DARKWEB

Investigator Course and Workshop

25 - 29 July 2022 (5 Days)
10.00 A.M to **6.00 P.M**
Venue: **Main Conference Hall RBVRR**
Telangana State Police Academy (TSPA),
Himayath Sagar, Hyderabad - 500091, India.
Trainer: **Mr. Mark Bentley**
(Former UK Police Officer & Trainer at ISS World)

Contact Details
Mr. Paul Ravi Kumar (Director)
Contact No: **+91 94904 21292**
Email ID: **info@digipol.org**
URL: **www.digipol.org**

DIGIPOL HYDERABAD

DTRAKS EMPOWERING GLOBAL LEAS

Digipol, 607, Block B, Asian Sun City, Whitefields, Gachibowli
Hyderabad, India – 500032

The Course

A 5-day course centering on Darkweb interaction and monitoring, with associated OSINT tools to perform the operations efficiently.

Mission Statement

The 5 Day workshop and masterclass covers the very best and up to date methods and tradecraft. It will equip today cyber investigator with the latest cutting-edge tools and proactive investigation methodology. The content of this unique course is **not offered anywhere else**.

This is not a general lecture course and is for experienced investigators to learn advanced topics. The course material:

1) Supported by real world examples and incidents.
2) Provides the student with the understanding of how to apply effective OSINT investigative techniques to real world cases.
3) Demonstrates the threat the Darknet poses and the investigative techniques to expose criminals in this space.
4) Allow investigators increase their skills to meet the new challenges offered by Internet investigations the anonymity of the Darknet.
5) The instructional material and course exercises are presented from an investigators point of view.
6) Those attending with a limited technical background will benefit from the step-by-step material and guides used in the course.
7) This course contains new and innovative law enforcement specific methodologies and techniques.

Registration for the course is strictly reserved for Government and law enforcement only.

Course Structure

The course is designed to take the student through the full spectrum of topics necessary to be an effective Cyber/Internet investigator. Whether it's chasing cryptocurrencies through the blockchain, tracking pedophiles through keywords or images, or simply finding buried historical data on your target, on the Darknet or the open web, this is the course for you. From network exploration and how we all leave digital footprints, to device tracking and bitcoin address analysis, the course focuses on all online offenders and organized criminal gangs from financial criminal behavior to offenders against children.

The course covers in detail many investigative topics including:

1) Tracking and tracing images.
2) Understanding Exif and meta-data.
3) Live internet searches.
4) Monitoring and digital surveillance
5) The review of webpage source code (both Clearnet and Darknet websites).

6) Using the Darknet.
7) Everything an investigator needs to know about encrypted anonymous networks. The investigator will clearly understand their use.
8) How darknet targets can be found.
9) Tracing data on hidden networks.
10) Honeypot operations to catch users
11) Understanding the purpose and history of cryptocurrency.
12) How cryptocurrency facilitates modern crime on the Darknet.
13) Understanding the basics of how law enforcement can trace and analyze cryptocurrency transactions.
14) How OSINT supports the investigation of Darknet cases.
15) Building your own Darknet site.
16) Social Networks and their tie to Darknet investigations.
17) Legend Building
18) And much, much more…

Workshops

This masterclass is a full hands-on interactive course where the methodology and best practice is explained, and then the students practice the tradecraft live and online. Please be advised that this course is almost 50% practical workshops and exercises, so your own laptop is essential. The course will be a presentation and demonstration of the techniques. Students are encouraged to follow along during the course on the own laptop.

Cases and examples, both current and historic will be given throughout, to add depth and relevance to the methodology.

Students Will Receive

Students will each receive an electronic copy of the course material, Step-by-step instructions for all exercise, handouts and cheat-sheets for quick reference to detailed information sources and a course USB drive with associated software and resource material. Included on the USB drive are the software tools used during the course, tutorials and over 1000 OSINT tool links to ensure they continue to have the tools they need, post course.

Elements and Modules

The following course content is **not offered anywhere else**. The session descriptions below are specifically short so as not to specifically publish specific techniques and methods. This course will fully explore each area during the individual sessions. Use of any of these new and innovative methods and techniques explained during the sessions will be up to the individual and the agencies to implement based on their ability and any legal constraints applied by their jurisdiction.

