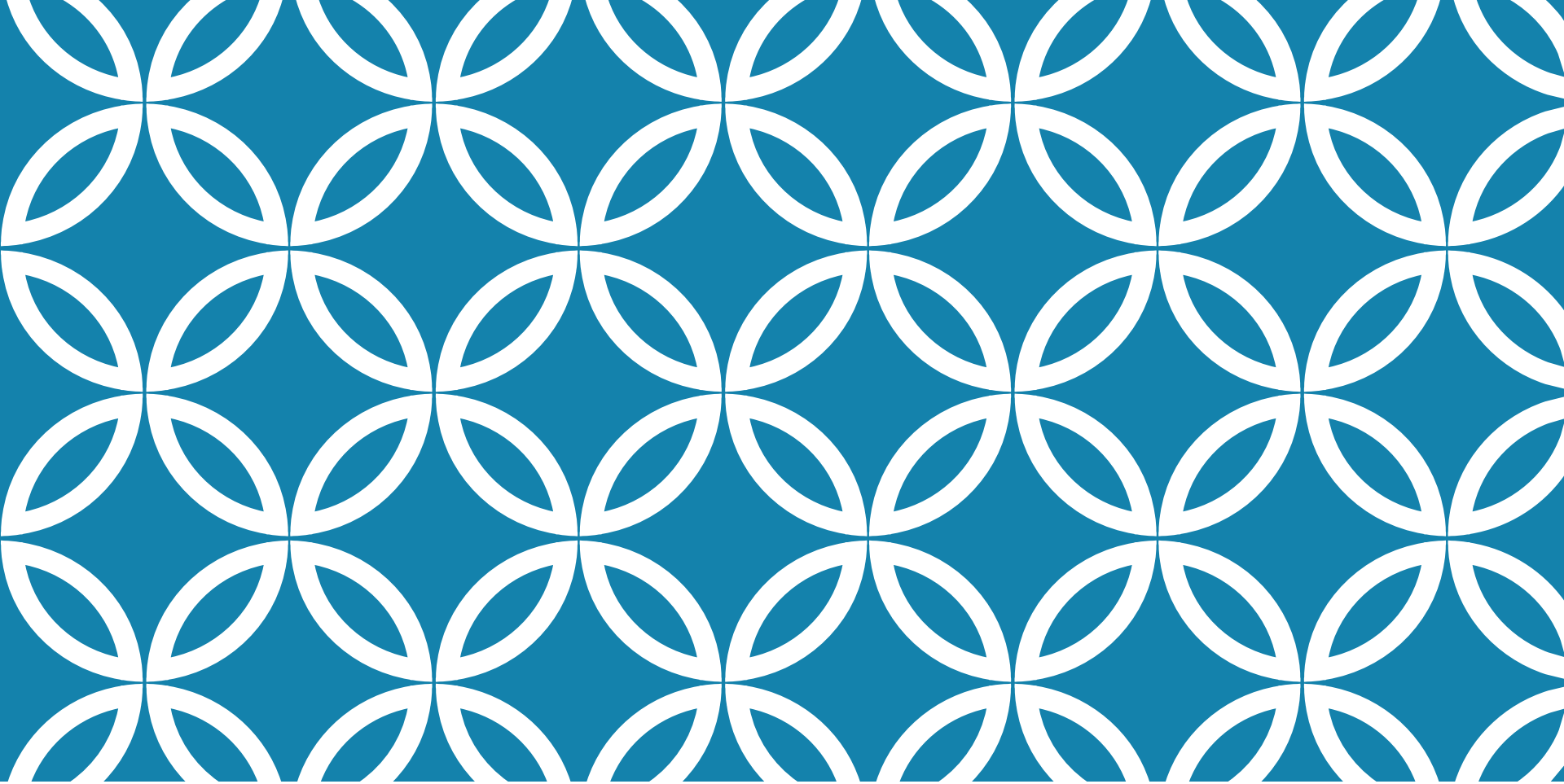


RECONNAISSANCE (RECON)

With great knowledge, comes successful attacks!

INTELLIGENCE GATHERING

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

Open **s**ource **int**elligence (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 attacker or competitor.

- OSINT is not only web searching!

OPEN SOURCE INTELLIGENCE (OSINT)

Takes three forms:

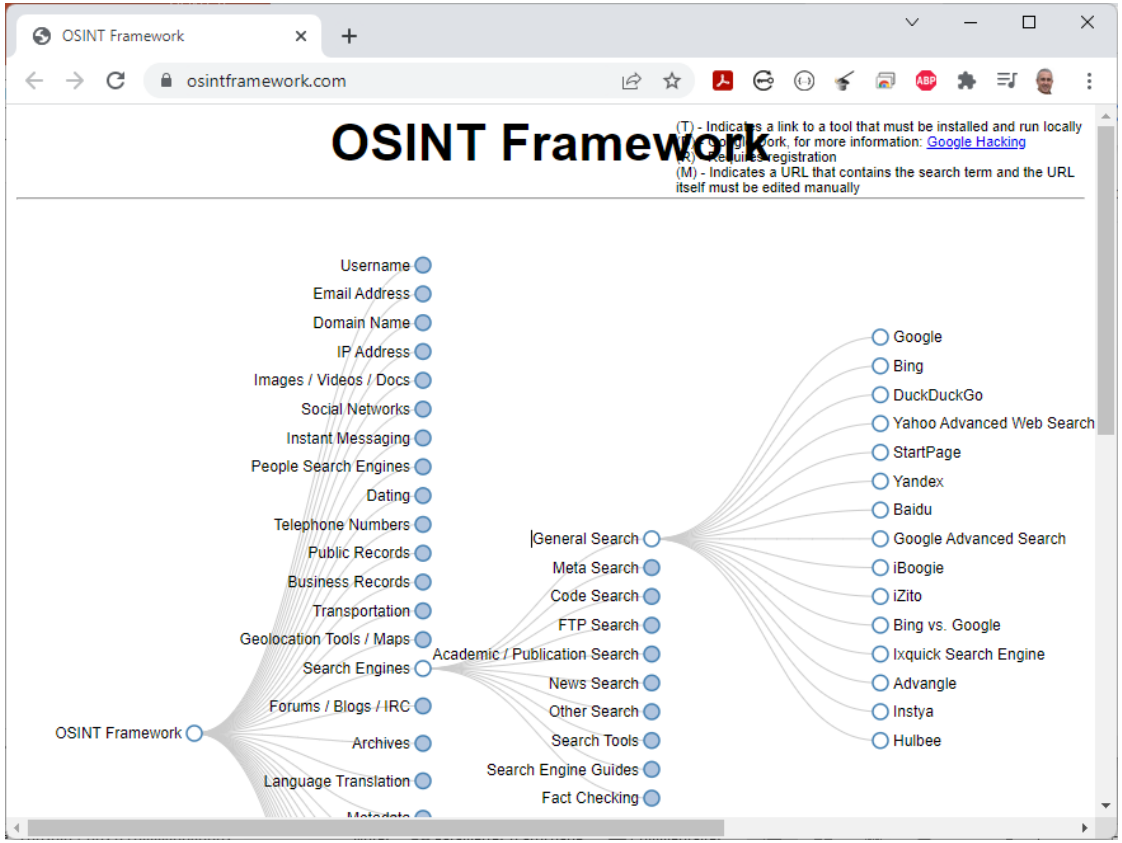
- Passive Information Gathering
- Semi-passive Information Gathering
- Active Information Gathering

Used for:

- Corporate
- Individuals

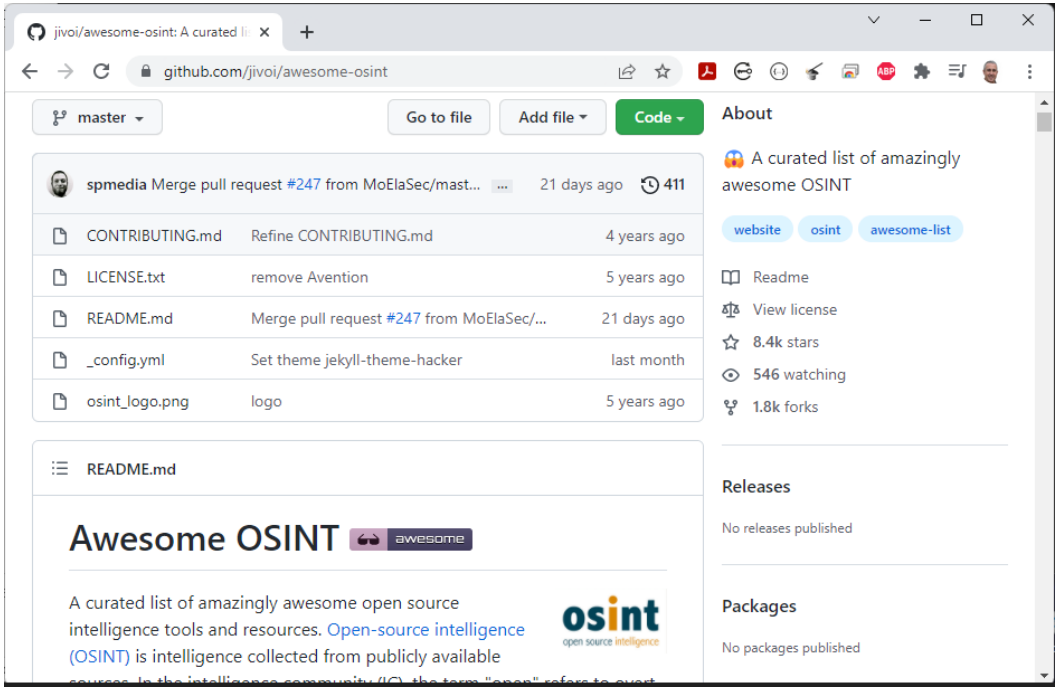
OPEN SOURCE INTELLIGENCE (OSINT)

https://osintframework.com



OPEN SOURCE INTELLIGENCE (OSINT)

https://github.com/jivoi/awesome-osint



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

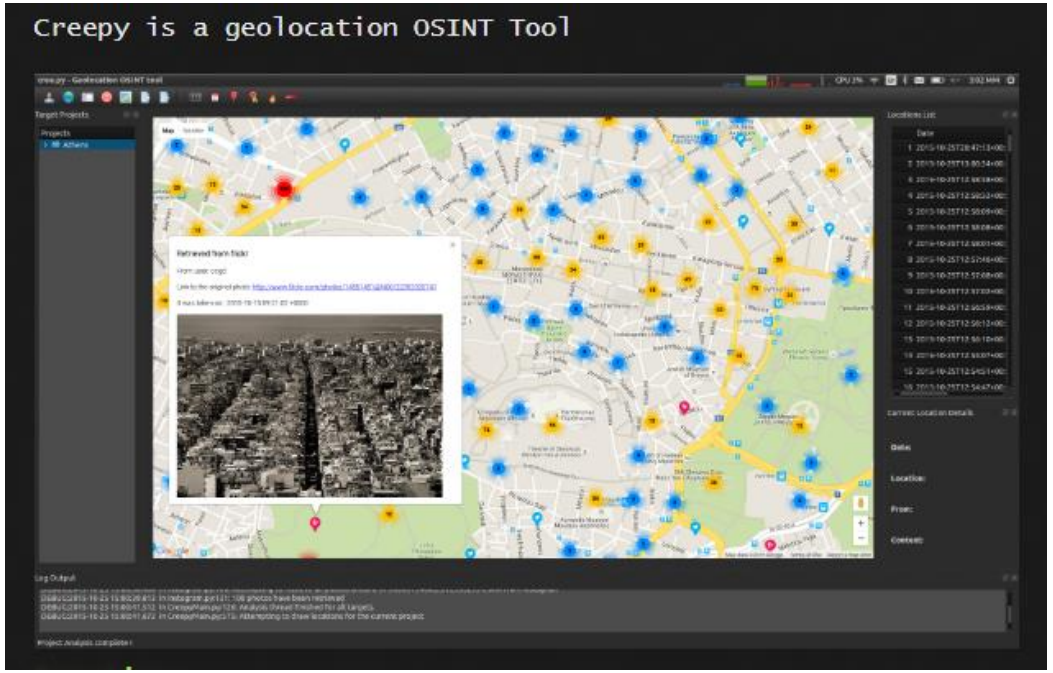
Location awareness

Social Media Presence

LOCATION AWARENESS - CREE.PY

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

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



Creepy by ilektrojohn

www.geocreepy.com

./ Creepy

A Geolocation OSINT Tool. Offers geolocation information gathering through social networking platforms.

Windows Downloads

Current version : v1.4.1

Download 64bit Windows installer | Download 32bit Windows installer

OSX Downloads

Current version : v1.4.1

Download OSX installer

Source Code Downloads

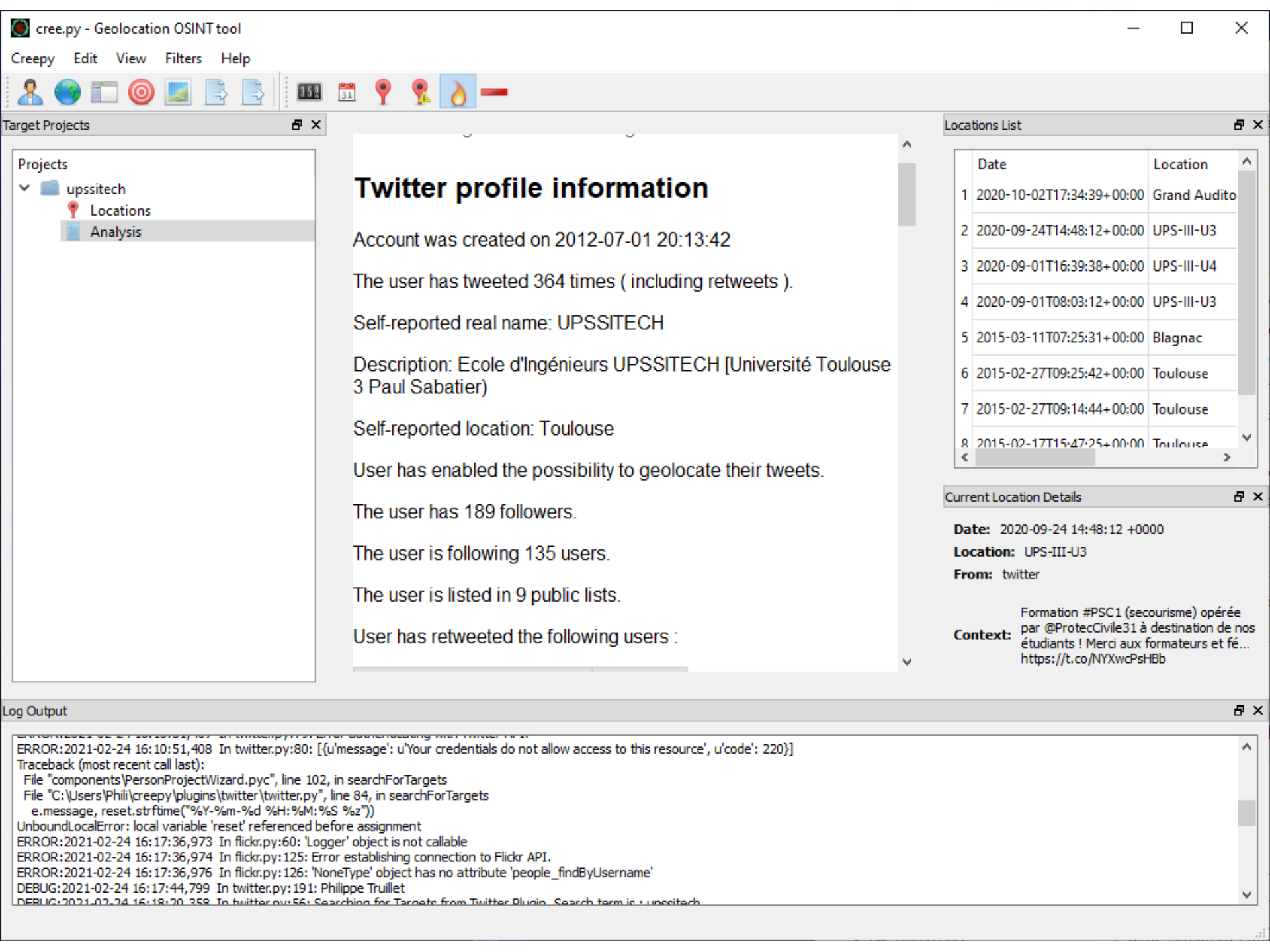
Download as .zip | Download as .tar.gz | View on GitHub

