[472];

7) отмените отправку «анонимной статистики», отключите предустановленные серверы telnet/ftp/smb, функцию удалённого доступа и всяческие зонды, характерные для вашего типа системы.

Наконец, думайте, кому вы доверяете. Дыры в архитектуре проприетарных программ сложнее вовремя обнаружить, чем у бесплатных аналогов с открытым исходным кодом. То же относится к ОС-ам: лучше отказаться от Windows или macOS в пользу семейства GNU/Linux из-за его прозрачности. Существуют **дистрибутивы Linux**, созданные для обеспечения приватности и анонимности. Являются продолжением развития ОС Incognito. Все исходящие соединения заворачиваются в анонимную сеть Tor, а все неанонимные блокируются. Примеры таких ОС: Whonix, Tails OS. Регистрируя аккаунты, всегда читайте политику конфиденциальности. Так, облачное хранилище mega.nz, которое шифрует весь контент алгоритмом AES, даже не скрывает, что смотрит файлы клиентов, удаляет их по своему усмотрению и банит неактивных пользователей. О похожей слежке не молчат популярные файлообменники и сервисы веб-почты — они должны будут повиноваться, когда полиция потребует ваши данные. В выборе поставщиков услуг пролистайте списки почтовых облачных[473] провайдеров, читая их правила и статистику удовлетворённых государственных запросов. Это же относится к сервисам текстовых заметок, из которых рекомендованы коллаборативные cryptpad.fr и titanpad.com. Всегда ищите отзывы и критику выбранных решений, авторитетные публикации исследователей об их надёжности. Если вы арендуете сервер, можно поднять на нём собственные облака из ownCloud[474] или Nextcloud[475] и синхронизировать их с другими веб-утилитами.

Один из главных залогов анонимности — неприметное и неотслеживаемое поведение. Не используйте одни и те же ники, адреса и телефоны для разных сфер своей деятельности. Различные мелочи, рассказанные о себе в дружеском флуде, могут с течением времени накопиться в полноценный деанон — именно так спецслужбы отловили[476] некоторых распространителей незаконного контента на даркнет-форумах. Увязав между собой ваши аккаунты с помощью обычного поиска или SOSINT-сервисов[477]

[470] http://www.checkshorturl.com/
[471] https://www.ccleaner.com/ru-ru
[472] https://www.bleachbit.org//
[473] https://lifehacker.com/the-best-cloud-storage-services-that-protect-your-priva-729639300
[474] https://owncloud.org/
[475] https://nextcloud.com/
[476] http://cripo.com.ua/gangsters/?p=216972/
[477] https://t.me/HowToFind_Bot

6.4 Защита данных

Из-за обилия[478] криптографических алгоритмов нельзя упомянуть всё, чему подолгу учат в ВУЗах на кафедрах по ИБ. В данной главе освещается несколько проверенных практик, начиная с **PGP** (Pretty Good Privacy) — известного стандарта ассиметричного шифрования[479] путём создания каждым собеседником пары из *открытого* и *закрытого* **ключей** — случайных больших чисел, которые почти невозможно подобрать. Первый нужен для шифровки, обладает продлеваемым сроком действия и передаётся незащищённо: постится в блоге или отправляется друзьям. Любой может скачать ваш открытый ключ (и оставить свой для получения ответа), зашифровать им текст и выслать его по вашему адресу. Но только вы прочтёте и расшифруете сообщение закрытым ключом, который держится в секрете и генерируется сложным паролем.

Несмотря на защиту криптосистемы от перехвата, нет гарантии общения с верным человеком. Злоумышленник может конфисковать (или взломать) устройство собеседника, украсть закрытый ключ и написать от его лица. Во избежание этого проводят **верификацию** — первичное подтверждение открытых ключей друг друга их обменом по альтернативному каналу связи: при реальной встрече, по телефону, а то и на *криптомонах*. Другой проверкой подлинности считается **цифровая подпись** — применение к посланию закрытого ключа, чтобы желающие могли расшифровать сообщение открытым ключом и связать его с вами. Так поступают разработчики открытого ПО при публикации новых релизов, чтобы убедить пользователей в отсутствии вирусов.

Технология **PGP** укомплектована в пакете GnuPG[480] и сочетается с почтово-новостным менеджером Mozilla Thunderbird[481] и плагином Enigmail[482], описанными в руководствах SSD[483], а также с XMPP и клиентом Psi(+)[484]. Тем не менее, она, как и P2P-протокол Bitmessage, малопригодна для моментальной связи, т.к. непортативна и требует постоянной ручной (де)шифровки. В этом PGP уступает мессенджерам со сквозными алгоритмами шифрования, как это реализовано в проприетарном и мобильном Threema[485] и свободном кроссплатформенном Wire[486]. При выборе таких средств вы рискуете хранением данных на чужих серверах, если не открыты их исходники. Криптографическая защита Skype, Telegram и Discord обесценивается их централизованностью и доступностью спецслужбам и хакерам. Им противоположны

[478] https://en.wikipedia.org/wiki/Category:Cryptographic_software
[479] https://ru.wikipedia.org/wiki/Криптосистема_с_открытым_ключом
[480] https://gnupg.org/
[481] http://mozilla.org/ru/thunderbird
[482] https://addons.thunderbird.net/ru/thunderbird/addon/enigmail/
[483] https://ssd.eff.org/ru
[484] https://habr.com/ru/post/50982/
[485] http://threema.ch/
[486] https://wire.com/en/

mesh-сети (см. главу 3.11) — распределённые системы поверх Интернета, где каждое устройство служит беспроводным (Bluetooth, Wi-Fi, ANT...) ретранслятором для остальных участников, имеющих равные права. Так работает платный мессенджер FireChat и развивающиеся Netsukuku[487] и Hyperboria[488], для присоединения к которым вы должны найти ближайший коммутатор или посетить одну из членских встреч. Увы, mesh-инфраструктура пока распространена в США и Европе, а не в России, за исключением экспериментов с Yggdrasil. Помимо интегрированных шифровальных функций, бывают и дополнения к небезопасным средствам. У жаббера это **OTR**(Off-the-Record) — двусторонний протокол защиты от прослушки, поддерживаемый Pidgin и Psi для PC и соединяющемся через Tor ChatSecure[489] для iOS и Android.
Верификация OTR возможна 3-мя способами:
1) по общему вопросу, ответ на который известен обоим собеседникам;
2) по сравнению отпечатка текущего и полученного вживую;
3) по паролю или QR-коду.
Однако чем больше ваша активность выделяется на фоне, тем вероятнее, что вы занимаетесь противоправной деятельностью. Показательно, как в Томске провайдера смутил[490] зашифрованный трафик, и он попытался его приостановить. Законодательство способно счесть нелегальным сам факт защиты данных, и когда он будет замечен, от вас потребуют ключ, который вы не сможете не разгласить. Людей раскрывают **метаданные** — информация о хранящемся, получаемом и отправляемом. Юрисдикция относится к ней менее конфиденциально, чем к содержимому инфообмена, и для детализации звонков хакеры перехватывают SMS-сообщения с кодами активации, а следователи обращаются к сотовому оператору. Распечатку вебсайтов и писем (их тем, отправителей и адресатов, длины текста) с привязкой ко времени получить так же просто, как и узнать, что у вас установлены шифровальные средства и их базы. Тот же KeePassX хранит пароли в файле уникального расширения .kdbx, который легко найти, если он не содержится удаленно.
Эти проблемы решает уже упомянутая в разделе анализа ARG **стеганография** — древнейшая междисциплинарная наука о передаче и хранении скрытого, когда сам факт его наличия неизвестен никому, кроме вас и/или получателя. Она не замещает криптографию, а дополняет её подобно матрёшке, т.к. сообщение контейнера зачастую зашифровано. Из истории до нас дошли многие методы его создания: например, невидимые чернила и микроточки, вытесненные компьютерными и цифровыми техниками. Они формализуются моделью «проблемы заключенных»[491] 16 и единой терминологией[492], но не определяются на практике: столкнувшись с обычной картинкой на сайте, вы заранее не знаете, есть ли у неё двойное дно. Посещая имиджборду,

[487] netsukuku.freaknet.org
[488] hyperboria.net
[489] https://chatsecure.org/
[490] https://roskomsvoboda.org/30879/
[491] https://ru.wikipedia.org/wiki/Алиса_и_Боб
[492] http://scipeople.ru/group/4720/topic/6430/

нельзя предугадать, что в тредах фотообмена говорят с помощью DesuDesuTalk![493], браузерного скрипта для псевдонимного общения, похожего на **нанооборду** — кочующую АИБ, посты которой спрятаны в изображениях других имиджборд. Цифровых алгоритмов всего около сотни[494] разной надёжности, и они служат для передачи, а не долгосрочного хранения, в отличие от компьютерных техник. К последним относится VeraCrypt[495] (описанный в гайде[496] форк скомпрометированного TrueCrypt), который шифрует HDD или внешний носитель «на лету» и создает в обычных файлах виртуальные тома. Они могут содержать еще один скрытый внутренний том, и если вы выдадите пароль от контейнера, человек увидит только поверхность хранилища.

