OSINT Cheat-Sheet

Investigative Resources - Summer 2019

INTELTECHNIQUES
.com

Methodology | Preparation | Execution | Documentation

Pre-Operational Considerations

- Ethical and Legal Assessment
- Deliverables and Scope
- Time and Resource Constraints
- Exposure/Risk Factors
- Adversary Sophistication
- Communication and Sit-reps
- Control Expectations

Workspace & Tools

- Clean/Secure Workstation
- Clean/Secure Connectivity
- Fresh Research Accounts
- Clean Browser w/Extensions
- Collection Tools
- Documentation System
- Storage/Archiving Solution

Investigative Steps

- Knoll Your Tools
- Define The Question
- Document Your "Knowns"
- Set Up Collection
- Query, Sweep, and Pivot
- Consolidate Findings
- Complete Reporting and Archive

OSINT Resources

- OSINTFramework.com
- OSINTBrowser.com
- Netbootcamp.org
- Workinukraine.space
- Investigativedashboard.org
- Start.me/p/b56xX8/osint

Tab Management

https://www.one-tab.com/ (Local Storage Only)
Simple Tab Management/Export For Chrome and Firefox

http://www.gettoby.com/ (Account Bases w/Sync)
Thumbnailed Tab Management For Chrome and Firefox

https://chrome.google.com/webstore/detail/graphitabs/dcfclemgmkccmnpgnldhldjmflphkimp?hl=en GraphiTabs - Tree View of Tabs

https://clusterwm.com/
Simple Tab Manager w/Export (Sync Premium Offered)

http://tabsoutliner.com/
Tab Management - Outline Format, Export, Sync (Paid version)

https://www.gettabli.com/
Simple, Private (offline-storage only) Tab Management

Link Analysis/Visualization

https://www.paterva.com/buy/maltego-clients.php
Maltego CE and CaseFile

https://vis.occrp.org/
Create Link Charts - Organized Crime & Corruption Project

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

https://www xmind.net/
Mind Mapping - Free and Paid Versions

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

http://www.visualsitemapper.com/
Domain Mapping

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

https://github.com/woj-ciech/Danger-zone
Link IPs, Domains, and Email Addresses

https://www.mindmup.com/
Mind Mapping - Free and Paid Tiers

https://www.nodexlgraphgallery.org/Pages/Registration.aspx
Powerful Graphing Client - Free and Paid Tiers

Useful Browser Extensions

https://www.onenote.com/clipper
Screen Capture and Tag (One-Note Users Only)

https://getfireshot.com/
Screen Capture and Annotation (as image or pdf)

https://github.com/ssborbis/ContextSearch-web-ext
Context Menu Search Menu

http://www.osintbrowser.com/
OSINT Bookmarks

https://github.com/az0/linkgopher/
Simple Link Extraction

https://github.com/marklieberman/downloadstar
Firefox - Download all items in a webpage that match a pattern

https://github.com/mozilla/multi-account-containers#readme
Firefox - Multi-Account Containers (Compartmentalization)

https://github.com/mozilla/multi-account-containers#readme
Firefox - Multi-Account Containers (Compartmentalization)

https://webrobots.io/
Scrape YP, Yelp, Ebay, Amazon, etc. Save as Excel or CSV

My Workstation Setup

Workstation - Win 10, PIA/ProtonVPN, Chrome/Firefox, Vbox, Buscador/Kali, Nox/Geny, Hunch.ly, UC Cable/Mifi, Keypass, Malwarebytes, Glasswire

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

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

Office Software - 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

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

Google Operators

Remember we can string multiple operators together

site:	Limit results to those from a specific domain site:apple.com
" "	Quotes indicate search for exact term "red rider BB gun"
AND	Only show results for both terms apple AND orange
OR	Search for term A, term B, or both. A pipe symbol is the same as OR. gun OR rifle is the same as gun | rifle
*	Wildcard for words in a phrase that you don't know wish * a star
( )	Group a set of words/operators separately (gun | pistol) ammo
-	Exclude results including this word chicago baseball -cubs
$	Search for a certain price "apple watch" $299
cache:	Most recent cached version of a domain cache:boston.gov
filetype:	Only search for specific filetype, ext: works the same filetype:pdf "confidential" or ext:pdf "confidential"
related:	Search for sites related to a domain related:sony.com
intitle:	Find pages with a term in the page title intitle:sabotage
inurl:	Find pages with a term in the url inurl:private
around(x)	Find pages with terms in X words proximity of each other microsoft (7) surface
info:	Sometimes shows related pages, cache date etc. info:chicago.gov
Adv. Search	https://www.google.com/advanced_search

More Operators: https://ahrefs.com/blog/google-advanced-search-operators/

DuckDuckGo

DuckDuckGo handles some operators a little differently

Cats dogs	Results about cats or dogs
"cats and dogs"	Results for exact term "cats and dogs". If no results are found, we'll try to show related results.
cats +dogs	More dogs in results
cats filetype:pdf	PDFs about cats. Supported file types: pdf, doc(x), xls(x), ppt(x), html
dogs site:example.com	Pages about dogs from example.com
Cats -site:example.com	Pages about cats, excluding example.com
intitle:dogs	Page title includes the word "dogs"
inurl:cats	Page url includes the word "cats"

Startpage

Startpage makes Google requests on your behalf (privacy)

Operators	Most standard Google operators work
Adv. Search	HTTPS://WWW.STARTPAGE.COM/EN/ADVANCED-SEARCH.HTML
Search Tips	https://support.startpage.com/index.php?/Knowledgebase/List/Index/1

Bing Operators

Most of the Google operators work in Bing

( )	Just like Google, terms or operators grouped in parenthesis are processed together and separate from other conditions
OR	All Bing searches are treated as AND searches unless you specify OR between terms goat OR pig OR cow
NOT	Exclude results with a specific term(s) the – symbol also works boat NOT (raft OR ship)
loc:	Return pages from a specific region(s) dogs (loc:GB OR loc:FR)
prefer:	Weight results in favor of a term prefer:tomato plum apple
near:x	Words in x proximity of each other red near:4 blue
ip	Finds sites hosted on an IP address ip:208.43.115.82
site/domain:	Filter for specific domain type site/.gov confidential
feed:	Finds RSS feeds based on search terms feed:osint
Bing Adv.	MS retired Bing's advanced search page

info:https://www.lifewire.com/bing-advanced-search-3482817

Yandex

Most standard Boolean operators work (Google operators) such as site: and "quotes"

Adv. Search	Click the ⚙ icon in the search bar
lang:	Language filter ccn lang:fr
mime:	Similar to filetype mime:docx gdpr
date:	Page modified date bombing date:20180416
url:	Similar to site: but adding a * to the end of the url pulls up any docs sharing that url url: Alice url:en.wikiquote.org/wiki/*

SPECIAL OPERATORS: HTTPS://YANDEX.COM/SUPPORT/DIRECT/KEYWORDS/SYMBOLS-AND-OPERATORS.HTML

Baidu

Most standard Google Operators work on Baidu

Adv. Search	https://www.baidu.com/gaoji/advanced.html
In English	http://www.baiduinenglish.com/
Search Tips	https://www.seomandarin.com/baidu-search-tips.html

Other International

Consider using a proxy or VPN to appear in the target region

Adv. Search	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

Don't forget Google - "site:twitter.com keyword"

Advanced Search	https://twitter.com/search-advanced
Toolset	http://tweetbeaver.com/
User Report	https://tinfoleak.com/
Analytics	https://socialbearing.com/
Analytics	https://analytics.mentionmapp.com/
Analytics	https://foller.me
Analytics	http://twiangulate.com/search/
Older Posts	http://staringispolite.github.io/twayback-machine/
Search	https://snapbird.org/
Followers	https://doesfollow.com
Video	https://twdown.net/
Visualization	https://treeverse.app/
Profile Changes	https://spoonbill.io/
Mapping	https://onemilliontweetmap.com
Inteltechniques	https://inteltechniques.com/menu/pages/twitter.tool.html
Legal Requests	https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#19

Snapchat

User Search	https://somesnapcode.com/
User Search	https://www.snapdex.com/
Loc Search	https://map.snapchat.com
Loc Search	https://sovip.io

https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf

Reddit

Don't Forget Google - site:reddit.com keyword

Topic Search	https://www.reddit.com/search?q=keyword
User Search	https://www.reddit.com/user/username
Analytics	https://pushshift.io/api-parameters/
Archives	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

Search	https://tiktokapi.ga/
Search	https://www.osintcombine.com/tiktok-quick-search
How To IOS	https://www.pageflows.com/post/ios/general-browsing/tiktok
How To Android	https://www.wikihow.tech/Find-Friends-on-Tik-Tok-on-Android
Downloader	https://en.savefrom.net/download-from-tiktok
Video Caputre	HTTPS://AIRMORE.COM/WATCH-TIK-TOK-PC.HTML
Legal Requests	https://www.tiktok.com/en/law-enforcement

Facebook

Warning: Many of these tools may not function correctly as Facebook continues to kill graph search capabilty. https://www.vice.com/en_ca/article/zmpgmx/facebook-stops-graph-search

FB Expand	http://com.hemiola.com/bookmarklet/
Messenger	https://www.messenger.com/
Mobile View	https://m.facebook.com/
FB Videos	https://www.facebook.com/watch
Video Download	https://www.fbdown.net/index.php
Video Download	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 runs some tracking scripts)
Graph Search	https://inteltechniques.com/menu/pages/facebook.tool.html (Reminder FB Graph Is Broken as of 8/2019)
Graph Search	http://socmint.tools/graph.htm
Graph Search	https://peoplefindthor.dk/
Graph Search	https://pitoolbox.com.au/facebook-tool/
Graph Search	https://searchisback.com/
Graph Search	https://whopostedwhat.com/
Graph Search	https://www.uk-osint.net/facebook.html
Graph Search	https://github.com/sowdust/searchbook
Graph Discussion	https://inteltechniques.com/blog/2019/08/02/the-privacy-security-osint-show-episode-133/
Legal & Privacy	https://www.facebook.com/safety/groups/law/guidelines

Instagram

User/Tag Search	https://www.yooying.com/search
User/Tag Search	https://www.social-searcher.com/
Hashtag Search	https://tagboard.com/
Analyze Followers	https://hypeauditor.com/
Location Search	https://www.osintcombine.com/instagram-explorer
Search	https://mulpix.com/
Media Capture	https://downloadgram.com/
Media Capture	https://instasave.xyz/
Downloader	https://www.4kdownload.com/products/product-stogram
Profile Pic	https://instadp.net/
Profile Pic	http://izuum.com/
Stories	https://storiesig.com/
Image Search	https://imgwonders.com/
User/Hashtag	http://picdeer.com/
User/Hashtag	https://www.pictame.com/
Inteltechniques	https://inteltechniques.com/menu/pages/instagram.tool.html

INTELTECHNIQUES .com

Site Archives

Searching pre-existing archives or requesting a capture

Wayback Machine	http://archive.org/web/
Archive Today	http://archive.fo/
How To - Bellingcat	https://www.bellingcat.com/resources/how-tos/2018/02/22/archive-open-source-materials/
How To - Tech.co	https://tech.co/news/tools-to-help-you-search-the-archived-internet-2018-06
Mass Archive Script	https://github.com/motherboardgithub/mass_archive

Photo/Image Search

Reminder: we do not upload sensitive photos to the internet

Search/Reverse	https://images.google.com/
Search/Reverse	https://tineye.com
Search/Reverse	https://www.bing.com/images/
Reverse Russia	https://www.yandex.com/images/
Reverse Asia	http://images.baidu.com/
Search	http://www.picsearch.com/
Twitter Search	http://twipho.net/
Flickr	https://www.flickr.com/map
Exif	http://exif.regex.info/exif.cgi
Edit Detection	http://www.errorlevelanalysis.com/
Basic Forensics	https://fotoforensics.com/
Text Recog.	https://www.newocr.com/
Stolen Check	www.stolencamerafinder.com/

Video

Extension	https://www.downloadhelper.net/
Youtube-DL	https://github.com/ytdl-org/youtube-dl
Extension	https://addons.mozilla.org/en-US/firefox/addon/video-downloader-profession/
Screen Capture	https://www.techsmith.com/screen-capture.html
Video Archives	https://archiving.witness.org/archive-guide/acquire/acquiring-raw-video-and-metadata/

Document Search

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

Maps/Locations

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/wayback/
https://www.gpsies.com/trackList.do	https://www.zillow.com/

Capture/Collection Tools

Although not open-source, Hunch.ly remains my go-to ;safety-net & collection too.

Hunch.ly	https://hunch.ly/try-it-now https://hunch.ly//guides
Screen Capture Extension	https://getfireshot.com/
Snip & Sketch	https://www.microsoft.com/en-us/p/snip-sketch/9mz-95kl8mr0l#activetab=pivot:overviewtab
Annotation	https://www.diigo.com/
OneNote Clip	https://www.onenote.com/clipper
Spiderfoot	https://www.spiderfoot.net/

Documentation Tools

Hunch.ly's Report Builder Is Great To Build Off Of

OneNote	https://www.onenote.com
Win Text Editor	https://notepad-plus-plus.org/
Mac Text Editor	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/
Private Notes	https://app.standardnotes.org/
Office Alternative	https://www.libreoffice.org/

OSINT Resource Lists

Collections curated by my favorite OSINT experts:

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/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit
Sprp77	https://drive.google.com/drive/folders/1CBcemFdorkAqJ-Sthsh67OVHgH4FQF05
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

Real Name

“People” search engines

TruePeopleSch	https://www.truepeoplesearch.com/
Spokeo	https://www.spokeo.com/
Thatsthem	https://thatsthem.com/
Adv Background	https://www.advancedbackgroundchecks.com/
Nuwber	https://nuwber.com/
FamTreeNow	https://www.familytreenow.com/
PeopelByNm	http://www.peoplebyname.com/
UFind	http://ufind.name/...
PublicRcrds	https://publicrecords.directory/
GoLookup	https://golookup.com/
PMR	http://publicemailrecords.com/name_listings
Radaris	https://radaris.com/
Cubib	https://cubib.com/
ComLullar	http://com.lullar.com/
Yasni	http://www.yasni.com/
TabSearch	https://www.zabasearch.com/
Spytox	https://www.spytox.com/
Intelius	https://www.intelius.com/
ZoomInfo	https://www.zoominfo.com/
Whoodle	https://www.whoodle.com/
PeekYou	https://peekyou.com/
Webmil	http://webmii.com/
CvGadget	https://cvgadget.com/
Classmates	https://www.classmates.com/
192 (UK)	https://www.192.com/
Inteltechniques	https://inteltechniques.com/menu/pages/person.tool.html

Email

Don’t Forget A Basic Google Search “user@domain.com”

Hunter.io	https://hunter.io/ (make a free account)
HIBP	https://haveibeenpwned.com/ (may be premium soon)
Verify	https://tools.verifyemailaddress.io/
Verifalia	https://verifalia.com/validate-email
Mailtester	http://www.mailtester.com/testmail.php
FindThatEmail	http://findthat.email/
AnyMailFinder	https://anymailfinder.com/
EmailMatcher	https://emailmatcher.com/
ProspectLinked	https://prospectlinked.com/#/home
MetricSparrow	http://metricsparrow.com/toolkit/email-permutator/
ThatsThem	https://thatsthem.com/reverse-email-lookup
Spokeo	https://www.spokeo.com/email-search
PsbDmp	https://psbdmp.ws/
HackedEmails	https://hacked-emails.com/
OCCRP	https://data.occrp.org/search?q=gmail.com
Dehashed	https://dehashed.com/
Hashes.org	https://hashes.org/leaks.php
Gravatar	https://en.gravatar.com/site/check/lorangb@gmail.com
ReverseGenie	http://www.reversegenie.com/searching=email
ManyContacts	https://www.manycontacts.com/en/mail-check
ComLullar	http://com.lullar.com/
Inteltechniques	https://inteltechniques.com/osint/menu.email.html
Basic Guide	https://www.blurbiz.io/blog/the-most-complete-guide-to-finding-anyones-email

OSINT Flow Charts: https://www.dfir.training/osint

User Names

Knowem	https://knowem.com/checksocialnames.php?u=
NameChk	https://namechk.com/
NameCheckr	https://www.namecheckr.com/
NameVine	https://namevine.com/
UserSearch	https://usersearch.org/
UserSherlock	http://usersherlock.com/
Profilr	https://www.profilr.social/search/
Tinder	https://www.gotinder.com/@user
Amazon	https://www.google.com/search?q=site%3Aamazon.com+%22name%22
SocialCatfish	https://socialcatfish.com/reverse-username-search/
WhatsMyName	https://github.com/webbreacher/whatsmyname
Sherlock	https://github.com/sherlock-project/sherlock
Inteltechniques	https://inteltechniques.com/menu/index.html

Classifieds

Ebay	https://www.ebay.com/
Fatfingers	http://fatfingers.com/default.aspx
Flippity	http://www.flippity.com/
Kijiji	https://www.kijiji.ca/
SearchAllJunk	http://www.searchalljunk.com/
SearchTempest	https://www.searchtempest.com/
NotiCraig	https://noticraig.com/
Oodle	https://www.oodle.com/local/burien-wa/
Offerup	https://offerup.com/
Craigslist	https://craigslist.org
Inteltechniques	https://inteltechniques.com/menu/pages/communities.links.html

INTELTECHNIQUES .com

Phone Numbers

For phone #s consider gov/paid options (OSINT is limited)

Zaba	https://www.zabasearch.com/reverse-phone-lookup/
USPhoneBook	https://www.usphonebook.com/
TruePeopleSearch	https://www.truepeoplesearch.com/#
Whitepages+	https://whitepages.plus/
ThatsThem	https://thatsthem.com/
TrueCaller	https://www.truecaller.com/
Whitepages	https://www.whitepages.com/reverse-phone | Reverse Phone Lookup
411	https://www.411.com/reverse-phone
CellRevealer	https://www.cellrevealer.com/
FoneFinder	http://www.fonefinder.net/
WhoCalld	https://whocalld.com/
SpyDialer	https://www.spydialer.com/
Searchbug	https://www.searchbug.com/tools/
NumberGuru	https://www.numberguru.com/phone/
ReverseGenie	http://www.reversegenie.com/
YellowPages	https://people.yellowpages.com/whitepages/?re=SP_people_search
Spokeo	https://www.spokeo.com/reverse-phone-lookup
PhoneValidator	https://www.phonevalidator.com/index.aspx
CallerIDTest	https://www.calleridtest.com/
IMEI	https://www.imei.info/
IMEI24	https://imei24.com/phone_base/
Sync	https://sync.me/
Infobel	https://www.infobel.com/
DialingCode	http://www.dialingcode.com/
OpenCnam	https://www.opencnam.com/
TeleFoonGids	https://telefoongids.2link.be/
ServiceObjects	https://www.serviceobjects.com/developers/lookups/geophone-plus
WTNG	http://www.wtng.info/index.html
SeanLawson	https://www.seanlawson.net/2019/02/use-chrome-developer-tools-view-masked-phone-numbers-for-free-people-search/
NANPA	https://www.nationalnanpa.com/enas/coCodeReportUnsecured.do?reportType=7
Inteltechniques	https://inteltechniques.com/osint/menu.phone.html

Vehicles

CarOwners	https://carsowners.net
NICB	HTTPS://WWW.NICB.ORG/VINCHECK
OReilly	https://www.oreillyauto.com/
Carvana	https://www.carvana.com/
CheckThatVIN	https://checkthatvin.com/ctv#/home
CarFax	https://www.carfax.com/processQuickVin.cfx
VehicleHistory	https://www.vehiclehistory.com/license-plate-search
CarOwners	https://carsowners.net/

Domains/IPs

Censys	https://censys.io
IntelX	https://intelx.io
Domaintools	https://www.domaintools.com/
CentralOps	https://centralops.net/co/
Whoxy	https://www.whoxy.com/
IPLocation	https://www.iplocation.net/
DNSLytics	https://dnslytics.com/reverse-ip
Randhome	https://www.randhome.io/blog/2018/02/23/harpoon-an-osint-/-threat-intelligence-tool/
CrimeFlare	http://crimeflare.org:82/
Spyonweb	http://spyonweb.com/
Pub-DB	http://pub-db.com/
Whoisology	https://whoisology.com/
Visualping	https://visualping.io/
WatchThatPage	http://watchthatpage.com/
PentestTools	https://pentest-tools.com/information-gathering/find-subdomains-of-domain#
SharedCount	https://www.sharedcount.com/
SmallSEO	https://smallseotools.com/backlink-checker/
SimilarWeb	https://www.similarweb.com/
Alexa	https://www.alexa.com/siteinfo/inteltechniques.com
Hunter.io	https://hunter.io/
ViewDNS	https://viewdns.info/
Robtex	https://www.robtex.com/?=
Majestic	https://majestic.com/
D-Me	http://d-me.info/
Netcraft	https://www.netcraft.com/
DomainBigData	https://domainbigdata.com/
Inteltechniques	https://inteltechniques.com/osint/domain.search.html
Inteltechniques	https://inteltechniques.com/blog/2018/04/24/searching-subdomains-with-findsubdomains-com/
IP6Locator	http://ipv6locator.net/
ViewDNS	https://viewdns.info/
Maxmind	https://www.maxmind.com/en/home
IP2Location	https://www.ip2location.com/demo/
IPFingerprints	https://www.ipfingerprints.com/
ThatsThem	https://thatsthem.com/reverse-ip-lookup
Netbootcamp	https://netbootcamp.org/websitetool.html
Shodan	https://www.shodan.io/
Inteltechniques	https://inteltechniques.com/menu/pages/ip.tool.html#

INTELTECHNIQUES.com

Business & Organizations

Google: resume AND "real name"

OpenCorp	https://opencorporates.com/
Rocketreach	https://rocketreach.co/
OCCRP	https://data.occrp.org/
CorpWiki	https://www.corporationwiki.com/
Recruitin	https://recruitin.net/
Indeed	https://www.indeed.com/
MarketVisual	http://marketvisual.com/
AihitData	https://www.aihitdata.com/
Glassdoor	https://www.glassdoor.com/Reviews/index.htm
LittleSis	https://littlesis.org/
OpenSanctions	https://www.opensanctions.org/
CEOEmail	https://ceoemail.com/
Enigma	https://public.enigma.com/browse/collection/corp-watch-company-subsidiaries/
Angel	https://angel.co/
RipoffReport	https://www.ripoffreport.com/
Sector035's Guide	https://medium.com/@sector035/gathering-company-intel-the-agile-way-6db12ca031c9

LinkedIn

site:linkedin.com inurl:pub -inurl:dir "at Microsoft" "Current"

site:linkedin.com "Real Name"

User Query	HTTPS://GITLAB.COM/INITSTRING/LINKEDIN2USERNAME
Email Query	https://github.com/pry0cc/GoogLinked
Breach Data	https://archive.org/details/LIUsers.7z
Inteltechniques	HTTPS://INTELTECHNIQUES.COM/MENU/PAGES/LINKEDIN.TOOL.HTML

Misc. Tools & Tricks

Efficiency and Organizational Tools That I Use

Better Windows File Search	https://www.voidtools.com/
Synced Notes	https://www.onenote.com
Encrypted Coms	https://signal.org/
Encrypted Coms	https://wire.com/en/
Encrypted Email	https://protonmail.com/ (use the free tier for burner/seed accounts)
Hotkey Panel	https://www.elgato.com/en/gaming/stream-deck
NAS/Local Cloud	https://www.synology.com/en-us
Screen Capture	https://www.techsmith.com/store/snagit
Screen Capture	https://getfireshot.com/buy.php (pro supports multi-page pdf)
Paper Notebooks	https://www.costco.com/Moleskine-Cahier-6-Pack-Extra-Large-Notebooks.product.100300742.html
Veracrypt	https://www.youtube.com/watch?v=cxo8xosH_TI Veracrypt containers are ideal for archiving cases or placing them on flash media for delivery to clients.
Tech Issues	https://stackoverflow.com/ Aside from Googling your tech issues, stackoverflow has discussion on just about any desktop or software issue.

Gaming

Legal requests: https://www.search.org/resources/isp-list/

Discord Search	https://www.discordportal.com/
Discord Search	https://discordservers.com/
Discord Search	https://discord.center/
Discord Search	https://disboard.org/
Discord Search	https://discord.me/
Discord Search	https://support.discordapp.com/hc/en-us/articles/115000468588-Using-Search
Discord Capture	https://dht.chylex.com/ | Discord History Tracker
Twitch	https://www.twitchtools.com/
Fortnite	https://fortnitetracker.com/profile/search?q=
PSN	https://psnprofiles.com/search/
Mixer	https://www.lifewire.com/what-is-mixer-4156866
Steam	https://steamrep.com/ or https://steamid.uk/

Speed Tricks

Saving a few seconds here and there adds up over time

Context Search	https://github.com/ssborbis/ContextSearch-web-ext
Add As Search Engine	https://www.wired.com/2014/07/tip-week-chrome-site-search/
Default to Last Year	https://thepracticalsysadmin.com/defaulting-google-search-results-to-the-past-year/
Keyboard Shortcuts	https://www.quinnssmtbrand.com/windows-keyboard-shortcut/

