An introduction to Open Source Intelligence
Introduction
Open Source Intel: what is it? where to find it? and why do we need it?
Data
Information
Intelligence
Closed vs Open Source

**Closed**
- Internal Corporate Information
- Intelligence Database
- Risk Management Documents
- Partner (Agency) Data
- Profiles: current + previous
- Website Analytics (Internal)
- BI Data
- Financial Data
- Intellectual Property
- CRMs
- HR records

**Open**
- Accounts
- Whois
- Google (search engines)
- Public facing documents
- News Channels
- **Peer to Peer Forum**
- Website Analytics (External)
- Social Media
- Company Information
- Personnel details
“When I took office, only high energy physicists had ever heard of what is called the World Wide Web, now even my cat has it’s own page.”

Bill Clinton, ex American President
We’re always looking for entities and links!

The more we have the clearer the picture
Investigation Environment
Things to consider?

- **Stand alone network/machine**
- **Dedicated broadband – dynamic IP address** (mobile broadband)
- **Back up broadband & network/machine**
- **Standard software – anti virus, firewall, IDS / IPS/ Operating System, browser etc.**
- **Specialist software – OSINT / intelligence / evidential software & capture tools**
- **Online legends**
- **Visualisation Tools**
- **Build a jumpkit**
Also consider...

- Define a set file structure
- Set a file naming convention
- Keep an investigation log / workbook
- Investigation Plan
- Risk assessment
- VPNs & Proxies (AWS)
- Set your standpoint on anonymity
Anonymity
Anonymity & Digital Footprints

- Digital footprints are the trail left by interactions with digital environments
- These interactions are used to profile you
- To footprint or not to footprint?
Operating Systems
Pros & Cons

• Linux
• Windows
• Mac OS
• Chrome
• IOS
• Android
• (Virtual Machines)
Browsers, Dev Options, Add-ons
Browsers
Lynx Text Browser

Lynx is a text browser for the World Wide Web. Lynx 2.8.3 runs on Unix, VMS, Windows 95/98/NT but not 3.1 or 3.11, on DOS (386 or higher) and OS/2 EMX. The current developmental version is also available for testing. Ports to Mac are in beta test.

- Many user questions are answered in the online help provided with Lynx. Press the '?' key to find this help.
- If you are encountering difficulty with Lynx you may write to lynx-dev@sig.net. Be as detailed as you can about the URL where you were on the Web when you had trouble, what you did, what Lynx version you have (try '=' key), and what OS you have. If you are using an older version, you may well need to upgrade.

Maintained by lynxdev@browser.org.

Commands: Use arrow keys to move. '?' for help. 'q' to quit, '<-' to go back.
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
Help Options Print Go Main screen Quit /=search [delete]-history list
Browsers Dev Options

Built for those who build the Web
The only browser made for developers like you.

Firefox Developer Edition
Firefox Privacy

Firefox Developer Edition automatically sends feedback to Mozilla. Learn more »
Browser Add-Ons
Demo - Lightbeam
Add-ons – a few more

• Exif Viewer – (Alan Raskin)
• FireShot
• Unshorten.it!
• User Agent Overrider
• Live http headers
• Cookies Manager+
If you don’t like something, Change it!

Windows + R `%APPDATA%
then Mozilla – Firefox - Profiles
Select the right profile
Select Extensions
Add-Ons will be in an xpi file
Extract as you would a zip file
Capture Tools
SnagIt / Camtasia
Httrack
Search Engines

• Google
• Bing
• Yahoo
• Duckduckgo
• Dogpile
• Httrack?
Google Hacking

• **Cache:**
  • Intitle:
  • Allintitle:
  • Inurl:
  • Allinurl:
  • Filetype: (or ext:)
  • Allintext:

• **Site:**
  • Link:
  • Inanchor:
  • Daterange:
  • Numrange:
  • View-source
Google Hacking

- **Cache:**
  ‘&strip=1’ used with the ‘cache:’ operator
- String search by use of speech marks ‘”’
- Logical (Boolean) Operators:
  - ‘AND’ ‘+’
  - ‘NOT’ ‘-’
  - ‘OR’ ‘|’
Other Google areas of interest:

- News
- Finance
- Groups
- Images
- Blogs
- Scholar
Google Hacking

Demonstration
Content Delivery Networks

• A system of distributed servers that accelerates delivery of websites, APIs, video content or other web assets.
Example – AWS CloudFront
Building a Jump Kit
Robtex
Domain Tools
A few more favs

• Companies House
• Companycheck.co.uk
• Namesense.com
• SamelD.net
• Builtwith.com
• Majestic.com (SEO Backlink Checker)
PortableApps

PortableApps.com
Your Digital Life, Anywhere™
Automation & Visualisation
Maltego
Man & Machine

Machines are good at automation = transforms
Humans are good at pattern recognition = visual graph
So we have...

Maltego concept:

• Entities: ‘things’ – information type
  • DNS Name / Person / Phone number / more...

• Transforms: moves one type of thing to another type
  • DNS resolving / Searching / Database access / Deep web
Maltego
Visual Programming via Rapidminer
Visual Programming

orange
DATA MINING
FRUITFUL & FUN

www.8arc.com