Hill Bingham Ltd

Using Open Source for Financial Crime Intelligence

There's nothing that cannot be found through some search engine

or on the Internet somewhere…

(Eric Schmidt)

Many institutions have a regulatory requirement to complete due diligence on all their applicants and customers. The main source of publicly held data is on the internet and certain skills and techniques are required to investigate this effectively. With the increased focus on tax havens and other financial crimes from the media, regulator and law enforcement it is essential banks train their staff to be able to detect and investigate financial crime effectively.

It is fair to say that today there is a plethora of data floating in cyber space and to an online investigator the Internet has become a vital tool as web browsers, search engines, social media monitoring tools have all developed with far more capabilities to assist in the retrieval of information – **if you know where to look.**

Objectives of the training and measures of success:

This course will upskill your staff who deal daily with financial crime related matters or suspicious activity to prevent:

- Fraud
- Money Laundering
- Terrorism
- Bribery and Corruption
- Regulatory Breaches
- Sanctions Breaches

Today financial institutions are reliant on their staff detecting suspicious activity, so it is essential that every financial organisation develops and improves training and awareness of their staff in key positions.

This training course will give delegates an insight into:

- Understanding the Internet and associated technology

- Effective use of the Internet as an investigative tool

- Search engines, meta browsers, deep web & people search techniques

- Due diligence tools including media checks

- Tracing domain name owners, origin of an email and black list checks

- Due diligence checks on companies & directors

- Investigating Web 2.0 - social networking, photo's & geolocation

- Protecting your privacy when investigating online

- Setting up an investigation toolkit and capturing data…

Course Outline (one or two day options available)

This course aims to introduce investigators to the concepts and the world around the Internet and its supporting tools for investigation/research. The following modules will unravel Internet search engine jargon and make investigators/intelligence analysts aware of the sources of evidence available to them in online investigations. The course will improve their ability to work with the current Internet technologies and to understand the control and investigative systems presented to them and to be able to prepare for the future.

Module One

Introduction to the Internet & WWW

- World Wide Web (WWW) vs. the Internet
- IP, DNS
- Understanding Internet protocols (http, https, ftp)
- What is a URL (Uniform Resource Locator)
- Effective use of a web browser
- Internet cache – retrieving
- The Dark Net

Module Two

Search Engines for Smarter Searching

- Surface search vs deep web search
- Google under the spot light
- Meta search engines
- Automated search techniques
- Semantic and cluster search engines
- Wild card searching & advanced operators
- Searching outside the UK – using international search engines

Module Three

Social Media Investigations

- Finding someone on social media
- People search sites
- Geo-location search
- Social network intelligence and monitoring tools
- Reverse image search & EXIF extraction
- Media searching – newspaper and regional news search

Module Four

Investigating Online – gaining background intelligence

- Company & director searching
- Determining the owner of a website
- PEP's , sanctions check tools
- Due diligence sites
- Global index of public registries
- Shipping and flight trackers
- Panama and paradise paper checks
- Darknet exploration

Module Five

Protecting your ID when Online

- How transparent are you?
- Disguising your ID
- Internet proxy servers & VPN's
- Protecting your browser
- Security issues going forward

Target Audience

This course is a must for anyone who needs to be able to find, manage and use financial crime intelligence including banks, investment management firms, law enforcement, internal audit, fraud & financial crime departments, investigators in the public & private sector including finance, retail, government, legal and the insolvency sector.

Each course can be customised and run over one or two days.

Our training is delivered by Dr Stephen Hill, a renowned specialist in this field with over 20 years' experience training organisations all over the world and advising high profile clients running internet-based investigations.

For further details please contact Dr Stephen Hill **- drshill@gmx.co.uk**

Why choose us? ... Feedback from our clients

I thought I had a sound grounding in internet intelligence but was proved wrong…an outstanding course

Deloitte

The best open source course I have attended with so much up to date intelligence

National Crime Agency

It was like a tsunami of information coming at me…it's a fantastic course

British Airways

Having attended many OSINT courses this was a real eye opener and by far the best – an excellent presenter with a wealth of knowledge

HSBC

This course was simply excellent and a real eye opener on how much intelligence is out there if you know which tools to use

Mischon de Reya

Other clients include: