

How I find Cool Stuff



Whoami

- SFDC Admin
- Linux/OSINT/ICS/other security



Plan

- Why is this worth learning? Passion
- Note on Opsec
- How do we set things up?
 - Browsers + Extensions
- Foray in to The Wayback Machine
- What is „cool“ stuff to find
- What are some things I have found?

DISCLAIMER

- This is for educational purposes only
- Research things at your own risk
- Not everyone needs to know everything you find
- Find out

Opsec



- Some countries look down on Google Dorking. Be mindful of your threat model; consider the individuals and entities you are investigating.
- Out-of-Scope today - could give presentation only on this. Still... *Pay attention*.
- Keep an eye on your scope, look at the tools you are using
- „Don't F*ck it up!" | Zoz, Defcon 22
<https://www.youtube.com/watch?v=J1q4Ir2J8P8>
- Thegrugq | grugq.substack.com

Why learn this?

- Transferrable: useful not just for hacking
- Keeps you searching for new things – broaden your views
- Because we can
- Filter out the noise
- Not just for Librarians
- Different way of using the web: cultivate a new mindset
- Fun
- Just because anybody can access it, does not mean it is simple to do.



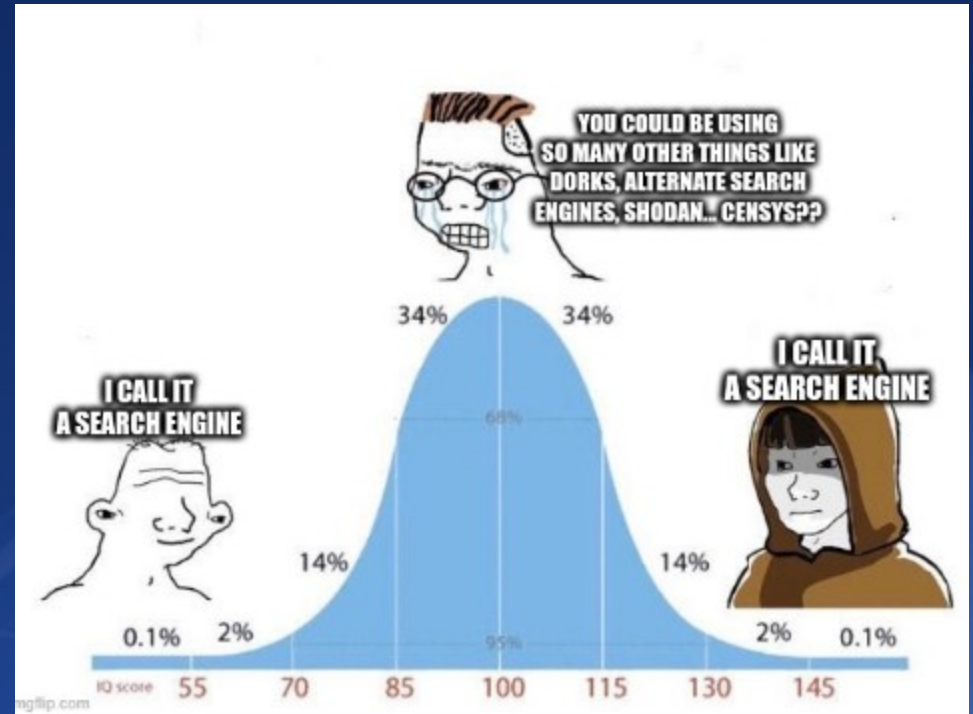
How I find cool stuff

- Browser Config
- Browser Extensions
- Wayback Machine
- Search Engine Dorks
- Lots of Browser Tabs
- Startpages
- Time
- Patience
- Persistence
- Failure

Who uses OSINT? (SANS)

- Government
- Law Enforcement
- Military
- Investigative Journalists
- Law Firms
- Human Rights Investigators
- Cyber Threat Intelligence
- Pentesters
- Social Engineers

YOU



Define an answerable research question

- 5W1H questions
 - What | what's the problem
 - Who | person relevant to the issue/situation
 - Where | exact location of issue or investigation
 - When | timeline, deadline, duration, or other details
 - Why | reason and objectives, need for action
 - How | methods on plan, step, etc
- What is Russia Doing in Ukraine? Doctoral Thesis
- What are Russian cyber forces doing in the donbas region of ukraine, during the first half of 2022, what are their TTPs, etc.
- Rocket-science level research cases + low-barrier cases
 - > Geolocation of adversaries, during an incident, or determining current location purely using OSINT

