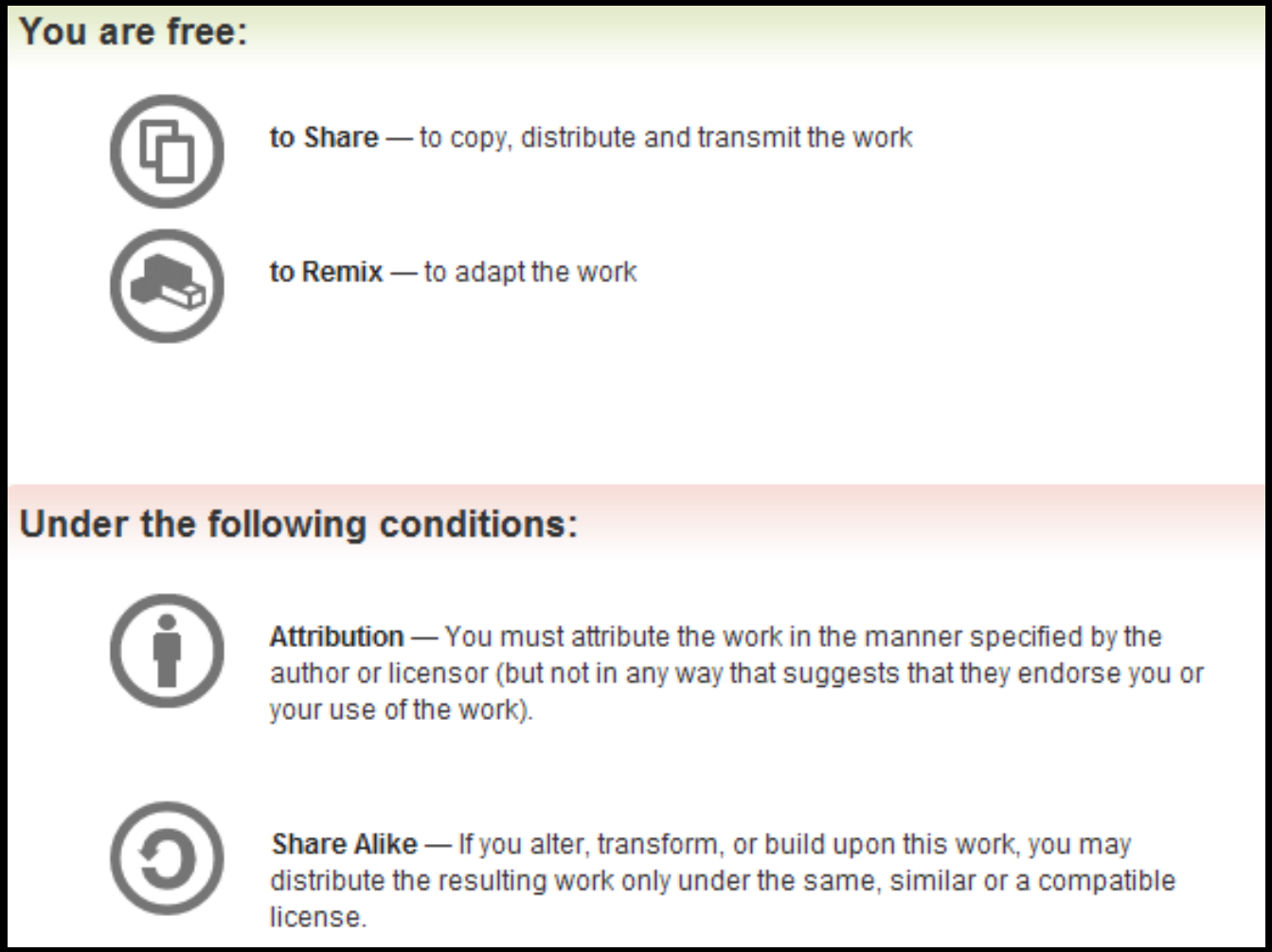
Hacking Techniques & Intrusion Detection

Ali Al-Shemery
arabnix [at] gmail

All materials is licensed under a Creative Commons "Share Alike" license.

- http://creativecommons.org/licenses/by-sa/3.0/



whoami

- Ali Al-Shemery
- Ph.D., MS.c., and BS.c., Jordan
- More than 14 years of Technical Background (mainly Linux/Unix and Infosec)
- Technical Instructor for more than 10 years (Infosec, and Linux Courses)
- Hold more than 15 well known Technical Certificates
- Infosec & Linux are my main Interests

Reconnaissance (RECON)

With great knowledge, comes successful attacks!

Outline - Reconnaissance

- Intelligence Gathering
- Target Selection
- Open Source Intelligence (OSINT)
- Covert Gathering
- Footprinting

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 publically (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, Yandex, Guruji, 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

- Bayt, http://bayt.com
- Monster, http://www.monster.com
- CareerBuilder, http://www.careerbuilder.com
- Computerjobs.com, http://www.computerjobs.com
- Indeed, LinkedIn, etc