6.5 Психологическая безопасность

Деятельность нетсталкера превращает его в своеобразного информационного выживальщика. Некоторые вещи, которые вы найдете в глубоком, а иногда и поверхностном интернете, могут вас шокировать или навредить вам. Не кликайте на все ссылки подряд, особенно если у вас эпилепсия или вы в общественном месте. Там может быть расчлененка или honeypot - тот же Fresh Onions часто предоставляет минимальные описания, что позволяет избежать очередного унылого ресурса с незаконщиной. Старайтесь не получать слишком большое количество травматичной для вас информации за раз, поскольку мозг склонен запоминать[497] негативный опыт лучше позитивного. Да и эмоции, получаемые в интернете, влияют на ваше тело так же, как почерпнутые из физического мира, о чём сейчас вещает даже реклама[498]. События виртуала мы бессознательно считаем такими же важными[499], как и IRL, если не приучили себя к обратному.
Помните, что ресурсы Darknet-сетей не более достоверны, чем в клирвебе, о чём напоминает даже крупнейший хостинг Tора Daniel's[500]. Ресурсы .onion полнятся скамом. Повышенное внимание к ним со стороны новичков - лишь проявление слепого доверия к общепринятым авторитетам, что напоминает о логической ошибке Argumentum ad verecundiam. В любой из сетей среди материалов или площадок общения вы можете столкнуться с риторикой, пытающейся эксплуатировать когнитивные искажения[501].
От **фейковой информации** можно обезопасить себя не только поиском доказательств и анализом изображений (см. главу 4.8), но и постоянным задаванием тексту вопроса «чем это подтверждается?». Постепенно вы будете автоматически видеть слабые места текстов и распознавать мошенничество или пропаганду.

[493] https://github.com/desudesutalk/desudesutalk
[494] jjtc.com/Steganography/tools.html
[495] veracrypt.fr/en/Home.html
[496] safe.rublacklist.net/veracrypt
[497] https://anywellmag.com/mozg-za-chto-pochemu-my-zapominaem-plohoe-luchshe-chem-horoshee-25365/
[498] https://www.sostav.ru/publication/ivi-39987.html
[499] https://telegra.ph/Realnoe-i-voobrazhaemoe-s-tochki-zreniya-mozga-04-09
[500] https://danwin1210.me/faq.php
[501] https://ru.wikipedia.org/wiki/Список_когнитивных_искажений

Fig. 27. Пример задавания вопросов к тексту

Наконец, **зависимость от нового** - то, что побуждает обычного пользователя скроллить специально спроектированную для этого[502] бесконечную ленту, а нетсталкера - раз за разом запускать тот или иной рандомайзер. Не удовлетворяйтесь лишь просмотром контента, найденным для вас ботами. Углубляйтесь в заинтересовавшие вас объекты. Раскапывайте, агрегируйте, делитесь и не стесняйтесь просить помощи.

Где-то в сети обязательно найдётся ваша собственная жемчужина в стоге сена. Не пройдите мимо неё.

[502]https://www.bbc.com/news/technology-44640959

7. Авторство

Archivist: Выражаю благодарность за содействие в составлении текста участникам ИИС, и в особеннности Wegwarte и yolo. Руководство посвящается памяти Шампуня, may he rest in peace.

Wegwarte: В этой книге объединён и систематизирован опыт многих людей. Она не была бы возможна без активного и упорного сообщества. Пусть каждый из нас ищет что-то своё, но это не мешает обмениваться мнениями, навыками и находками, что доказала история «Точки Сбора». Нетсталкинг постоянно развивается, поэтому когда-нибудь и эти страницы будут дополнены.

Здесь завершается работа, которую мы начали с Архивистом и Шампунем в январе 2017. Дальше действовать будете вы.

Points: Если вы нашли нерабочие ссылки, или у вас остались пожелания к улучшению этой книги, то можете написать письмо на netstalking_manual@protonmail.com, и я вас услышу.

Другие авторы:

- Информация о дорках и их примеры: CapyB
- AnoNET и анонимные сети: Abslimit
- Ресурсы для картосталкинга: Антибезпредел
- Анализ документов: Ян Майкл Винсент
- Omegaproject: Dematerium
- Freenet: Raymond
- Баннер-граббинг: meguminkonosuba
- Вычитка и форматирование: ld3301, Cino Folko, Eva

Коммьюнити: Благодарим сообщество «Точка Сбора» и участников группы «Открытый чат Руководства по нетсталкингу»[503] за исправления и предложения по улучшению этой книги.

[503] https://t.me/netstalking_guide