OSINT

Teaching you how to find anything online

https://da.gd/xcrxz5

Sign in… or else

https://da.gd/xcrxz5

Previously in Bronco CPTC….

Reconnaissance

1 Identifying your target

Exploitation

2 Getting initial access

Post-Exploitation

3 Escalating your privilege

Lateral Movement

4 Moving around the environment

Previously in Bronco CPTC....

IP addresses

Domain names

Websites

Subdomains

Employee social media

Usernames

Phone numbers

Email addresses

Compromised credentials

Culture

Language

Timezone

Hours of business

Documents

3rd party services

Software in use

API's

Agenda

1

What is OSINT?

What is OSINT and when is it appropriate.

2

Tools for OSINT

Tools commonly used for OSINT

3

Maltego

TIME TO DANCE BABEYYYY

4

CTF

Learn by doing.

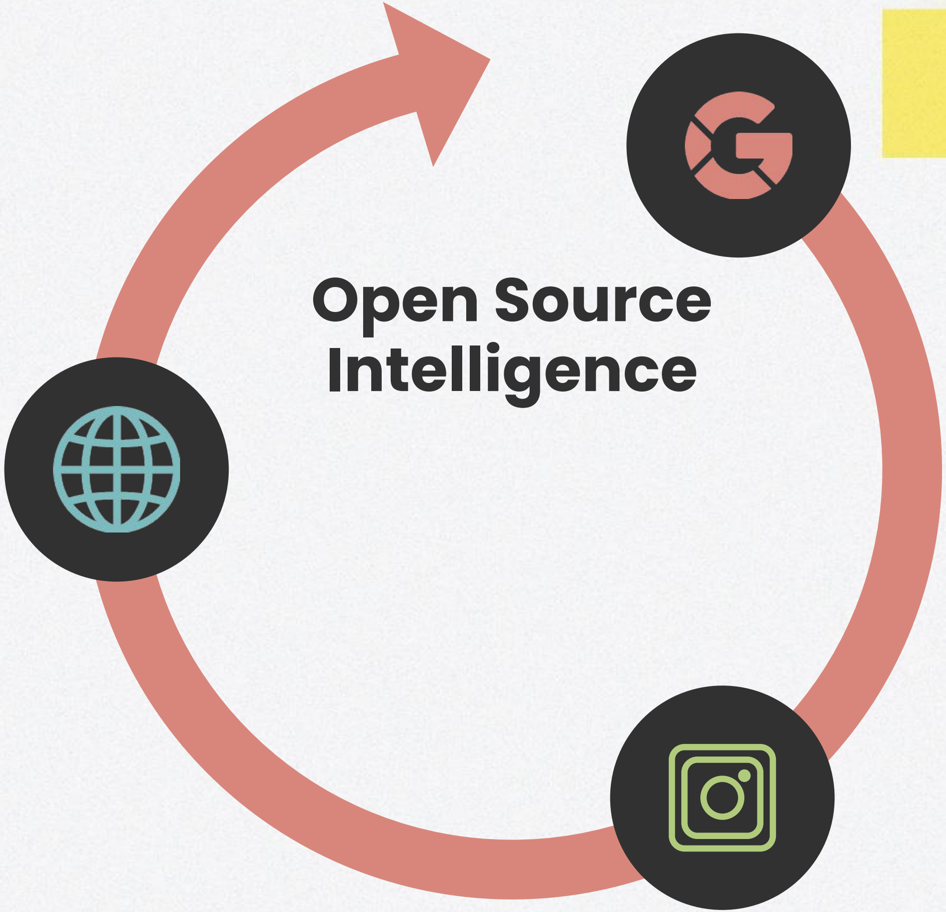
01

What is OSINT?

WHY????

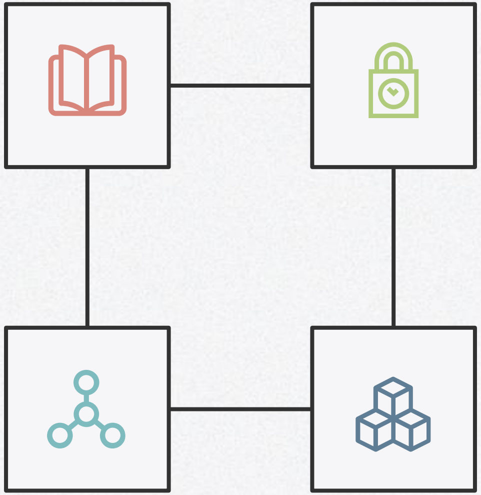
Keep things legal,
Respect Privacy

What is OSINT?



