Threat Intelligence Episode 2: OSINT sneak

A picture containing diagram

Description automatically generated

**Disclaimer- Please use the below information only for learning, if the below information is used for any unethical activity, I am not accountable for that.**

**HELPFUL TO KNOW-**

**People you may want to connect with:** Jeff M (OSINT professional with 22years of experience); [Null Byte](https://medium.com/@NullByteWht); [Tracelabs](https://twitter.com/TraceLabs) ;

**To Recommend one book through every episode:** [OSINT Techniques](https://www.amazon.in/Open-Source-Intelligence-Techniques-Information/dp/1984201573/ref=sr_1_14?adgrpid=1321614582780216&hvadid=82601169790296&hvbmt=be&hvdev=c&hvlocphy=154949&hvnetw=o&hvqmt=e&hvtargid=kwd-82601792032167%3Aloc-90&hydadcr=25403_2099850&keywords=osint+books&qid=1681649536&sr=8-14),

**Links to Read/learn through every episode:**

<https://medium.com/codex/master-at-google-hacking-dorking-27d14e7249be>

<https://www.youtube.com/watch?v=qwA6MmbeGNo> OSINT by Cyber Mentor

**Useful Website:** [OSINT framework](https://osintframework.com/); [Tracelabs](https://www.tracelabs.org/) ; [mysudo](https://mysudo.com/) ; [temporary email solutions](https://temp-mail.org/en/) ; [TextFree](https://textfree.us/) ;

**Resource:** [Google Dorking](https://medium.com/@kumarishefu.4507/search-smartly-on-google-using-google-dorks-a842ab20bf00), , [Google Hacking Database](https://www.exploit-db.com/google-hacking-database), [Hunter io](https://hunter.io/), Buscador VM, Tracelabs VM, Maltego, <https://osintcurio.us/> , [OSIRT](https://osirtbrowser.com/), <https://exif.tools/> , [canary tokens](https://canarytokens.org/generate) , [start me](https://about.start.me/),

**What is OSINT**- “OSINT is data collected from publicly available sources to be used in an intelligence context. In the Intelligence community, the term “open” refers to overt, publicly available sources (as opposed to covert or clandestine sources). It is not related to open-source software or public intelligence.

**What can be find with OSINT-**

* Email address
* Phone numbers
* Addresses
* Identities
* Background checks
* Social media accounts and information
* Criminal records
* Scams, etc.

**NOTE:** It is important to learn about proper method of doing reporting, so please don’t forget to explore **OSINT Report Template**.

**How to get started in OSINT investigation?**

Begin installing Virtual Machine on your HOST machine. Visit [Tracelabs](https://www.tracelabs.org/) website to [download the ova file](https://www.tracelabs.org/initiatives/osint-vm#downloads) of tracelabs to configure TL OSINT VM.

A screenshot of a computer screen

Description automatically generated with medium confidence

**What is a SOCK PUPPET?**

This is an account that we can use that is not associated to us in any way. Uses a fake name, can use a fake location, job, image, personality, etc. Your sock puppet account should never contain – your real name, real address, real job, real phone number, links or associations back to you. The account can be as real as you want, as minimal as you need to browse profiles and posts. Need of sock puppet to keep you real identity hidden from the people you are investigating and collection data about as they could be dangerous.

**Tips:**

* Always use your account in your OSINT VM
* Run a clean VM for each investigation
* If you run a VPN (which is generally a good idea) Facebook my flag your account
* Using TOR is also a good option (but you may run into the same issue with Facebook here as well as TOR works on TOR relays)

**Data Collection:**

**Doing an OSINT Investigation-**

* Contact information
* Scope of work
* What is considered out of scope
* Special considerations
* Timeline
* Special data retention requests (encrypted, file shared…)
* Information in writing (email, letter..)

Additional:

* Keep your investigation and data isolated to you VM
* Prefer keeping your data collected in encrypted form in VM (encrypted & password protected) [KeePassXC](https://keepassxc.org/)
* Never directly contact the target in any way
* Prepare oriented notes of the investigation, findings and target
* Unless necessary do not share specific information about your investigation to anyone outside investigation group

**Advance Searching:**

* Google Advanced Operators – [Google Dorking](https://null-byte.wonderhowto.com/how-to/use-google-hack-googledorks-0163566/) , [Google Hacking Database](https://www.exploit-db.com/google-hacking-database)
* Other resources are Google maps, [Google images](https://www.google.com/imghp), Bing images, Yandex images -yandex.com/image, pimeyes.com, [Google Alerts](https://www.google.com/alerts) ,
* Reverse Images search – [TinEye](https://tineye.com/) Reverse image search,
* Geolocation – [Geo tagging](https://www.geoimgr.com/) photos, <https://tool.geoimgr.com/> , <https://what3words.com/toddler.geologist.animated>

**Reverse Searchers:**

* <https://www.beenverified.com/>
* <https://hunter.io/>
* <https://haveibeenpwned.com/>
* <https://www.spytox.com/> (for US and Europe)
* <https://www.numlookup.com/>
* <https://www.usphonebook.com/>
* Detection of deep fake/altered images - <https://sensity.ai/deepfakes-detection/> , <https://deepware.ai/>

**Website OSINT:**

* Spiderfoot - <https://github.com/smicallef/spiderfoot> ,
* Builtwith, wappalyzer, [HTTrack](https://www.httrack.com/) or wget, Metagoofil
* Wayback Machine- <https://archive.org/web/>

**Dark Web OSINT:**

* [ search engines – DuckDuckGo, TORCH, Not evil, Ahima, ] TOR browser (ONION ROUTER) or we can also use Tor within Tails
* <https://github.com/fastfire/deepdarkCTI>
* Darknet OSINT guide - <https://medium.com/the-sleuth-sheet/darknet-osint-guide-984f68fb7ab3>
* [“OSINT Investigations: We know what you did that summer” Notes | by Chad Warner | Medium](https://warnerchad.medium.com/osint-investigations-we-know-what-you-did-that-summer-notes-8d4e7b53ac04)
* [Can TOR Keep You Anonymous? See How FBI Arrested An Illegal TOR User | by CyberSec\_Sai | Coinmonks | Medium](https://medium.com/coinmonks/can-tor-keep-you-anonymous-see-how-fbi-arrested-an-illegal-tor-user-ef8288f3480e)

Please let me know if this has helped you in any way. You can also add your views through comments. I will be back next time with some more sharp insights on TI Episodes.

-by Shefali Kumai

For more cyber security learning follow me here-

<https://www.youtube.com/channel/UCf-F-eATCUXYaUVk8Xl7OOQ>

<https://www.instagram.com/cybersecurity.cyber_seek/>

<https://twitter.com/Shefali37920461>