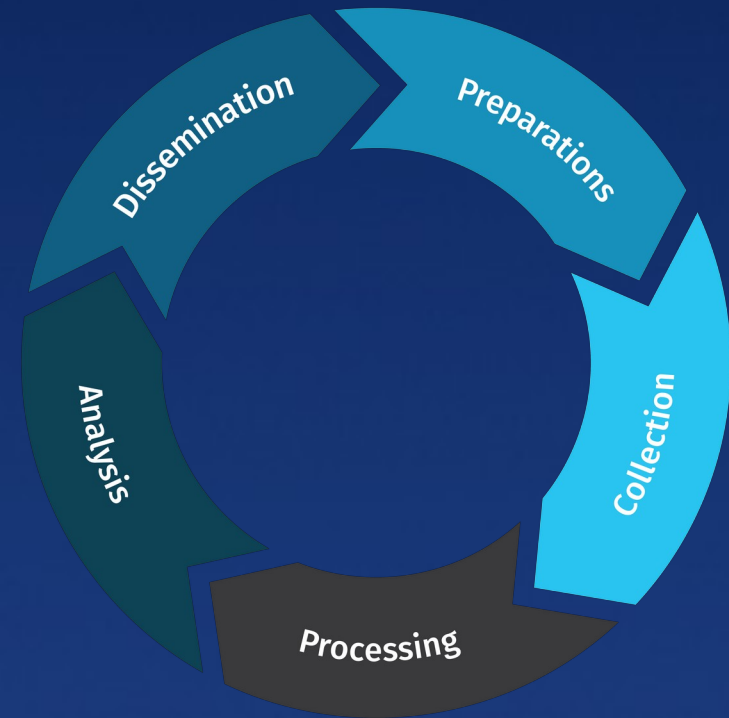
OSINT Fuzzy Areas

- Bellingcat
 - Condensed summary of HOURS or DAYS of work. Don't be deterred by only success stories and cool geolocation
- Seeing whatsapp, signal is NOT OSINT. These are closed sources. You have to define if you are interacting with the target or not.. Cyber-enabled HumINT is a different skillset. That's communicating with someone.
- Close line to Cyber Threat Intelligence and Human Intelligence.
 - e.g. people posting all the freaky antennas on Russian Embassies all over the place.. all you need is time and the internet.

Money in OSINT

- Government Funding
- Insurance, Finance, etc.
- Almost any question can have an OSINT aspect.
- e.g. Recent bank run on SVB – Niko Dekkens knew about 24hrs ahead of the rest of the world that Silicon Valley Bank (SVB) was in trouble – used all known American, European, Asian banks, with “bank run” “uncertain,” etc. Simply negative words surrounding financial situation.
- This is about identifying the social networks that individuals may be using, channels organizations are using, and which corners of the internet an entity will exist on. Remember, even someone who’s conducting criminal activities needs to be visible if they are trying to garner business. Usually, people who are criminals have lives in which they are not doing criminal activities.
“Bad guys order pizza too” – Shadowdragon CTO

Intelligence Cycle



- **Preparation** - needs and requirements of request are assessed, such as determining objectives.
- **Collection** - primary step
- **Processing** - organizing and collating data
- **Analysis and Production** - interpretation of the collected information to make sense of what was collected, draw conclusions, etc.
- **Dissemination** - presentation of open-source findings, written reports, timelines, recommendations, etc.
- If you're doing OSINT, you're going to fail. And probably quickly.

ElonJet - an example of OSINT Loophole

- ADSBExchange, Flightradar24, PlaneMapper, planespotter
- College Student Jack Sweeney's @ElonJet
- Resurfaced nearly immediately as @ElonJetNextDay



<https://wikiless.org/wiki/ElonJet?lang=en>

<https://subredditstats.com/r/elonjettracker>

<https://reddit.com/r/elonjettracker>

<https://elonjet.io>

@elonjet | @elonjetnextday



A 19-year-old built a flight-tracking Twitter bot. Elon Musk tried to pay him to stop.

"I've put a lot of work into it, and \$5k is just really not enough."