Plugin Downloads

Download as .zip | Download as .tar.gz

Creepy

Creepy is a geolocation OSINT Tool


cree.py - Geolocation OSINT tool
Creepy Edit View Filters Help
Target Projects
Projects
upssitech
Locations
Analysis
Twitter profile information
Account was created on 2012-07-01 20:13:42
The user has tweeted 364 times (including retweets).
Self-reported real name: UPSSITECH
Description: Ecole d'Ingénieurs UPSSITECH [Université Toulouse 3 Paul Sabatier)
Self-reported location: Toulouse
User has enabled the possibility to geolocate their tweets.
The user has 189 followers.
The user is following 135 users.
The user is listed in 9 public lists.
User has retweeted the following users :
Locations List
Date
Location
1 2020-10-02T17:34:39+00:00 Grand Audito
2 2020-09-24T14:48:12+00:00 UPS-III-U3
3 2020-09-01T16:39:38+00:00 UPS-III-U4
4 2020-09-01T08:03:12+00:00 UPS-III-U3
5 2015-03-11T07:25:31+00:00 Blagnac
6 2015-02-27T09:25:42+00:00 Toulouse
7 2015-02-27T09:14:44+00:00 Toulouse
Current Location Details
Date: 2020-09-24 14:48:12 +0000
Location: UPS-III-U3
From: twitter
Context: Formation #PSC1 (secourisme) opérée par @ProtecCivile31 à destination de nos étudiants ! Merci aux formateurs et fé... https://t.co/NYXwcPsHBb
Log Output
ERROR:2021-02-24 16:10:51,408 In twitter.py:80: [{u'message': u'Your credentials do not allow access to this resource', u'code': 220}]
Traceback (most recent call last):
File "components\PersonProjectWizard.pyc", line 102, in searchForTargets
File "C:\Users\Phili\creepy\plugins\twitter\twitter.py", line 84, in searchForTargets
e.message, reset.strftime("%Y-%m-%d %H:%M:%S %z"))
UnboundLocalError: local variable 'reset' referenced before assignment
ERROR:2021-02-24 16:17:36,973 In flickr.py:60: 'Logger' object is not callable
ERROR:2021-02-24 16:17:36,974 In flickr.py:125: Error establishing connection to Flickr API.
ERROR:2021-02-24 16:17:36,976 In flickr.py:126: 'NoneType' object has no attribute 'people_findByUsername'
DEBUG:2021-02-24 16:17:44,799 In twitter.py:191: Philippe Truillet

