

RECONNAISSANCE (RECON)

With great knowledge, comes successful attacks!

INTELLIGENCE GATHERING

- What is it
- Why do it
- What is it not

Open source intelligence (OSINT) is a form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence.

OPEN SOURCE INTELLIGENCE (OSINT)

Simply, it's locating, and analyzing publicly (open) available sources of information.

Intelligence gathering process has a goal of producing current and relevant information that is valuable to either an <u>attacker</u> or <u>competitor</u>.

- OSINT is not only web searching!

OPEN SOURCE INTELLIGENCE (OSINT)

Takes three forms:

- Passive Information Gathering
- Semi-passive Information Gathering
- Active Information Gathering

Used for:

- Corporate
- Individuals

TARGET SELECTION

- Identification and Naming of Target
- Consider any Rules of Engagement limitations
- Consider time length for test
- Consider end goal of the test

CORPORATE - PHYSICAL

Locations

 Public sites can often be located by using search engines such as: Google, Yahoo, Bing, Ask.com, Baidu, etc.

Relationships

CORPORATE - LOGICAL

Business Partners

Business Clients

Competitors

Product line

Market Vertical

Marketing accounts

Meetings

Significant company dates

Job openings

Charity affiliations

Court records

Political donations

Professional licenses or registries

JOB OPENINGS WEBSITES

- Monster, http://www.monster.com
- LinkedIn, https://www.linkedin.com/mynetwork,
- Viadeo (France), http://fr.viadeo.com/fr

•••

CORPORATE – ORG. CHART

Position identification

Transactions

Affiliates

CORPORATE – ELECTRONIC

Document Metadata

Marketing Communications

CORPORATE – INFRASTRUCTURE ASSETS

Network blocks owned

Email addresses

External infrastructure profile

Technologies used

Purchase agreements

Remote access

Application usage

Defense technologies

Human capability

CORPORATE – FINANCIAL

Reporting

Market analysis

Trade capital

Value history

INDIVIDUAL - HISTORY

Court Records

Political Donations

Professional licenses or registries

INDIVIDUAL - SOCIAL NETWORK PROFILE(S)

Metadata Leakage

Location awareness

Social Media Presence

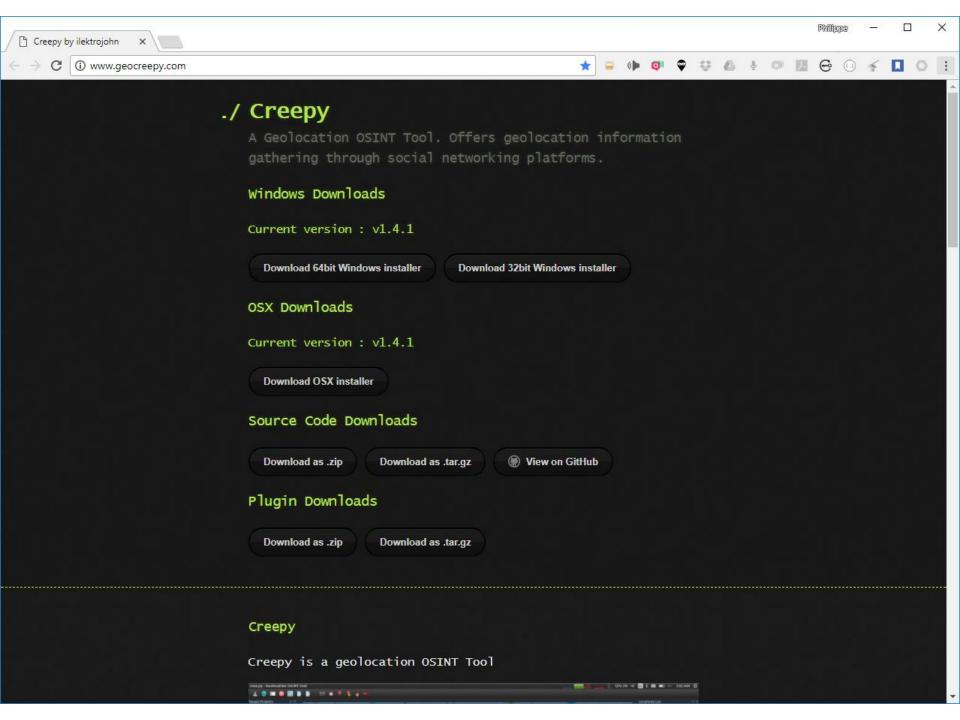
LOCATION AWARENESS - CREE.PY

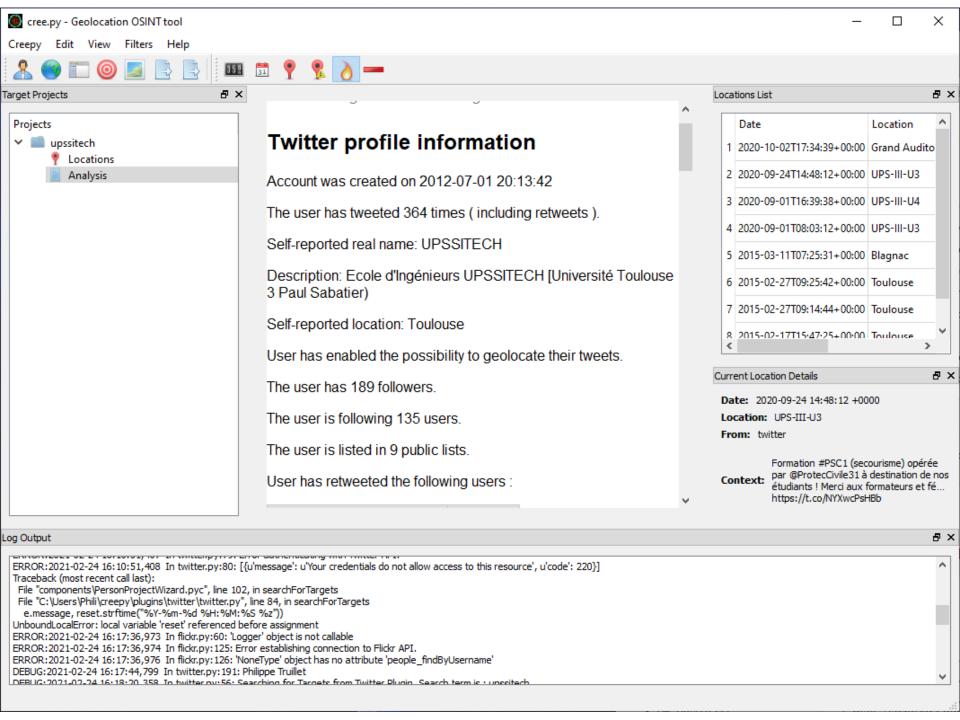
Cree.py (http://www.geocreepy.com) is an open source intelligence gathering application.

Can gather from Twitter and any geo-location data from several

websites.







