



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.

TARGET SELECTION

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

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

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

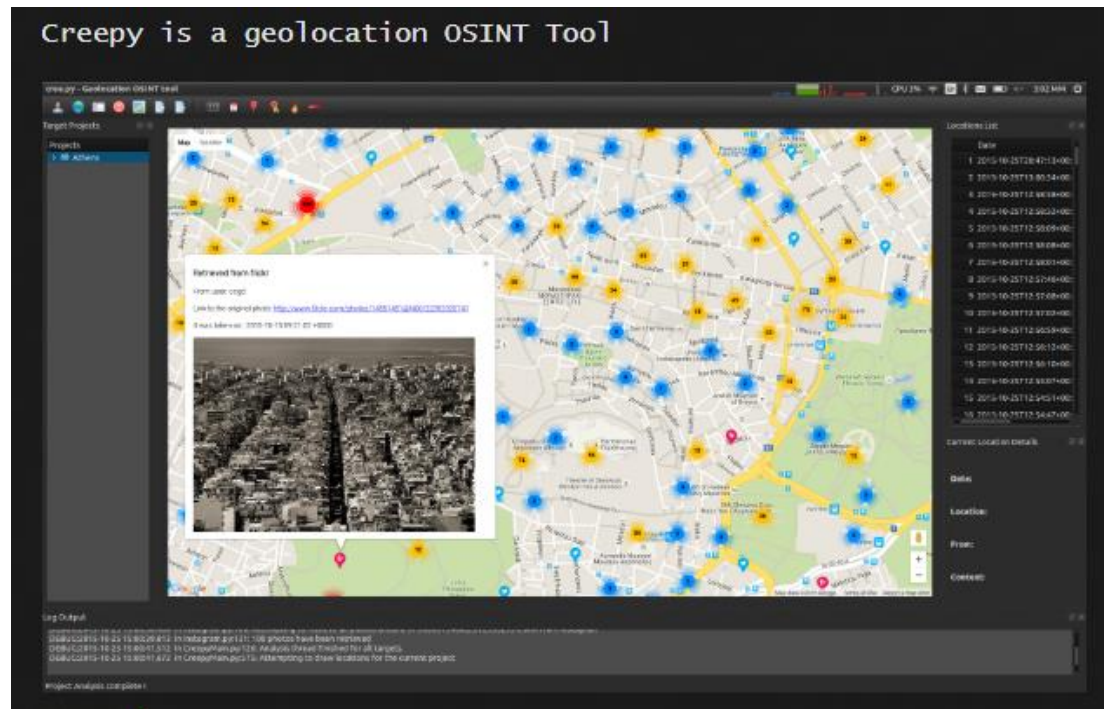
Location awareness

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.



./ 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

Creepy

Edit

Help

Targets

Map View


Fill in the details for your targets or use the search function below

Twitter Username

Flickr UserID

(XXXXXXXXX@XXX)

Geolocate Target



Use the form below to search for twitter users if necessary

Search for:

Search


Clear

Screen Name

Full Name

Photo

Twitter Results



Use the form below to search for flickr users if necessary

Search for:

Search

Search for real name

Clear

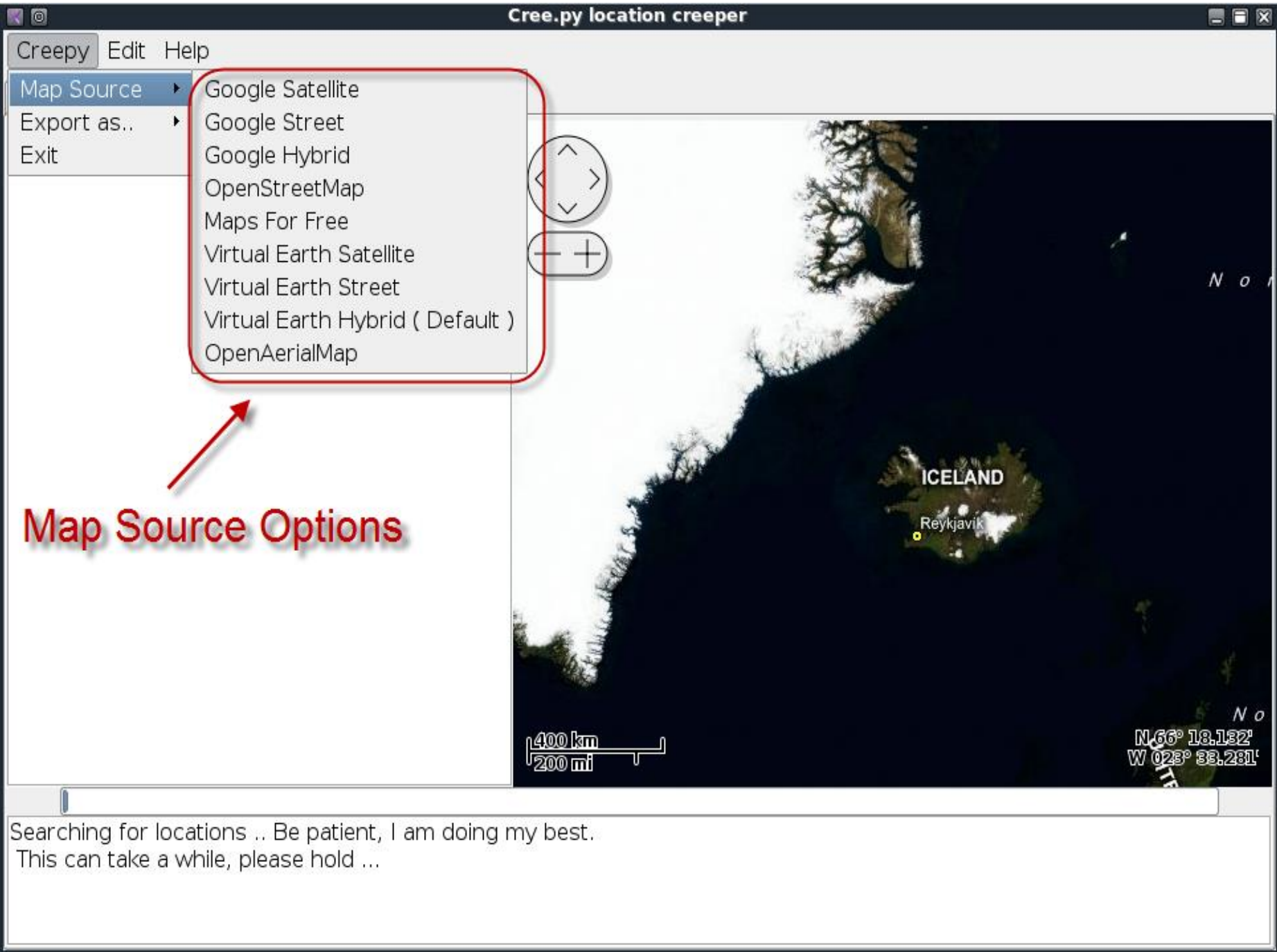
Username

Full Name

Location

Photo

Flickr Results



INDIVIDUAL - INTERNET PRESENCE