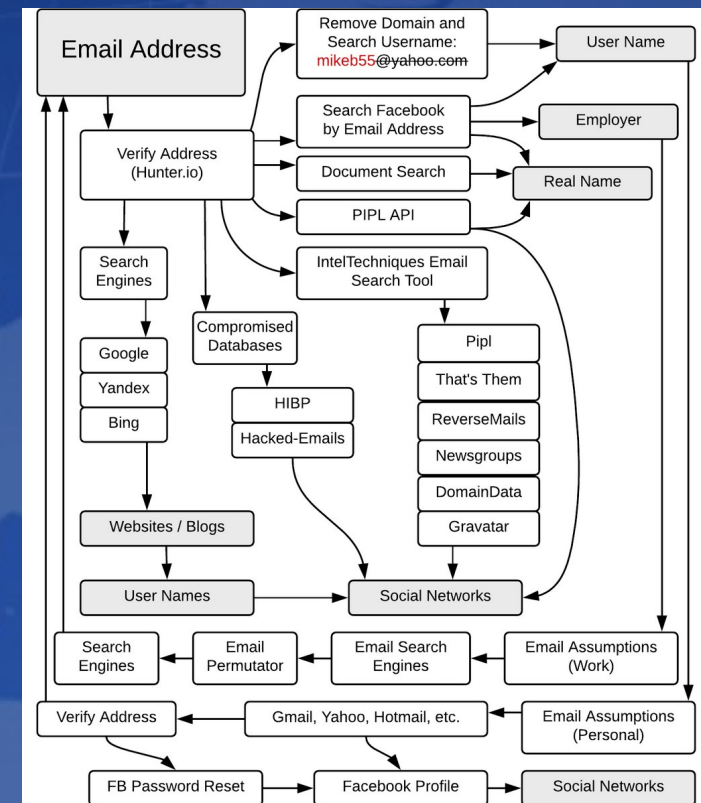
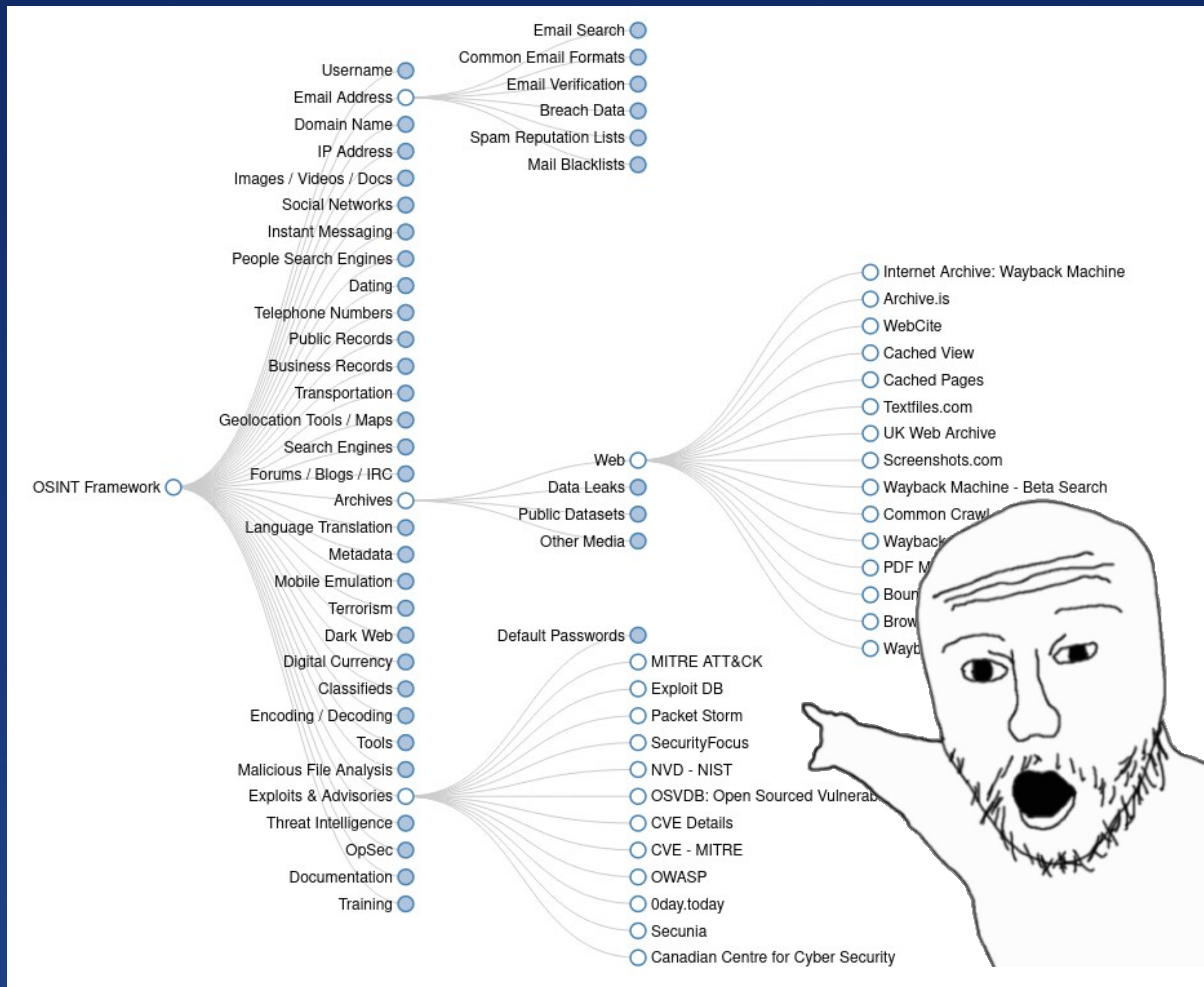