The Darknet/Dark Web, what it is and what it is not

The technology behind the Darknet is not a single program or location. This session will explore what the Darknet is and how it differs from the Deepweb providing the investigator with the understanding of this new environment.

Tor and its use in an investigation

Attendees will set up and access The Onion Router (Tor). They will learn how the network hides its users and makes investigating users a challenge. This session will look at the Tor network works and methods for using it successfully during an investigation.

Cryptocurrency as misused by criminals

This session will provide investigators with the ability to understand and deal with cryptocurrencies during investigations. Attendees will have a clear understanding of how the use of Bitcoins are effecting investigations. They will learn to how to track the funds through various cryptocurrencies. Attendees will understand how wallets work, where evidence in the cryptocurrency system resides, how the blockchain works and investigators can track transactions through the system.

Going Undercover on the Darknet

Darknet investigations require the use of a persona like any other investigation. It also requires that you understand the equipment you are using and practice online officer safety techniques specialized for online/Darknet investigations. This session will look at the requirements and investigator has equipment and persona background specializing in Darknet investigations.

Technology and techniques to locate a suspect on the Darknet

Anonymous networks are intentionally designed to hide users. Are there legally available methods which we can implement to identify anonymous users on the Internet? The answer is definitely yes. The attendees will learn techniques to locate targets online using various code. The attendees will build tools to assist in an investigation. The potential legal issues when implementing these techniques will also be discussed.

Meta data use on the Internet in Images and documents

This block exposes the investigator to the use of Meta Data in files. How tracking duplicates, the sources uploading, revealing Exif data in images and other identifiers used to establish device location, source and tracking. How Hashing and searching can identify additional actionable intelligence or investigative leads.

Monitoring and webserver exploits (theory)

How to set up a darkweb server and monitoring station.

Tools

Provision and access to over 1200 OSINT tools on Bentac's dedicated investigator training site. This library of tools has been collected over the last 35 years in LEA. The investigative tools cover a wide spectrum of OSINT investigation and give the investigator access to Historic and specific searching tool and the latest available information on social media. Course attendees will be given access to the site forever. Plus 1000+ on the USB to every student.

Website analysis

Attendees will learn the "Deep" searching of links and connections into a website; common or accessed sites sharing the same server space. Identifying IP and owners of sites and upload location. Possible server vulnerabilities and exploits

Target Attribution

Our technology can often let us track a device to a physical location. However, placing a target actually behind the keyboard of a computer or cell device is a challenge for most prosecutors and investigators. This block will provide attendees with the investigative clues there may be to prove ownership and use of a computer or device.

Human anthropology Versus digital foot printing

How we live, move and react with the real world is reflected in the digit footprint we leave in the virtual world. This session will look at where to look for clues in the data and footprint, to profile and help identify the person leaving it

Social engineering tricks and exploits

This session gives the delegate an understanding of the origins, impact and harm that the modern criminal social engineer plays in crime and intelligence security in the modern day internet. It covers both attack and defence. Can we identify, exploit and copy their tactics?

Geo location

Tracking and identifying devices on the internet and their speed direction and use by the target. Includes vehicle telematics, association, speed, data sources and non visual surveillance. Identifying buildings/ locations (public and private) that the device uses and frequents.

Lifestyle analysis

Identifying targets by their device movement and location. Identifying public wifi spots used and interrogation.

Legislation

Covers all aspects of relevant legislation in respect of paint research - pitfalls and considerations regarding Intercept and AP. Also cover the transition to evidence from intel online, Business data without applying for it, and identifying company interests and ownership which were not available or known.

Social Networking

Identifying which sites are used by the target quickly, then interrogation of the sites by searching the data not by using the site. Links between targets on the same and different SN sites. Direct and historic chats between multiple profiles to prove association and analysis. Analysis online of a subjects location when uploading / tweeting/ blogging AND the identity and location of the people in their online group.

Tradecraft

Covert (non attrib) and non identifying search methods. Deep searching and analysis. Alternative tool and site searching. footprint reduction and incognito browsing. Non identifying profile creation using virtual mobiles and emails to allow registration.

OSINT legend building

Non attributable SN profile and legend building, tradecraft and good digital hygiene around this area.

Other identifiers of value

Mac IMSI and IMEI, SSID and BSSID identifiers that will be of significant value to the investigation. Their anomalies, values, and potential. Port scanning and network analysis