Email Address

Personal Handles/Nicknames

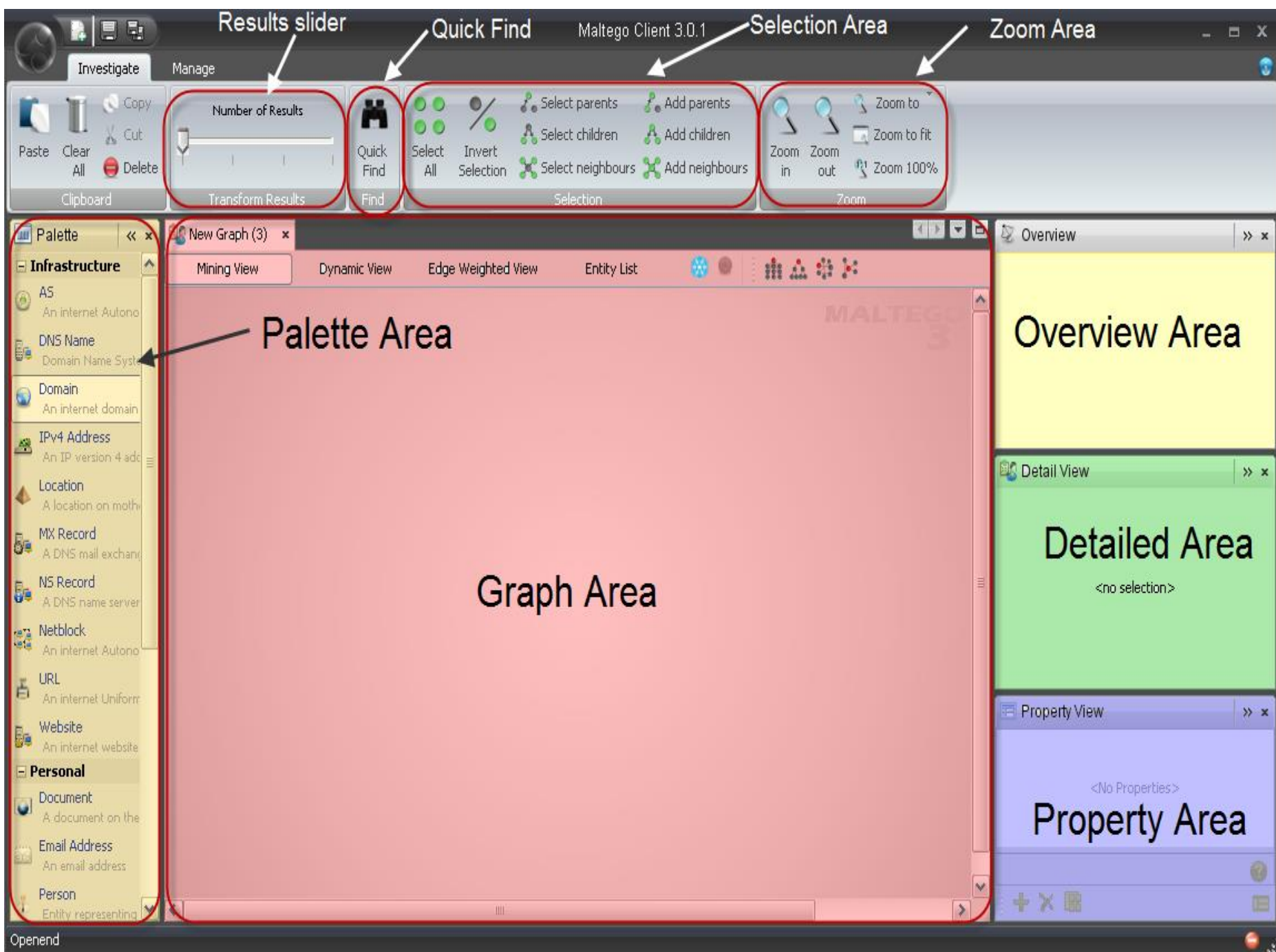
Personal Domain Names registered

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.



Investigate

Manage



Clipboard

Number of Results



Transform Results



Quick Find

Find



Selection



Zoom

Palette

Infrastructure

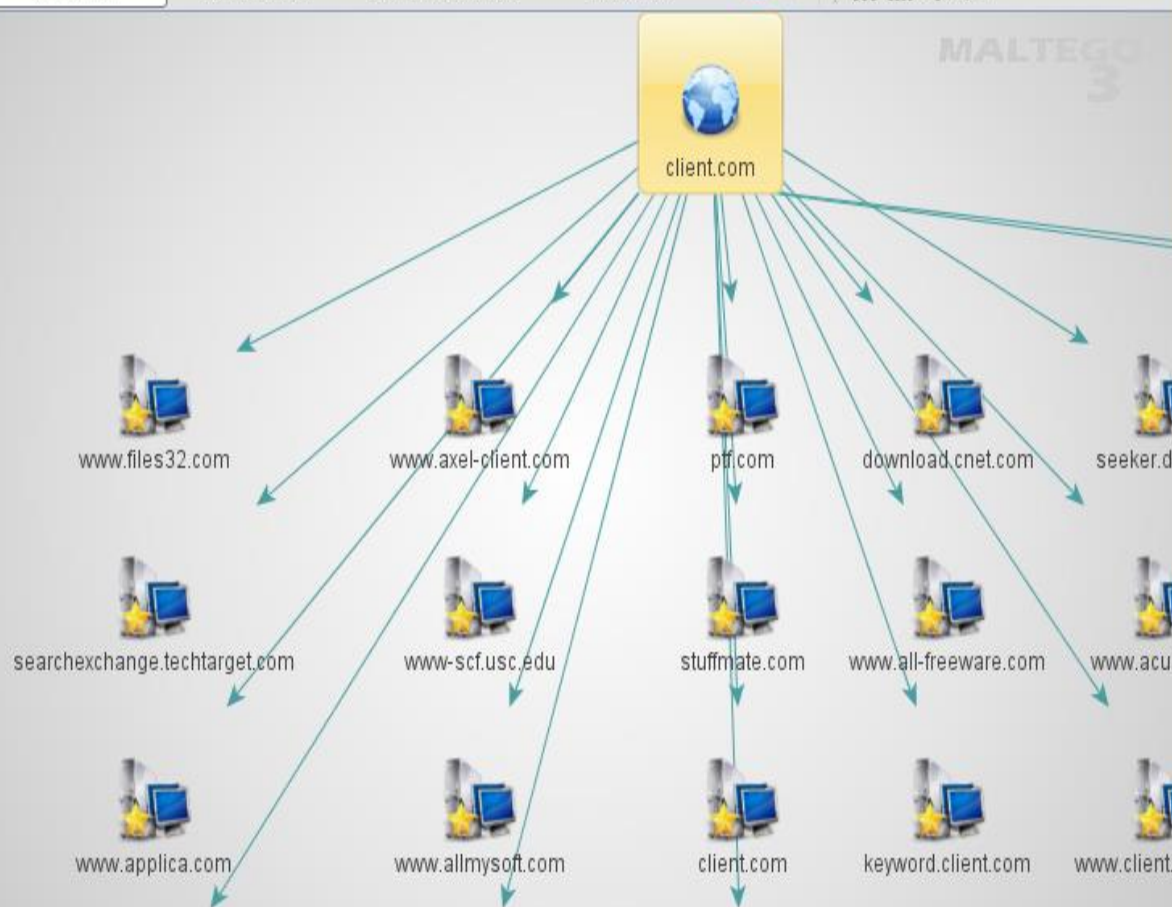
- AS
An internet Autonomous System
- DNS Name
Domain Name System
- Domain
An internet domain
- IPv4 Address
An IP version 4 address
- Location
A location on mother Earth
- MX Record
A DNS mail exchange record
- NS Record
A DNS name server record
- Netblock
An internet Autonomous System
- URL
An internet Uniform Resource Locator
- Website
An internet website
- Personal
- Document
A document on the Internet
- Email Address
An email address
- Person
Entity representing a person

Mining View

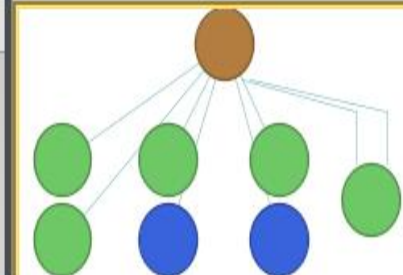
Dynamic View

Edge Weighted View

Entity List



Overview



Detail View



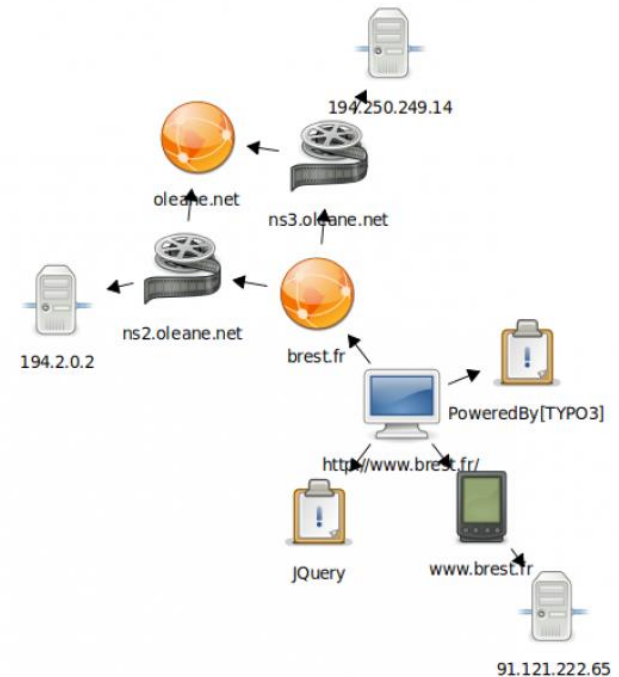
Property View

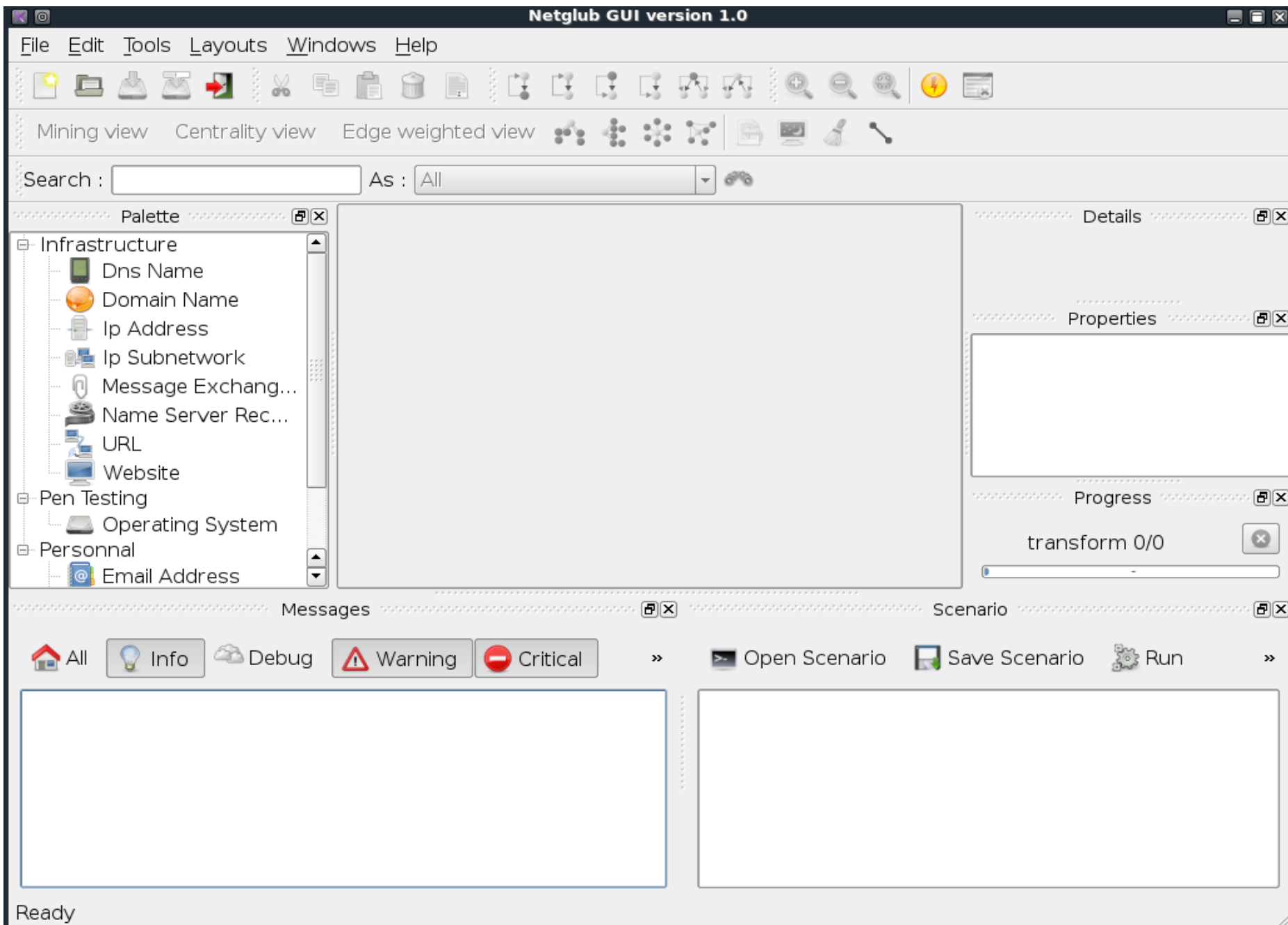
Properties	
Type	Domain
Domain Name	client.com
WHOIS Info	null
Graph info	
client.com	

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

Personal

Email Address

Default Graph 1.ng

Details

Domain Name

google.com

Properties

Name	value
Entity Informations	
Domain name	goo...
Graph Informations	
Nb In Edges	0

Progress

transform 3/10

Messages

All

Info

Debug

Warning

Critical

15:46:58 : *** Transform from google.com To MX [Dig] finish
15:46:58 : *** Transform from google.com To Domain [Top Le
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] finishe
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

Scenario

Open Scenario

Save Scenario

Run

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>

```

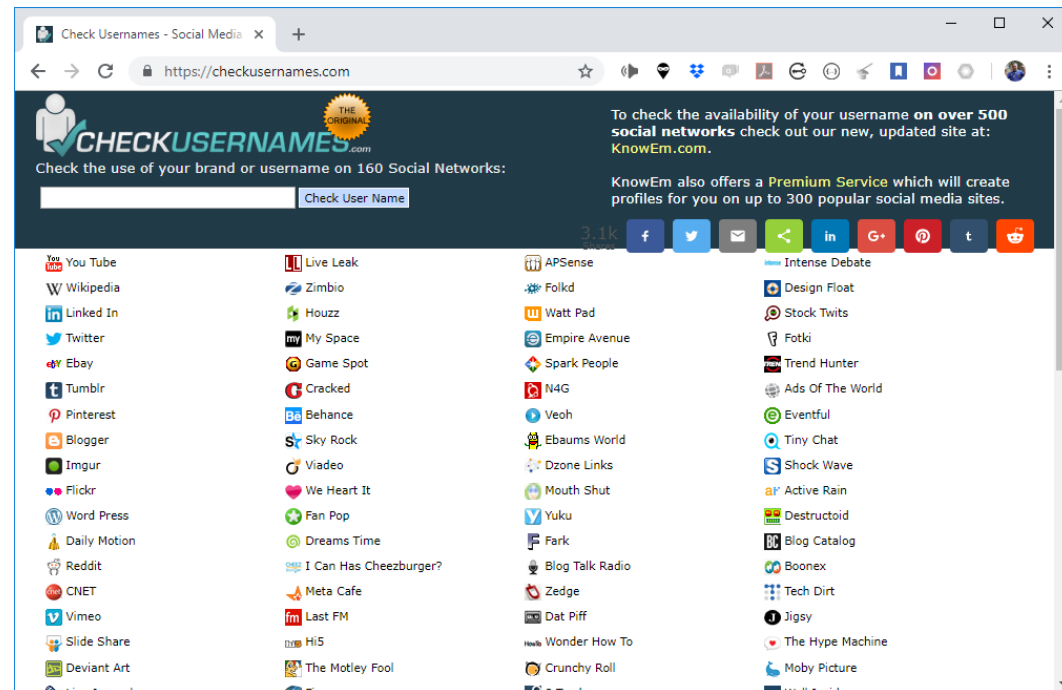
*****
*
* | | | | _ _ _ _ _ \ / \ / _ _ _ _ _ | | _ _ _ _ _
* | | | ' \ / _ \ / / / / _ \ | ' \ \ / / _ \ | / _ \ ' |
* | | | | | | _ / _ / ( | | | \ \ / _ \ \ \ | | _ / |
* \ | | | | \ | \ / / \ , | | \ / \ | | _ \ \ | |
*
* theHarvester 3.0.6 v183
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@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.

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

Announcements [\(more\)](#)

[Digital Lending Library](#)

[Over 1 Million Digital Books Now Available Free to the Print-Disabled](#)

[Millions of documents from over 350k federal court cases now freely available](#)

Web

150 billion pages



[Advanced Search](#)

Welcome to the Archive

[RSS](#)

The Internet Archive, a 501(c)(3) non-profit, is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public.

Moving Images

314,413 movies

[Browse](#)
(by keyword)

Curator's Choice [\(more\)](#)



[Dining Together](#)

Thanksgiving dining etiquette for young children.

Recent Reviews

[The Gold Rush](#)

Average rating: ★★★★★

[The Absolute Truth About Muhammad in the Bible With Arabic Subtitles](#)

Average rating: ★★★★★

Live Music Archive

82,620 concerts

[Browse](#)
(by band)

Curator's Choice [\(more\)](#)



[Grateful Dead Live at West High Auditorium on...](#)

Set 1 d1t01 [14:48] Sugaree > d1t02 [07:49] Minglewood d1t03 [07:04] Candyman d1t04 [03:00] Me And...

Recent Reviews

[Bonorama Live at Surfside Live Outdoor Concert Series on 2010-08-28](#)

Average rating: ★★★★★

[Grateful Dead Live at The Spectrum on 1988-09-08](#)

Average rating: ★★★★★

Audio

681,732 recordings

[Browse](#)
(by keyword)

Curator's Choice [\(more\)](#)



[Presente \[PN011\]](#)

"Presente", the first electronic symphony of "Equipo", is born from audio-visual project created by...

