RN Trust
The Digital Trust Company

FINANCIAL INVESTIGATION TECHNIQUES OPEN SOURCE INTELLIGENCE (5 DAYS)

This course focuses on the ability to gather information on people, companies and financial data available online only from the free online available sources. In addition to using advanced web searches and other web sites, this course will be leveraging the tools available to look 'under the surface' of the internet, accessing data trough database API's, website crawlers and others. Participants will learn frameworks and basic procedures necessary to perform financial investigation. Trainers will show and explain techniques on how to get information from dark web, how to analyse cryptocurrencies, explore blockchain based on real case scenarios. The workshop is dedicated to money fraud analysis, financial investigations, cryptocurrencies transactions, online data exchange.

Course Objectives:

By the end of this workshop, all the students will be able to:

- Properly prepare their workstation for OSINT investigations
- Recognize the danger of data leakage and how to prevent it on time
- Set up toolkit for OSINT investigations
- Conduct compliance checks in financial investigations
- Use search engines to investigate people, companies and financial data available online
- Investigate emails on basic level
- Find and recognize forensic value of data breaches available online
- Use Maltego tool for financial forensic investigations
- Perform online investigation on documents, pictures and their metadata
- Connect information about people and their social contacts by using social media
- Search for forensically important data on dark web
- Understand how blockchains, cryptocurrencies and wallets function and what is their forensic value
- Perform OSINT investigations on mobile money and frauds
- Create detail report with all important data gained through OSINT tools

Prerequisites:

The students should have a basic understanding of open source intelligence gathering and be comfortable with different kinds of online researching.

Syllabus

DAY 1

Workshop starts with setting up correct mindset for this kind of investigations. Students are learning how to prepare their workstation for the forensic analysis, what are the main security issues that every forensic investigator need to be aware of and how to prevent them. A lot of attention is given to VPNs, their setup, usage; settings of virtual machines and benefits from them. At the end of day1, students are introduced to recommended investigation toolkit and Financial OSINT framework.

I. Correct mindset

II. Preparing the workstation

- Basics of networking
  - Network
  - IP
  - DNS
  - Proxy
  - Websites
- Data leaking
- VPN's
  - Settings
  - Benefits and forensic value
  - VPN recommendations
- Virtual machines
  - Software and Setup
- Fake accounts for investigations
- Investigation toolkit
  - Web browsers and privacy
  - Plugins and search engines
  - Antivirus and antimalware
  - Maltego Case File
  - Hunchly

III. OSINT framework

DAY 2

Day 2 starts with the most recent case study. Based on that case study, students will get information about the financial investigation framework and how and on what online services to conduct compliance checks. Students will also use different search engines to get information about people, companies and financial data available online. The workshop continues with the basic email analysis, data breaches and introduction to Maltego tool.

I. Case study – no1

II. Introduction to financial analysis

- Basics of economics
  - Transaction
  - SWIFT
  - On-line transactions
  - App payments
  - Bookkeeping
  - Financial reports
  - Balance reports
- Regulations
- Others
  - Duck Duck Go
  - Start Page
  - FTP search
  - Global file search
  - Nerdy data
- Searching for people
- Searching for companies
- Financial data available online

- Agencies
- EU legislations

III. Financial investigation framework

IV. Compliance checks

- ❖ Sources
- ❖ Connecting people and companies
- ❖ Reading reports
- ❖ Making connections based on location, people, owners

V. Search engines

- Google
  - ❖ Search operators
  - ❖ Google custom search engines
  - ❖ Search engines in financial world
- International search engines

VI. Email

- Basic email analysis and specifics

VII. Data breaches

- Where to find data and how to use them in analysis
- Data leakage in financial world
- Compromised accounts – BEC (Business Email Compromise)

VIII. Investigating infrastructure

- Maltego

DAY 3

On day three, students will be introduced to the second big case study. Based on that case study, trainers will explain how to investigate documents by using online services, how can pictures and their geolocations be important in financial investigations, and finally, why are social networks and free information they provide, important and very useful in forensic analysis.

I. Case study – no 2

II. Documents

- Google searching
- Google docs
- Metadata viewers
- Pastebin

III. Pictures and geolocation in financial investigations

- How is that useful?
- Google images
- Reverse image search
- Exif data
- Geolocation
- Maps

IV. Social networks

- Linkedin
- Twitter
- Instagram
- Connecting dots on social networks

DAY 4

Day 4 is dedicated to websites in general, dark web and mobile money issues. Students learn how to find data on websites by using page crawlers and what information from metadata could be crucial for their investigation. The workshop continues with the dark web basics, TOR search engines analysis, blockchain, cryptocurrencies and wallets investigations. Day four ends with the mobile money issues, explanation how it works and frauds conducted through them.

I. Websites
- Crawlers
- Metadata

II. Dark Web
- General
- Tor search engines
  - ❖ Analyzing Tor nodes
- Blockchain
  - ❖ Connecting the world to crypto
  - ❖ Establishment of the company on Blockchain
- Cryptocurrencies and wallets
  - ❖ Crypto exchanges – friends of the investigators

III. Mobile money
- The idea behind it
- Trust issues
- Frauds

DAY 5

On the last day of the workshop, students learn how to create final report for the case, how to export data from OSINT tools and what are valuable information for the report. At the end, students are given the list of free tools sorted by categories which they can use in their investigations. The workshop ends with the final exam, survey and certification ceremony for the successful students.

I. Reports
- How to export from OSINT tools
- What is important for report

II. List of free tools by categories

III. Final exam

IV. Survey and certification ceremony