INDIVIDUAL - INTERNET PRESENCE

Email Address

Personal Handles/Nicknames

Personal Domain Names registered

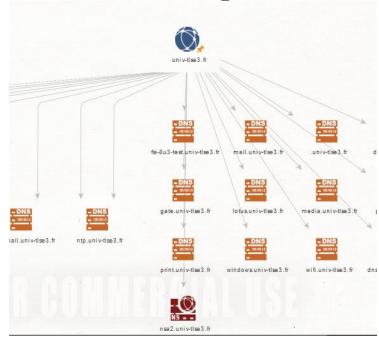
Assigned Static IPs/Netblocks

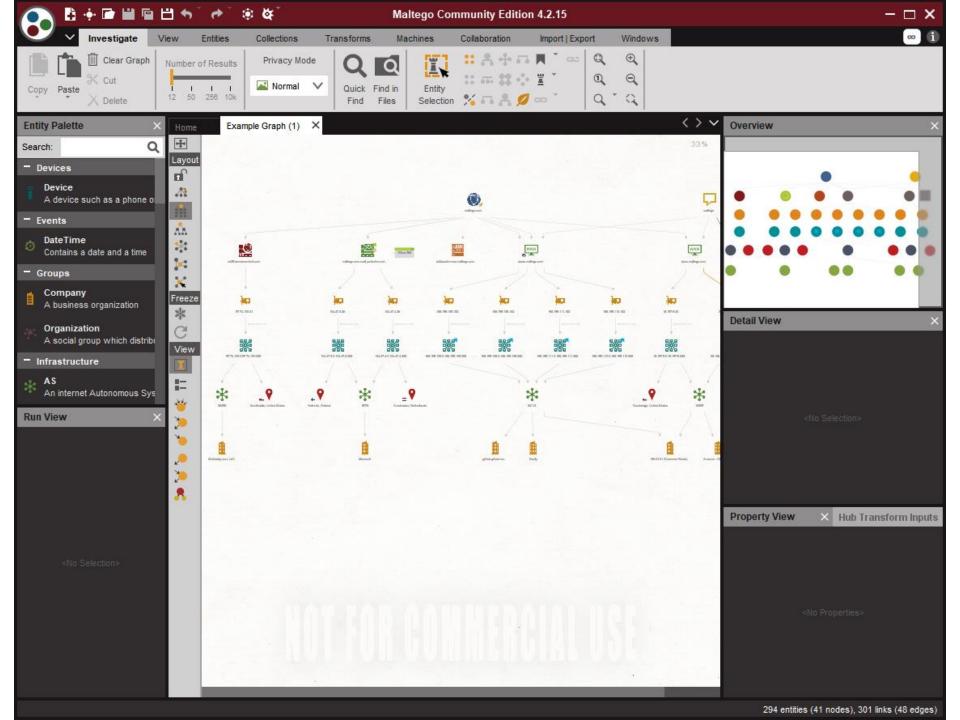
MALTEGO

Paterva Maltego (https://www.paterva.com) is a data mining and information-gathering tool that maps the information gathered into a format that is easily understood and manipulated.

It saves you time by automating tasks such as email harvesting and

mapping subdomains.