A new subreddit dedicated to the Elon Musk jet tracker is one of the fastest-growing pages on the website, with almost 40,000 members in 2 days

Kieran Press-Reynolds Dec 16, 2022, 2:02 PM MST



OSINT Frameworks / methodologies



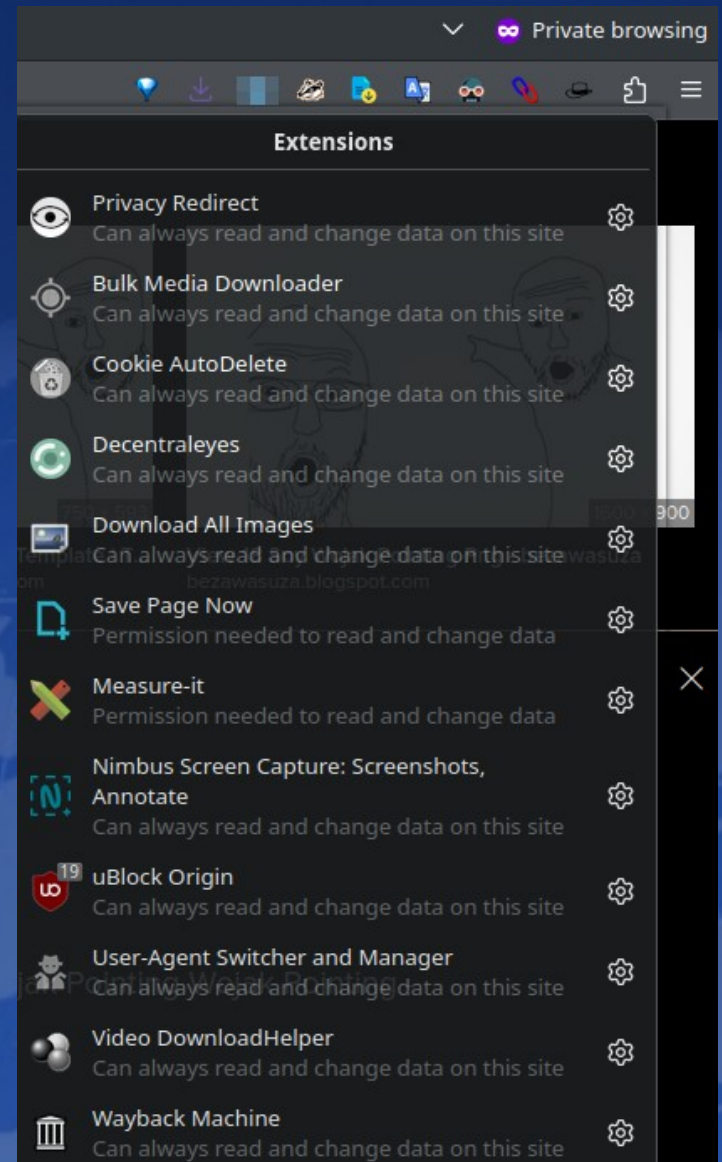
Browsers

- There is no ideal tool.
- Whatever works best for you



Browser Extensions

- Wayback Machine
- Save Page Now
- Web Archives
- TinEye Reverse Image Search
- OneTab
- Dark Reader
- Translate Web Pages
- User-Agent Switcher and Manager
- Download All Images
- Link Gopher