Open Source Intelligence

Why Practice OSINT?



Integral to Information Gathering.

Somewhat neglected Subject.

Good general skill to have.

Promotes Lateral Thinking.

Lateral Thinking Puzzle

Every two weeks a woman sits down and writes two words on 60 sheets of paper. Why does she do this?

Lateral Thinking Puzzle

Every two weeks a woman sits down and writes two words on 60 sheets of paper. Why does she do this?

The woman owns her own business with 60 employees. Every week she signs her name on their paychecks.

02

OSINT Tools

Tools you can use for osint.

Google Dorking

Makes your Google searches more specific

site:site.com	Search specific site
filetype:pdf	Search for specific filetypes
+, -, OR	Add, exclude, or combine
@	Search social media usernames
“Quoted text”	Search for exact string matches

Resources

https://en.wikipedia.org/wiki/Google_hacking

https://www.cybrary.it/blog/0p3n/advanced-google-dorking-commands/

https://da.gd/dorkks

IP Address

Private IP ranges:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

127.0.0.1 - Local Host

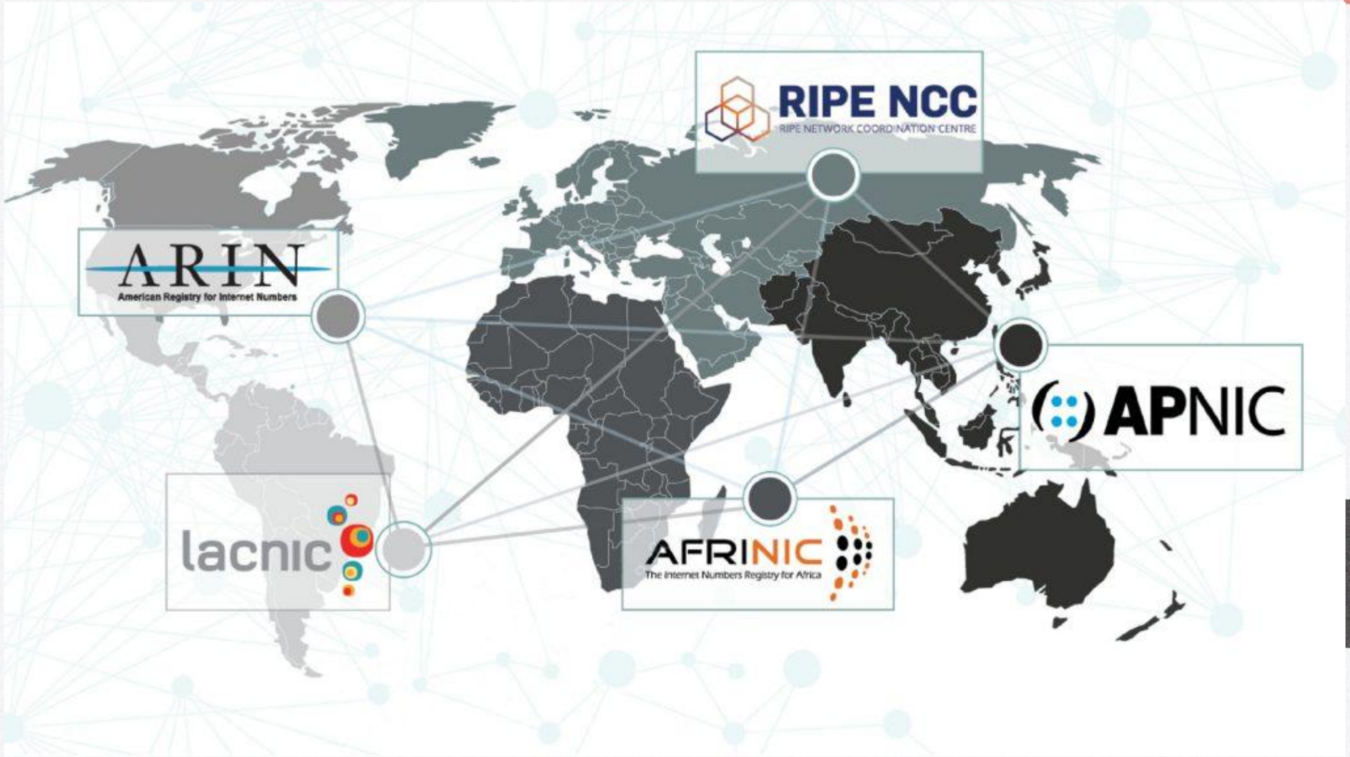
Whois
- whois.domaintools.com

IP Locations
- viewdns.info/iplocation

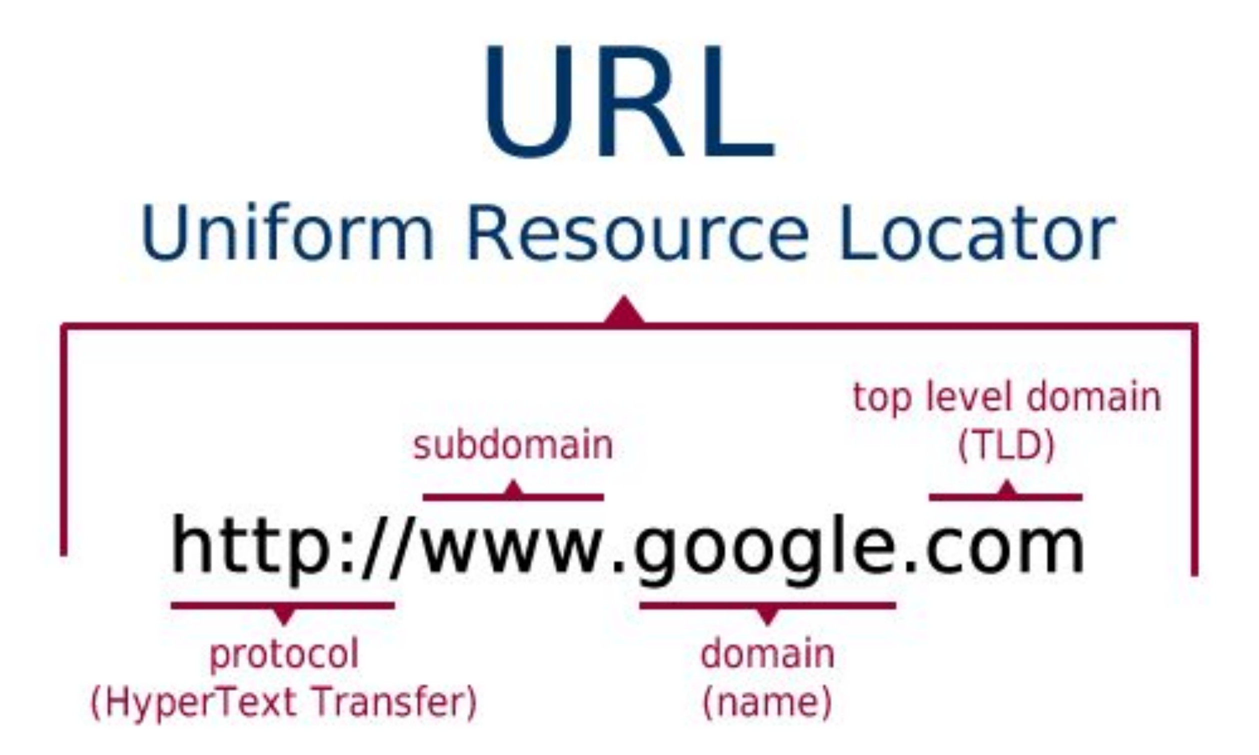
IP Reputation
- threatcrowd.org

Reverse IP
- viewdns.info/reverseip

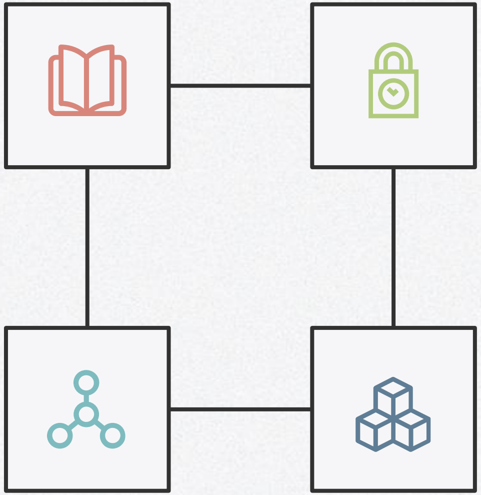
IP Address – Regional Authorities


RIPE NCC
RIPE NETWORK COORDINATION CENTRE
ARIN
American Registry for Internet Numbers
APNIC
lacnic
AFRINIC
The Internet Numbers Registry for Africa

