WM188-15 Digital Forensics Fundamentals

25/26

Department
WMG
Level
Undergraduate Level 1
Module leader
Harjinder Lallie
Credit value
15
Module duration
30 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

At its core this module is concerned with doing science well. It is about drawing the correct inference from the digital data which pervades modern society. There are a number of challenges with drawing inference from modern digital data: it is fragile, its quantity may be overwhelming, it may be transient or volatile, it may not be legally accessible, it may not be technically accessible, its structure may be unclear. And it is not merely that drawing inference from the data is complicated; attributing inference back to an individual or organisation is especially vexed.

Set against these significant challenges is the reality that the digital footprint left by a member of modern society may have been left as a consequence of some wrongdoing. Digital forensics seeks to overcome the substantial challenges of drawing correct inference from digital data, so that decisions about the identity of the wrongdoer, and the sanctions that follow, may be made with greater confidence from a better informed perspective.

There are a number of principles that have been established by the digital forensics community. From these a range of tools and techniques have been developed for doing standard things in typical circumstances. Analysing the capabilities and limitations of these tools and techniques is an important part of the module. Representing what has been inferred to a non-specialist audience is also a critical part of any investigation and is practised in the module. Ultimately, this module

exposes the student to the entire investigative lifecycle of a case.

Module aims

Develop a critical understanding of the process of digital investigation both from a criminal and corporate perspective.
Develop an applied understanding of how to perform a digital investigation both from a criminal and corporate viewpoint.
Expose students to a cutting edge digital investigation scenario and equip students with the tools and knowledge required to complete the investigation.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Digital Evidence

- Understanding evidence
- Features of digital evidence, fragility and integrity,

Investigation:

- briefing document,
- record keeping, contemporaneous notes, negatives and positives,
- valid inferences, testing of non-standard techniques in novel situations,

Judicial systems:

- the scope of criminal, civil and enterprise investigations,
- ACPO guidelines.

Digital investigation lifecycle
- Crime scene Management, first response, seizure, chain of custody, contamination
- Acquisition, hashing
- Examination and Analysis, investigative modus operandi, bookmarking, intepreting data/evidence, basic file systems (volumes, partitions, deleted material, persistence of earlier material)
- Reporting and presentation. Producing an investigation report, Expert witness testimony.

Learning outcomes

By the end of the module, students should be able to:

- Understand the principles of digital forensics
- Demonstrate the ability to conduct a digital forensic examination of a given digital forensic image against a given investigation brief
- Demonstrate the ability to apply appropriate forensic tools to investigate a given problem

- Present the outcome of an investigation as a report aimed at a given target such as a court of law

Indicative reading list

Holt, T.J., Bossler, A.M. and Seigfried-Spellar, K.C., 2022. Cybercrime and digital forensics: An introduction. Routledge.
Hayes, 2020, Paractical guide to digital forensics investigations, 2nd ed, Pearson

The books below are fundamental books which must be included in the reading list.
E. Casey, Digital evidence and computer crime: forensic science, computers, and the Internet: Academic Press, 2011.
Carrier, B., File System Forensic Analysis. 2005, Addison Wesley

Interdisciplinary

Includes elements of Law and criminology

Subject specific skills

Subject specific skills
Knowledge of types of evidence, sources of evidence, methods of extracting the evidence
State-of-the-art forensics methods
Forensics practices.

Transferable skills

Jurisdiction and law
Report writing
Analytical thinking.

Study

Study time

Type	Required
Lectures	18 sessions of 1 hour (12%)
Supervised practical classes	18 sessions of 1 hour (12%)
Online learning (independent)	18 sessions of 1 hour (12%)
Private study	36 hours (24%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Mixture of lab exercise repeats plus further reading

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time	Eligible for self-certification
Digital investigation	40%	25 hours	Yes (extension)
Perform a digital investigation of a given artefact against a brief.			
Digital investigation	60%	35 hours	Yes (extension)
Perform a digital investigation of a given artefact against a brief. The investigation will involve a more complex investigation than the first report, and may involve the investigation of disparate items of evidence such as dashcams, mobile phones, or other devices.			

Feedback on assessment

Written feedback provided with the mark via tabula.

Availability

There is currently no information about the courses for which this module is core or optional.