Online Operations Limited

Cybercrime Investigator - Advanced

Module Summary

This is a hands on, practical and immersive module suitable for those **who investigate serious and complex 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**. Delegates should have attended the First Response Cybercrime Investigator (Foundation Module) or similar.

Module Learning Outcomes

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

Describe methods used by Hackers and Hacktivists and how to conduct investigations against them.

Describe and identify technical tools used in the commission of cybercrime.

Demonstrate the use of Wi-Fi in cybercrime investigations.

Conduct enhanced Internet investigations using Open Source Intelligence.

Discuss the role of the Deep and dark Web in cybercrime.

Demonstrate the handling and investigation of Unix based systems

Describe the International organisations and partners that can support a complex cybercrime investigation.

Prepare and present case papers to a prosecutor as they relate to a complex cybercrime investigation.

Session 1	Session 2	Session 3		Session 4	Session 5	
Introductions and Course Outline	Review of Foundation Course Learning 1.1	Investigation of Hacking and Denial of Service crimes 1.2		Technical Tools and Techniques Employed by Cyber Criminals 1.3		
Introduction to Wi-Fi and Wi-Fi Surveys 2.1				Enhanced Open Source Tools and Techniques 2.2		
The Deep and Dark Web 3.1		Dealing with Apple and Unix Based Systems 3.2		International Partners and Law Enforcement Procedures 3.3	Preparation and presentation of digital evidence in a complex 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

Review of Foundation Course Learning

1.1.1 What is cybercrime?
1.1.2 Computer networks and the Internet
1.1.3 Digital forensic principles
1.1.4 Identification, securing and presenting digital evidence

Investigation of Hacking and Denial of Service (DOS, DDOS) crimes

1.2.1 The hacking cycle
1.2.2 Who are the hackers?
1.2.3 Types of hacking attack
1.2.4 Preventing and identifying hacking attacks
1.2.5 Investigative techniques in hacking crimes
1.2.6 Investigative techniques in denial of service crimes

Technical Tools and Techniques Employed by Cyber Criminals

1.3.1 Online hacking tools
1.3.2 Installable hacking tools
1.3.3 Social engineering techniques
1.3.4 Hacker forums and channels (clear and dark web)
1.3.5 Data leaks and distribution of data
1.3.6 Penetration testing
1.3.7 Virtualisation

Introduction to Wi-Fi and Passive Wi-Fi Surveys

2.1.1 Description of Wi-Fi
2.1.2 Optimising Wi-Fi signal and reception
2.1.3 Wi-Fi signatures and probes
2.1.4 Wi-Fi passive survey tools
2.1.5 Wi-Fi capture tools
2.1.6 Wireshark and capture analysis

Enhanced Open Source Tools and Techniques

2.2.1 Commercial open source tools
2.2.2 Enhanced free open source tools
2.2.3 Social media exploitation
2.2.4 Geolocation tools and services
2.2.5 Data mapping and analysis
2.2.6 Digital image analysis
2.2.7 Email analysis

Investigating the Deep Web and TOR

3.1.1 What is the Deep Web?
3.1.2 What is the Dark Web?
3.1.3 Hidden tools and services
3.1.4 Internet relay chat (IRC)
3.1.5 Alternative dark web networks

Dealing with Apple and Unix Based Systems

3.2.1 Introduction to Unix and Linux systems
3.2.2 Introduction to Mac OS
3.2.3 Capturing evidence from Unix, Linux and Mac OS
3.2.4 Unix based forensic tools

International Partners and Law Enforcement Procedures

3.3.1 European partnerships
3.3.2 International partnerships
3.3.3 MLAT and other treaties
3.3.4 Computer Emergency Response Team (CERT)

Preparation and presentation of digital evidence in a complex cybercrime investigation

3.4.1 Sanitisation and redaction of complex 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