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

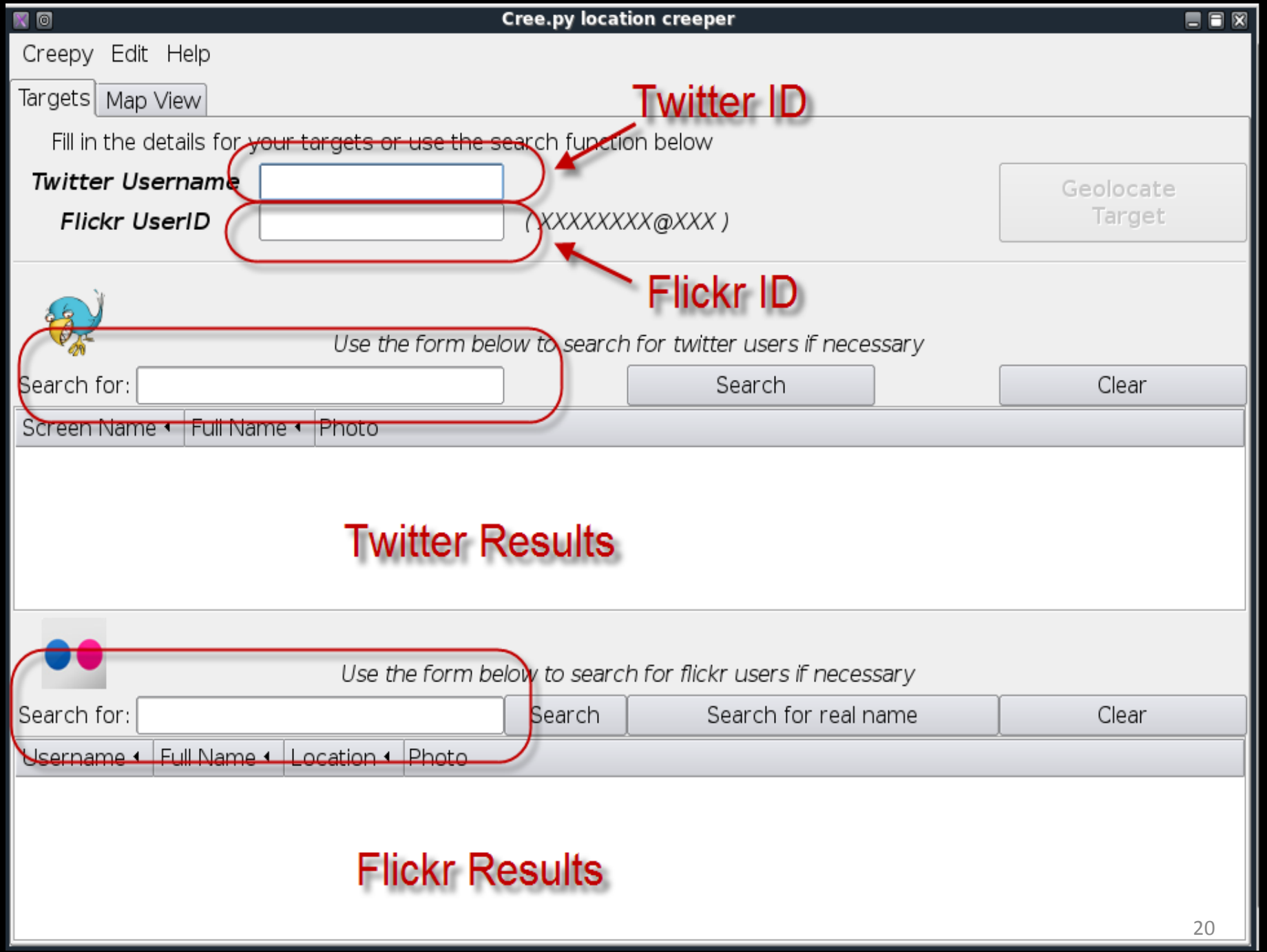
- Court Records
- Political Donations
- Professional licenses or registries

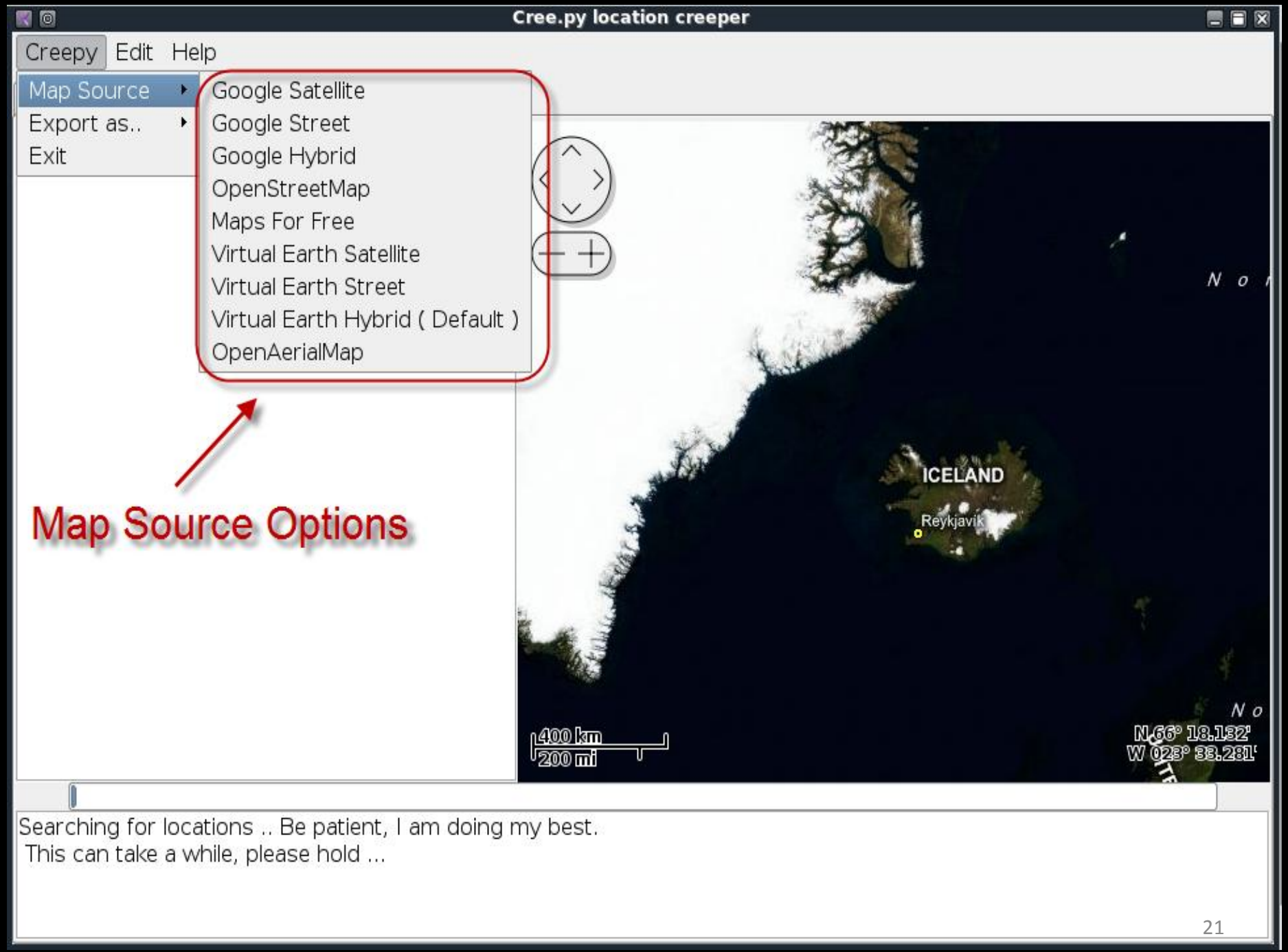
Individual - Social Network (SocNet) Profile