Helpful CLI tools

■ Wayback Machine

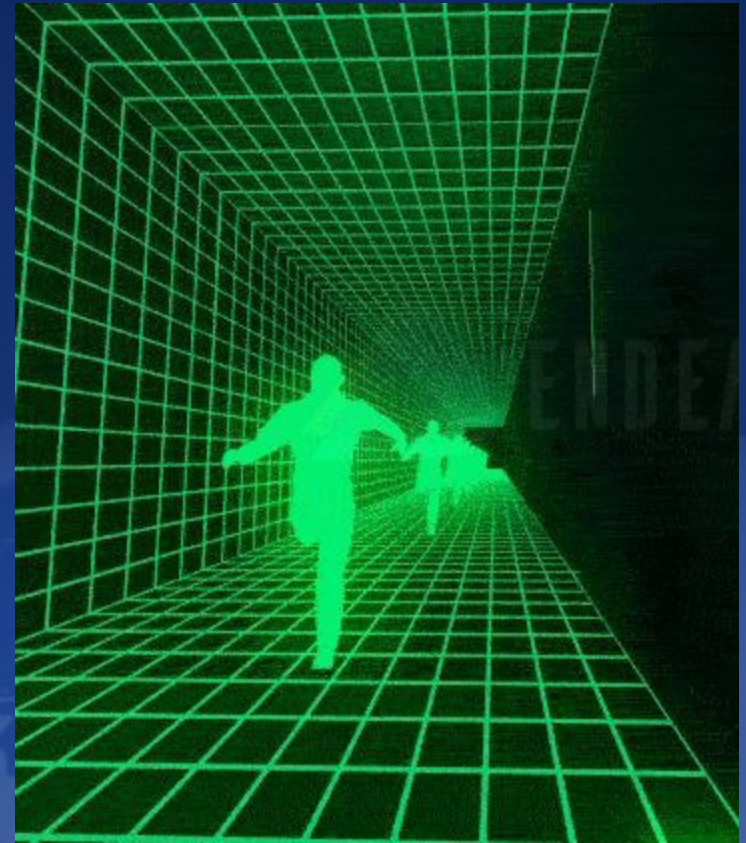
- Waybackpy
- Wayback-machine-archiver
- Wayback-machine-scraper
- WaybackURLs (a go tool)
- TheTimeMachine: weaponize things