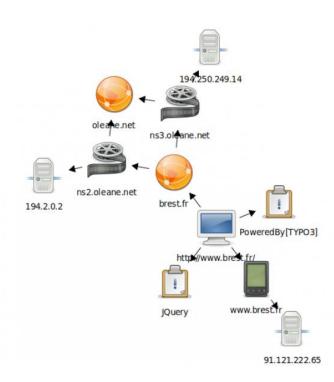


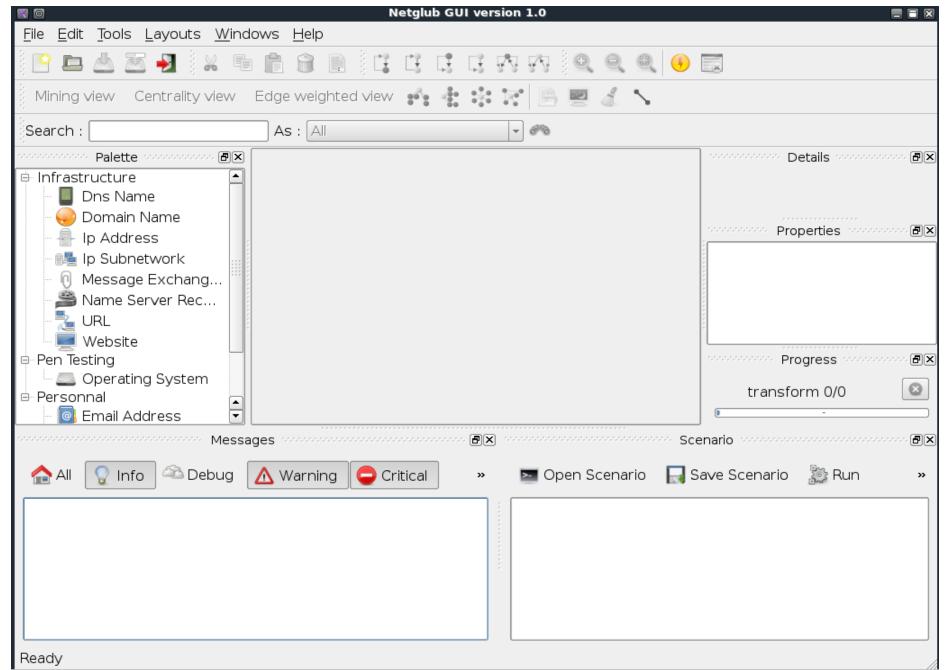


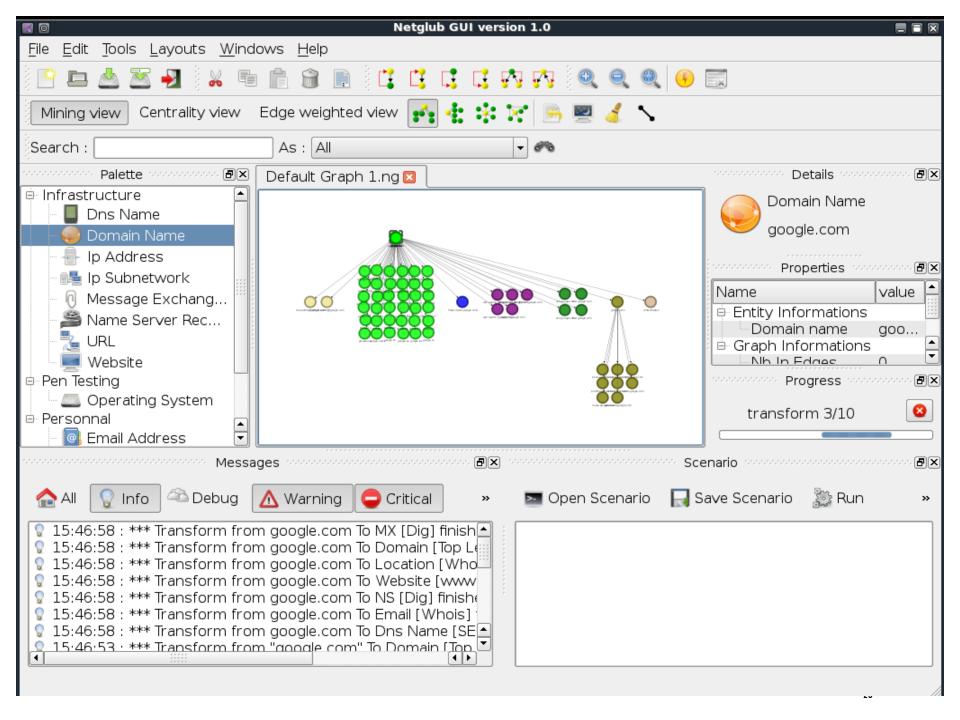
NETGLUB

NetGlub (http://www.netglub.org) is an open source data mining and information-gathering tool that presents the information gathered in a format that is easily understood, (Similar to Maltego).

Consists of: Master, Slave, and GUI







THE HARVESTER

TheHarvester (https://github.com/laramies/theHarvester) is a tool, written by Christian Martorella, that can be used to gather e-mail accounts and subdomain names from different public sources (search engines, pgp key servers).

→ http://www.edge-security.com



SOCIAL NETWORKS

Check Usernames - Useful for checking the existence of a given username across 160 Social Networks.

http://checkusernames.com



SOCIAL NETWORKS

Newsgroups

Google - http://www.google.com

Yahoo Groups - http://groups.yahoo.com

Mail Lists

The Mail Archive - http://www.mail-archive.com

AUDIO / VIDEO

Audio

```
iTunes, http://www.apple.com/itunes
Podcast.com, http://podcast.com
```

Video

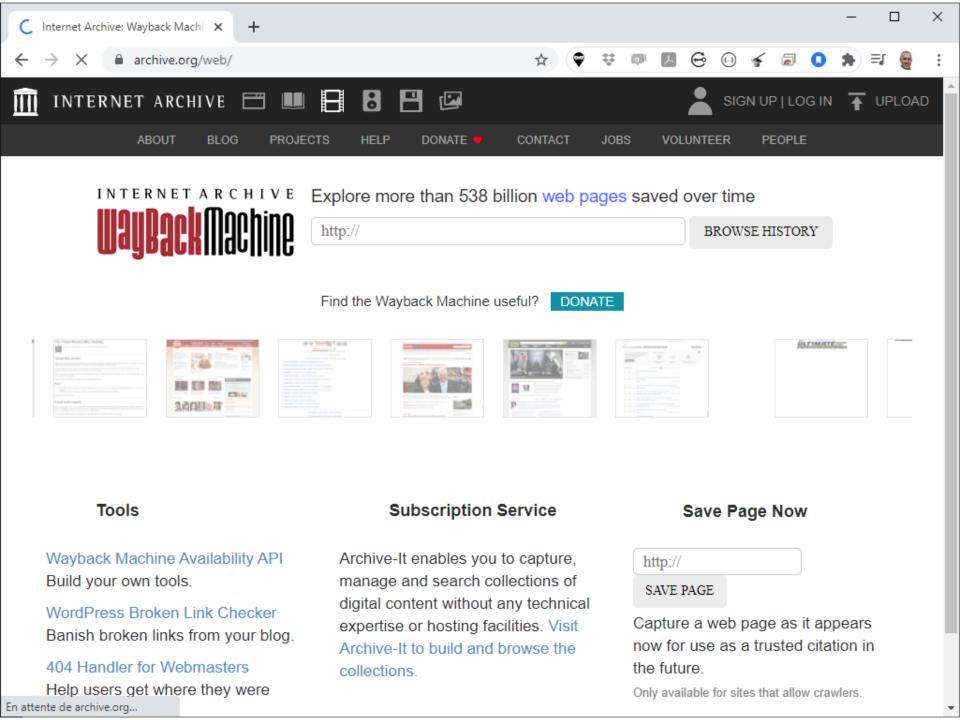
```
YouTube, http://youtube.com
Vimeo, http://vimeo.com
...
```

