Online Operations Limited

Introduction to Digital Material & Evidence for Prosecutors and Judiciary Members

Module Summary

This is a practical and immersive module suitable for those **who prosecute or hear criminal or civil trials where Digital Material is presented.**

Day 2 of this module includes an immersive group based case study, exercise and debrief.

This module is designed to be delivered over **2 days**.

Module Learning Outcomes

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

Describe digital material and its components

Describe open source material and its components

Discuss the Collection, Acquisition, Examination, Analysis and Reporting of digital material.

Describe the 4 principles of digital evidence – best practice

Describe the 5 elements of the Budapest Convention on Cybercrime

Recognise methods used to add integrity to digital material

Discuss the benefits of Authorisations, Policies and Procedures

Demonstrate the review processes of digital evidence

Describes risks of using digital material in judicial proceedings

Discuss the application of the Computer Misuse Act 1990

Discuss the application of the serious Crime Act 2015

0900-1000	1000-1100	1130-1230	1330-1500	1530-1630
Welcome and Introductions 1.0	What is Digital Material? 1.1	What is Open Source Material? 1.2	How Digital Material is obtained? 1.3	Digital Evidence Best Practice 1.4
Providing Integrity to Digital Evidence 2.1	Risks surrounding Digital Material 2.2	Interactive Case Study 2.3	Interactive Case Study continued and full Debrief 2.4	Plenary Session, Module Review and Closure 2.5

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 Digital Material?

1.1.1 How does Digital Material present itself?
1.1.2 Sources of Digital Material
1.1.3 Why is Digital Material important in investigations?
1.1.4 Challenges of Digital Material
1.1.5 Evidence v Intelligence
1.1.6 What are investigators taught?

What is Open Source Material?

1.2.1 What does Open Source mean?
1.2.2 Where can Open Source material be found?
1.2.3 Challenges of Open Source Material
1.2.4 What are investigators taught?
1.2.5 Equipment considerations

How is Digital Material Obtained?

1.3.1 On scene collection and acquisition
1.3.2 Remote collection and acquisition
1.3.3 Third party productions
1.3.4 What is a forensic image?
1.3.5 The ‘ First responder’
1.3.6 Tools and Techniques
1.3.7 What are investigators taught?

Digital Evidence – Best Practice

1.4.1 The 4 Principles of Digital Evidence
1.4.2 The 5 Principles of the Budapest Convention on Cybercrime
1.4.3 Handling of Digital Material – the chain of custody
1.4.4 The Triage Trap
1.4.5 Qualifications, accreditations and experience – the balance
1.4.6 Revelation and Disclosure issues

Providing Integrity to Digital Evidence

2.1.1 The forensic hashing process
2.1.2 Meta data and what it tells us
2.1.3 Examination, Analysis and Reporting
2.1.4 The chain of custody revisited
2.1.5 What are investigators taught?

Risks Surrounding Digital Evidence

2.2.1 Data contamination and damage
2.2.2 Malicious manipulation of data
2.2.3 Poor records and chain of custody
2.2.4 ‘Knowledge Drift’
2.2.5 Communication of technical information

Interactive Case Study

2.3.1 Digital feed to facilitate immersive group discussion and debate.
2.3.2 Trainer support throughout

Legislation and Procedures

2.4.1 Full trainer led debrief of case study
2.4.2 What are the challenges?
2.4.3 What are the positives?
2.4.4 How would this work in practice?

Plenary Session, Module Review and Closure

2.5.1 Question and Answer session with trainer and facilitators
2.5.2 Review of module learning outcomes
2.5.3 Course Closure