- Metadata Leakage
- Tone
- Frequency
- Location awareness
- Social Media Presence

Location Awareness - Cree.py

- Cree.py is an open source intelligence gathering application.
- Can gather from Twitter.
- Cree.py can gather any geo-location data from flickr, twitpic.com, yfrog.com, img.ly, plixi.com, twitrpix.com, foleext.com, shozu.com, pickhur.com, moby.to, twitsnaps.com and twitgoo.com.


Cree.py location creeper
Creepy Edit Help
Targets
Map View
Twitter ID
Fill in the details for your targets or use the search function below
Twitter Username
Flickr UserID
(XXXXXXXX@XXX)
Geolocate Target
Flickr ID
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

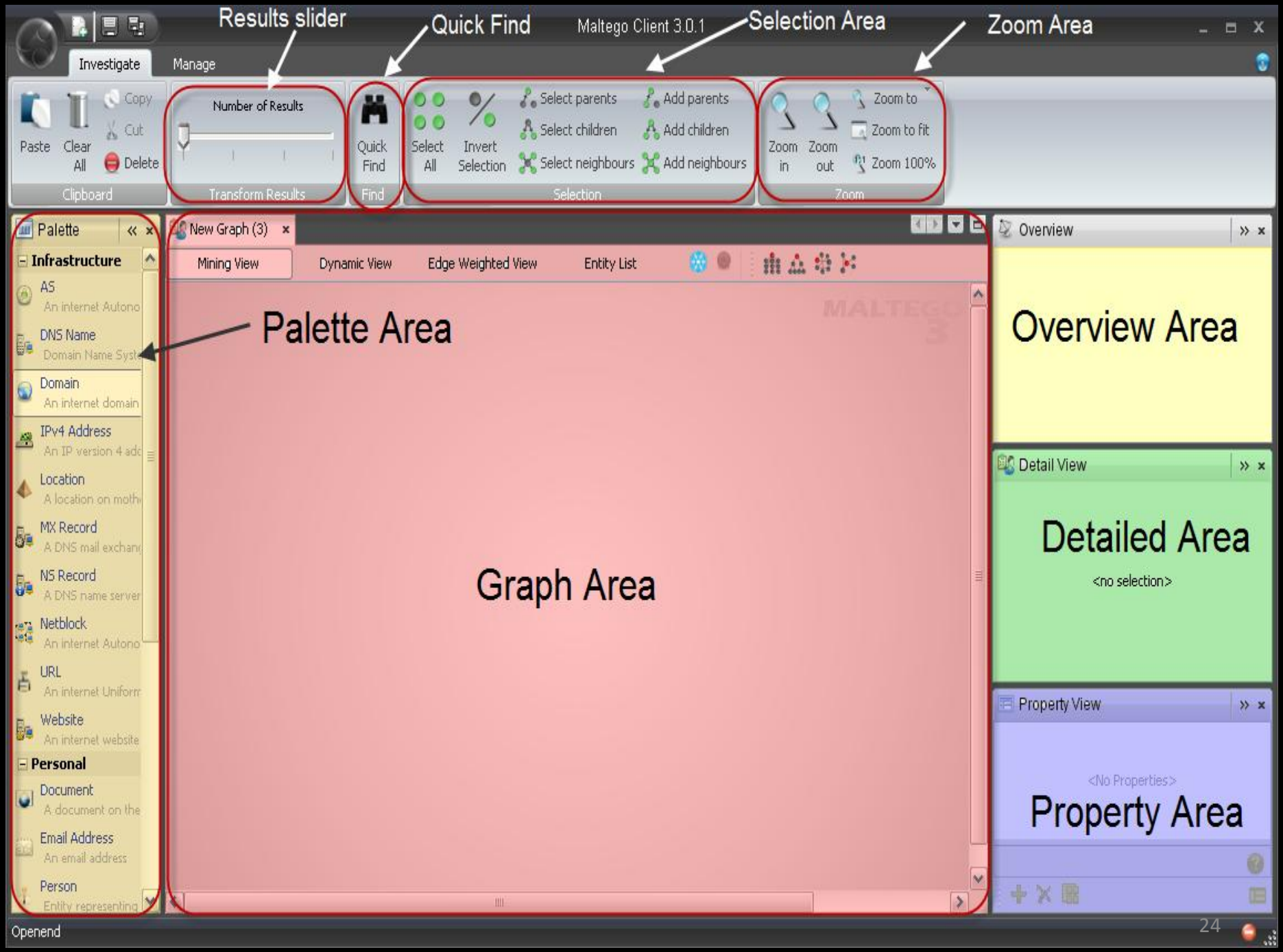

Cree.py location creeper
Creepy
Edit
Help
Map Source
Export as..
Exit
Google Satellite
Google Street
Google Hybrid
OpenStreetMap
Maps For Free
Virtual Earth Satellite
Virtual Earth Street
Virtual Earth Hybrid (Default)
OpenAerialMap
Map Source Options
ICELAND
Reykjavik
400 km
200 mi
N 66° 18.132'
W 023° 33.281'
Searching for locations .. Be patient, I am doing my best.
This can take a while, please hold ...

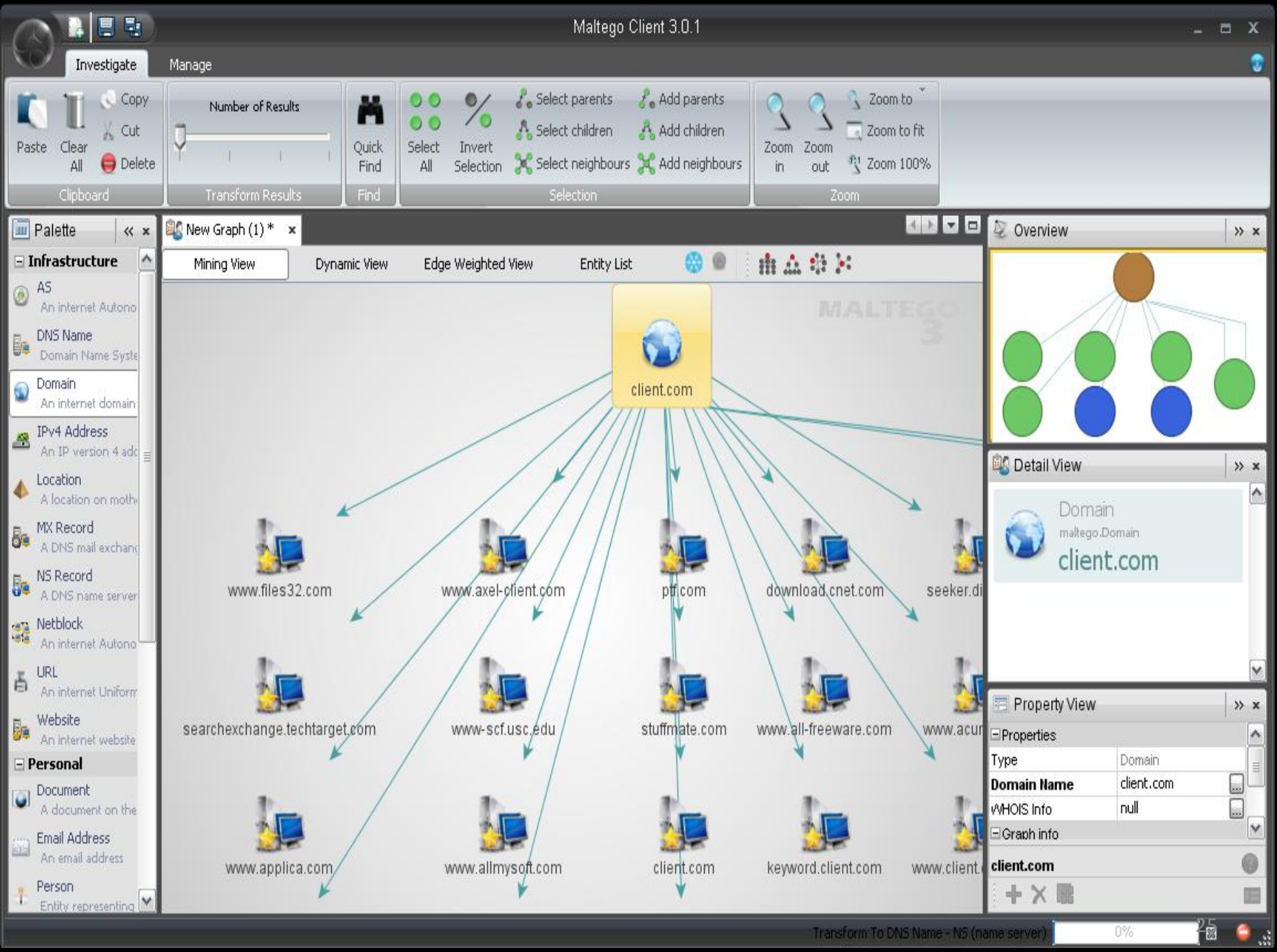
Individual - Internet Presence

- Email Address
- Personal Handles/Nicknames
- Personal Domain Names registered
- Assigned Static IPs/Netblocks