Recent Reviews

[\[experiments with 49animals\]\[49animal011\] antybiotix - flying inside your mind](#)

Average rating: ★★★★★

[ContraMundi - Full Album - JPA](#)

Average rating: ★★★★★

Texts

2,479,372 texts

[Browse](#)
(by keyword)

Curator's Choice [\(more\)](#)



[The toy shop : a romantic story of Lincoln the man](#)
Monaghan, J. Lincoln bibliography

Recent Reviews

[Overcoming Satan with one short sentence.](#)

Average rating: ★★★★★

[Leipziger Studien zur classischen Philologie](#)

Average rating:

Most recent posts (write a post by going to a forum) [more...](#)

Subject	Poster	Forum	Replies	Date
Re: something new at the top of the list	shakeitupnow	GratefulDead	0	34 minutes ago
Re: something new at the top of the list	shakeitupnow	GratefulDead	0	2 hours ago
EFFENDORF: &B (EP)/TACHYON netlabel	room101	netlabels	0	2 hours ago
EFFENDORF: &B (EP)/TACHYON netlabel	room101	audio	0	2 hours ago

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://regex.info/exif.cgi>

METADATA LEAKAGE - FOCA

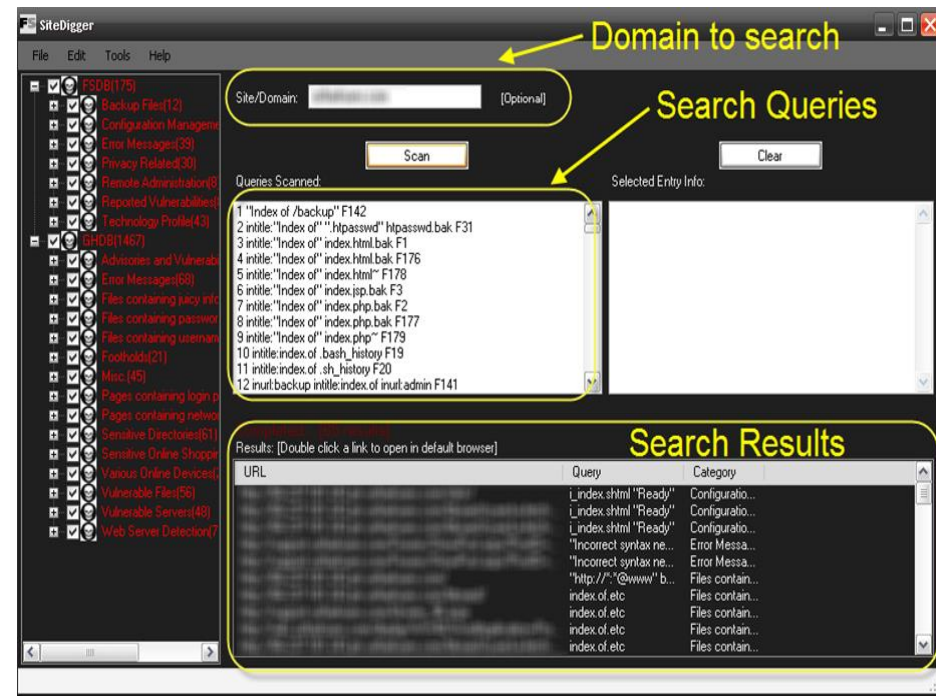
FOCA (<https://github.com/ElevenPaths/FOCA>) is a tool that reads metadata from a wide range of document and media formats.

FOCA pulls the relevant usernames, paths, software versions, printer details, and email addresses.



METADATA LEAKAGE - FOUNDSTONE SITEDIGGER

Foundstone has a tool, named **SiteDigger** (<http://www.testingtoolsguide.net/tools/sitedigger>), which 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, .doc, .xls, .ppt, .odp, .ods) available on the client's websites.

Metagoofil generates an html results 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

Physical Location

INDIVIDUAL - 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)

- Dumpster diving

- 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).

(see FabSpace: <https://www.irit.fr/FabSpace> for instance ;))