Domains


URL
Uniform Resource Locator
top level domain
(TLD)
subdomain
http://www.google.com
protocol
(HyperText Transfer)
domain
(name)

Domains



WHOIS:
viewdns.info/whois
domainhistory.net

Identifying Technologies:

- builtwith.com
- wappalyzer

Archive pages:

- archive.org

Finding Other domains:

- analyzeid.com

Flyover:

- aquatone
- visualping.io

Files

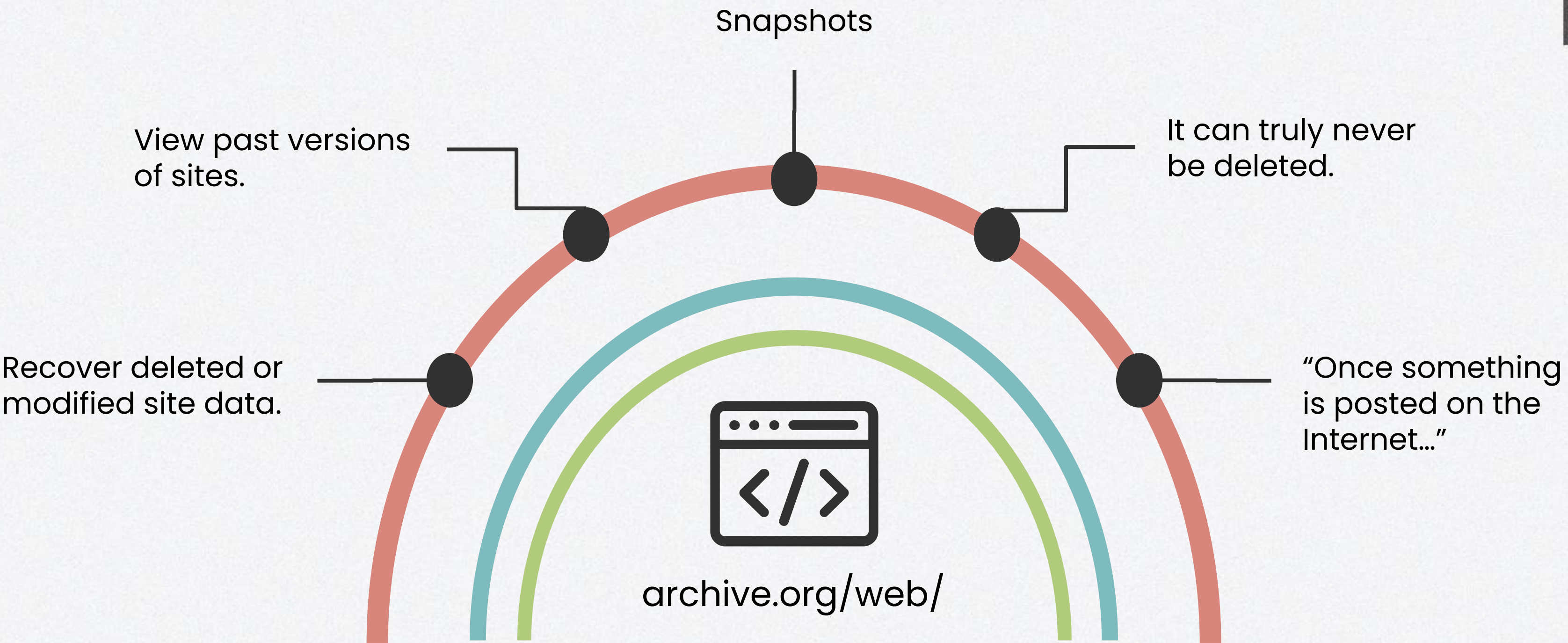
filetype:pdf
- site:docs.google.com

Document Metadata
- extractmetadata.com

Reverse Image Search
- tineye.com
- Google Images reverse search

Document Metadata
- futureboy.us/stegano/decinput.html
- stylesuxx.github.io/steganography/

Archived Pages



Snapshots

View past versions of sites.

It can truly never be deleted.

Recover deleted or modified site data.