■ Unshorten.me API

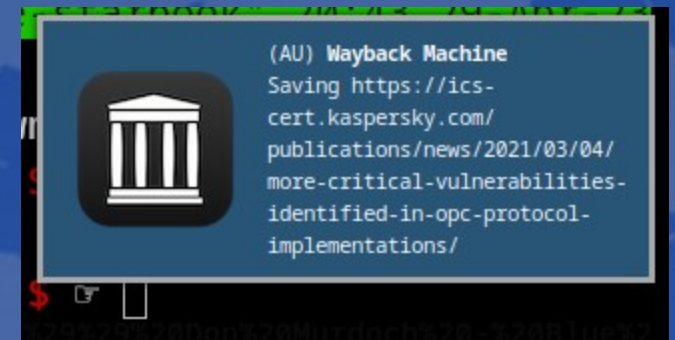
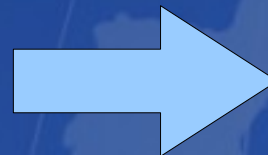
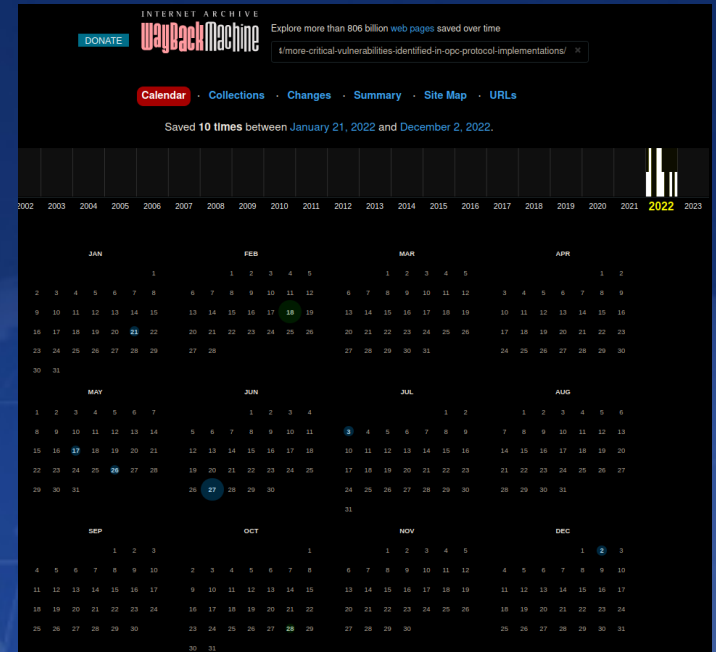
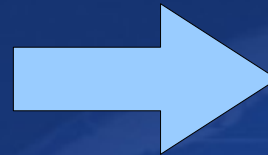
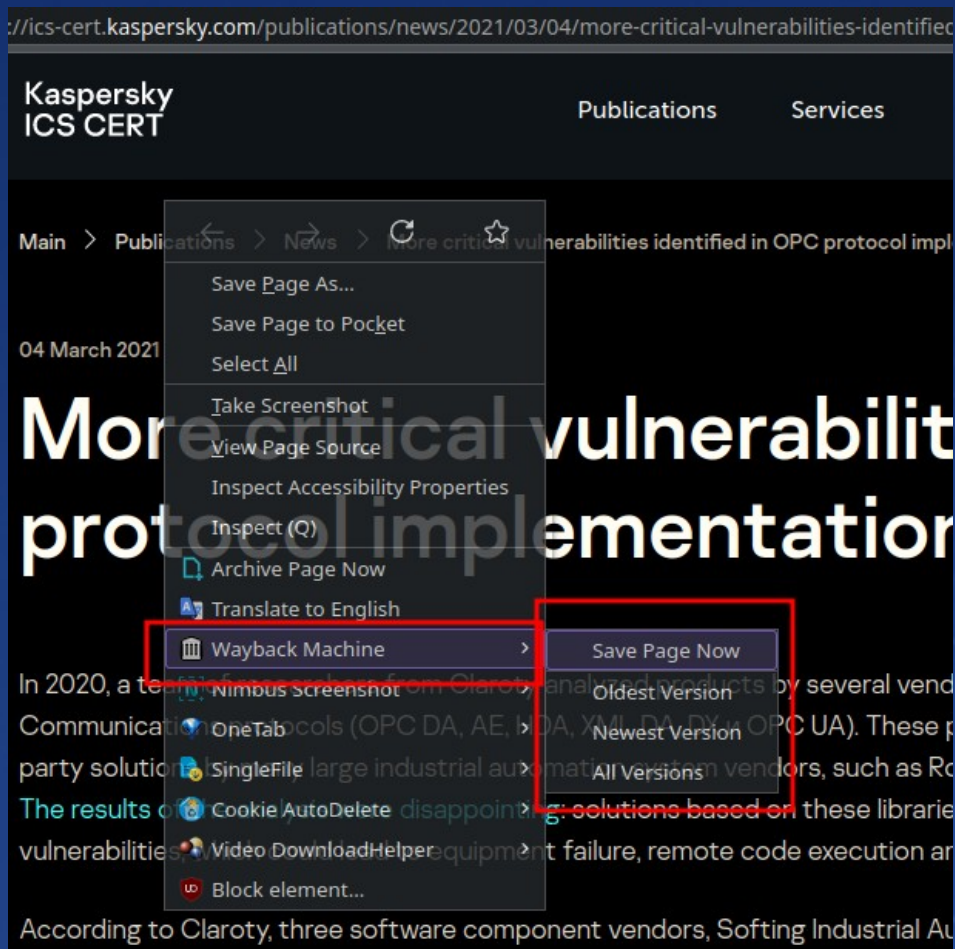
- Curl `https://unshorten.me/s/goog.gl/IG1LE`

■ URL *shortener*:


- Curl `-s tinyurl.com/api-create.php?url=<link>`



Wayback Examples



Wayback Browser Extensions



Save Page Now to the Wayback Machine

by tqdv

⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

[Learn more](#)

Easily save web pages to the Internet Archive's Wayback Machine using Save Page Now

[Remove](#)

16 Users

1 Review

★★★★★ 5 Stars

5 ★	1
4 ★	0
3 ★	0
2 ★	0
1 ★	0

[DONATE](#)



Saving page <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a> [Done!](#)


A snapshot was captured. Visit page: [/web/20230430033946/https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a](https://web/20230430033946/https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a)

```
https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a
https://www.cisa.gov/core/modules/system/css/components/ajax-progress.module.css?rtofsc
https://www.cisa.gov/core/modules/system/css/components/autocomplete-loading.module.css?rtofsc
https://fonts.googleapis.com/css?family=Montserrat:wght@400;500;600;700&family=Public+Sans:wght@400;500;600;700&display=swap
https://www.cisa.gov/core/modules/system/css/components/fieldgroup.module.css?rtofsc
https://www.cisa.gov/core/modules/system/css/components/clearfix.module.css?rtofsc
https://www.cisa.gov/core/modules/system/css/components/container-inline.module.css?rtofsc
https://www.cisa.gov/core/modules/system/css/components/hidden.module.css?rtofsc
https://www.cisa.gov/core/modules/system/css/components/details.module.css?rtofsc
```

If something goes wrong please click [here](#) to send us an error report.

Downloaded elements: 69

[Return to Save Page Now](#)



Wayback Machine

by Internet Archive

⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

[Learn more](#)

Welcome to the Official Internet Archive Wayback Machine Browser Extension! Go back in time to see how a website has changed through the history of the Web. Save websites, view missing 404 Not Found pages, or read archived books & papers.


[Remove](#)

22,870 Users

258 Reviews

★★★★★ 3.9 Stars

5 ★	134
4 ★	40
3 ★	29
2 ★	30
1 ★	25



Last Saved May 1, 2023

Search URL

[Save Page Now](#)

[Outlinks](#) [Screenshot](#)

[Oldest](#) [Newest](#)

[URLs](#) [Collections](#)

[Site Map](#) [Word Cloud](#)

[Annotations](#) [My Archive](#)

[Search Tweets](#)

There are more great features in Settings!

[Settings](#) [Help](#) [Feedback](#) [Share](#)

Waybackpy

```
waybackpy --url https://start.me/p/YaPkaN --save  
Archive URL:  
https://web.archive.org/web/20230430030717/https://start.me/p/YaPkaN  
Cached save:  
False
```



wayback-machine-archiver

← → ↻ Extension (Link Gopher) moz-extension://50884e8e-f579-4986-9bff-
<https://lobuhi.github.io/?#>
<https://map.malfrats.industries/>
<https://onbranding.start.me/p/QRBxaA/osint-tools>
<https://osintframework.com/>
<https://recontool.org/>
<https://sector035.nl/articles/category/week-in-osint>
<https://start.me/p/0PGKad/darkweb>
<https://start.me/p/0PhXom/osint-diegy-hasbi-widhana>
<https://start.me/p/0Pqbdg/osint-500-tools>
<https://start.me/p/0PwOGI/osint-all>
<https://start.me/p/1kBgQN/backpacking>
<https://start.me/p/1kJKR9/commandergirl-s-suggestions>
<https://start.me/p/1kPn8Y/spy-planes>
<https://start.me/p/1kRbXN/cyherdeck>
<https://start.me/p/1kgAYY/ethical-hacking>
<https://start.me/p/1kvvxN/faros-osint-resources>
<https://start.me/p/1kxyw9/v3nari-bookmarks>
<https://start.me/p/2p0Aje/dutchhackers-nl>
<https://start.me/p/2pMv6d/international-security-research>
<https://start.me/p/4K0DXg/social-media>
<https://start.me/p/5vPmbr/ics-scada>
<https://start.me/p/6rlqdK/ukraine-experts-livemap>
<https://start.me/p/7klY9R/osint-china>
<https://start.me/p/7kYPRY/con>
<https://start.me/p/7kg05R/wishlist>
<https://start.me/p/7kmvEK/oster>
<https://start.me/p/7krRmv/offensivesecurity>

```
18 https://start.me/p/BnrMKd/01-ncso
19 https://start.me/p/DPAL4o/search-party
20 https://start.me/p/DPYPMz/the-ultimate-osint-collection
21 https://start.me/p/DPKqAz/misc_trading
22 https://start.me/p/GE7JQb/osint
23 https://start.me/p/GEQXv7/osint-us
24 https://start.me/p/JDzoG2/reconnaissance
25 https://start.me/p/KMAbKB/osint-south-africa
26 https://start.me/p/L10kJ6/australian-osint
27 https://start.me/p/MEw7be/1-osint-toolset
28 https://start.me/p/Pwy0X4/osint-inception
29 https://start.me/p/QRg5ad/officercia
30 https://start.me/p/RMKQv/search-social-media
31 https://start.me/p/ZGAzN7/verification-toolset
32 https://start.me/p/b5yn0Q/srpr77-search-engines
33 https://start.me/p/ek2p4x/internetrecherche-2-0
34 https://start.me/p/ekq7A1/digital-forensics
35 https://start.me/p/gy1BgY/osint-tools-and-resources
36 https://start.me/p/jj2XEr/osint-global-non-us
37 https://start.me/p/jj8klr/hacking-ctf
38 https://start.me/p/kx462X/osint-tools-miscellaneous
39 https://start.me/p/kx5qL5/osint-darkweb-russia
40 https://start.me/p/kxGLzd/hun-osint
41 https://start.me/p/lLzzg7/tomoko-discovery-osint
42 https://start.me/p/nRzYnq/mrabricotier
43 https://start.me/p/p1Ba7E/basic-osint-tools
44 https://start.me/p/q6mw4Q/forensics
45 https://start.me/p/q6naJo/osint-links
46 https://start.me/p/ix6Qj8/nixintel-s-osint-resource-list
47 https://start.me/p/ixekAP/osint-research
48 https://start.me/p/wMbXrL/wefreeinternet
49 https://start.me/p/wMoArN/using-your-sourcing-super-powers-for-good
50 https://start.me/p/xBYdR/iyp-1
startmeURLS-archive.txt [ + ]
```