Maltego

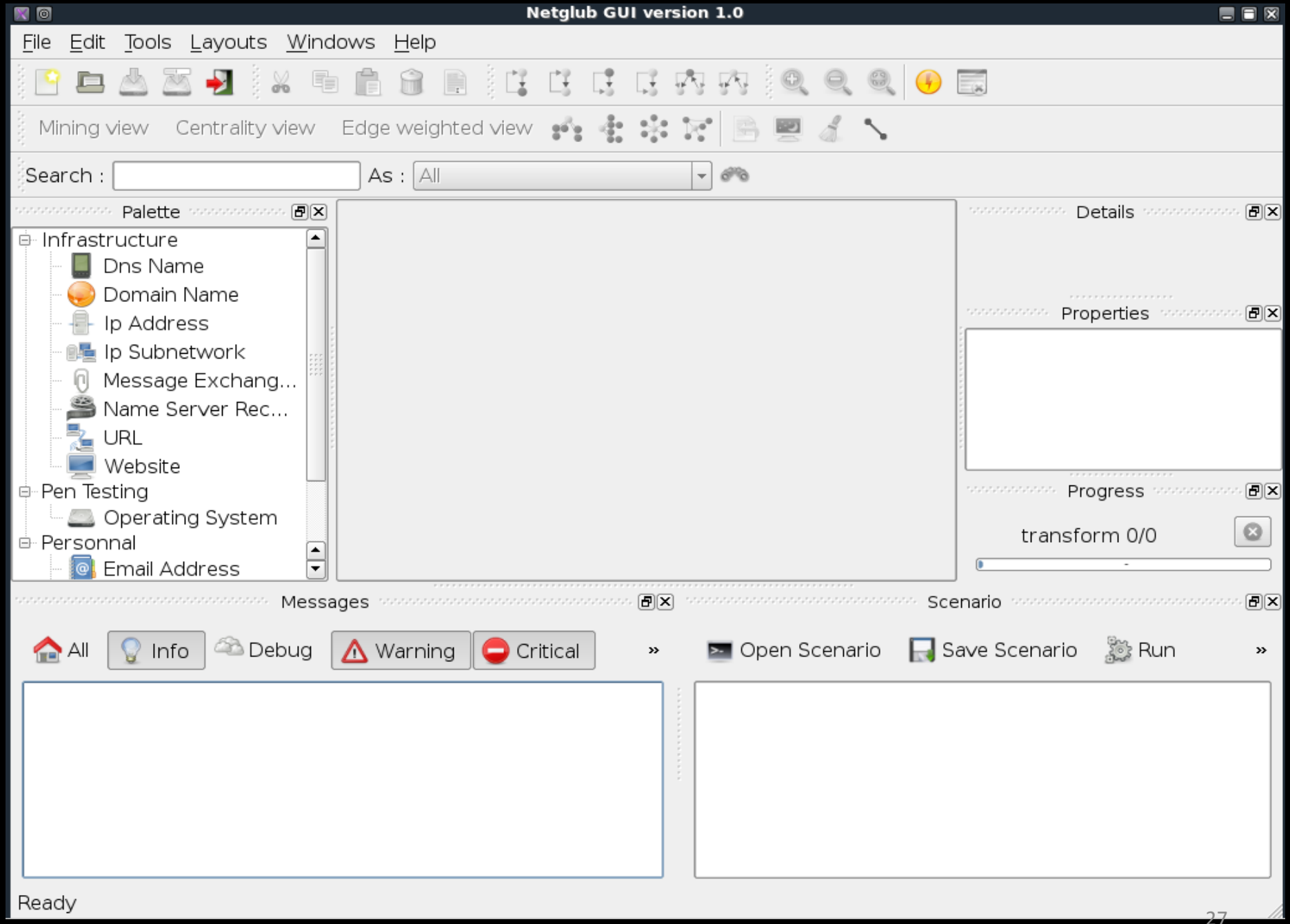
- Paterva Maltego is a data mining and information-gathering tool that maps the information gathered into a format that is easily understood and manipulated.
- It saves you time by automating tasks such as email harvesting and mapping subdomains.

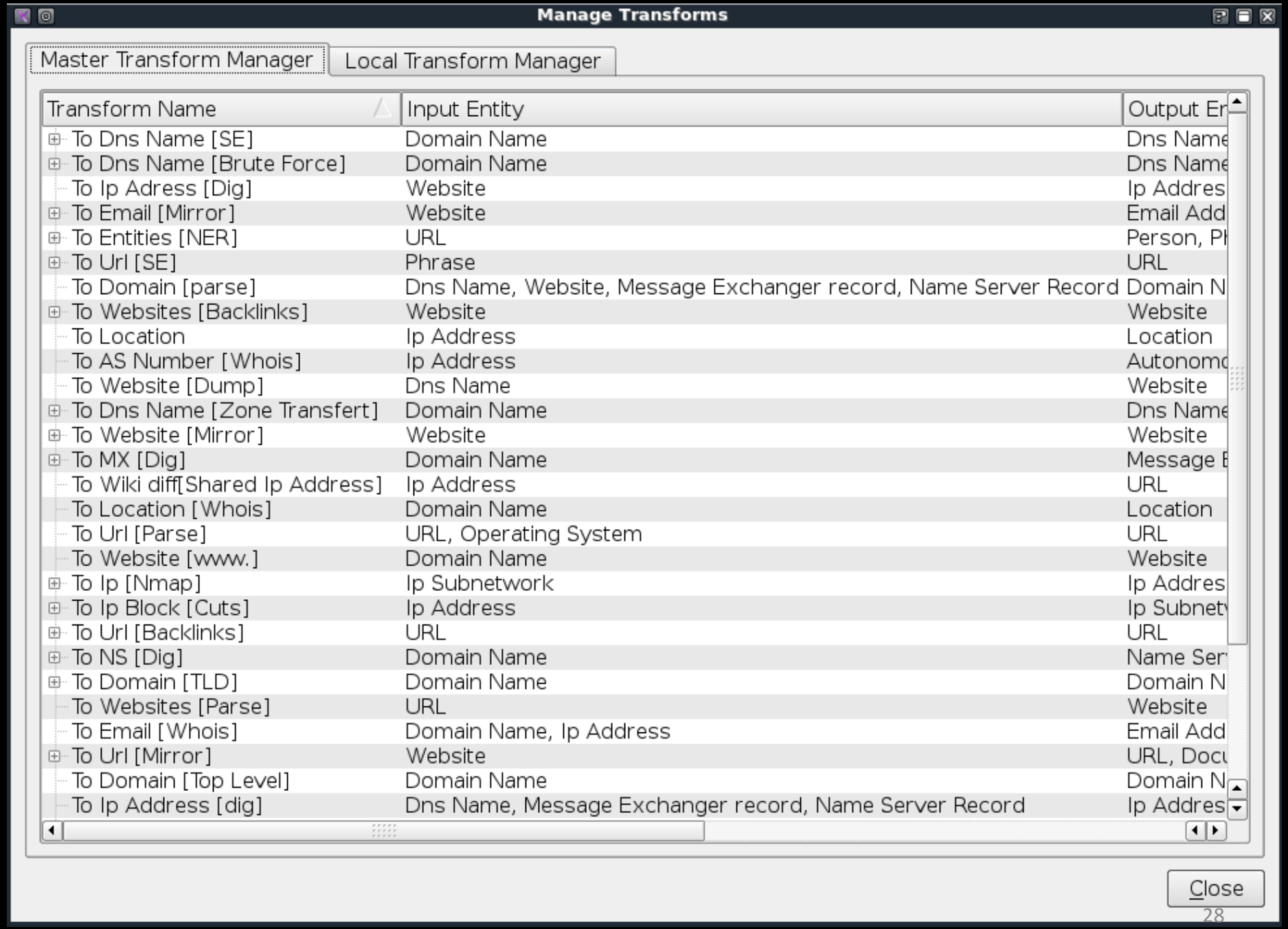

Results slider
Quick Find
Maltego Client 3.0.1
Selection Area
Zoom Area
Investigate
Manage
Copy
Cut
Paste
Clear All
Delete
Clipboard
Number of Results
Transform Results
Quick Find
Find
Select All
Invert Selection
Select parents
Select children
Select neighbours
Add parents
Add children
Add neighbours
Selection
Zoom in
Zoom out
Zoom to
Zoom to fit
Zoom 100%
Zoom
Palette
Infrastructure
AS
DNS Name
Domain
IPv4 Address
Location
MX Record
NS Record
Netblock
URL
Website
Personal
Document
Email Address
Person
Palette Area
New Graph (3)
Mining View
Dynamic View
Edge Weighted View
Entity List
Graph Area
Overview
Overview Area
Detail View
Detailed Area
<no selection>
Property View
<No Properties>
Property Area
Openend
24

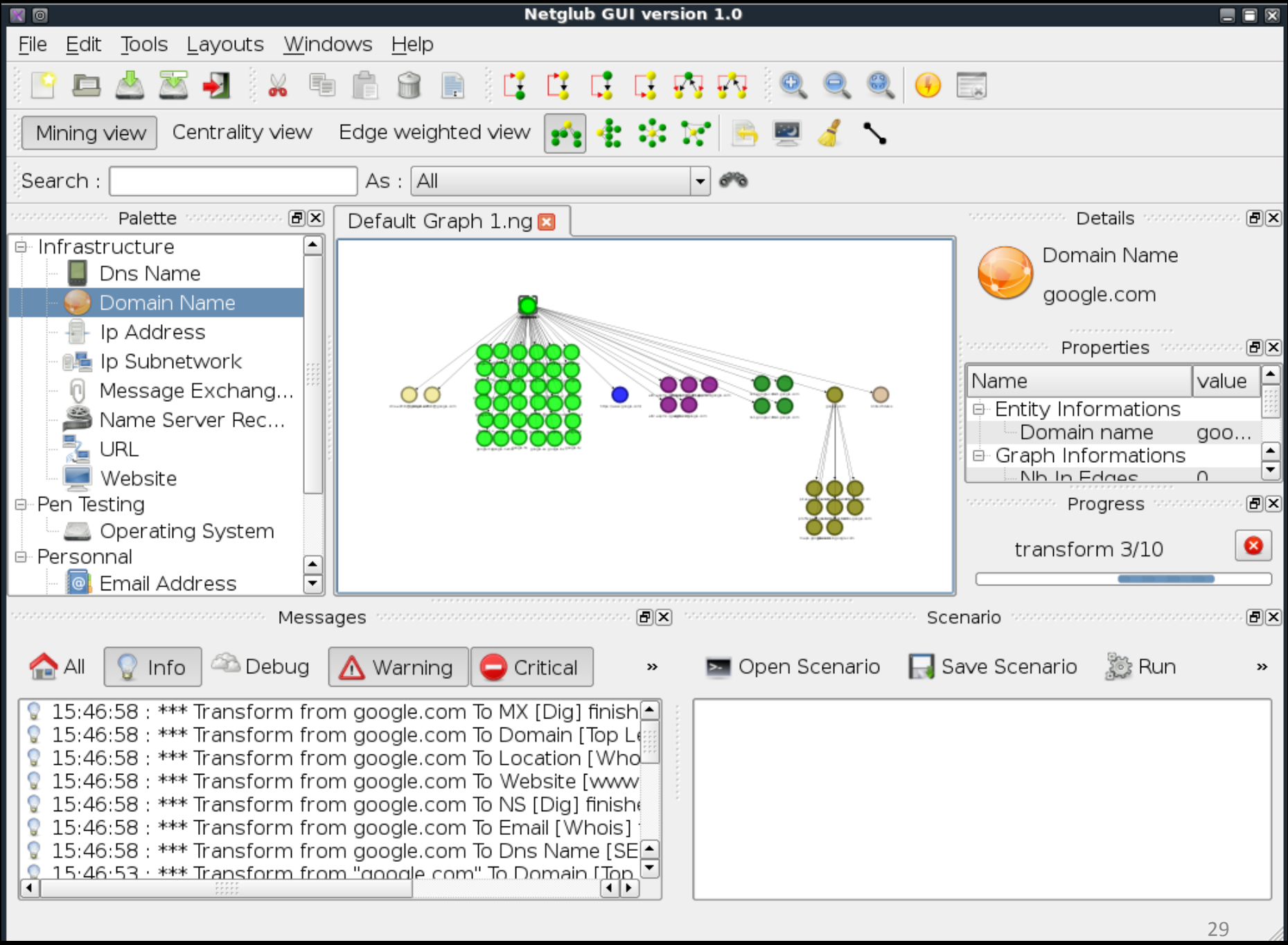

Maltego Client 3.0.1
Investigate
Manage
Paste
Clear All
Copy
Cut
Delete
Clipboard
Number of Results
Transform Results
Quick Find
Find
Select All
Invert Selection
Select parents
Select children
Select neighbours
Add parents
Add children
Add neighbours
Selection
Zoom in
Zoom out
Zoom to
Zoom to fit
Zoom 100%
Zoom
Palette
Infrastructure
AS
An internet Autono
DNS Name
Domain Name Syste
Domain
An internet domain
IPv4 Address
An IP version 4 adc
Location
A location on moth
MX Record
A DNS mail exchan
NS Record
A DNS name server
Netblock
An internet Autono
URL
An internet Uniform
Website
An internet website
Personal
Document
A document on the
Email Address
An email address
Person
Entity representing
New Graph (1) *
Mining View
Dynamic View
Edge Weighted View
Entity List
client.com
www.files32.com
www.axel-client.com
ftf.com
download.cnet.com
searchexchange.techtarget.com
www-scf.usc.edu
stuffmate.com
www.all-freeware.com
www.applica.com
www.allmysoft.com
client.com
keyword.client.com
Overview
Detail View
Domain
maltego.Domain
client.com
Property View
Properties
Type
Domain
Domain Name
client.com
WHOIS Info
null
Graph info
client.com
Transform To DNS Name - NS (name server)
0%

NetGlub

- NetGlub 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


Manage Transforms
Master Transform Manager
Local Transform Manager
Transform Name
Input Entity
Output Er
To Dns Name [SE]
Domain Name
Dns Name
To Dns Name [Brute Force]
Domain Name
Dns Name
To Ip Adress [Dig]
Website
Ip Addres
To Email [Mirror]
Website
Email Add
To Entities [NER]
URL
Person, P
To Url [SE]
Phrase
URL
To Domain [parse]
Dns Name, Website, Message Exchanger record, Name Server Record
Domain N
To Websites [Backlinks]
Website
Website
To Location
Ip Address
Location
To AS Number [Whois]
Ip Address
Autonomo
To Website [Dump]
Dns Name
Website
To Dns Name [Zone Transfert]
Domain Name
Dns Name
To Website [Mirror]
Website
Website
To MX [Dig]
Domain Name
Message
To Wiki diff[Shared Ip Address]
Ip Address
URL
To Location [Whois]
Domain Name
Location
To Url [Parse]
URL, Operating System
URL
To Website [www.]
Domain Name
Website
To Ip [Nmap]
Ip Subnetwork
Ip Addres
To Ip Block [Cuts]
Ip Address
Ip Subnet
To Url [Backlinks]
URL
URL
To NS [Dig]
Domain Name
Name Ser
To Domain [TLD]
Domain Name
Domain N
To Websites [Parse]
URL
Website
To Email [Whois]
Domain Name, Ip Address
Email Add
To Url [Mirror]
Website
URL, Docu
To Domain [Top Level]
Domain Name
Domain N
To Ip Address [dig]
Dns Name, Message Exchanger record, Name Server Record
Ip Addres
Close


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

TheHarvester

- 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).

DEMO:

- ./theHarvester.py -d linuxac.org -l 500 -b google

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
- Podcast Directory, http://www.podcastdirectory.com

Video

- YouTube, http://youtube.com
- Yahoo Video, http://video.search.yahoo.com
- Bing Video, http://www.bing.com/
- Vemo, http://vemo.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).

INTERNET ARCHIVE

Web | Moving Images | Texts | Audio | Software | Patron Info | About IA | Projects