“Once something is posted on the Internet…”

archive.org/web/

People

Social Networks
- usersearch.org

Shady site for PII
- doxbin.com

Family Info
-familytreenow.com

Search for person
- Peekyou.com

Email Addresses

SENDER IP IS CONTAINED IN THE HEADERS

METADATA ISN'T REMOVED FROM PHOTOS

Privacy Tip:

If your goal is to stay anonymous online, you should be very careful about how you use email

Email Addresses

LinkedIn Email Scraper
- getprospect.com/linkedIn-email-finder-chrome-extension

Find out email Formats
- email-format.com

Email Identity
- thatsthem.com

Verify Email Validity
- hunter.io/email-verifier

Usernames

Search for Available Usernames/Domain Names - namevine.com

Search Used Usernames - Peekyou.com

Search Usernames globally - knowem.com

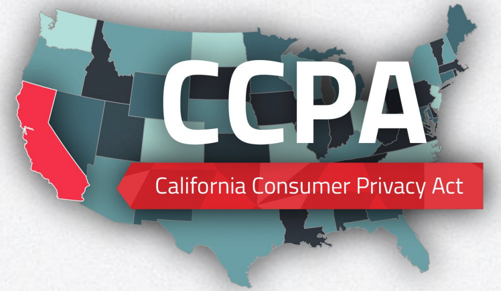
Social Media

Themed Based Group
Interpersonal Communications

Social Activities

Personal Information

Clean your online identity.



https://oag.ca.gov/privacy/ccpa

joindeleteme.com/help/

wiki.onerep.com (Danger)