Virtual Machines

Follow written steps verbatim when installing VMs

Buscador	https://inteltechniques.com/buscador/
Virtualbox	https://www.virtualbox.org/wiki/Downloads
VBox Extensions	https://download.virtualbox.org/virtualbox/6.0.10/Oracle_VM_VirtualBox_Extension_Pack-6.0.10.vbox-extpack
Kali Linux	https://www.kali.org/downloads/
Tails	https://tails.boum.org/
Update Linux	apt-get update && apt-get upgrade
Update Youtube-DL	sudo -H pip install --upgrade youtube-dl
Common Error	Make sure virtualization is enabled in BIOS settings
Host Key	Win - Right Control Key Mac - Left Command Key
Vbox Scale Issues	host + f, to switch to full screen mode, if not yet, host + c, to switch to/out of scaled mode, host + f, to switch back normal size, if need
3rd Party Overview	https://www.youtube.com/watch?v=7Y_fKC5EN10

INTELTECHNIQUES .com

Common Missteps

Methodology is more important that tools or techniques because those things change. Invest in defining strong process.

Failure to use non-OSINT approaches and strategies ie: social engineering (consider a friendly phone call)

Are you signed into a live session for the platform you are querying? ie: make sure you are signed into FB in another tab

Including a space at the end when pasting a account ID or other keyword into a query form field.

Do you have script blockers that might be preventing data from loading on a page? (ie:privacy badger, ublock, ghostery)

Location. Your search results are being scewed by yoru perceived location, consider using VPN to “relocate”.

Start looking at page source to see what is going on behind the scenes. If you only look at the gui, you are missing alot.

Tenacity wins the day. Most answers are not going to fall into your lap. **Patience** and **persistence** above all else.

More OSINT Resources

https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/ **(Bellingcat Toolkit)**

https://github.com/Ph055a/OSINT-Collection **(OSINT.Team Collection)**

https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT_Handbook_June-2018_Final.pdf **(I-Intelligence Collection)**

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

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

Operational Security - Browsers

Browser, Session, and Site Tests	
Device Fingerpint	https://panopticlick.eff.org/
Browser Fingerpint	https://amiunique.org/fp
Browser Fingerpint	https://www.deviceinfo.me/
Browser Fingerpint	https://browseraudit.com
Browser Fingerpint	https://browserleaks.com/
Browser Fingerpint	https://pixelprivacy.com/resources/browser-fingerprinting/
Browser Fingerpint	https://detectmybrowser.com/
IP Leaks	https://ipleak.net
DNS Leaks	https://www.dnsleaktest.com/
Email Leaks	https://www.emailprivacytester.com
Site Privacy Test	https://webbkoll.dataskydd.net/en/
Privacy Resources	https://inteltechniques.com/links.html

Operational Security - Windows

Recommended Tools For Windows Security	
Create Non-Privledged User	https://support.microsoft.com/en-us/help/4026923/windows-10-create-a-local-user-or-administrator-account
Anti-Virus	https://www.microsoft.com/en-us/windows/comprehensive-security
Anti-Malware	https://www.malwarebytes.com/mwb-download/
Anti-Spyware	https://www.safer-networking.org/
Windows Privacy	https://ssd.eff.org/en/module/how-delete-your-data-securely-windows
Win10 Privacy	https://www.thewindowsclub.com/privatewin10-advanced-windows-10-privacy-tool
Win10 Privacy	https://fdossena.com/?p=w10debotnet/index_1903.frag
Check Your MicroSoft Data	https://account.microsoft.com/account/privacy
Network Activity	https://www.glasswire.com/
Password Manager	https://keepassxc.org/
Cleaner	https://www.bleachbit.org/download/windows
Cleaning Manually	https://www.makeuseof.com/tag/best-way-clean-windows-10-step-step-guide/

Basic Investigative Steps

Working up your first case with your new tools and techniques

1. Set up your note-taking and data collection to track your work - paper notebook, One-Note, Hunch.ly, directory on encrypted flash drive, etc.
2. List your investigative goals - full profile, locate for apprehension, identify associates, collect digital evidence, etc. (are you collecting intel or evidence for court?)
3. List your seed info - emails, phone numbers, names, etc.
4. Run all of your paid and/or gov queries and use those to add to your seed information. If possible get a hold of a booking or DOL photo for comparison while researching social media.
5. Run Accurint (Lexis-Nexis), TLO, or Clear reports.
6. Fire up firefox/chrome with your plugins of choice - noscript, https everywhere, ghostery, fireshot, one-tab (or use browsers in Buscador VM)
7. If it’s a serious investigation I turn on hunch.ly and enter my "selectors" (keywords from seed info)
8. I do a quick Google search and check my people finder site of choice for that week. ["James McIntire" "Denver"] and then this week truepeoplesearch.com These are just quick for low hanging fruit.
9. Go to https://inteltechniques.com/menu.html (or your OSINT toolset of choice ie: osintframework.com) and use the tabs on the left hand side to select the categories that match your seed info. My typical order is email, real name, search engines, Facebook, twitter and then the rest depending on what you have to go on.
10. I exhaust inteltechniques.com tools closing any tabs that return false positives or no useful results. Any page that is important I note any identifiers (account IDs, user names, etc) on my notepad and fireshot a pdf of the page. That pdf is saved in the case directory. On a case with multiple targets create subfolders for each person of interest.
11. Either periodically or when I'm done with my research I copy/paste or manually enter any pertinent info into a profile or case report in either word or one-note. I embed any pertinent screen captures, pdfs such as lexis-nexis reports, and good photos of the targets, any vehicles and addresses.
12. I go over that report with the case detective or agent to explain my investigation and see if they have any questions or want any additional info.
13. My rough notes, workbooks, hunch.ly files, and/or cloned VMs (if I used buscador) are usually saved in case I need them for court. The exceptions are things like intel gathering for operations, events, threat assessments, etc. A hunch.ly export might be burned to disc as evidence but be cautious of any unintended data that might have been unintentionally saved during that session. The VM backup should not go into evidence as it would divulge trade-craft. Treat it as an undercover laptop that you can refer to, but avoid exposing it unless you are forced to (work with your prosecutor to fight this). If you don't need that VM for court, do not keep it (hording data comes with custodial responsibilities and potential liabilities).
14. I make sure I have a fresh VM for the next case or crisis that comes up. I also make new accounts to have in pocket if any of my research accounts were burned. Better to prepare for the next case at the end of the previous and be ready to go at a moments notice
15. Wash, rinse, repeat. Track successes to justify more equipment, staffing, and training.

