Online Operations Limited

Cybercrime Investigator - Foundation

Module Summary

This is a hands on, practical and immersive module suitable for those **who investigate Cyber Enabled and Cyber Dependent Crime.** 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:

Identify cyber dependent and cyber enabled crime.

Describe the types and functions of malware

Describe the role of the cybercrime first responder.

Prepare a cybercrime investigative strategy or plan.

Understand the concepts of computer networks and how they relate to a cybercrime investigation.

Understand the concepts of digital forensics in a cybercrime investigation

Identify, secure and preserve digital evidence.

Demonstrate the value and use of open source information in a cybercrime investigation.

Describe the role of authorisations, procedures and policies in a cybercrime investigation.

Prepare a risk management plan in relation to a cybercrime investigation.

Deal with victims, witnesses and suspects as they relate to a cybercrime investigation.

Prepare and present cybercrime material to a prosecutor.

Session 1	Session 2	Session 3		Session 4	Session 5	
Introductions and Course Outline	What is cybercrime? 1.1	Planning a Cybercrime Investigation. Role of the First responder 1.2		Computer Network Architecture 1.3	Internet Architecture 1.4	
Introduction to Digital Forensics 2.1				Identifying, Securing and Preserving Digital Evidence 2.2		
Open Source Investigation 3.1		Legislation, Procedures and Risk Management 3.2		Dealing with suspects, victims and witnesses 3.3	Preparation and presentation of digital evidence in a cybercrime investigation 3.4	
Exercise 4.1				Exercise Debrief 4.2	Review of learning 4.3	**Course Closure**

All courses are fully customisable to clients bespoke requirements

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

What is Cybercrime

1.1.1 What is Cyber enabled crime?
1.1.2 What is Cyber Dependent crime?
1.1.3 Examples of Cybercrime
1.1.4 Malware and Cyber security
1.1.5 Cybercrime investigation case study

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
1.2.6 The role and challenges of the cybercrime first responder

Computer Network Architecture

1.3.1 What is a computer network?
1.3.2 Network devices
1.3.3 Network protocols
1.3.4 Logs and traces
1.3.5 Routers and Switches
1.3.6 Router examination and preservation
1.3.7 Using the command line

Internet Architecture

1.4.1 What is the Internet?
1.4.2 Internet Protocols
1.4.3 Domain Name Service (DNS)
1.4.4 Unique Resource Locators (URL)
1.4.5 Shortened and Obscuficated URL's
1.4.6 Virtual Private Networks
1.4.7 Anonymisation techniques

Introduction to Digital Forensics

2.1.1 What is forensics?
2.1.2 Investigation principles
2.1.3 Triage
2.1.4 Types of digital data and data integrity
2.1.5 Devices and convergence
2.1.6 File systems
2.1.7 Drives, storage and partitions

Identifying, Securing and Preserving Digital Evidence

2.2.1 Free and commercial forensic tools
2.2.2 Imaging of drives and data acquisition techniques
2.2.3 Examination of acquired data and interpretation of results
2.2.4 Evidence integrity and the chain of custody
2.2.5 Evidence security and storage
2.2.6 Meta data

Open Source Investigation

3.1.1 What is open source material?
3.1.2 Online resources, databases and tools
3.1.3 Social media investigation
3.1.4 Evidence capture tools and techniques
3.1.5 Introduction to Geolocation

Legislation and Procedures

3.2.1 Legislation effecting Internet investigation
3.2.2 Stated cases influencing online investigative tactics
3.2.3 Online Surveillance
3.2.4 National law enforcement guidance (country specific)
3.2.5 Local procedure and policy

Dealing with Suspects, Victims and Witnesses

3.3.1 Identifying witnesses and achieving compliance
3.3.2 Dealing with victim's and their devices and data
3.3.3 Preparing digital material for interview of suspects

Preparation and presentation of digital evidence in a cybercrime investigation

3.4.1 Sanitisation and redaction of digital material
3.4.2 Providing material to defence advocates
3.4.3 Challenges in dealing with prosecutors and judiciary
3.4.4 Proving integrity and chain of custody

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

Review of Learning

4.3.1 Review of course learning outcomes
4.3.2 Summary of principles discussed
4.3.3 Distribution of course USB thumb drive
4.3.4 Question and Answer session

Module Closure

4.4.1 Review of learning outcomes
4.4.2 Feedback from delegates
4.4.3 Presentation of certificates of attendance