

Шпаргалка OSINT

Следственные Ресурсы - Лето 2019



INTELTECHNIQUES

Куплено
благодаря
Skladchik.com

Методология | Подготовка | Внедрение | Документация

Предэксплуатационные соображения

Этическая и правовая оценка

Результаты и сфера применения

Временные и ресурсные ограничения

Воздействие/Факторы Риска

Изогренность противника

Коммуникация и оперативная сводка

Контрольные ожидания

Следственные действия

Расширьте ваши инструменты

Задать вопрос

Документируйте свои знания

Создавайте коллекции

Запрос, развертка, и закрепление

Объединение результатов

Полная отчетность и архивирование

Рабочее пространство&Инструменты

Чистая/Безопасная Рабочая Станция

Чистое/Безопасное Подключение

Новые аккаунты для исследования

Чистый браузер с расширениями

Инструменты для сбора данных

Система документации

Хранение/архивация решений

OSINT ресурсы

[OSINTFramework.com](https://osintframework.com)

[OSINTBrowser.com](https://osintbrowser.com)

[Netbootcamp.org](https://netbootcamp.org)

[Workinukraine.space](https://workinukraine.space)

[Investigativedashboard.org](https://investigativedashboard.org)

[Start.me/p/b56xX8/osint](https://start.me/p/b56xX8/osint)

INTELTECHNIQUES
.com



Работа с вкладками

<https://www.one-tab.com/> (Только локальное хранение)
Простое управление вкладками/экспорт для Chrome и Firefox

<http://www.gettoby.com/> (Аккаунт с синхронизацией)
Управление миниатюрами вкладок для Chrome и Firefox

<https://chrome.google.com/webstore/detail/graphitabs/dcfclmgmkccmnpnpgnldhldjmfphkimp?hl=en> GraphiTabs - Древовидное представление вкладок

<https://clusterwm.com/>
Простой менеджер вкладок с экспортом(С премиумом)

<http://tabsoutliner.com/>
Управление вкладками - формат контура, экспорт, синхронизация (платная версия)

<https://www.gettabli.com/>
Простой, Приватный (только для автономного хранения)
Управление вкладками

Анализ ссылок/Визуализация

<https://www.paterva.com/buy/maltego-clients.php>
Maltego CE и CaseFile

<https://vis.occrp.org/>
Создание Диаграмм Ссылок - Организованная преступность и Коррупционные проекты

<https://gephi.org/>
<http://www.automatingosint.com/blog/category/gephi/>

<https://www.xmind.net/>
Mind Mapping - бесплатные и платные версии

<https://medium.com/@raebaker/using-lampyre-for-basic-email-and-phone-number-osint-e0e36c710880> (Lampyre)

<http://www.visualsitemapper.com/>
Карта доменов

<https://www.draw.io/>
<https://github.com/michenriksen/drawio-threatmodeling>

<https://github.com/woj-ciech/Danger-zone>
Ссылки на IP , домены, и Email адреса

<https://www.mindmup.com/>
Mind Mapping - Бесплатные и платные уровни

<https://www.nodexlgraphgallery.org/Pages/Registration.aspx>
Мощный графический клиент - бесплатные и платные уровни

Полезные браузерные расширения

<https://www.onenote.com/clipper>
Захват экрана и заметки(Только для пользователей OneNote)

<https://getfireshot.com/>
Захват экрана и аннотации (как изображение или pdf)

<https://github.com/ssborbis/ContextSearch-web-ext>
Поиск контекста

<http://www.osintbrowser.com/>
OSINT закладки

<https://github.com/az0/linkgopher/>
Простое извлечение ссылок

<https://github.com/marklieberman/downloadstar>
Firefox - загрузка всех элементов на веб-странице, соответствующих шаблону

<https://github.com/mozilla/multi-account-containers#readme>
Firefox - Мульти-аккаунт контейнер (Компартментализация)

<https://github.com/mozilla/multi-account-containers#readme>
Firefox - Мульти-аккаунт контейнер (Компартментализация)

<https://webrobots.io/>
Поиск с YP, Yelp, Ebay, Amazon, etc. Сохранить как Excel или CSV

Настройка Моей Рабочей Станции

Рабочии станции - Win 10, PIA/ProtonVPN, Chrome/Firefox, Vbox, Bus-cador/Kali, Nox/Geny, Hunch.ly, UC Cable/Mifi, Keypass, Malware-bytes, Glasswire

Смартфоны - iPhone, MySudo, Signal, Wire
- Android, burner, unlocked, on Mint sim kit

Email/Платежи - Prontonmail, GMX, Fastmail, Blur, 33mail, Privacy.com, Vanilla Visa

Офисное ПО - Libre, OneNote, Notepad++, CherryTree, Standard Notes, Paper notebook, Teams/Slack/Mattermost/Rocket

Alt-Hardware: MacBook Air, Atom Text Editor, VMware Fusion, Chrome/Firefox, Little Snitch

Гипервизоры: Virtualbox, Buscador Linux, Kali Linux, Genymotion, Nox

Google Операторы	
Помните, что мы можем связать несколько операторов вместе	
site:	Ограничивает результаты результатами из определенного домена site:apple.com
" "	Кавычки указывают на поиск точного условия "red rider BB gun"
AND	Показывает результаты только для обоих условий apple AND orange
OR	Поиск термина А,Б или обоих. Символ трубы тоже самое что и ИЛИ gun OR rifle = gun rifle
*	Подстановочный знак для слов в фразе, которую вы не знаете wish * a star
()	Группирует набор слов/операторов отдельно (gun pistol) ammo
-	Исключает результаты, включающие это слово chicago baseball -cubs
\$	Поиск по определенной цене "apple watch" \$299
cache:	Самая последняя кэшированная версия домена cache:boston.gov
filetype:	Поиск только по определенному типу файла,ext: работает так же filetype:pdf "confidential" или ext:pdf "confidential"
related:	Поиск сайтов, связанных с доменом related:sony.com
intitle:	Поиск страниц с условием в заголовке страницы intitle:sabotage
inurl:	Выводит страницы, содержащие указанное слово в URL inurl:private
around(x)	Страницы, содержащие два слова или фразы на расстоянии X слов друг от друга. microsoft (7) surface
info:	Найти информацию о конкретной странице, включая время последнего кэширования in-fc:chicago.gov
Продвин.поиск	https://www.google.com/advanced_search

Больше операторов: <https://ahrefs.com/blog/google-advanced-search-operators/>

DuckDuckGo	
DuckDuckGo обрабатывает некоторые операторы немного по-другому	
Cats dogs	Результаты о кошках или собаках
"cats and dogs"	Результаты для "кошки и собаки". Если результаты не будут найдены, будет попытка показать соответствующие результаты
cats +dogs	Больше собак в результате
cats filetype:pdf	PDF файлы о кошках. Поддерживаемые типы файлов: pdf, doc(x), xls(x), ppt(x), html
dogs site:example.com	Страницы о собаках из example.com
Cats -site:example.com	Страницы о кошках, за исключением example.com
intitle:dogs	Заголовок страницы включает в себя слово "собаки"
inurl:cats	Url страницы включает в себя слово "кошки"

Начальная страница

Начальная страница делает запросы Google от вашего имени	
Операторы	Большинство стандартных операторов работает
Продвин.поиск	https://www.startpage.com/en/advanced-search.html
Советы по поиску	https://support.startpage.com/index.php?/Knowledgebase/List/Index/1

Bing Операторы	
Большинство операторов Google работают и в Bing	
()	Точно так же, как Google, термины или операторы, сгруппированные в скобку, обрабатываются вместе и отдельно от других условий
OR	Все запросы Bing рассматриваются как И если вы не укажете условия или между ними goat OR pig OR cow
NOT	Исключает результаты с опр. термином,символ – тоже работает boat NOT (raft OR ship)
loc:	Возвращает страницы из определенного региона(ов) dogs (loc:GB OR loc:FR)
prefer:	Дает приоритет условию поиска или другому оператору prefer:tomato plum apple
near:x	Слова в x близости друг от друга red near:4 blue
ip	Находит сайты размещенные на IP адресе ip:208.43.115.82
site/domain:	Фильтр для конкретного типа домена site/.gov confidential
feed:	Находит RSS-каналы на основе поисковых запросов feed:osint
Bing Adv.	Документация Microsoft

Информация:<https://www.lifewire.com/bing-advanced-search-3482817>

Yandex	
Большинство стандартных логических операторов работают (операторы Google), такие как site: и "quotes"	
Продвинутый поиск	Нажмите на  значок в строке поиска
lang:	Фильтр языка ccn lang:fr
mime:	Похоже на filetype mime:docx gdpr
date:	Дата изменения страницы bombing date:20180416
url:	Похоже на site: Но добавляет * в конец url и показывает все документы на странице url: Alice url:en.wikiquote.org/wiki/*
Специальные операторы: https://yandex.com/support/direct/keywords/symbols-and-operators.html	

Baidu	
Большинство стандартных операторов Google работают и на Baidu	
Продвин.поиск	https://www.baidu.com/gaoji/advanced.html
На английском	http://www.baiduinenglish.com/
Советы по поиску	https://www.seomandarin.com/baidu-search-tips.html

Другие интернациональные

Возможно нужен VPN или прокси для отображения в целевом регионе

Продвин.поиск	https://www.alexa.com/topsites/countries
Colossus	http://www.searchenginecolossus.com/
Occrp	https://data.occrp.org/
Int. OSINT	https://start.me/p/W2kwBd/sources-cnty
UK	https://investigativedashboard.org/databases/

<http://www.rba.co.uk/search/TopSearchTips.html>

INTELTECHNIQUES.com



Twitter

Не забудьте Google - "site:twitter.com keyword"

Расширенный поиск	https://twitter.com/search-advanced
Набор тулов	http://tweetbeaver.com/
Пожаловаться	https://tinfoleak.com/
Аналитика	https://socialbearing.com/
Аналитика	https://analytics.mentionmapp.com/
Аналитика	https://foller.me
Аналитика	http://twiangulate.com/search/
Старые посты	http://staringispolite.github.io/twayback-machine/
Поиск	https://snapbird.org/
Подписчики	https://doesfollow.com
Видео	https://twdown.net/
Визуализация	https://treeverse.app/
Изменения профиля	https://spoonbill.io/
Mapping	https://onemilliontweetmap.com
Inteltechniques	https://inteltechniques.com/menu/pages/twitter-tool.html
Юр. запросы	https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#19

Snapchat

Поиск пользователей	https://somesnapcode.com/
Поиск пользователей	https://www.snapdex.com/
Поиск пользователей	https://map.snapchat.com
Поиск пользователей	https://sovip.io
	https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf

Reddit

Не забудьте Google - site:reddit.com keyword

Поиск по теме	https://www.reddit.com/search?q=keyword
Поиск пользователей	https://www.reddit.com/user/username
Аналитика	https://pushshift.io/api-parameters/
Архивы	https://web.archive.org/web/*/https://www.reddit.com/user/username
Inteltechniques	https://inteltechniques.com/menu/pages/communities.tool.html

TikTok

<https://www.ticktick.com>

Поиск	https://tiktokapi.ga/
Поиск	https://www.osintcombine.com/tiktok-quick-search
Как на IOS	https://www.pageflows.com/post/ios/general-browsing/tiktok
Как на Android	https://www.wikihow.tech/Find-Friends-on-Tik-Tok-on-Android
Загрузчик	https://en.savefrom.net/download-from-tiktok
Захват видео	HTTPS://AIRMORE.COM/WATCH-TIK-TOK-PC.HTML
Юр. запросы	https://www.tiktok.com/en/law-enforcement

Facebook

Важно: Многие из этих инструментов могут работать неправильно, поскольку Facebook продолжает убивать возможности поиска графиков. https://www.vice.com/en_ca/article/zmpgmx/facebook-stops-graph-search

Полноэкранный FB	http://com.hemiola.com/bookmarklet/
Чаты	https://www.messenger.com/
Мобильная версия	https://m.facebook.com/
FB видео	https://www.facebook.com/watch
Скачать видео	https://www.fbdown.net/index.php
Скачать видео	https://www.tubeninja.net/how-to-download/facebook
NetBootcamp	http://netbootcamp.org/facebook.html (Warning: Netbootcamp.com does run tracking scripts)
Research Tools	http://www.researchclinic.net/facebook/
User -> ID	https://lookup-id.com/ (lookup-id.com запускает некоторые сценарии отслеживания)
Поиск по графам	https://inteltechniques.com/menu/pages/facebook-tool.html (Напоминания фейсбука сломан 8/2019)
Поиск по графам	http://socmint.tools/graph.htm
Поиск по графам	https://peoplefindthor.dk/
Поиск по графам	https://pitoolbox.com.au/facebook-tool/
Поиск по графам	https://searchisback.com/
Поиск по графам	https://whopostedwhat.com/
Поиск по графам	https://www.uk-osint.net/facebook.html
Поиск по графам	https://github.com/sowdust/searchbook
Обсуждение Графика	https://inteltechniques.com/blog/2019/08/02/the-privacy-security-osint-show-episode-133/
Законность И Конфиденциальность	https://www.facebook.com/safety/groups/law/guidelines

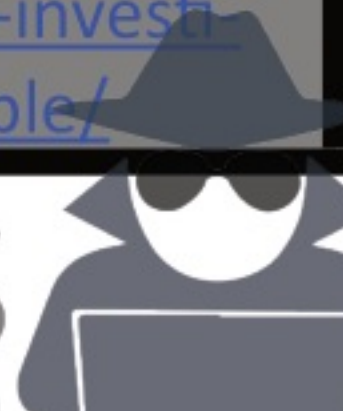
Instagram

Поиск Пользователей/Тегов	https://www.yooying.com/search
Поиск Пользователей/Тегов	https://www.social-searcher.com/
Поиск по #	https://tagboard.com/
Анализ подписчиков	https://hypeauditor.com/
Поиск локации	https://www.osintcombine.com/instagram-explorer
Поиск	https://mulpix.com/
Захват медиа	https://downloadgram.com/
Захват медиа	https://instasave.xyz/
Загрузчик	https://www.4kdownload.com/products/product-stogram
Профиль фотографии	https://instadp.net/
Профиль фотографии	http://izuum.com/
Истории	https://storiesig.com/
Поиск фото	https://imgwonders.com/
Пользователь/#	http://picdeer.com/
Пользователь/#	https://www.pictame.com/
Inteltechniques	https://inteltechniques.com/menu/pages/instagram-tool.html



Архивы сайтов	
Поиск в уже существующих архивах или запрос на захват	
Wayback Machine	http://archive.org/web/
Archive Today	http://archive.fo/
Как - Belling-cat	https://www.bellingcat.com/resources/how-tos/2018/02/22/archive-open-source-materials/
Как - Tech.co	https://tech.co/news/tools-to-help-you-search-the-archived-internet-2018-06
Массовый архивный скрипт	https://github.com/motherboardgithub/mass_archive
Поиск фото/изображений	
Напоминание: мы не загружаем конфиденциальные фотографии в интернет	
Поиск/Реверс	https://images.google.com/
Поиск/Реверс	https://tineye.com
Поиск/Реверс	https://www.bing.com/images/
Реверс Россия	https://www.yandex.com/images/
Реверс Азия	http://images.baidu.com/
Поиск	http://www.picsearch.com/
Twitter поиск	http://twipho.net/
Flickr	https://www.flickr.com/map
Exif	http://exif.regex.info/exif.cgi
Анализатор ошибок	http://www.errorlevelanalysis.com/
Базовая форензика	https://fotoforensics.com/
Анализатор текста	https://www.newocr.com/
Проверка краденного	www.stolencamerafinder.com/
Видео	
Расширения	https://www.downloadhelper.net/
Youtube-DL	https://github.com/ytdl-org/youtube-dl
Расширения	https://addons.mozilla.org/en-US/firefox/addon/video-downloader-profession/
Снимок экрана	https://www.techsmith.com/screen-capture.html
Архив видео	https://archiving.witness.org/archive-guide/acquire/acquiring-raw-video-and-metadata/
Поиск документов	
Google "keyword AND ext:pdf OR ext:docx OR ext:txt OR ext.xlsx"	
https://psbdmp.ws	http://www.findpdfdoc.com/
http://cryptome.org	https://www.base-search.net/
http://megasearch.co	https://psbdmp.ws
Карта/Локации	
https://www.google.com/maps	https://www.osintcombine.com/social-geo-lens
https://www.mapillary.com/	https://openstreetcam.org
https://ctrlq.org/maps/address/	https://livingatlas.arcgis.com/way-back/
https://www.gpsies.com/track-List.do	https://www.zillow.com/