Note: My standard setup is an off-grid windows pc, on a UC cable modem or mifi (VPN as appropriate).

For quick checks such as events, threats, etc. I stay in windows and just use chrome/Firefox and the links on inteltechniques.com. This is for convenience and speed with less fuss when there's less of a need for compartmentalization, security, and/or anonymity. For investigations I typically use Buscador with Hunch.ly installed, and all fresh research account. Quick utility vs. backstopped single purpose - use the right tool for each mission.

Building Reliable Research Accounts

This is a list of recommended steps for creating investigative/research social media accounts. These are largely based on feedback from our community and their experiences with having their accounts locked or suspended. Where applicable steps are in order of preference in regards to successfully avoiding security challenges.

Equipment Setup – It may seem simple, but the equipment and connection you are on matters.

1. Avoid VPNs during account creation, most of their IP ranges are flagged
2. Mifi's or dynamic IP devices work quite well for account creation
3. Public networks (Starbucks Wi-Fi) but be aware that you are being exposed and cross-correlated with other users on that network
4. Phone #- A real non-VOIP phone number will save you a lot of hassle, we recommend a $5 Mint sim card kit paired with an unlocked smart phone (mintmobile.com)
5. Online Footprint – "Google" your name and employer. Print the first two pages of results and include this in your binder as the "low hanging fruit" of personal data.

Covert Accounts

1. We usually make FB, IG, and Twitter at once and tie them in as one covert profile. Each adds depth and veracity to the others (intentional cross correlation).
2. Keep notes on your covert details either in a paper notebook or a digital format like a password manager or spread sheet, having your security requirements in mind.
3. If it is a sensitive or deep infiltration case make sure to compartmentalize this profile from the get-go (connection, browser, device (use VM to isolate), etc.)
4. Connection:
    - a. no VPN during account creation, most VPN IP blocks are flagged
    - b. Cellular data connections (MiFi's) are good – dynamic/shared IPs
    - c. Another technique is to get a free tier AWS EC2 or Digital Ocean VM and use it to make the account as then you will have an AWS IP, this is more advanced but works pretty well if you are comfortable with VMs and learning to navigate AWS. Some groups even run full investigative VMs on AWS, but again this is a more advanced setup that takes some work to sort out.
    - d. Another advanced technique is to roll your own VPN thru AWS as the providers tend not to flag AWS https://github.com/StreisandEffect/streisand
5. Email Address:
    - a. no Gmail, Hotmail, yahoo, or other top free mail (Gmx is an exception for now)
    - b. Private domains work best, grab a Namecheap or GoDaddy domain and webmail for cheap and make a bunch of account with them
    - c. Gmx.us accounts seem to work ok (for now) and require no existing email or contact info
    - d. Sudomail and Protonmail addresses work ok, not as good as a private domain though
6. Phone #:
    - a. You might get lucky and not get the phone number requirement, but also sometimes it won't require it at first but then a couple hours or days in it will throw it at you as a security requirement
    - b. No VOIP – most number blocks are flagged
    - c. Mint test kits and an unlocked phone are a cheap way to get 7 days on a real number
        1. Make sure you have Mint coverage in your area
        2. https://www.amazon.com/Mint-Mobile-Starter-Verify-Compatibility/dp/B0786RD524 ($5 for two sims)
        3. You might then port the number over to google voice
        4. Some groups buy these in bulk
    - d. You can also use an extra # on a real account (i.e.: Verizon) and then port it over to google voice and then draw a new # for that Verizon account
    - e. Some people will also use hotel phones and the like when traveling to roll accounts, but that is kind of

7. Once we get into our new account, we do not leave it fallow, start making it feel real right away
8. Choose a name that is generic, but not too generic
    a. i.e.: Nicky Robinson, Hunter Reynolds, etc.
    b. http://howmanyofme.com/
9. Name, gender, city, employer (school) should make sense, remember a real person at FB will likely look at your profile if it is reported as suspicious, we want to pass the smell test
10. Profile/cover photo
    a. We don't ever purport to be a specific individual without consent (i.e.: no identity theft)
    b. Pikwizard.com – Good source for free for anything licensed photos
    c. Pixabay.com is also decent
    d. Avatar makers are another option https://mashable.com/2007/09/12/avatars/#mn3Ph1PwgZqi
    e. fiverr.com – You can buy profile photos for cheap or anything else really…avoid buying bulk accounts, they are often locked, scams, or stolen
    f. I also like taking a pic from images.bing.com of a large crowd (road race, sporting event, concert), use the snip tool to crop it, and then post the still large group shot, it's unclear who we are in the group and yet it's the kind of content people post for profiles or banners because the internet is all about bragging
    g. Get creative – general rule is snip, crop, filter, logical pic choice
1. Time to flesh out our profile by making some friends
    a. Join Groups – anything that has large groups that accept anyone
    b. Nerdy groups and pop culture are my favs: video games, cosplay (cause then costumed profiles make sense), etc.
    c. If you are doing a deep infiltration you may have to research your targets groups, don't join her/his groups directly, join similar and work your way in slowly after you have some history
    d. Do some liking and commenting in groups for a day or two
    e. then https://www.facebook.com/find-friends/browser/ and let FB recommend friends. We never cold call friends anymore, we let FB tell who it's already cross correlated with our profile. This reduces chances of getting flagged significantly.
2. Posts: August 1st Facebook cut off all 3rd part app access except for messenger or FB pages. We formerly used IFTTT and WordPress to auto-post but they are broken for now. IFTTT still works for twitter.
3. Avoid political chat and comments. Politics and social issues are high on the radar of the FB watchdogs due to the fake news and voter tampering concerns.
4. Keep track of covert accounts in a spread sheet or better yet a password manager.
5. Sim jacking Twitter accounts is very popular so use long passphrases even on your sock accounts and consider 2-factor if they are mature or otherwise valuable accounts
6. Know your agencies policies around things like friending and any levels of approval or documentation required
7. …and of course, we always use our powers for good so we always assume that our investigation will eventually see the light of day so make sure you are proud of how your activity will look in retrospect by an objective 3rd party in regard to reasonable and responsible

Note: This is purely anecdotal, but in addition to "getting into character" and making our accounts feel real, I suspect that there may be some value to occasionally clicking on ads and other content that the platform is pushing at you. This is not a privacy/security best practice, but there are detection algorithms that may favor revenue positive accounts. Again, this is just a theory.

