DIGIPOL
HYDERABAD

DTRAKS
EMPOWERING GLOBAL LEAS

10th Jan to 14th Jan 2022 (5 Days)

10.00 A.M to 6.00 P.M

Venue: Hotel Green Park, Greenlands Hyderabad, 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

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

- An investigator with 40 Years of experience talking and training investigators on their level.
- Numerous practicals throughout to track suspects and build up analysis of digital footprint
- Hands on live tracking and deep web searching
- Best Professional practice the digital hygiene and evidence gathering
- Online Legend and Personal building and use
- FREE Exclusive access to online database of 200+ OSINT tools
- FREE Exclusive access to online practical advice and tutorials
- FREE included OSINT software for you to take away and keep
- FREE USB with 1000+ OSINT tools links, glossaries and OSINT manuals
- FREE Email support and advice post course

Syllabus

- **The Darknet/Dark Web, What it is and what it is not**
  Understanding what the Darknet really is can be a challenge. 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.
- **Darkweb familiarisation and covert monitoring**
  Setting uo 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 investigator
- **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.

- **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 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. 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.

Day wise Schedule

Day1	Day2	Day3	Day4	Day5
Introductions and Setup	Good Digital Hygiene – **DO IT RIGHT**	Search Techniques and approach – Boolean, Lateral Thinking	Geo Tools and Cell site tracking how deep into the digital family can we go?	Exercises – People Tracking
Tea Break				
How the internet works and where footprints are left	Legislation awareness – surveillance obfuscation **DO IT LEGALLY**	Open Source tools – where and how to look covertly – Terms of service loopholes	Tracking and Searching exercises – lets go hunting	Exercises – Research
Lunch Break				
Device Traces – What trace does our device leave	Legend building and hidden social network account setup **BE HIDDEN**	Target analysis, Alternative search term consideration	Exercise Continued	USB tools workshop
Tea Break				
Evidence Traces – How to create viable evidence	The art of effective open source – no virtual stone unturned. Identify the dark corners. **GET IT ALL**	Images, Exif and meta data, hash data, Location ID and target device ID, Source code tracing	Vehicle Telematics – the future of digital surveillance	Tools Practice
Tea Break				
IP and MAC – tracking and Identifying	What is OSINT? – Good tradecraft	Last session continued	Last Session Continued	Debrief and Close