RN Trust
The Digital Trust Company

Open Source Intelligence (5 days)

This technical workshop focuses on the ability to gather information on people, groups or companies from the Internet. In addition to using advanced web searches and other web sites this technical workshop will be leveraging the tools available to look 'under the surface' of the internet, accessing data trough database, deep web, various data collection methods and other. The technical workshop is 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.

This technical workshop will provide participants with the skills needed to carry out highly advanced techniques of searching the Internet whilst remaining anonymous. With this technical workshop participants will understand and practically apply various techniques to gather underlaying data and how to properly interpret it.

At the end of the technical workshop all participants will be given an exam and official certificate for attending the technical workshop.

Technical workshop Objectives:

- To equip the student with the skills to carry out highly advanced techniques of searching the Internet whilst remaining anonymous
- To enable the student to be familiar with specialist software tools and understand the results
- The introduce little known online resources
- For the student to understand and practically apply API techniques to directly talk to the underlying databases of Social Network sites

Prerequisites:

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

Syllabus

DAY 1

Day one is focused on giving a wide overview of what OSINT is and the relevance behind it. The class will show number of different scenarios that will get the participants into the right mindset that will enable them to better understand the relevance of found data. Lateron, participant will learn all about legal restrictions, creating their right environment for conducting OSINT investigations

- **I. OSINT defined**
- **II. Preparing the right mindset**
- **III. Organisation**
- **IV. Methodology**
- **V. How internet works**
  - **Networks and Internet**
  - **DNS**
  - **Proxy**
  - **VPN's**
  - **TOR**
  - **Dark web introduction**
- **VI. Legal restrictions**
- **VII. Preparing the workstation and the investigation environment**
  - Settings
    - Web browsers and privacy
    - Web browser plugins
    - VPN's
    - Antivirus and antimalware
- **VIII. Data leaking – benefits for us**
  - Where to find data and how to use them in analysis
  - Where do we cross the line of legacy?

DAY 2

Day will continue on day one with setting up the right environment that will prevent any data leaking from the investigators side and enable them to conduct covert quarries. Having the right mindset and knowledge about data leakage is crucial in all OSINT investigations. In the second part of the day, participants will learn how to create advanced searches with most popular search engines and will learn about other more specialized search engines that will provide additional data

- **I. Virtual machines**
- **II. Setting up your own false identities**
- **III. Learn Maltego and Maltego Case file**
  - **Investigating network infrastructure**
- **IV. Search engines**
  - **Google**
    - Search operators
    - Google custom search engines
    - Google images
    - Web archives
  - **International search engines**
  - **Others**
    - Duck Duck Go
    - Start Page
    - FTP search
    - **Global file search**
    - **Nerdy data**
- **V. Google custom search engine**
  - Creating our own news aggregators
- **VI. People search engines**
- **VII. Documents**
  - Google searching
  - Google docs
  - Presentation repositories
  - Metadata viewers
  - Pastebin

DAY 3

Participants will begin to use different tool that speed up specific searching, learn how to investigate emails, pictures, geolocation and mapping, camera information and working with video evidence. Last part of the day three is all about using a virtual mobile device for OSINT investigation.

I. Emails
- Email headers
- Email assumptions
- Email permutations
- Compromised accounts – BEC (Business Email Compromise)

II. Pictures and videos

III. Google images

IV. Reverse image search

V. Exif data
- Geolocation
- Camera trace

VI. Video
- Reverse video search
- Youtube
- Downloading videos

VII. Websites
- Crawlers
- Metadata
- Bruce forcing folders

VIII. Virtualizing mobile devices
- Using virtual mobile OS for OSINT investigation

DAY 4

During day four, participants will learn how to work and investigate data breaches that have proved to be one of the most interesting data sources for OSINT. In addition, there will be more case studies and exercise that will utilize all that has been learned in the previous days. End of day will be devoted to investigating social networks.

I. Checking if hackers have released your/corporate information
- Using and investigating data breaches

II. Finding cameras/printers and other resources -find publicly available private data
- Shodan search

III. Social networks
- Facebook
- Instagram
- Twitter
- Linkedin
- Others
- Social media communication

DAY 5

Last day will cover topics such dark web investigation and cryptocurrencies. With the conclusion of the last day, participants will also learn how to do proper reporting and analysis of the found data and conduct one last final case scenario that will tide all that has been learned in the previous days.

I. Dark web
- Analysing Tor nodes
- Cryptocurrencies and wallets
- Blockchain

II. Investigatory Framework
- Email address
- User name
- Real name
- Telephone
- Domain name
- Location

III. Reports

IV. How to export from OSINT tools
- What is important for report
- Final exam