archiver https://onbranding.start.me/p/QRBxaA/osint-tools

→ archiver --file startmeURLS-archive.txt

Stuff I have found

- REDACTED
- Pastebin Dumps of IOCs, etc.

[illegible]

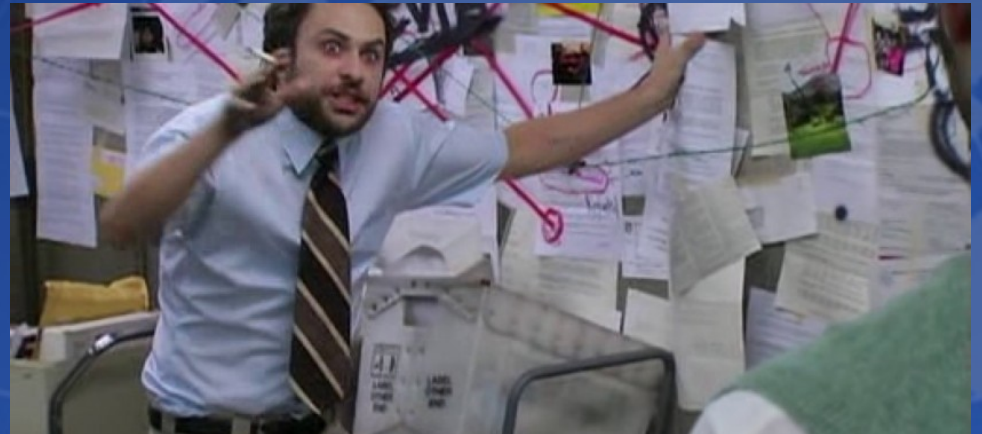
Know WHEN and WHERE to Stop

- Be careful if you look around in the AI Space
- Know when to take breaks
- Burnout is real. ...Vicarious trauma is real
- Knoll your tools: organize resources+tools so they are ready to go once you start work. Like a surgeon's sanitized instruments. Ongoing process. "Give me half a day to chop down a tree..."
- At the end of the day.. YOU are the ultimate tool. Truly valuable and powerful OSINT techniques are going to require an individual investigator's manual work. Do not let a program be more beneficial than you and your creativity.
- Personal defense against OSINT is as important as offense.

Ideas for future talks

- OSINT'ing your way towards jobs you want
- Mistakes made in beginner Pentest workflows: ALL the tools vs. one simple set.
- ICS and OT walkthrough: OSINT and protocols revisited
- It can't ALL be a Bash shell, can it? Automating your OSINT workflows
- Ethics and OSINT: not just Ethical Hacking

Thank YOU!



OSINT Names + Resources

- Joe Gray (c3_pjoe)
- Rae Baker
- Nico Dekkens (Dutch OSINT Guy)
- Jake Creps
- Michael Bazzell
- OSINT Framework
- Osintcurious
- The Osintion
- Aware-Online