ARCHIVED INFORMATION

There are times when we will be unable to access web site information due to the fact that the content may no longer be available from the original source.

Being able to access archived copies of this information allows access to past information.

- Perform Google searches using specially targeted search strings: cache:<site.com>
- Use the archived information from the Wayback Machine (http://www.archive.org/web).



METADATA LEAKAGE

The goal is to identify data that is relevant to the target corporation.

It may be possible to identify locations, hardware, software and other relevant data from Social Networking posts.

Examples:

- ixquick http://ixquick.com
- MetaCrawler http://metacrawler.com
- Dogpile http://www.dogpile.com
- Search.com http://www.search.com
- Jeffery's Exif Viewer http://exif.regex.info/exif.cgi

METADATA LEAKAGE - FOCA

FOCA (https://github.com/ElevenPaths/FOCA) is a tool that reads metadata from a wide range of document and media formats.

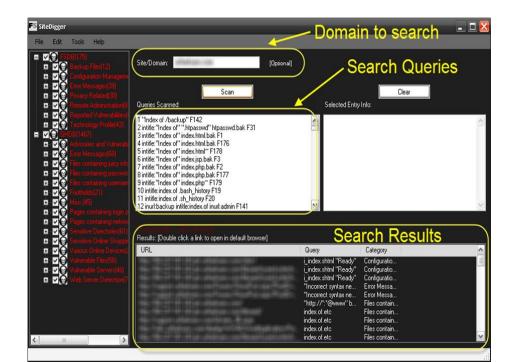
FOCA pulls the relevant usernames, paths, software versions, printer

details, and email addresses.



METADATA LEAKAGE -FOUNDSTONE SITEDIGGER

SiteDigger (https://sitedigger.software.informer.com/3.0/) allows us to search a domain using specially strings from both the Google Hacking Database (GHDB) and Foundstone Database (FSDB).



METADATA LEAKAGE - METAGOOFIL

Metagoofil (https://github.com/laramies/metagoofil) is a Linux based information gathering tool designed for extracting metadata of public documents (.pdf, .docx, .xlsx, .pptx, .odp, .ods) available on the client's websites.

Metagoofil generates an html result page with the results of the metadata extracted, plus a list of potential usernames that could prove useful for brute force attacks. It also extracts paths and MAC address information from the metadata.

INDIVIDUAL

Physical Location

Mobile footprint

Phone #

Device type

Installed applications

COVERT GATHERING -CORPORATE

On-Location Gathering

Physical security inspections

Wireless scanning / RF frequency scanning

Employee behavior training inspection

Accessible/adjacent facilities (shared spaces)

Types of equipment in use

Offsite Gathering

Data center locations

Network provisioning/provider

OTHER GATHERING FORMS

Human Intelligence (**HUMINT**)

Methodology always involves direct interaction - whether physical, or verbal.

Gathering should be done under an assumed identity (remember pretexting?).

- Key Employees
- Partners/Suppliers

OTHER GATHERING FORMS

Signals Intelligence (SIGINT):

Intelligence gathered through the use of interception or listening technologies.

Example:

- Wired/Wireless Sniffer
- TAP devices

OTHER GATHERING FORMS

Imagery Intelligence (IMINT):

Intelligence gathered through recorded imagery, i.e. photography.

IMINT can also refer to satellite intelligence, (cross over between IMINT and OSINT if it extends to Google Earth and its equivalents).

- https://www.geoportail.gouv.fr
- https://remonterletemps.ign.fr
- https://earth.google.com/web