Инструменты Захвата/Сбора Данных	
Хоть и не с открытым кодом, Hunch.ly остается моим путем в safety-net & коллекции тоже.	
Hunch.ly	https://hunch.ly/try-it-now https://hunch.ly/guides
Расширение для захвата экрана	https://getfireshot.com/
Snip & Sketch	https://www.microsoft.com/en-us/p/snip-sketch/9mz-95kl8mr0l#activetab=pivot:overviewtab
Аннотации	https://www.diigo.com/
OneNote Клип	https://www.onenote.com/clipper
Spiderfoot	https://www.spiderfoot.net/
Инструменты Документирования	
Hunch.ly отлично подходит для построения отчетов.	
OneNote	https://www.onenote.com
Текстовый редактор WIN	https://notepad-plus-plus.org/
Текстовый редактор MAC	https://atom.io/
Backnote	https://chrome.google.com/webstore/detail/backnote/gcikdkpooobdlgkkimomdgochmclliek?hl=en-US
Paliscope	https://www.paliscope.com (Free Standard Ed for LE)
Zotero	https://www.zotero.org/
Приватные записки	https://app.standardnotes.org/
Альтернатива Office	https://www.libreoffice.org/
Список ресурсов OSINT	
Коллекции курируются моими любимыми экспертами OSINT:	
OSINT.Team	https://osint.team/home (OSINT rocket chat group)
Ph055a	https://github.com/Ph055a/OSINT-Collection#ph055as-osint-collection
Bellingcat Tool-Kit	https://docs.google.com/document/d/1BfLPJpRty-q4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit
Sprp77	https://drive.google.com/drive/folders/1CBcemF-dorkAqJ-Stsh67OVHgH4FQF05
Baywolf88	https://www.learnallthethings.net/osint-resources
Sector0355	https://medium.com/@sector035
Justin Nordine	https://osintframework.com/
Start.me's: Technisette Bruno Mortier Emmanuelle -Welch Travis Birch	https://start.me/p/7kxL6K/search-engines https://start.me/p/b56xX8/osint https://start.me/p/gyXexK/dating-apps-and-sites https://start.me/p/kx72n5/databases https://start.me/p/rxeRqr/aml-toolbox https://start.me/p/ZME8nR/osint
Reuser	http://arnoreuser.com/osint-repertorium/
Phonexicum	https://phonexicum.github.io/infosec/osint.html#tools
i-intelligence	https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT_Handbook_June-2018_Final.pdf
PI Links	https://diligentiagroup.com/due-diligence/101-investigative-links-for-digging-up-information-on-people/

INTELTECHNIQUES.com

Настоящее имя		Email	
Поиск людей		Не забывайте о простом поиске в Google "user@domain.com"	
TruePeopleSch	https://www.truepeoplesearch.com/	Hunter.io	https://hunter.io/ (Создать бесплатный аккаунт)
Spokeo	https://www.spokeo.com/	HIBP	https://haveibeenpwned.com/ (может стать премиумным)
Thatsthem	https://thatsthem.com/	Verify	https://tools.verifyemailaddress.io/
Adv Background	https://www.advancedbackgroundchecks.com/	Verifalia	https://verifalia.com/validate-email
Nuwber	https://nuwber.com/	Mailtester	http://www.mailtester.com/testmail.php
FamTreeNow	https://www.familytreenow.com/	FindThatEmail	http://findthat.email/
PeopelByNm	http://www.peoplebyname.com/	AnyMailFinder	https://anymailfinder.com/
UFind	http://ufind.name/...	EmailMatcher	https://emailmatcher.com/
PublicRcrds	https://publicrecords.directory/	ProspectLinked	https://prospectlinked.com/#/home
GoLookup	https://golookup.com/	MetricSparrow	http://metricsparrow.com/toolkit/email-permutator/
PMR	http://publicemailrecords.com/name_listings	ThatsThem	https://thatsthem.com/reverse-email-lookup
Radaris	https://radaris.com/	Spokeo	https://www.spokeo.com/email-search
Cubib	https://cubib.com/	PsbDmp	https://psbdmp.ws/
ComLullar	http://com.lullar.com/	HackedEmails	https://hacked-emails.com/
Yasni	http://www.yasni.com/	OCCRP	https://data.occrp.org/search?q=gmail.com
TabSearch	https://www.zabasearch.com/	Dehashed	https://dehashed.com/
Spytox	https://www.spytox.com/	Hashes.org	https://hashes.org/leaks.php
Intelius	https://www.intelius.com/	Gravatar	https://en.gravatar.com/site/check/lorangb@gmail.com
ZoomInfo	https://www.zoominfo.com/	ReverseGenie	http://www.reversegenie.com/searching=email
Whoodle	https://www.whoodle.com/	ManyContacts	https://www.manycontacts.com/en/mail-check
PeekYou	https://peekyou.com/	ComLullar	http://com.lullar.com/
Webmil	http://webmii.com/	Inteltechniques	https://inteltechniques.com/osint/menu.email.html
CvGadget	https://cvgadget.com/	Basic Guide	https://www.blurbiz.io/blog/the-most-complete-guide-to-finding-anyones-email
Classmates	https://www.classmates.com/	OSINT Блок-схемы: https://www.dfir.training/osint	
192 (UK)	https://www.192.com/		
Inteltechniques	https://inteltechniques.com/menu/pages/person.tool.html		
Никнеймы		Объявления	
Knowem	https://knowem.com/checksocialnames.php?u=	Ebay	https://www.ebay.com/
NameChk	https://namechk.com/	Fatfingers	http://fatfingers.com/default.aspx
NameCheckr	https://www.namecheckr.com/	Flippity	http://www.flippity.com/
NameVine	https://namevine.com/	Kijiji	https://www.kijiji.ca/
UserSearch	https://usersearch.org/	SearchAllJunk	http://www.searchalljunk.com/
UserSherlock	http://usersherlock.com/	SearchTempest	https://www.searchtempest.com/
Profilr	https://www.profilr.social/search/	NotiCraig	https://noticraig.com/
Tinder	https://www.gotinder.com/@user	Oodle	https://www.oodle.com/local/burien-wa/
Amazon	https://www.google.com/search?q=site%3Aamazon.com+%22name%22	Offerup	https://offerup.com/
SocialCatfish	https://socialcatfish.com/reverse-username-search/	Craigslist	https://craigslist.org
WhatsMyName	https://github.com/webbreacher/whatsmyname	Inteltechniques	https://inteltechniques.com/menu/pages/communities.links.html
Sherlock	https://github.com/sherlock-project/sherlock		
Inteltechniques	https://inteltechniques.com/menu/index.html		

Номера телефонов		Домены/IP	
Для телефонов #s рассмотрим гос/платные опции (OSINT ограничен)			
Zaba	https://www.zabasearch.com/reverse-phone-lookup/	Censys	https://censys.io
USPhoneBook	https://www.usphonebook.com/ +1	IntelX	https://intelx.io
TruePeopleSearch	https://www.truepeoplesearch.com/#	Domaintools	https://www.domaintools.com/
Whitepages+	https://whitepages.plus/	CentralOps	https://centralops.net/co/
ThatsThem	https://thatsthem.com/	Whoxy	https://www.whoxy.com/
TrueCaller	https://www.truecaller.com/	IPLocation	https://www.iplocation.net/
Whitepages	https://www.whitepages.com/reverse-phone Reverse Phone Lookup	DNSlytics	https://dnslytics.com/reverse-ip
411	https://www.411.com/reverse-phone	Randhome	https://www.randhome.io/blog/2018/02/23/harpoon-an-osint/-threat-intelligence-tool/
CellRevealer	https://www.cellrevealer.com/	CrimeFlare	http://crimeflare.org:82/
FoneFinder	http://www.fonefinder.net/	Spyonweb	http://spyonweb.com/
WhoCalld	https://whocalld.com/	Pub-DB	http://pub-db.com/
SpyDialer	https://www.spydialer.com/	Whoisology	https://whoisology.com/
Searchbug	https://www.searchbug.com/tools/	Visualping	https://visualping.io/
NumberGuru	https://www.numberguru.com/phone/	WatchThatPage	http://watchthatpage.com/
ReverseGenie	http://www.reversegenie.com/	PentestTools	https://pentest-tools.com/information-gathering/find-subdomains-of-domain#
YellowPages	https://people.yellowpages.com/whitepages/?re=SP_people_search	SharedCount	https://www.sharedcount.com/
Spokeo	https://www.spokeo.com/reverse-phone-lookup	SmallSEO	https://smallseotools.com/backlink-checker/
PhoneValidator	https://www.phonevalidator.com/index.aspx	SimilarWeb	https://www.similarweb.com/
CallerIDTest	https://www.calleridtest.com/	Alexa	https://www.alexa.com/siteinfo/inteltechniques.com
IMEI	https://www.imei.info/	Hunter.io	https://hunter.io/
IMEI24	https://imei24.com/phone_base/	ViewDNS	https://viewdns.info/
Sync	https://sync.me/	Robtex	https://www.robtex.com/?=
Infobel	https://www.infobel.com/	Majestic	https://majestic.com/
DialingCode	http://www.dialingcode.com/	D-Me	http://d-me.info/
OpenCnam	https://www.opencnam.com/	Netcraft	https://www.netcraft.com/
TeleFoonGids	https://telefoongids.2link.be/	DomainBigData	https://domainbigdata.com/
ServiceObjects	https://www.serviceobjects.com/developers/lookups/geophone-plus	Inteltechniques	https://inteltechniques.com/osint/domain.search.html
WTNG	http://www.wtng.info/index.html	Inteltechniques	https://inteltechniques.com/blog/2018/04/24/searching-subdomains-with-findsubdomains-com/
SeanLawson	https://www.seanlawson.net/2019/02/use-chrome-developer-tools-view-masked-phone-numbers-for-free-people-search/	IP6Locator	http://ipv6locator.net/
NANPA	https://www.nationalnanpa.com/enas/coCodeReportUnsecured.do?reportType=7	ViewDNS	https://viewdns.info/
Inteltechniques	https://inteltechniques.com/osint/menu.phone.html	Maxmind	https://www.maxmind.com/en/home
Машины		IP2Location	https://www.ip2location.com/demo/
CarOwners	https://carsowners.net	IPFingerprints	https://www.ipfingerprints.com/
NICB	HTTPS://WWW.NICB.ORG/VINCHECK	ThatsThem	https://thatsthem.com/reverse-ip-lookup
OReilly	https://www.oreillyauto.com/	Netbootcamp	https://netbootcamp.org/websitetool.html
Carvana	https://www.carvana.com/	Shodan	https://www.shodan.io/
CheckThatVIN	https://checkthatvin.com/ctv#/home	Inteltechniques	https://inteltechniques.com/menu/pages/ip.tool.html#
CarFax	https://www.carfax.com/processQuickVin.cfx		
VehicleHistory	https://www.vehiclehistory.com/license-plate-search		
CarOwners	https://carsowners.net/		

Бизнес и организации		Игры	
Google: Резюме AND "Реальное имя"		Юр.запросы: https://www.search.org/resources/isp-list/	
OpenCorp	https://opencorporates.com/	Discord поиск	https://www.discordportal.com/
Rocketreach	https://rocketreach.co/	Discord поиск	https://discordservers.com/
OCCRP	https://data.occrp.org/	Discord поиск	https://discord.center/
CorpWiki	https://www.corporationwiki.com/	Discord поиск	https://disboard.org/
Recruitin	https://recruitin.net/	Discord поиск	https://discord.me/
Indeed	https://www.indeed.com/	Discord поиск	https://support.discordapp.com/hc/en-us/articles/115000468588-Using-Search
MarketVisual	http://marketvisual.com/	Захват Discord	https://dht.chylex.com/ Discord History Tracker
AihitData	https://www.aihitdata.com/	Twitch	https://www.twitchtools.com/
Glassdoor	https://www.glassdoor.com/Reviews/index.htm	Fortnite	https://fortnitetracker.com/profile/search?q=
LittleSis	https://littlesis.org/	PSN	https://psnprofiles.com/search/
OpenSanctions	https://www.opensanctions.org/	Mixer	https://www.lifewire.com/what-is-mixer-4156866
CEOEmail	https://ceoemail.com/	Steam	https://steamrep.com/ or https://steamid.uk/
Enigma	https://public.enigma.com/browse/collection/corp-watch-company-subsidiaries/	Скоростные трюки	
Angel	https://angel.co/	Экономия нескольких секунд здесь и там складывается со временем	
RipoffReport	https://www.ripoffreport.com/	Контекстный поиск	https://github.com/ssborbis/ContextSearch-web-ext
Sector035's Guide	https://medium.com/@sector035/gathering-company-intel-the-agile-way-6db12ca031c9	Добавить как поисковую систему	https://www.wired.com/2014/07/tip-week-chrome-site-search/
LinkedIn		Старые запросы	https://thepracticalsysadmin.com/defaulting-google-search-results-to-the-past-year/
site: linkedin.com inurl:pub -inurl:dir "at Microsoft" "Current"		Комбинации Клавиш	https://www.quinnssmtbrand.com/windows-keyboard-shortcut/
site: linkedin.com "Настоящее имя"			
Запрос юзера	HTTPS://GITLAB.COM/INITSTRING/LINKEDIN2USERNAME		
Email запрос	https://github.com/pry0cc/GoogLinked		
Нарушение Данных	https://archive.org/details/LIUsers.7z		
Inteltechniques	HTTPS://INTELTECHNIQUES.COM/MENU/PAGES/LINKEDIN.TOOL.HTML		
Разные инструменты & Хитрости		Виртуальные машины	
Эффект. и организац. инструменты,которые я использую		При установке виртуальных машин дословно следуйте инструкциям	
Лучший Поиск Файлов Windows	https://www.voidtools.com/	Buscador	https://inteltechniques.com/buscador/
Синхронизированные записки	https://www.onenote.com	Virtualbox	https://www.virtualbox.org/wiki/Downloads
Зашифрованные сообщения	https://signal.org/ https://wire.com/en/	VBox Extensions	https://download.virtualbox.org/virtualbox/6.0.10/Oracle_VM_VirtualBox_Extension_Pack-6.0.10.vbox-extpack
Зашифрованный Email	https://protonmail.com/ (Используйте бесплатный уровень)	Kali Linux	https://www.kali.org/downloads/
Панель горячих клавиш	https://www.elgato.com/en/gaming/stream-deck	Tails	https://tails.boum.org/
NAS/локальное облако	https://www.synology.com/en-us	Обновление Linux	apt-get update && apt-get upgrade
Снимок экрана	https://www.techsmith.com/store/snagit	Обновление Youtube-DL	sudo -H pip install --upgrade youtube-dl
Снимок экрана	https://getfireshot.com/buy.php (pro supports multi-page pdf)	Распространенная ошибка	Убедитесь, что виртуализация(AMD-V) включена в BIOS
Блокнот	https://www.costco.com/Moleskine-Cahier-6-Pack-Extra-Large-Notebooks.product.100300742.html	Host Key	Win - Правый CTRL Mac - Левый Command Key
Veracrypt	https://www.youtube.com/watch?v=cxo8xosH TI Vera-срут идеально подходят для архивирования дисков или размещения их на флэш-носителях для доставки клиентам	Vbox проблемы с масштабом	host + f, для переключения в полноэкранный режим, если не работает, host + с, для переключения в/из масштабируемого режима, host + f, вернуть назад
Tech Issues	https://stackoverflow.com/ Помимо поиска в Google ваших технических проблем, stackoverflow обсуждает практически любую проблему ПО		



Распространенные ошибки

Методология более важна, чем инструменты или методы, потому что эти вещи меняются. Инвестируйте в определение сильного процесса.