INDIVIDUAL - INTERNET PRESENCE

Email Address

Personal Handles/Nicknames

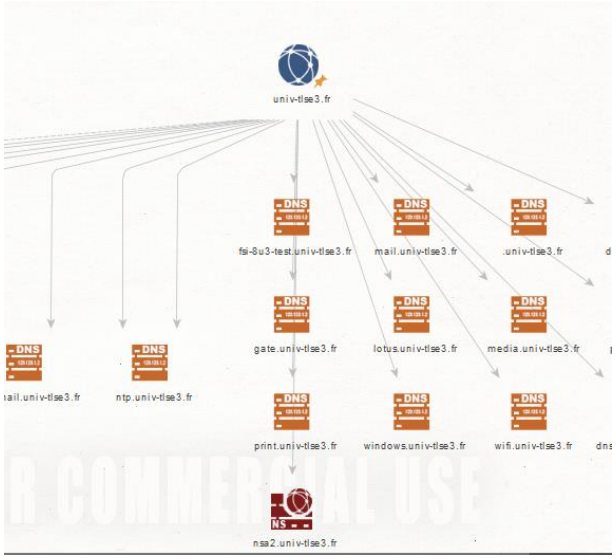
Personal Domain Names registered

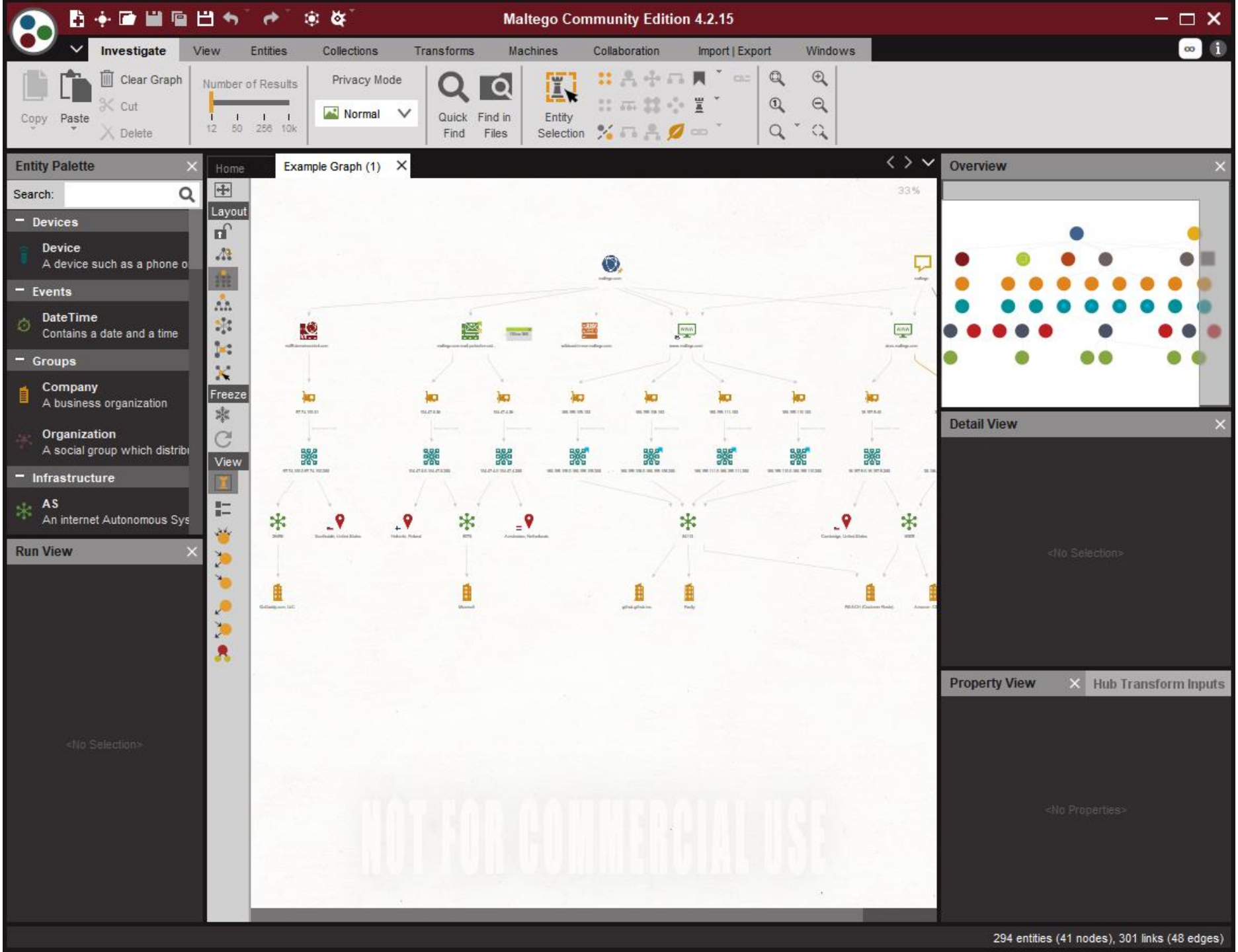
Assigned Static IPs/Netblocks

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.