Universal access to all knowledge

Forums | FAQs | Contributions | Jobs | Donate

Search: [ ] All Media Types GO! Advanced Search

Anonymous User (login or join us) Upload

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

WaybackMachine

http://

Take Me Back 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

Bonerama 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: ★★★½

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

Done

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

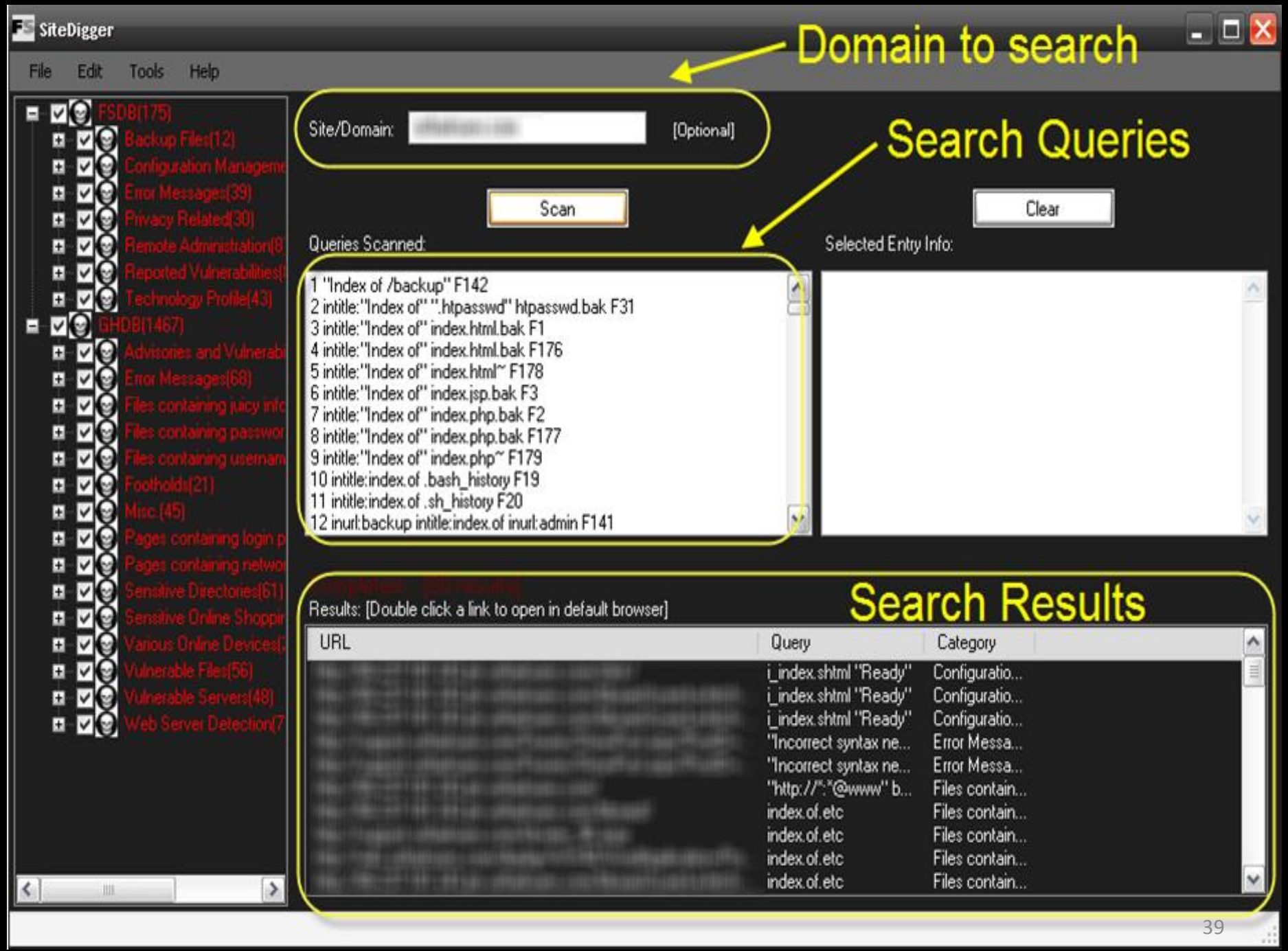
Metadata leakage - FOCA

- FOCA 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.

- DEMO (WinXP VM_Box)

Metadata leakage - Foundstone SiteDigger

- Foundstone has a tool, named SiteDigger, which allows us to search a domain using specially strings from both the Google Hacking Database (GHDB) and Foundstone Database (FSDB).


SiteDigger
File
Edit
Tools
Help
Domain to search
Site/Domain:
[Optional]
Search Queries
Scan
Clear
Queries Scanned:
1 "Index of /backup" F142
2 intitle:"Index of" ".htpasswd" htpasswd.bak F31
3 intitle:"Index of" index.html.bak F1
4 intitle:"Index of" index.html.bak F176
5 intitle:"Index of" index.html~ F178
6 intitle:"Index of" index.jsp.bak F3
7 intitle:"Index of" index.php.bak F2
8 intitle:"Index of" index.php.bak F177
9 intitle:"Index of" index.php~ F179
10 intitle:index.of .bash_history F19
11 intitle:index.of .sh_history F20
12 inurl:backup intitle:index.of inurl:admin F141
Selected Entry Info:
FSDB(175)
Backup Files(12)
Configuration Manageme
Error Messages(39)
Privacy Related(30)
Remote Administration(8
Reported Vulnerabilities(
Technology Profile(43)
GHDB(1467)
Advisories and Vulnerab
Error Messages(68)
Files containing juicy info
Files containing passwor
Files containing usernam
Footholds(21)
Misc.(45)
Pages containing login p
Pages containing netwo
Sensitive Directories(61)
Sensitive Online Shoppi
Various Online Devices(
Vulnerable Files(56)
Vulnerable Servers(48)
Web Server Detection(7
Search Results
Results: [Double click a link to open in default browser]
URL
Query
Category
i_index.shtml "Ready"
Configuratio...
i_index.shtml "Ready"
Configuratio...
i_index.shtml "Ready"
Configuratio...
"Incorrect syntax ne...
Error Messa...
"Incorrect syntax ne...
Error Messa...
"http://":"@www" b...
Files contain...
index.of.etc
Files contain...
index.of.etc
Files contain...
index.of.etc
Files contain...
index.of.etc
Files contain...

Metadata leakage - Metagoofil

- 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).