LOGO HERE

Company/Org Name
Section or Analyst Name

Open Source Investigative Profile

Summary of Findings

Subject ID

Name: ____________________ DOB: ____________________

Address: ____________________ Phone #1: ____________________

____________________ Phone #2: ____________________

Employer: ____________________ SS#: ____________________

Vehicles: ____________________ Relatives: ____________________

____________________ ____________________

Alternate Identities and Associations

Email #1: ____________________ Email #2: ____________________

Email #3: ____________________ Email #4: ____________________

User Name: ____________________ UN #2 ____________________

Facebook : ____________________ FB # ____________________

Twitter: ____________________ TW #: ____________________

Instagram: ____________________ IG #: ____________________

____________________ ____________________

Photos/Video

	Description	**Source**
☐Photos		
☐Video		

Attachments

☐ Excel Profile Report
☐ Data Source DVD
☐ Photographs
☐ Hunch.ly Archive
☐ Link Analysis Report
☐ Comprehensive TLO, Clear, Accurint Report
☐ DOL/GOV Checks
☐ Other: ____________________

SHORTCUTS & HOT-KEYS

COMPLETING 1,000 SMALL TASKS A LITTLE FASTER

Windows Shortcut Keys	Shortcuts for Mac
Windows Key + R: Opens the Run menu.	Command + X: Cut selected text and copy it.
Windows Key + E: Opens Explorer.	Command + C: Copy selected text.
Alt + Tab: Switch between open programs.	Command + V: Paste copied text.
Windows Key + Up Arrow: Maximize current window.	Command + Z: Undo previous command.
Ctrl + Shift + Esc: Open Task Manager.	Command + A: Select all items.
Windows Key + Break: Opens system properties.	Command + F: Open Find window to search text.
Windows Key + F: Opens search for files and folders.	Command + H: Hide windows of the front app.
Windows Key + D: Hide/display the desktop.	Command + N: Open a new document or window.
Alt + Esc: Switch between programs in order they were opened.	Command + O: Open a selected item.
Alt + Letter: Select menu item by underlined letter.	Command + P: Print current document.
Ctrl + Esc: Open Start menu.	Command + S: Save current document.
Ctrl + F4: Close active document (does not work with some applications).	Command + W: Close front window.
Alt + F4: Quit active application or close current window.	Command + Q: Quit the app.
Alt + Spacebar: Open menu for active program.	Command + M: Minimize the front window to the Dock.
Ctrl + Left or Right Arrow: Move cursor forward or back one word.	Command + Spacebar: Open Spotlight search field.
Ctrl + Up or Down Arrow: Move cursor forward or back one paragraph.	Command + Tab: Switch between open apps.
F1: Open Help menu for active application.	Command + B: Bold selected text.
Windows Key + M: Minimize all windows.	Command + I: Italicize selected text.
Shift + Windows Key + M: Restore windows that were minimized with previous keystroke.	Command + U: Underline selected text.
Windows + F1: Open Windows Help and Support.	Command + Semicolon (;): Find misspelled words in document.
Windows + Tab: Open Task view.	Option + Command + Esc: Choose an app to force quit.
Windows + Break: Open the System Properties dialog box.	Shift + Command + Tilde (~): Switch between open windows.
Hold Right SHIFT key for eight seconds: Switch FilterKeys on and off.	Shift + Command + 3: Take a screenshot.
Left Alt + Left Shift + Print Screen: Switch High Contrast on and off.	Fn + Up Arrow: Scroll up one page.
Left Alt + Left Shift + Num Lock: Switch Mouse keys on and off.	Fn + Down Arrow: Scroll down one page.
Press Shift five times: Switch Sticky keys on and off.	Fn + Left Arrow: Scroll to beginning of document.
Hold Num Lock for five seconds: Switch Toggle keys on and off.	Fn + Right Arrow: Scroll to end of document.
Ctrl+Tab Switch Between Program Groups	
F11 Maximize Window	**Finder Shortcuts**
Ctrl+A Select Text (Expanded with Windows 10)	Shift + Command + F: Open All My Files window.
Ctrl+C Copy Text	Shift + Command + K: Open Network window.
Ctrl+V Paste Text	Option + Command + L: Open Downloads folder.
Win+R, then type ‘cmd’ Command Prompt	Shift + Command + O: Open documents folder.
Tab Autocomplete Folder or File Name	Shift + Command + U: Open Utilities folder.
Alt-Tab Switch Between Open Applications	Option + Command + D: Show or hide the Dock.
Windows logo key + Tab Task View	Shift + Command + N: Create a new folder.
Windows logo key + X Shutdown Your Workstation	Command + Delete: Move selected item to the Trash.
Windows logo key + L Lock Your Workstation	Shift + Command + Delete: Empty Trash.

