Online Operations Limited

Open Source Investigation - Foundation - 2 days

Module Summary

This is a hands on, practical and immersive **foundation** module suitable for those **who use the Internet to conduct open source investigations or intelligence research**. Delegates will undertake several interactive exercises throughout the module.

This module is designed to be delivered over **2 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 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

9-10	10-11	11-1230			1330-1500	1515-1630	
Introductions and Course Outline 1.0	Communication Profiles 1.1	Planning an Online Investigation 1.2	Internet Architecture 1.3		Browser Based Tools 1.4	Basic and Advanced Searching Techniques 1.5	Evidence Capture Tools 1.6
Investigating Emails and Email Traces 2.1	Investigating Digital Images 2.2	Investigating Websites 2.3	Legislation and Procedures 2.4		Social Networks and Online False Personas 2.5	Handling Internet Evidence and Intelligence 2.6	**Course Closure and Review of Learning 2.7**

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

Internet Architecture

1.3.1 What is a network?
1.3.2 What is the Internet?
1.3.3 Internet Protocols
1.3.4 Domain Name Service
1.3.5 Uniform Resource Locators (URL)

Browser Based Tools and Customisation

1.4.1 Selecting the correct browser
1.4.2 Customising your browser
1.4.3 Browser based tools and add-ons

Basic and Advanced Search Techniques

1.5.1 Google and other major search engines basic search
1.5.2 Interpreting search results
1.5.3 Cached results
1.5.4 Meta search tools
1.5.5 Google and other major search engine advanced tools
1.5.6 Search tools and specialist search engines
1.5.7 Managing search results

Evidence Capture Tools

1.6.1 Why capture?
1.6.2 What should we capture?
1.6.3 Capture tools and software
1.6.4 Dealing with captured material

Investigating Email and Email Traces

2.1.1 Capturing email headers
2.1.2 Manual examination of email headers
2.1.3 Automated examination of email headers
2.1.4 Information contained in email headers

Investigating Digital Images

2.2.1 What is Meta and EXIF data?
2.2.2 Examination tools and techniques
2.2.3 Extraction websites
2.2.4 Removing Meta and EXIF data
2.2.5 Introduction to Geolocation

Investigating Websites and Website Traces

2.3.1 Resolving domain names
2.3.2 Regional Internet Registries
2.3.3 Historic and cached websites
2.3.4 Hidden links
2.3.5 Offline viewing tools
2.3.6 HTML and other source code
2.3.7 Website update alerts

Legislation and Procedures

2.4.1 Legislation effecting internet investigation
2.4.2 Online Surveillance
2.4.3 National law enforcement guidance
2.4.4 Local procedure and policy

Social Networks and Online False Personas

2.5.1 What is a Social Network?
2.5.2 Usernames, associations and other traces
2.5.3 Social network search tools and services
2.5.4 Exploiting geo-located social network posts
2.5.5 Planning an Online False Persona

Handling Internet Evidence and Intelligence

2.6.1 Evaluating internet material (2015 procedures)
2.6.2 Giving integrity to digital material
2.6.3 Revelation and disclosure issues

Module Closure

2.7.1 Review of learning outcomes and plenary session
2.7.2 Feedback from delegates