

OSINT

INVESTIGATOR COURSE AND WORKSHOP

18 - 22 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**

www.digipol.org



DIGIPOL
HYDERABAD



OSINT INVESTIGATOR COURSE AND WORKSHOP

THE COURSE

The course is intended for the internet cyber crime investigator and researcher, in order to take them from the basic researcher who understands the basics of internet investigation. To advanced open source researcher who understands the basics of internet investigation, to advanced open source researcher, able and proficient in providing high quality reports and evidence relating to online investigations and intelligence.

PRE-REQUISITES

1. Participant should have the ability to use search engines on a PC
2. Participant should carry Laptop and Internet Dongle

KEY ELEMENTS

1. An investigator with 40 years of experience talking and training investigators on their level.
2. Numerous practical's throughout to track suspects and build up analysis of digital footprint
3. Hands on live tracking and deep web searching
4. Best Professional practice the digital hygiene and evidence gathering
5. Online Legend and Personal building and use
6. FREE Exclusive access to online database of 200+ OSINT tools
7. FREE Exclusive access to online practical advice and tutorials
8. FREE included OSINT software for you to take away and keep
9. FREE USB with 1000+ OSINT tools links, glossaries and OSINT manuals
10. FREE Emails support and advice post course

SYLLABUS

THE DARKNET/DARK WEB, WHAT IT IS AND WHAT IT IS NOT

Understanding what the Darknet really it can be a challenge. The technology behind the Darknet is not a single program or location. This will explore what the Darknet is and how it differs from the Deepweb.

DARKWEB FAMILIARIZATION AND CONVERT MONITORING

Setting up and using Tor may in itself be easy, but finding what you want on the Tor network can be a challenge. This session will look at the Tor network how it works and methods for using it during an investigation.

CRYPTO CURRENCY AND ITS USE IN THE DARKNET

New to Investigations involving bitcoin? Need to understand how to track the funds through various crypto currencies? How do wallets work and is there any evidence I can use when I find one? This session will provide you with the ability to understand and deal with Bitcoin and other crypto currencies during your investigations.

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 personal background specializing in Darknet investigations.

USING WEB BUGS AND OTHER TECHNOLOGY TO LOCATE A SUSPECT

How can we locate targets online through the use of various code? How can it be done and what skills does the investigator need? What are the potential legal issues?

ADVANCED DARKNET/DARK WEB INVESTIGATIONS, IDENTIFYING THE ANONYMOUS USER

Are there legally available methods which we can implement to identify anonymous users on the Internet? The answer is definitely yes. This session will discuss the techniques available to the investigator to identify users of anonymization on the Internet.

OSINT INVESTIGATOR COURSE AND WORKSHOP

IMAGES, EXIF AND META TABS

Tracking duplicates, sources uploading, meta data and exif data interrogation and identifiers to establish device, location, source and tracking. Hashing and Searching for sharing and uploading significant images. Providing sufficient data and intel to support dissemination to active teams and support warrants and DSA.

TOOLS

Provision and access to over 1200 OSINT tools on my dedicated investigator training site which is a library of tools collected over the last 20 years in LEA. These cover everything. Delegates will be given access forever. Historic and specific searching.

WEBSITE ANALYSIS AND META DATA SCRAPPING

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.

ATTRIBUTION

A headache for most prosecutors and investigators. We can put a device at a location but how do we show who was there with the device. What other clues are there to prove ownership and use? Let us look at them all.

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 and 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? Can we use fake news as a weapon to combat crime?

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 building/locations (public and private) that the device uses and frequents.

LIFESTYLE ANALYSIS

Identifying targets by their device movement and location. Identifying public 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. Impact of GDPR and DPA.

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 identify and location of the people in their online group.

TRADECRAFT

Covert (non attribution) 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 passive SN profile and legend building, tradecraft and good digital hygiene around this area.

HUMAN TRAFFICKING AWARENESS, TRACKING AND OCG DISRUPTION

Trafficking awareness, chat rooms, organised criminal group identification and methodology

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.