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

Chrome

Shortcut Keys	Description
Alt+Home	Open your homepage.
Alt+Left Arrow	Back a page.
Alt+Right Arrow	Forward a page.
F11	Display the current website in full-screen mode. Pressing F11 again will exit this mode.
Esc	Stop loading the page or a download from loading.
Ctrl+(- or +)	Zoom in or out of a page, "-" will zoom out and "+" will zoom in on the page.
Ctrl+1-8	Pressing Ctrl and any number 1 through 8 moves to the corresponding tab in your tab bar.
Ctrl+9	Switch to last tab.
Ctrl+0	Reset browser zoom to default.
Ctrl+Enter	This combination is used to quickly complete an address. For example, type "computerhope" in the address bar and press Ctrl+Enter to get https://www.computerhope.com.
Ctrl+Shift+Del	Open the Clear browsing data window to quickly clear private data.
Ctrl+Shift+B	Toggle the bookmarks bar between hidden and shown.
Ctrl+A	Select everything on a page.
Ctrl+D	Add a bookmark for the page currently opened.
Ctrl+F	Open the "find" bar to search text on the current page.
Ctrl+O	Open a file in the browser.
Ctrl+Shift+O	Open the Bookmark manager.
Ctrl+H	Open browser history in a new tab.
Ctrl+J	Display the downloads window.
Ctrl+K or Ctrl+E	Moves your text cursor to the omnibox so that you can begin typing your search query and perform a Google search.
Ctrl+L	Move the cursor to the browser address bar and highlight everything in it.
Ctrl+N	Open New browser window.
Ctrl+Shift+N	Open a new window in incognito (private) mode.
Ctrl+P	Print current page or frame.
Ctrl+R or F5	Refresh the current page or frame.
Ctrl+S	Opens the Save As window to save the current page.
Ctrl+T	Opens a new tab.
Ctrl+U	View a web page's source code.
Ctrl+W	Closes the currently selected tab.
Ctrl+Shift+W	Closes the currently selected window.
Ctrl+Shift+T	This combination reopens the last tab you've closed. If you've closed multiple tabs, you can press this shortcut key multiple times to restore each of the closed tabs.
Ctrl+Tab	Moves through each of the open tabs going to the right.
Ctrl+Shift+Tab	Moves through each of the open tabs going to the left.
Ctrl+Left-click	Open a link in a new tab in the background.
Ctrl+Shift Left-click	Open a link in a new tab and switch to the new tab.
Ctrl+Page Down	Open the browser tab to the right.
Ctrl+Page Up	Open the browser tab to the left.
Spacebar	Moves down a page at a time.
Shift+Spacebar	Moves up a page at a time.
Home	Go to top of page.
End	Go to bottom of page.
Alt+Down Arrow	Display all previous text entered in a text box and available options on a drop-down menu.
	*Shortcut List Source: www.computerhope.com

Firefox	
Shortcut Keys	**Description**
F5	Refresh current page, frame, or tab.
F11	Display the current website in fullscreen mode. Pressing F11 again will exit this mode.
Esc	Stop page or download from loading.
Spacebar	Moves down a page at a time.
Alt+Home	Open your homepage.
Alt+Down arrow	Display all previous text entered in a text box and available options on drop-down menu.
Alt+Left Arrow	Back a page.
Alt+Right Arrow	Forward a page.
Ctrl+(- or +)	Increase or decrease the font size, pressing '-' will decrease and '+' will increase. Ctrl+0 will reset back to default.
Ctrl+D	Add a bookmark for the page currently opened.
Ctrl+F	Access the Find option, to search for any text on the currently open web page.
Ctrl+H	View browsing history.
Ctrl+I	Display available bookmarks.
Ctrl+J	Display the download window.
Ctrl+K or Ctrl+E	Move the cursor to the search box.
Ctrl+L	Move cursor to address box.
Ctrl+N	Open New browser window.
Ctrl+O	Access the Open File window to open a file in Firefox.
Ctrl+P	Print current page or frame.
Ctrl+T	Opens a new tab.
Ctrl+U	View a web page's source code.
Ctrl+F4 or Ctrl+W	Closes the currently selected tab.
Ctrl+F5	Refresh the page, ignoring the Internet cache (force full refresh).
Ctrl+Enter	Quickly complete an address.
Ctrl+Tab	Moves through each of the open tabs.
Ctrl+Shift+Del	Open the Clear Data window to quickly clear private data.
Ctrl+Shift+B	Open the Bookmarks window, to view all bookmarks in Firefox.
Ctrl+Shift+J	Open the Browser Console to troubleshoot an unresponsive script error.
Ctrl+Shift+P	Open a new Private Browsing window.
Ctrl+Shift+T	Undo the close of a window.
Ctrl+Shift+W	Close the Firefox browser window.
Shift+Spacebar	Moves up a page at a time.
Ctrl+Shift+Tab	Moves through each of the open tabs going to the left.
Ctrl+Left-click	Open a link in a new tab in the background.
Ctrl+Shift Left-click	Open a link in a new tab and switch to the new tab.
Ctrl+Page Down	Open the browser tab to the right.
Ctrl+Page Up	Open the browser tab to the left.
Spacebar	Moves down a page at a time.
Shift+Spacebar	Moves up a page at a time.
Home	Go to top of page.
End	Go to bottom of page.
Alt+Down Arrow	Display all previous text entered in a text box and available options on a drop-down menu.
	*Shortcut List Source: www.computerhope.com

Installation Notes (2.0)

You will need a Virtual Machine application in order to use this system. VirtualBox is free and will suffice for most investigations. Some users prefer a more robust option with VMWare Workstation for Windows or VMWare Fusion for Mac. Any of these options will get you started.

VirtualBox Installation and Configuration:

* Make sure you have latest version of VirtualBox and VirtualBox Extension Pack installed
1) In the VirtualBox menu, click on File > Import Appliance
2) Navigate to the OVA file that was downloaded (Buscador)
3) Choose this file and select “Import”
4) Before starting the new machine, highlight it and choose “Settings”
5) Under General > Basic, rename this machine as desired (Buscador?)
6) Under General > Advanced, change Shared Clipboard to Bi-Directional
7) Under System > Motherboard, increase the RAM if you have ample resources (half of total system)
8) Under Display > Screen, increase the Video Memory to 128MB is available
9) Under Shared Folders, click the “plus” on the right, choose folder to store evidence, select “Auto-Mount”
10) Click “OK” twice, then launch the new machine (Double Click)
11) Upon boot, log into the user “osint” with the password of osint
12) In the VirtualBox Menu, select Devices > “Insert Guest Additions CD Image”
13) Click “Cancel” when the dialogue box pops up.
14) Open Terminal (Tilex)
15) In Terminal, Create a directory on the Desktop titled vbox: mkdir ~/Desktop/vbox
16) Copy everything from the CD media on the Desktop to vbox folder (copy/paste)
17) In Terminal, input the following commands:

```
cd Desktop/vbox
chmod +x *.sh
./autorun.sh
(type password when prompted)
```

18) Allow the image to be installed, and reboot upon completion.
19) Start the Terminal in the new VM and type sudo adduser osint vboxsf
20) Provide the password as needed (osint)
21) Reboot

You should now have access to the shared directory in order to save data to the host operating system (evidence). It can be found in the File Manager (Home), on the left column, titled “sf_” followed by the name of the folder to which it is connected. This shared folder will also be on your desktop for easy access. You can make the machine full-screen, copy and paste text to and from the image, and you are ready to begin using the applications.

Support & Updates

Open Tilix (Terminal), and enter the following commands:

NOTE:
Update_scripts no longer needed!

Video Download Update:

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

Spiderfoot Update:

```
cd /opt/spiderfoot
git reset --hard
git pull
sudo reboot
```