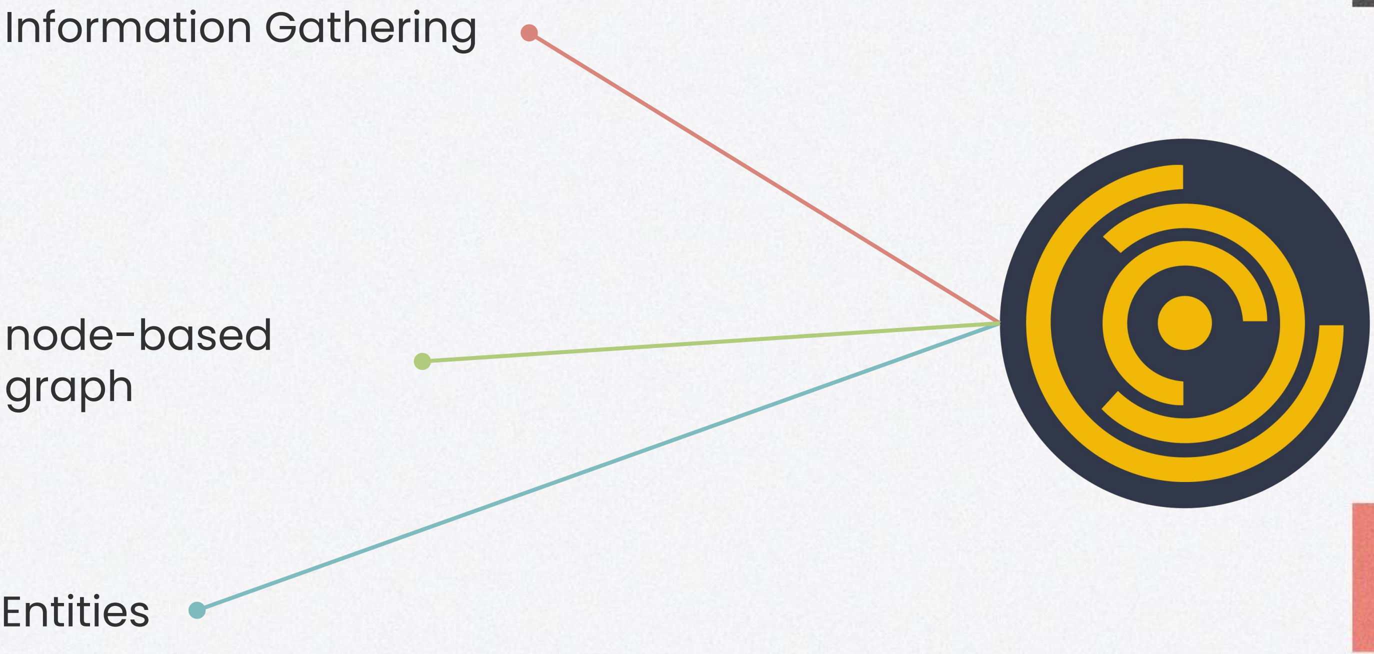
bbb.org

03

Maltego

TIME TO DANCE

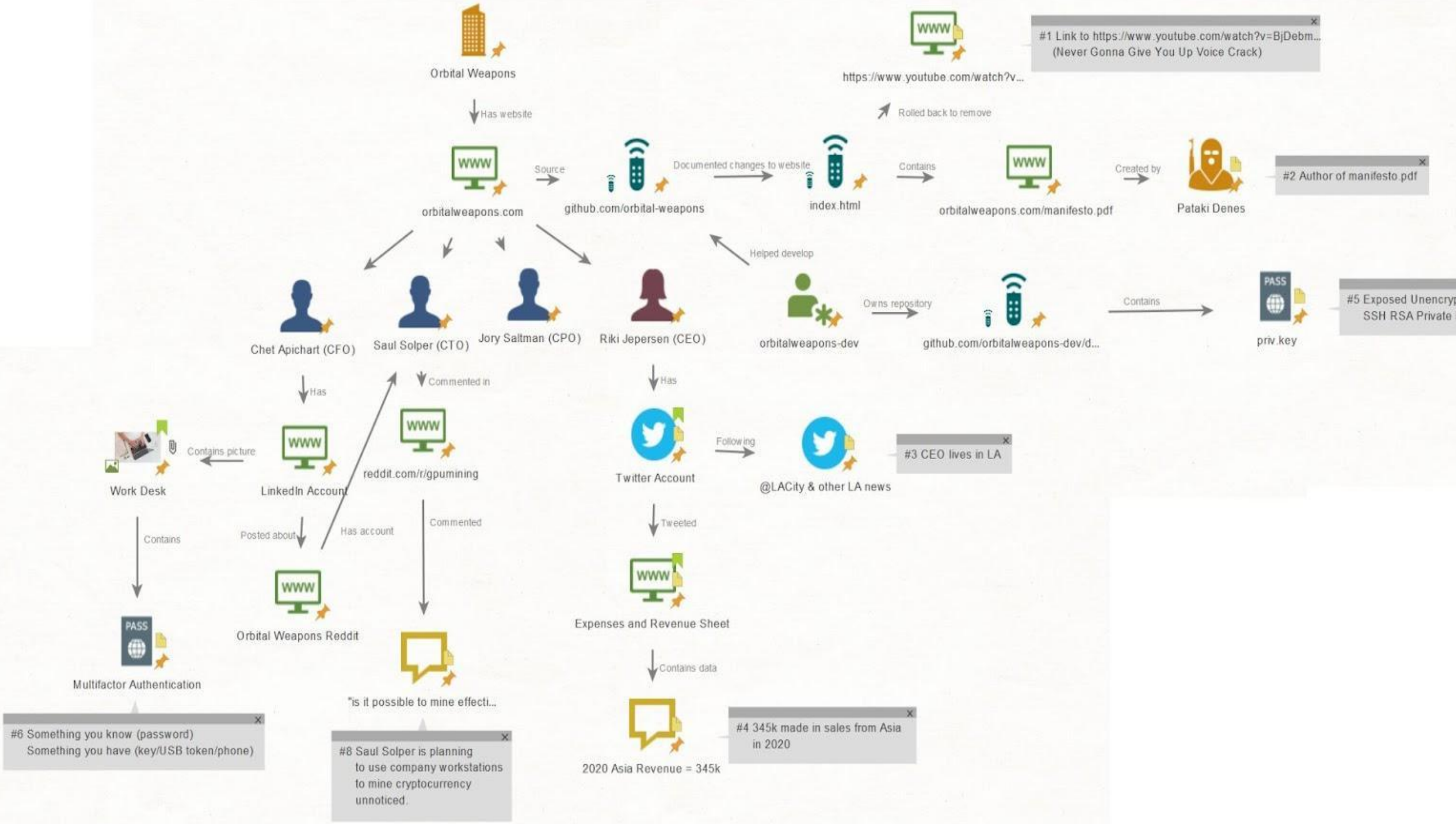
What is Maltego? (Tango? Nah MALtego!!!)



Information Gathering

node-based graph

Entities



#1 Link to https://www.youtube.com/watch?v=BjDebm...
(Never Gonna Give You Up Voice Crack)

#2 Author of manifesto.pdf

#3 CEO lives in LA

#4 345k made in sales from Asia
in 2020

#5 Exposed Unencryp
SSH RSA Private

#6 Something you know (password)
Something you have (key/USB token/phone)

#8 Saul Solper is planning
to use company workstations
to mine cryptocurrency
unnoticed.

04

CTF

Something smells nice