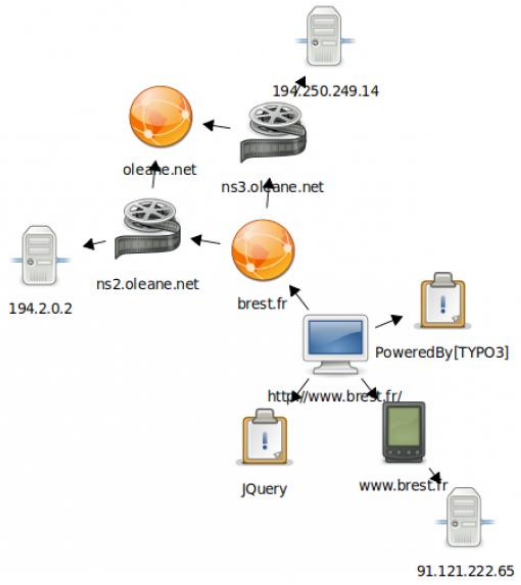


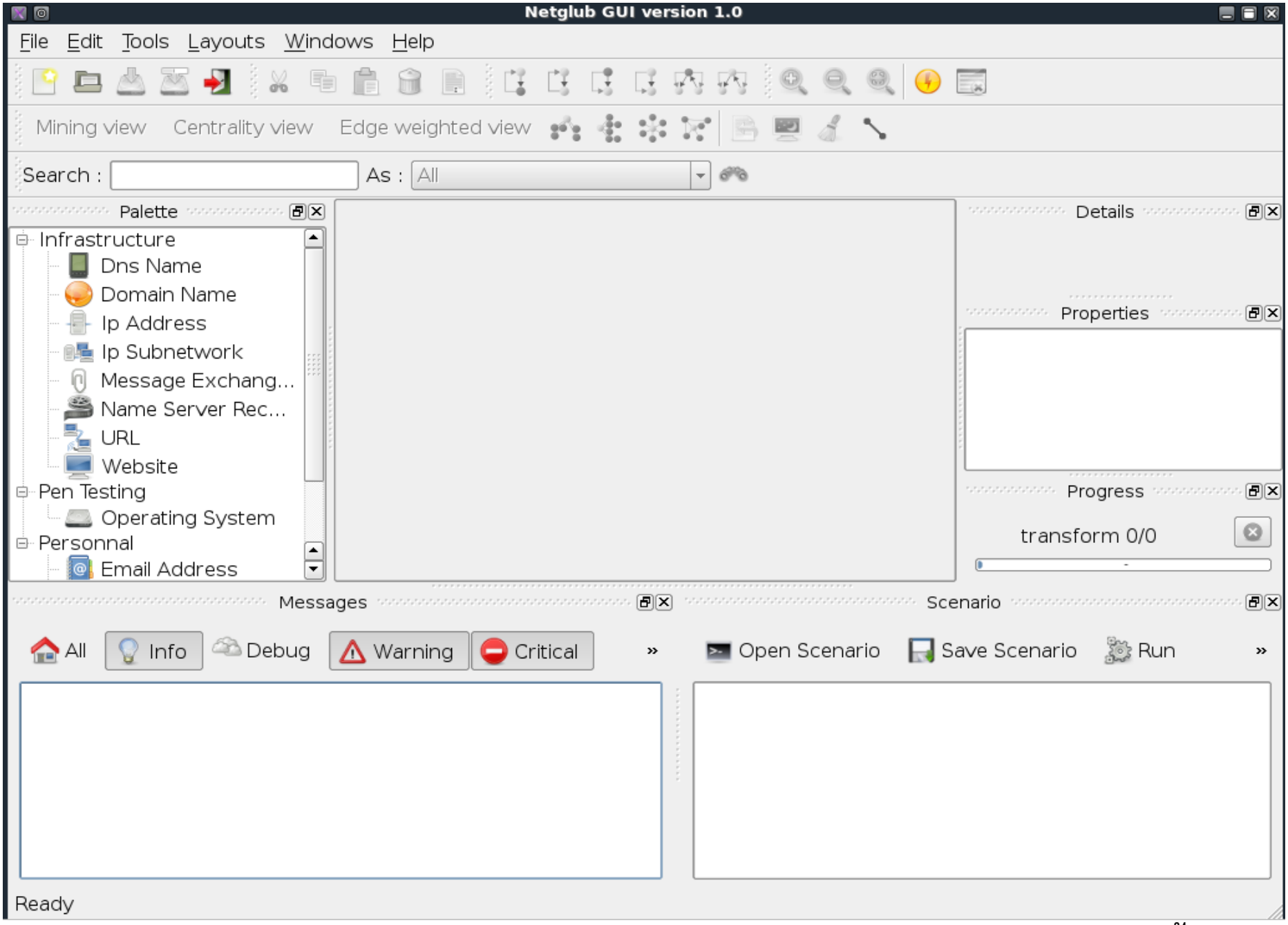

Maltego Community Edition 4.2.15
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
12
50
256
10k
Privacy Mode
Normal
Quick Find
Find in Files
Entity Selection
Entity Palette
Search:
Devices
Device
A device such as a phone o
Events
DateTime
Contains a date and a time
Groups
Company
A business organization
Organization
A social group which distribu
Infrastructure
AS
An internet Autonomous Sys
Run View
<No Selection>
Home
Example Graph (1)
Layout
Freeze
View
33%
Overview
Detail View
<No Selection>
Property View
Hub Transform Inputs
<No Properties>
NOT FOR COMMERCIAL USE
294 entities (41 nodes), 301 links (48 edges)