Отказ от использования OSINT подходов и стратегий, например: соц. инженерия (К примеру дружеский телефонный звонок)

Вы вошли в живой сеанс для платформы, которую вы запрашиваете? т.е. убедитесь, что вы вошли в FB на другой вкладке

Включать пробел в конце при копировании учетной записи или другого ключевого слова в поле формы запроса

Есть ли у вас блокировщики скриптов, которые могут препятствовать загрузке данных на страницу? (ie: privacy badger, ublock, ghostery)

Геолокация. Ваши результаты поиска искажаются вашей примерной геолокацией, подумайте над использованием VPN для "переезда"

Начните смотреть на источник страницы, чтобы увидеть, что происходит за кулисами. Если вы только посмотрите на графический интерфейс, вы многое упускаете.

Упорство побеждает день. Большинство ответов не попадут вам в руки. Терпение и настойчивость превыше всего.

Дополнительные ресурсы OSINT

<https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjm-GnyVkfE2HYolCKOGguA/> (Набор инструментов Bellingcat)

<https://github.com/Ph055a/OSINT-Collection> (Командная коллекция OSINT)

<https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT-Handbook-June-2018-Final.pdf> (Сбор разведданных)

<https://www.osinttechniques.com/osint-tools.html>

[@sector035](https://medium.com/@sector035) (@sector035)

<https://www.learnallthethings.net/creepyosint> (@baywolf88)

<https://osintcurio.us/10-minute-tips/>

<https://atlas.mindmup.com/digintel/digital-intelligence-training/index.html>

Операционная Безопасность - Браузеры

Браузер, сессия и сайты для тестирования	
Отпечаток девайса	https://panopticklick.eff.org/
Отпечаток браузера	https://amiunique.org/fp
Отпечаток браузера	https://www.deviceinfo.me/
Отпечаток браузера	https://browseraudit.com
Отпечаток браузера	https://browserleaks.com/
Отпечаток браузера	https://pixelprivacy.com/resources/browser-fingerprinting/
Отпечаток браузера	https://detectmybrowser.com/
Слив IP	https://ipleak.net
Слив DNS	https://www.dnsleaktest.com/
Слив Email	https://www.emailprivacytester.com
Тест на приватность сайта	https://webbkoll.dataskydd.net/en/
Ресурсы приватности	https://inteltechniques.com/links.html

Операционная Безопасность - Windows

Рекомендуемые Инструменты Для Обеспечения Безопасности Windows	
Создать не привилегированного пользователя	https://support.microsoft.com/en-us/help/4026923/windows-10-create-a-local-user-or-administrator-account
Антивирус	https://www.microsoft.com/en-us/windows/comprehensive-security
Антивирус	https://www.malwarebytes.com/mwb-download/
Антишпион	https://www.safer-networking.org/
Приватность Windows	https://ssd.eff.org/en/module/how-delete-your-data-securely-windows
Приватность Windows 10	https://www.thewindowsclub.com/privatewin10-advanced-windows-10-privacy-tool
Приватность Windows 10	https://fdossena.com/?p=w10debotnet/index_1903.frag
Проверьте свои данные Microsoft	https://account.microsoft.com/account/privacy
Активность интернета	https://www.glasswire.com/
Менеджер паролей	https://keepassxc.org/
Очиститель	https://www.bleachbit.org/download/windows
Очистить самому	https://www.makeuseof.com/tag/best-way-clean-windows-10-step-step-guide/

Основные Следственные Действия

Работа над вашим первым делом с новыми инструментами и методами

1. Настройте свои заметки и сбор данных для отслеживания вашей рабочей тетради, One-Note, Hunch.ly, каталог на зашифрованной флешке, и т.д.
2. Перечислите свои цели расследования - полный профиль, поиск для задержания, идентификация партнеров, сбор цифровых доказательств и т. д. (вы собираете информацию или доказательства для суда?)
3. Составьте личную информацию - Email, телефонные номера, имена, и т.д.
4. Запустите все ваши платные и/или правительственные запросы и используйте их для добавления к вашей исходной информации. Если это возможно, возьмите в руки фотографию бронирования или DOL для сравнения во время исследования социальных сетей.
5. Запустите Accurint (Lexis-Nexis), TLO.
6. Откройте firefox/chrome с вашими скриптами на выбор - noscript, https everywhere, ghostery, fireshot, one-tab (или используйте браузер в Buscador VM)
7. Если это серьезное расследование, я включаю hunch.ly и ~~включаю~~ ~~м~~переключатели" (слова из личной информации)
8. Я делаю быстрый поиск в Google и проверяю свой сайт поиска людей по выбору на эту неделю. ["Джеймс Макинтайр" "Денвер"],а потом проверяю на truepeoplesearch.com
9. Перейдите в <https://inteltechniques.com/menu.html> (или ваш набор инструментов OSINT по выбору например: osintframework.com) и используйте вкладки слева, чтобы выбрать категории, соответствующие вашей исходной информации. Мой типичный заказ -это электронная почта, настоящее имя, поисковые системы, Facebook, twitter, а затем все остальное в зависимости от того, что вам нужно сделать.
10. Я выжимаю инструмент inteltechniques.com и закрываю все бесполезные вкладки. Любую полезную вкладку я помечаю как важную (ID аккаунта, никнеймы и т.д) в моем блокноте и создаю pdf важной страницы. Этот pdf-файл сохраняется в каталоге с делом. В случае с несколькими целями создайте вложенные папки для каждого интересующего вас лица.
11. Периодически или когда я заканчиваю свое исследование, я копирую/вставляю или вручную ввожу любую соответствующую информацию в профиль или отчет о случае в word или one-note. Я вставляю любые соответствующие снимки экрана, PDF-файлы, такие как отчеты lexis-nexis, и хорошие фотографии целей, любых транспортных средств и адресов.
12. Я просматриваю этот отчет с детективом или агентом по делу, чтобы объяснить свое расследование и посмотреть, есть ли у них какие-либо вопросы или нужна дополнительная информация.
13. Мои черновики,книжки hunch.ly файлы и/или клонированные VM (если я использовал buscador) обычно сохраняются на случай,если они мне понадобятся для суда. Исключение составляют такие вещи, как сбор информации для операций, событий, угроз и т. д. hunch.ly экспорт может быть записан на диск в качестве доказательства, но будьте осторожны с любыми нежелательными данными, которые могли быть непреднамеренно сохранены во время этого сеанса. Резервная копия VM не должна входить в доказательства,так как она будет разглашать нашу коспирацию. Относитесь к нему как к тайному ноутбуку, на который вы можете ссылаться, но избегайте разоблачения его, если только вас не заставят (работайте с вашим прокурором, чтобы бороться с этим). Если вам не нужна эта виртуальная машина для суда, не храните ее (хранение данных связано с обязанностями по хранению и потенциальными обязательствами).
14. Я удостоверяюсь, что у меня есть свежая VM для следующего случая или кризиса, который возникает. Я также делаю новые аккаунты, чтобы иметь в кармане, если какой-либо из моих исследовательских аккаунтов был забанен. Лучше подготовиться к следующему делу в конце предыдущего и быть готовым уйти в любой момент.
15. Промыть,прополоскать,повторить. Отслеживайте успехи, чтобы оправдать большее количество оборудования, персонала и обучения.

Примечание: мой стандартный сетап-это автономный ПК с windows, подключенный к кабельному модему UC или mifi (VPN в зависимости от обстоятельств).

Для быстрых проверок, таких как события, угрозы и т. д. Я остаюсь в Windows и просто использую Chrome/Firefox и ссылки на inteltechniques.com. Это делается для удобства и скорости с меньшей суетой, когда меньше необходимости в разделении, безопасности и/или анонимности. Для расследования я, как правило, использую VM Buscador с установленной Hunch.ly , и все свежие аккаунты для исследования. Быстрые утилиты против утилиты для одной цели - используйте правильный инструмент для каждой миссии.

