Online Operations Limited

Open Source Investigation Module

Module Summary

This is a hands on, practical and immersive module suitable for those **who use the internet to conduct open source investigations or intelligence research**. Delegates will undertake a number of online exercises throughout the module with a final exercise using the skills developed throughout the module.

This module is designed to be delivered over **4 days**.

Module Learning Outcomes

At the conclusion of this module, delegates will be able to:

Apply basic and advanced internet search techniques

Discuss the structure of the internet

Apply appropriate evidence capture methodologies in internet investigations

Identify evidential and intelligence opportunities to develop internet investigations

Apply appropriate safeguards when operating online to protect tactics including anonymisation

Demonstrate the investigative value of digital images and websites

State legislation and procedural practices which may influence internet investigations

Demonstrate the techniques for investigating the deep / dark web and associated networks effectively

Demonstrate the creation and maintenance and effective deployment of an Online False Persona

Demonstrate the tracing of subjects and commodities through current and historic websites, IP and email traces using specialist network investigation techniques

Discuss the process preparing internet material for court or tribunal presentation

Discuss currently emerging technologies and subsequent impact on investigations.

Session 1	**Session 2**	**Session 3**		**Session 4**	**Session 5**	
Introductions and Course Outline	Communication Profiles	Investigation Styles & Planning an Online Operation		Open Source Resources	Internet Architecture	
Anonymisation	Evidence Capture	Evidence Handling		Basic and Advanced Searching	Investigating Digital Images	
Investigating Websites and Traces	Investigating Email and Traces	Legislation, Procedures and Risk Management		Investigating the Dark Web, TOR. Internet Relay Chat, Newsgroups and Forums	Online Market Places	Investigating Social Media
Investigating Social Media (continued)		Exercise		Exercise Debrief	**Emerging Technologies, Course Closure and Review**	

Module Delivery Sessions

Module Opening

1.0.1 Health and Safety
1.0.2 Module Outline
1.0.3 Learning Outcomes and Timetable
1.0.4 Introductions

Communication Profiles

1.1.1 What is a communication Profile?
1.1.2 Why do we need Communication Profiles?
1.1.3 What should be included in a Communication Profile
1.1.4 Keeping a Communications Profile current
1.1.5 Source of Information for a Communications Profile

Investigation Styles and Planning an Online Investigation

1.2.1 Covert and Overt investigations
1.2.2 Proactive and Reactive investigations
1.2.3 The briefing process, investigation parameters and expectations
1.2.4 Authorisations, policies and procedures
1.2.5 Equipment considerations

Open Source Resources

1.3.1 What is Open Source material?
1.3.2 Databases
1.3.3 Accuracy of information

Internet Architecture

1.4.1 What is a network?
1.4.2 What is the Internet?
1.4.3 Internet Protocols
1.4.4 Routers and Switches
1.4.5 Domain Name Service
1.4.6 Unique Resource Locators (URL)
1.4.7 Shortened and Obscuficated URL's
1.4.8 Using the command line

Anonymisation

2.1.1 Why anonymise?
2.1.2 Virtual Private Networks
2.1.3 Browser based tools
2.1.4 Other anonymisation techniques

Evidence Capture

2.2.1 Why capture?
2.2.2 What should we capture?
2.2.3 Capture tools and software?
2.2.4 Dealing with captured material

Evidence Handling

2.3.1 Identification of exhibits
2.3.2 Continuity and chain of custody
2.3.3 Adding integrity to material – the hashing process

Basic & Advanced Searching Techniques

2.4.1 Google and other major search engines
2.4.2 Search tools and specialist search engines
2.4.3 Filters and managing search results

Investigating Digital Images

2.5.1 What is Meta and EXIF data?
2.5.2 Examination tools and techniques
2.5.3 Extraction websites
2.5.4 Removing Meta and EXIF data
2.5.5 Introduction to Geolocation

Investigating Websites and Internet Traces

3.1.1 Resolving domain names
3.1.2 Regional Internet Registries
3.1.3 Historic and cached websites
3.1.4 Hidden links
3.1.5 Offline viewing tools
3.1.6 HTML and other source code
3.1.7 Website update alerts

Investigating Email and Email Traces

3.2.1 Capturing email headers
3.2.2 Manual examination of email headers
3.2.3 Automated examination of email headers
3.2.4 Information contained in email headers

Legislation and Procedures

3.3.1 Legislation effecting internet investigation
3.3.2 Stated cases influencing online investigative tactics
3.3.3 Directed surveillance online
3.3.4 National law enforcement guidance
3.3.5 Local procedure and policy

Investigating the Deep Web and TOR

3.4.1 What is the Deep Web?
3.4.2 What is TOR?
3.4.3 How does TOR work?
3.4.4 Installing TOR
3.4.5 Risks of using the deep web in investigations
3.4.6 TOR Search tools and techniques

3.4.7 What is Internet Relay Chat (IRC)?
3.4.8 Configuring the IRC client
3.4.9 Evidence gathering on IRC
3.4.10 Gathering evidence from newsgroups
3.4.11 Interrogating internet forums

Online Marketplaces

3.5.1 Types of Online Marketplaces
3.5.2 Searching techniques applicable to online marketplaces
3.5.3 Evidential opportunities presented by online market places
3.5.4 Payment methods and techniques, including BitCoin.

Social Networks and Online False Personas

3.6.1 What is a Social Network?
3.6.2 Usernames, associations and other traces
3.6.3 Social network advanced search tools and services
3.6.4 Exploiting geo-located social network posts
3.6.5 Planning an Online False Persona
3.6.6 Deploying an Online False Persona
3.6.7 Risks associated with social networks

Final Exercise

4.1.1 Exercise briefing
4.1.2 Exercise supported by trainers

Final Exercise Debrief

4.2.1 Exercise Debrief
4.2.2 Review of learning points from exercise

Emerging Technologies

4.3.1 Internet of things
4.3.2 Mobile devices and internet access
4.3.3 BLE beacons
4.3.4 Cyber enabled and cyber dependant crimes

Module Closure

4.4.1 Review of learning outcomes
4.4.2 Feedback from delegates
4.4.3 Presentation of course material media
4.4.4 Presentation of certificates of attendance