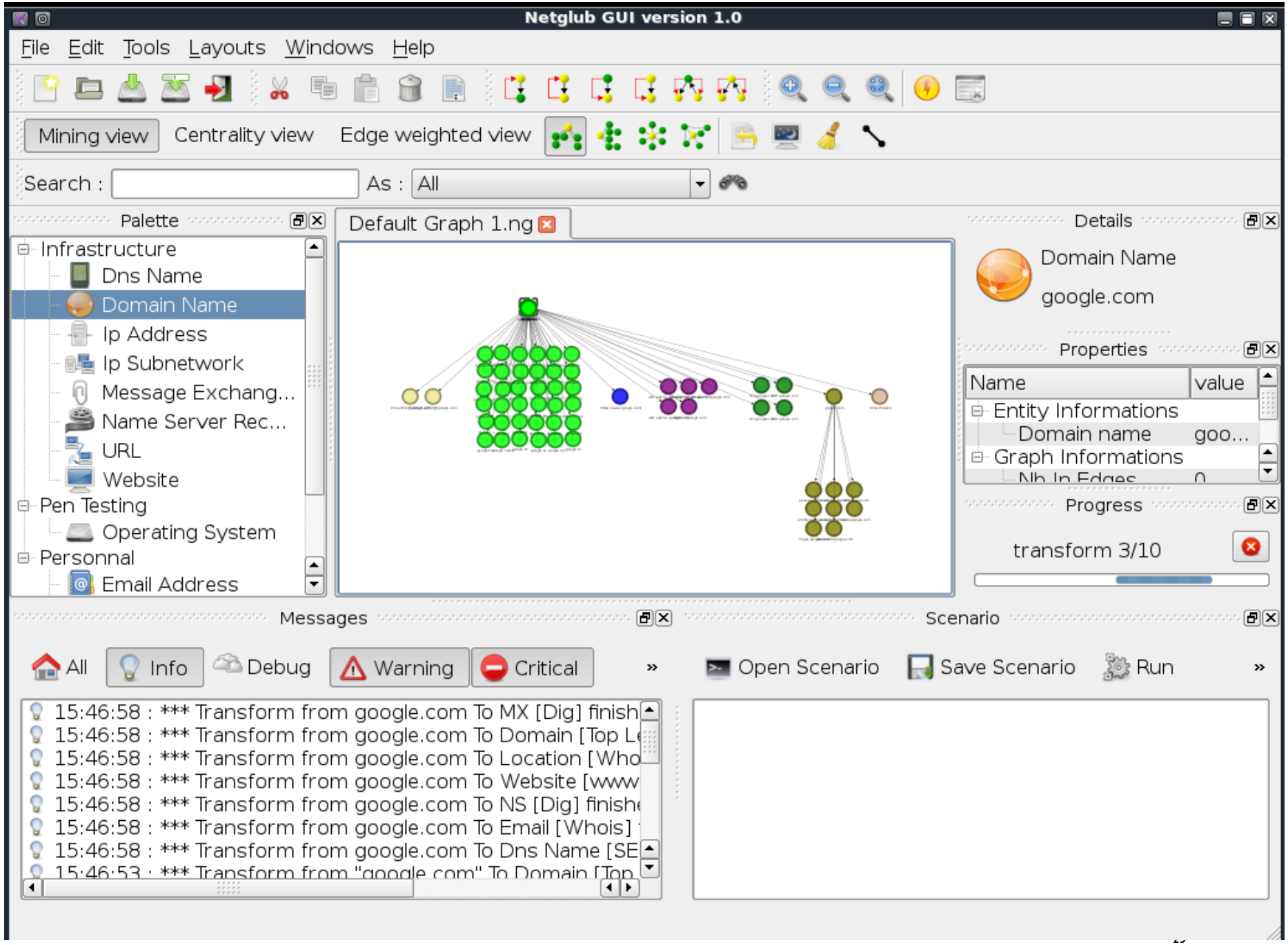
NETGLUB

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



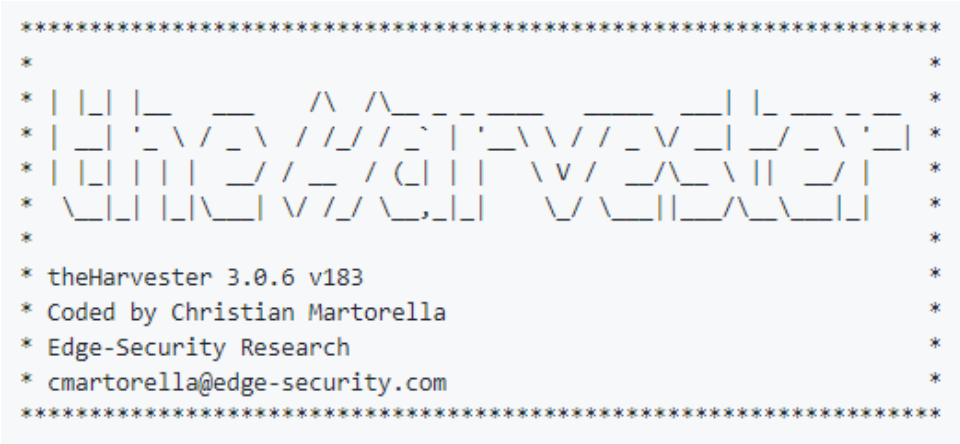

Netglub GUI version 1.0
File Edit Tools Layouts Windows Help
Mining view
Centrality view
Edge weighted view
Search :
As :
All
Palette
Infrastructure
Dns Name
Domain Name
Ip Address
Ip Subnetwork
Message Exchang...
Name Server Rec...
URL
Website
Pen Testing
Operating System
Personnal
Email Address
Details
Properties
Progress
transform 0/0
Messages
Scenario
All
Info
Debug
Warning
Critical
Open Scenario
Save Scenario
Run
Ready


Netglub GUI version 1.0
File Edit Tools Layouts Windows Help
Mining view
Centrality view
Edge weighted view
Search :
As : All
Palette
Infrastructure
Dns Name
Domain Name
Ip Address
Ip Subnetwork
Message Exchang...
Name Server Rec...
URL
Website
Pen Testing
Operating System
Personnal
Email Address
Default Graph 1.ng
Details
Domain Name
google.com
Properties
Name
value
Entity Informations
Domain name
goo...
Graph Informations
Progress
transform 3/10
Messages
All
Info
Debug
Warning
Critical
Scenario
Open Scenario
Save Scenario
Run
15:46:58 : *** Transform from google.com To MX [Dig] finish
15:46:58 : *** Transform from google.com To Domain [Top L
15:46:58 : *** Transform from google.com To Location [Who
15:46:58 : *** Transform from google.com To Website [www
15:46:58 : *** Transform from google.com To NS [Dig] finish
15:46:58 : *** Transform from google.com To Email [Whois]
15:46:58 : *** Transform from google.com To Dns Name [SE
15:46:53 : *** Transform from "google.com" To Domain [Top

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).

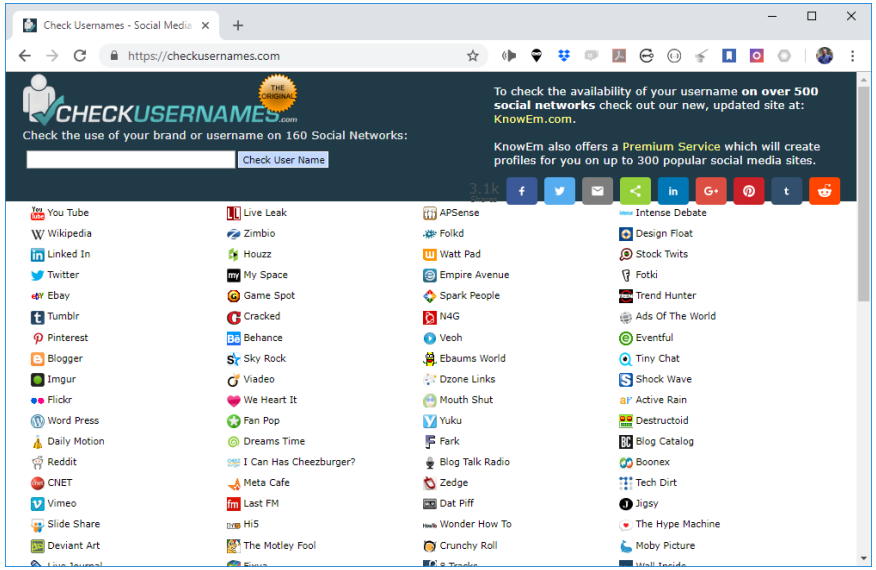
→ **http://www.edge-security.com**



SOCIAL NETWORKS

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

http://checkusernames.com



Mail Lists

The Mail Archive - https://www.mail-archive.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.

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

Internet Archive: Wayback Machi

archive.org/web/

INTERNET ARCHIVE

SIGN UP | LOG IN UPLOAD

ABOUT BLOG PROJECTS HELP DONATE CONTACT JOBS VOLUNTEER PEOPLE

INTERNET ARCHIVE
WayBackMachine

Explore more than 538 billion web pages saved over time

http://

BROWSE HISTORY

Find the Wayback Machine useful? DONATE

Tools

Wayback Machine Availability API
Build your own tools.

WordPress Broken Link Checker
Banish broken links from your blog.

404 Handler for Webmasters
Help users get where they were

Subscription Service

Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. Visit Archive-It to build and browse the collections.

Save Page Now

http://

SAVE PAGE

Capture a web page as it appears now for use as a trusted citation in the future.

Only available for sites that allow crawlers.

En attente de archive.org...

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

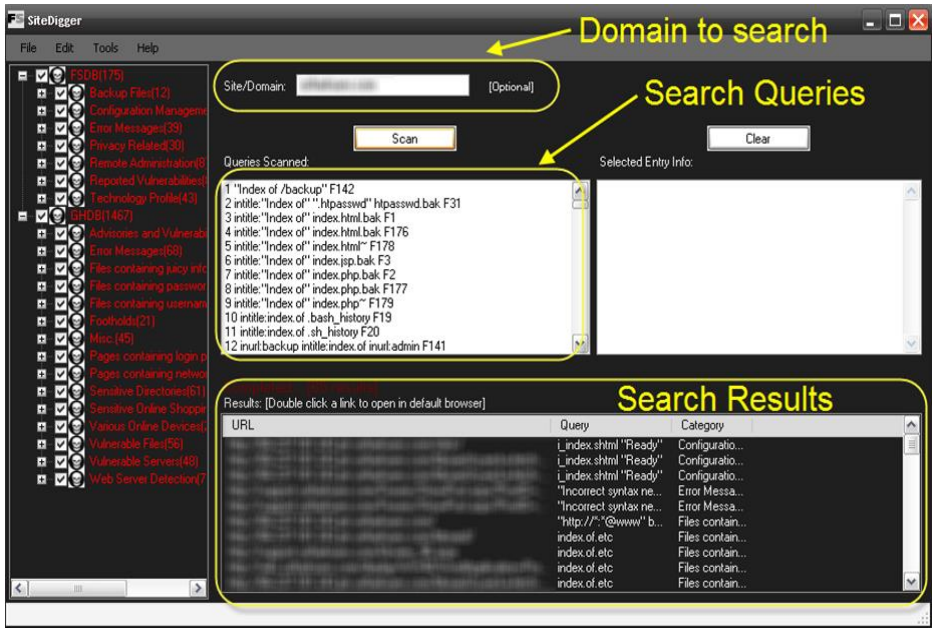
METADATA LEAKAGE - FOCA

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