Digital Intelligence Gathering Using Maltego

Allan Vein
Tallinn 2011
Overview

- Open Source Intelligence and Forensics application
- Unix, Mac and Windows Compatible
- Client-Server architecture
- Emphasizes on the relations
- GUI to detect and evaluate the relationships
Open Source Intelligence

Open source intelligence 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. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or classified sources); it is not related to open-source software or public intelligence.
Entities 1/2

- People
- Groups of People (Social Networks)
- Companies
- Organizations
- Web Sites
Entities 2/2

- Internet infrastructure such as
  - Domains
  - DNS Names
  - IP addresses
- Phrases
- Affiliations
- Documents and Files
Transformations

- Numerous “queries” that are Entity specific
  - DNS lookup
  - MX lookup
  - Social media
  - Customizable
  - Etc
Maltego Community Edition

- Not for commercial use!
- Maximum of 12 results per transform
- You need to register on our website to use the client
- API keys expire every couple of days
- Runs on a (slower) server that is shared with all community users
Maltego Community Edition 2/2

- Communication between client as server is not encrypted
- Not updated until the next major version (and we know there are some bugs)
- No end user support – you are on your own...
- No updates of transforms on server side
Data Presentation

- GUI with a lot of presentation options
  - Data mining view (default)
  - Edge Weighted View
  - Dynamic View
- Editable relations
- Easy to comprehend and good visualization
Privacy/Security

- Borderline legal (Personal Data Protection Laws)
- Client-Server architecture, your queries are most likely saved in their databases
Practical Presentation

- Video if technical trouble :)
- http://www.youtube.com/watch?v=qiv4-wy3mxo&feature=related (no sound presentation)
- http://www.youtube.com/watch?v=QMypTK-dVal&feature=related (with sound)
Summary

- Powerful and customizable
- Emphasizes on relations
- Easy to use, hard to master
- Graphical GUI has a lot of interesting views and helps to get an overall picture