СОЗДАНИЕ АККАУНТА 101

ПОСТРОЕНИЕ ЭФФЕКТИВНОГО, ВОСПРОИЗВОДИМОГО И ЧЕТКО СФОРМУЛИРОВАННОГО ПРОЦЕССА

Создание надежных аккаунтов для расследования

Это список рекомендуемых шагов для создания следственных/исследовательских аккаунтов в социальных сетях. Они в значительной степени основаны на обратной связи с нашим сообществом и их опытом блокировки или приостановки своих учетных записей. Там, где это применимо, шаги делаются в порядке предпочтения в отношении успешного избежания проблем безопасности.

Настройка оборудования – это может показаться простым, но оборудование и подключение важно.

1. Избегайте VPN во время создания учетной записи, большинство их диапазонов IP помечены флажками
 2. Mifi или динамические IP-устройства довольно хорошо работают для создания учетной записи
 3. Общедоступные сети (Starbucks Wi-Fi), но имейте в виду, что вы подвергаетесь воздействию и кросс-корреляции с другими пользователями этой сети
 4. Телефон # - реальный номер телефона без VOIP избавит вас от многих хлопот, мы рекомендуем комплект SIM-карт Mint стоимостью \$5 в паре с разблокированным смартфоном (mintmobile.com)
 5. онлайн-след – “Google” это ваше имя и работодатель. Распечатайте первые две страницы результатов и включите их в свою папку скрытых счетов как “легкая добыча” личных данных.
1. Мы обычно делаем FB, IG, и Twitter одновременно и связываем их в качестве одного скрытого профиля. Каждый из них добавляет глубину и достоверность другим (намеренная перекрестная корреляция).
 2. Храните заметки о ваших скрытых деталях либо в бумажном блокноте, либо в цифровом формате, например в менеджере паролей или на электронном листе, имея в виду ваши требования безопасности.
 3. 3. Если это чувствительный или глубокий случай проникновения, обязательно разделите этот профиль с самого начала (подключение, браузер, устройство (используйте виртуальную машину для изоляции) и т. д.)
 4. Подключение:
 - a. отсутствие VPN во время создания учетной записи большинство IP-блоков VPN помечаются флагом
 - b. Соединения для мобильной передачи данных (MIFI) хорошие динамические/общие IP
 - c. Другой метод заключается в том, чтобы получить бесплатную виртуальную машину уровня AWS EC2 или Digital Ocean и использовать ее для создания учетной записи, так как тогда у вас будет IP AWS, это более продвинутый метод, но он работает довольно хорошо, если вы комфортно работаете с виртуальными машинами и учитеесь ориентироваться в AWS. Некоторые группы даже запускают полные следственные виртуальные машины на AWS, но опять же это более продвинутая настройка, которая требует некоторой работы, чтобы разобраться.
 - d. Еще один продвинутый метод заключается в том, чтобы запустить свой собственный VPN через AWS, поскольку провайдеры, как правило, не помечают AWS <https://github.com/StreisandEffect/streisand>
 5. Адреса Email:
 - a. Не использовать Gmail, Hotmail, yahoo или другую топовую бесплатную почту (Gmx пока является исключением)
 - b. Частные Домены работают лучше всего, возьмите домен Namecheap или GoDaddy и веб-почту по дешевке и сделайте с ними кучу аккаунтов
 - c. Gmx.us аккаунты работают хорошо (по крайней мере сейчас) и не требует никакой существующей электронной почты или контактной информации
 - d. Sudomail и Protonmail работают хорошо, но не так хорошо как частный домен
 6. Номера #:
 - a. Вам может повезти, и вы не получите требование к номеру телефона, но также иногда он не будет требовать его сначала, но затем через пару часов или дней провайдер бросит его вам в качестве требования безопасности
 - b. Без VOIP – Большинство номеров помечаются
 - c. Mint test kits и разблокированный телефон-это дешевый способ получить 7 дней на реальный номер
 1. Убедитесь, что у вас есть покрытие Mint в вашем районе
 2. <https://www.amazon.com/Mint-Mobile-Starter-Verify-Compatibility/dp/B0786RD524> (\$5 для двух сим-карт)
 3. Затем вы можете перенести номер в google voice
 4. Некоторые группы покупают их оптом
 - d. Вы также можете использовать дополнительный # на реальном аккаунте (например, Verizon), а затем перенести его в google voice, а затем нарисовать новый # для этого аккаунта Verizon
 - e. Некоторые люди так же используют гостиничные телефоны и т.п когда путешествуют чтобы создать аккаунты

СОЗДАНИЕ АККАУНТА (ПРОДОЛЖЕНИЕ)

ПОСТРОЕНИЕ ЭФФЕКТИВНОГО, ВОСПРОИЗВОДИМОГО И ЧЕТКО СФОРМУЛИРОВАННОГО ПРОЦЕССА

7. Как только мы попадаем в наш новый аккаунт, мы не оставляем его, начинаем делать его реальным сразу же
 8. Выберите имя, которое является общим, но не слишком общим
 - a. Например.: Николай Жуковский, Михаил Попов, и т.д.
 - b. <http://howmanyofme.com/>
 9. Имя, пол, город, работодатель (школа) должны иметь смысл, помните, что реальный человек в FB, скорее всего, посмотрит ваш профиль, если он будет сообщен как подозрительный, мы хотим пройти тест на запах(тест на доверие)
 10. Фото профиля/обложки
 - a. Мы никогда не претендуем на то, чтобы быть конкретным человеком без его согласия (т. е. не воровать личность)
 - b. Pikwizard.com – Хороший источник лицензионных фотографий
 - c. Pixabay.com это тоже подходит
 - d. Создатели аватаров-это еще один вариант <https://mashable.com/2007/09/12/avatars/#mn3Ph1PwgZqi>
 - e. fiverr.com – Вы можете купить фотографии профиля по дешевке или что-нибудь еще...избегайте покупки массовых аккаунтов, они часто блокируются или крадутся
 - f. Я также люблю взять фотографии из images.bing.com большой толпы(дороги, гонки, спортивное мероприятие, концерт), обрезать его, чтобы было непонятно,кто мы есть в группе и все же это тот вид контента, который люди публикуют для профилей или баннеров, потому что интернет-это все о хвастовстве
 - g. Проявите творческий подход – общее правило-это обрезка,, фильтр, логический выбор рисунка
 11. Время чтобы завести друзей
 - a. Присоединяйтесь к группам – все, кто имеет большие группы, которые принимают кого угодно
 - b. Занудные группы и поп-культура-мои любимые: видеоигры, косплей (потому что тогда костюмированные профили имеют смысл) и т. д.
 - c. Если вы делаете глубокое проникновение можно исследовать целевые группы, не присоединяйтесь к её/его группе напрямую, присоединяйтесь в похожие и проделывайте ваш путь медленно после того как у вас появится какая-то история
 - d. Сделайте несколько лайков и комментариев в группах в течение дня или двух
 - e. Потом <https://www.facebook.com/find-friends/browser/> И позвольте FB порекомендовать друзей. Мы больше не холодные друзья, мы позволяем FB сказать нам,кто уже перекрестно коррелирует с нашим профилем. Это значительно снижает вероятность того, что вас заметят.
 12. Посты: 1 августа Facebook отключил доступ ко всем приложениям 3-й части, за исключением страниц messenger или FB. Раньше мы использовали IFTTT и WordPress для автоматической публикации, но сейчас они сломаны. IFTTT по-прежнему работает для twitter.
 13. Избегайте политических чатов и комментариев. Политика и социальные вопросы находятся высоко на радаре сторожевых псов ФБ из-за фальшивых новостей и проблем фальсификации избирателей.
 14. Следите за скрытыми учетными записями в электронной таблице или, еще лучше, в менеджере паролей.
 15. Sim-джекинг аккаунтов Twitter очень популярен, поэтому используйте длинные парольные фразы даже на своих фейк аккаунтах и выключайте 2-фактор, если они являются зрелыми или другими ценными аккаунтами
 16. Знайте политику своих агентств в отношении таких вещей, как дружба и любые необходимые уровни одобрения или документации
 17. ...и конечно, мы всегда используем наши силы во благо, поэтому мы всегда предполагаем, что наше расследование в конечном итоге увидит свет , поэтому убедитесь, что вы гордитесь тем, как ваша деятельность будет выглядеть в ретроспективе объективно
- 3-я сторона в отношении разумного и ответственного

Примечание: это чисто анекдотический случай, но в дополнение к тому, чтобы “войти в характер” и заставить наши аккаунты чувствовать себя реальными, я подозреваю, что может быть какая-то ценность в том, чтобы время от времени нажимать на рекламу и другой контент, который платформа толкает на вас. Это не лучшая практика конфиденциальности/безопасности, но существуют алгоритмы обнаружения, которые могут способствовать положительному рейтингу. Опять же, это всего лишь теория.

ЛОГОТИП ЗДЕСЬ

Название компании/
раздел организации
или имя аналитика

Следственный Профиль С Открытым Исходным Кодом

Резюме выводов

Идентификатор субъекта

Имя:		Дата рождения:	
Адрес:		Телефон #1:	
		Телефон #2:	
Работодатель:		НСС#:	
Машины:		Родственники:	

Альтернативные личности или ассоциации

Email #1:		Email #2:	
Email #3:		Email #4:	
Никнейм:		UN #2	
Facebook :		FB #	
Twitter:		TW #:	
Instagram:		IG #:	

Фото/видео

	Описание	Источник
☐ Фото		
☐ Видео		

Вложения

- | | |
|--|---|
| ☐ Профиль в Excel | ☐ Отчет Об Анализе Ссылок |
| ☐ Источник данных DVD | ☐ Всесторонний TLO, Clear, Accurint Report |
| ☐ Фотоматериалы | ☐ DOL/GOV проверки |
| ☐ Hunch.ly Архив | ☐ Другое: _____ |

ГОРЯЧИЕ КЛАВИШИ

ВЫПОЛНЕНИЕ 1,000 НЕБОЛЬШИХ ЗАДАНИЙ НЕМНОГО БЫСТРЕЕ

Сочетания Клавиш Windows	Сочетания Клавиш Mac
Windows Key + R: переход к окну "Выполнить"	Command + X: вырезание выделенного объекта и его копирование в буфер.
Windows Key + E: войти в окно "Компьютер"	Command + C: копирование выделенного объекта в буфер обмена.
Alt + Tab: переключиться между открытыми приложениями.	Command + V: вставка содержимого буфера обмена.
Windows Key + Up Arrow: Развернуть открытое окно.	Command + Z: отмена предыдущей команды.
Ctrl + Shift + Esc: Открыть диспетчер задач.	Command + A: выбор всех объектов.
Windows Key + Break: Открывает настройки системы.	Command + F: поиск объектов в документе или открытие окна Find.
Windows Key + F: переход в Центр отзывов или снимок экрана.	Command + H: скрывание окна активного приложения.
Windows Key + D: открыть рабочий стол.	Command + N: создание новой папки в Finder.
Alt + ESC: переключиться между элементами в порядке, в котором они открывались.	Command + O: открытие папки «Документы».
Alt + Letter: Выберите пункт меню по нажатой букве.	Command + P: Печатать документ.
Ctrl + Esc: Открывает стартовое меню.	Command + S: Сохранить документ.
Ctrl + F4: Закрыть активное окно.	Command + W: Закрыть активное окно.
Alt + F4: Выйти из активного приложения.	Command + Q: Выйти из приложения.
Alt + Spacebar: открыть контекстное меню окна.	Command + M: свертывание активного окна в значок на панели Dock.
Ctrl + Left or Right Arrow: Перемещение курсора вперед или назад на одно слово.	Command + Spacebar: отображение или скрывание поля поиска Spotlight.
Ctrl + Up or Down Arrow: Перемещение курсора вперед или назад на один абзац.	Command + Tab: переключение на следующее приложение.
F1: вызов справки.	Command + B: Обрезать выделенный текст.
Windows Key + M: Минимизировать все окна.	Command + I: Выделить текст курсивом.
Shift + Windows Key + M: свернуть все открытые окна.	Command + U: Подчеркнуть выделенный текст.
Windows + F1: Открывает поддержку windows.	Command + Semicolon (;): Найти в документе слова с ошибками.
Windows + Tab: запуск представления задач.	Option + Command + Esc: Выбрать приложение для выхода.
Windows + Break: Открывает диалоговое окно Свойства системы.	Shift + Command + Tilde (~): Переключение между открытыми окнами.
Удерживайте правую клавишу SHIFT в течение восьми секунд: Включить или отключить фильтрацию ввода.	Shift + Command + 3: Сделать скриншот.
Left Alt + Left Shift + Print Screen: вкл. и выкл.высокой контрастности.	Fn + Up Arrow: Прокроллить вверх.
Left Alt + Left Shift + Num Lock: вкл и выкл клавиш мыши.	Fn + Down Arrow: Прокроллить вниз.
Нажмите Shift пять раз: вкл и выкл липкие клавиши.	Fn + Left Arrow: Прокрутка к началу документа.
Удерживайте Num Lock в течение пяти секунд: вкл и выкл тумблеры.	Fn + Right Arrow: Прокрутка к концу документа.
Ctrl+Tab передвижение по вкладкам вперед.	
F11 свернуть или развернуть текущее окно.	Finder Shortcuts
Ctrl+A выделить все элементы в окне или документе.	Shift + Command + F: Открыть все мои файлы.
Ctrl+C Копировать.	Shift + Command + K: открытие окна «Сеть».
Ctrl+V Вставить.	Option + Command + L:открытие папки «Загрузки».
Win+R, потом напечатать 'cmd' Командная строка.	Shift + Command + O: открытие папки «Документы».
Tab Автозаполнение имени папки или файла.	Shift + Command + U: открытие папки «Утилиты».
Alt-Tab Переключение Между Открытыми Приложениями.	Option + Command + D: отображение или скрывание панели Dock.
Windows logo key + Tab запуск представления задач.	Shift + Command + Nсоздание новой смарт-папки.
Windows logo key + X Выключить.	Command + Delete: перемещение выделенного объекта в корзину.
Windows logo key + L Заблокировать.	Shift + Command + Delete: очистка корзины.

*www.quinnssmtbrand.com/windows-keyboard-shortcut/



ГОРЯЧИЕ КЛАВИШИ

ВЫПОЛНЕНИЕ 1,000 НЕБОЛЬШИХ ЗАДАНИЙ НЕМНОГО БЫСТРЕЕ

Chrome	
Горячая клавиша	Описание
Alt+Home	Открыть домашнюю страницу в текущей вкладке
Alt+Left Arrow	Открыть предыдущую страницу из истории просмотров в текущей вкладке
Alt+Right Arrow	Открыть следующую страницу из истории просмотров в текущей вкладке
F11	Включить или отключить полноэкранный режим
Esc	Остановить загрузку страницы
Ctrl+(- or +)	Приблизить или отдалить
Ctrl+1-8	Перейти на определенную вкладку
Ctrl+9	Перейти на крайнюю правую вкладку
Ctrl+0	Восстановить масштаб страницы по умолчанию
Ctrl+Enter	Эта комбинация используется для быстрого заполнения адреса. Например, введите "computerhope" в адресной строке и нажмите Ctrl+Enter, чтобы получить https://www.computerhope.com .
Ctrl+Shift+Del	Открыть окно "Очистить историю"
Ctrl+Shift+B	Показать/скрыть панель закладок
Ctrl+A	Выделить всё
Ctrl+D	Добавить текущую веб-страницу в закладки
Ctrl+F	Открыть панель поиска, чтобы найти текст на текущей странице
Ctrl+O	Открыть сохраненный на компьютере файл в Chrome
Ctrl+Shift+O	Открыть менеджер закладок.
Ctrl+H	Открыть историю просмотров в новой вкладке
Ctrl+J	Открыть страницу "Скачанные файлы" в новой вкладке
Ctrl+K or Ctrl+E	Выполнить поиск из любой области страницы
Ctrl+L	Перейти к адресной строке
Ctrl+N	Открыть новое окно
Ctrl+Shift+N	Открыть новое окно в режиме инкогнито
Ctrl+P	Открыть параметры печати текущей страницы
Ctrl+R or F5	Обновить текущую страницу
Ctrl+S	Открыть параметры сохранения текущей страницы
Ctrl+T	Открыть новую вкладку и перейти на нее
Ctrl+U	Просмотреть HTML-код текущей страницы (без возможности редактирования)
Ctrl+W	Заккрыть активную вкладку
Ctrl+Shift+W	Закрывает выбранное в данный момент окно.
Ctrl+Shift+T	Открыть закрытые вкладки в порядке закрытия
Ctrl+Tab	Перейти на следующую открытую вкладку
Ctrl+Shift+Tab	Перейти на предыдущую открытую вкладку
Ctrl+Left-click	Открывает ссылку в новой вкладке в фоновом режиме.
Ctrl+Shift Left-click	Открыть ссылку в новой вкладке и переключиться на новую вкладку.
Ctrl+Page Down	Перейти на следующую открытую вкладку
Ctrl+Page Up	Перейти на предыдущую открытую вкладку
Spacebar	Прокрутить веб-страницу вниз (одно нажатие – один экран)
Shift+Spacebar	Прокрутить веб-страницу вверх (одно нажатие – один экран)
Home	Перейти к верхней части страницы
End	Перейти к нижней части страницы
Alt+Down Arrow	Отображение всего предыдущего текста, введенного в текстовое поле, и доступных параметров в раскрывающемся меню.

*Shortcut List Source: www.computerhope.com



ГОРЯЧИЕ КЛАВИШИ

ВЫПОЛНЕНИЕ 1,000 НЕБОЛЬШИХ ЗАДАНИЙ НЕМНОГО БЫСТРЕЕ

Firefox	
Горячая клавиша	Описание
F5	Обновить
F11	Включить/выключить полноэкранный режим
Esc	Остановить загрузку страницы
Spacebar	Перейти вниз/вверх на высоту экрана
Alt+Home	Перейти на домашнюю страницу
Alt+Down arrow	Отображение предыдущего текста, введенного в поле, и доступных параметров в раскрывающемся меню.
Alt+Left Arrow	Назад
Alt+Right Arrow	Вперед
Ctrl+(- or +)	Увеличьте или уменьшите размер шрифта, нажав " - " уменьшится, а " + " увеличится. Ctrl +0 вернет значение по умолч
Ctrl+D	Перейти к адресной строке
Ctrl+F	Найти на этой странице
Ctrl+H	Журнал посещений
Ctrl+I	Закладки
Ctrl+J	Загрузки
Ctrl+K or Ctrl+E	Поиск в Интернете
Ctrl+L	Выделить весь текст в панели адреса
Ctrl+N	Новое окно
Ctrl+O	Открыть файл
Ctrl+P	Печать
Ctrl+T	Открыть новую вкладку
Ctrl+U	Исходный код страницы
Ctrl+F4 or Ctrl+W	Закрыть вкладку
Ctrl+F5	Принудительное обновление (не использовать закэшированные данные)
Ctrl+Enter	Дополнить адрес доменным суффиксом .com
Ctrl+Tab	Прокрутка недавно открытых вкладок
Ctrl+Shift+Del	Удалить недавнюю историю
Ctrl+Shift+B	Боковая панель закладок
Ctrl+Shift+J	Открывает консоль
Ctrl+Shift+P	Новое приватное окно
Ctrl+Shift+T	Открыть закрытые вкладки в порядке закрытия
Ctrl+Shift+W	Закрыть текущее окно
Shift+Spacebar	Прокрутить веб-страницу вверх (одно нажатие – один экран)
Ctrl+Shift+Tab	Прокрутить веб-страницу вверх (одно нажатие – один экран)
Ctrl+Left-click	Открыть ссылку в новой вкладке в фоновом режиме.
Ctrl+Shift Left-click	Открыть ссылку в новой вкладке и переключиться на новую вкладку.
Ctrl+Page Down	Прокрутить веб-страницу вниз (одно нажатие – один экран)
Ctrl+Page Up	Прокрутить веб-страницу вверх (одно нажатие – один экран)
Spacebar	Прокрутить веб-страницу вниз (одно нажатие – один экран)
Shift+Spacebar	Прокрутить веб-страницу вверх (одно нажатие – один экран)
Home	Начальная страница
End	Вниз страницы
Alt+Down Arrow	Отображение всего предыдущего текста, введенного в текстовое поле, и доступных параметров в раскрывающемся меню.

*Shortcut List Source: www.computerhope.com

BUSCADOR 2.0

OSINT LINUX ДИСТРИБУТИВ

Примечания По Установке (2.0)

Для использования этой системы вам понадобится приложение виртуальной машины. VirtualBox является бесплатным и будет достаточно для большинства исследований. Некоторые пользователи предпочитают более надежный вариант с VMWare Workstation для Windows или VMWare Fusion для Mac. Любой из этих вариантов поможет вам начать работу.

Установка и настройка VirtualBox:

* Убедитесь, что у вас установлена последняя версия VirtualBox и VirtualBox Extension Pack

- 1) в меню VirtualBox выберите Файл > импорт устройства
- 2) Перейдите к файлу OVA, который был загружен (Buscador)
- 3) Выберите этот файл и выберите пункт “Импорт”
- 4) Перед запуском новой машины выделите ее и выберите пункт “Настройки”
- 5) В разделе Общие > основные переименуйте эту машину по желанию (Buscador?)
- 6) В разделе Общие > дополнительно измените общий буфер обмена на двунаправленный
- 7) В разделе Система > материнская плата увеличьте объем оперативной памяти, если у вас достаточно ресурсов (половина от общей системы)
- 8) В разделе Дисплей > экран увеличьте объем видеопамати до 128 МБ
- 9) В разделе Общие папки нажмите кнопку “плюс” справа, выберите папку для хранения доказательств, выберите пункт “автоматическое монтирование”
- 10) Дважды нажмите кнопку “ОК”, затем запустите новую машину (двойной щелчок)
- 11) При загрузке войдите в систему пользователя “osint” с паролем osint
- 12) В меню VM, выберите "устройства" > “вставить гостевые дополнения образа диска ”
- 13) Нажмите кнопку “Отмена”, когда появится диалоговое окно.
- 14) Открыть терминал (Tilex)
- 15) в терминале создайте каталог на рабочем столе под названием vbox: `mkdir ~/Desktop/vbox`
- 16) скопируйте все с компакт-диска на рабочем столе в папку vbox (Скопировать/Вставить)
- 17) В терминале введите следующие команды:

```
cd Desktop/vbox
```

```
chmod +x *.sh
```

```
./autorun.sh
```

(Введите пароль при появлении запроса)

18) Разрешите установку образа и перезагрузите его после завершения работы.

19) Запустите терминал в новой виртуальной машине и введите `sudo adduser osint vboxsf`

20) Укажите пароль по мере необходимости (osint)

21) Перезагрузитесь

Теперь у вас должен быть доступ к общему каталогу, чтобы сохранить данные в операционной системе хоста (evidence). Его можно найти в файловом менеджере (Главная страница), в левой колонке, озаглавленной “sf_”, за которой следует имя папки, к которой он подключен. Эта общая папка также будет находиться на вашем рабочем столе для легкого доступа. Вы можете сделать машину полноэкранной, скопировать и вставить текст на изображение и обратно, и вы готовы начать использовать приложения.

Поддержка И Обновления

Откройте Tilex (терминал) и введите следующие команды:

Запуска:

Update_scripts больше не нужны!

Обновление Video Download

```
sudo -H pip install --upgrade youtube-dl
```

Обновление Spiderfoot:

```
cd /opt/spiderfoot
```

```
git reset --hard
```

```
git pull
```

```
sudo reboot
```