



Advanced Open Source Intelligence Gathering

By

Nick Furneaux – CSITech Ltd

Course Description

This course is aimed at those who already have a foundation knowledge in open source information gathering. It focuses on the investigators ability to gather information on people, groups or companies from the Internet. Rather than just using 'advanced' Google searches and other web sites we will be leveraging many different tools available to look 'under the surface' of the internet, building data scrapers for the likes of Twitter, Instagram and other sites. Our collection methods are based on a specific mindset and proven methodology, used in our commercial OSI casework. Real world examples form the basis of the material covered.

The 4-day course is completely hands-on and will teach a range of skills from staying anonymous, setting up false online identities, extracting data without using a 'web site', collating the data using Maltego and graphing and visualizing data both historical and in real-time.

The final exam will pit your new skills against the online world as you work to discover all you can about a person, their friends and what they are planning to do! We have seeded the Internet with the false identities of subjects you will be investigating on this final challenging assessment.

Other Open Source courses are available, but not like this.

The course includes a course license for Maltego Classic, 3 months international VPN access, a 32 Gig USB 3 drive, a large number of software tools, bookmarks and a full colour hard copy of the slide deck.

Course Goals

1. To equip the student with the skills to carry out highly advanced techniques of searching the Internet whilst remaining anonymous.
2. To enable the student to be familiar with specialist software tools and understand the results.
3. To introduce little known online resources and techniques.
4. For the student to understand and practically apply data scraping techniques.
5. To understand how to search for material on the internet that exists, but may not have been indexed by search engines.
6. To enjoy a 'hands-on' course throughout the 4 days

Course Content

Preparing the right mindset

Legal restrictions

Creating the right toolkit

- Encryption of data

- Understanding the dangers of system caches

- Overview of using Virtual Machines

Preventing the leaking of our own data

Visual data gathering from images and videos

Solar shadow and distance estimation analysis

Bouncing anonymously round the world – Proxies and VPN's

Setting up your own false identities

Extensive Maltego Classic training

- Fundamentals of Maltego

- Using Maltego to collect open source information

- Building custom data viewlets and machines

- Analysis of large amounts of data
- Graphing trends and seeing the future
- Advanced mapping techniques
- Web site and Internet Network mapping and detailed information gathering
- Finding and analyzing data relationships
- Exploiting leaked databases
 - Accessing databases
 - Password decryption
 - Attributing leaked data to real world target
- Doing bad things with Google
 - Finding Documents and meta data extraction
 - Using your skills to understand your own vulnerabilities
- Building complex searches to find devices and leverage network information
 - Finding online control systems
 - Finding cameras/printers and other resources
 - Find devices that REALLY shouldn't be public!
- Understanding and exploiting email
- Getting under the hood of Social Media
 - Building data scrapers
 - Downloading videos from social networks
 - Including Instagram stories
 - Twitter tools and techniques
 - Facebook hints and tips
 - LinkedIn
- In depth, real world practicals to test the skills you have learned

Requirements

The student should have a basic understanding of Open Source Intelligence¹ gathering and be comfortable with online researching.

The student will also need access to a laptop with the ability to download and install software, have unrestricted internet and USB key access.

Cost

Total cost - £1850 + VAT including manual, software and USB key. Lunches and snacks also included.

¹ For example - Open Source Internet Intelligence Investigation Course (Foundation)
<https://csilearn.learnupon.com/store/411432-open-source-internet-intelligence-investigation-course-foundation>