WM046-15 Digital Forensics

23/24

Department
WMG
Level
Taught Postgraduate Level
Module leader
Harjinder Lallie
Credit value
15
Module duration
1 week
Assessment
Multiple
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

For students to grasp the relationship between artefact, actor, event, attribution, interpretation and confidence in the realm of digital forensics..

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:

- the nature of evidence, chain of custody, contamination,
- specific features of digital evidence, fragility and integrity, hashing,
- capturing, preserving, replicating,

Interpreting:

- structure of digital material in a variety of forms,
- structure of stored material, volumes, partitions, filesystems, deleted material, persistence of earlier material,
- other sources of stored digital material (phones, cameras etc)

Tools and techniques:

- validation and verification, scientific process,
- selected standard tools (imaging, carving, triage), capabilities and limitations,
- open source, commercial.

Investigation:

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

Presentation:

- eye-witness, expert witness testimony, responsibility,

Incident response:

- preparation, trusted toolset,
- issues, maintaining power vs cutting power, transmitting devices, live systems, encrypted storage.

Judicial systems:

- jurisdiction (national vs international context), agencies,.
- cyber -specific issues, geo-locale of actor, agent, data, communications, agency cooperation,
- the scope of criminal, civil and enterprise investigations,
- ACPO guidelines.

Learning outcomes

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

- Critically evaluate the relevant digital forensic characteristics of selected digital electronic devices
- Investigate digital artefacts against a realistic brief, preserving, analysing, and interpreting the evidence
- Apply scientific techniques appropriately in the context of digital forensic analysis
- Present digital forensic evidence against a given legal context

Indicative reading list

Journals:
Digital Investigation: The International Journal of Digital Forensics & Incident Response (http://www.elsevier.com/wps/find/journaldescription.cws_home/702130/description#description)
Journal of Digital Forensics, Security and Law (http://www.jdfsl.org/)
International Journal of Forensic Computer Science (http://www.ijofcs.org/webjournal/index.php/ijofcs)
Advances in Digital Forensics (http://www.springer.com/computer/book/978-0-387-30012-2)

Books:
B. Nelson, A. Phillips, and C. Steuart, Guide to Computer Forensics and Investigations, 4th ed. Boston, USA: Cengage Technology, 2010.
C. R. Brown, Computer Evidence Collection And Preservation, 2nd ed. Canada: Course Technology PTR, 2010.
E. Casey, Digital evidence and computer crime: forensic science, computers, and the Internet: Academic Press, 2011.
Volonino, L., et al., Computer Forensics Principles and Practice, 2007, Pearson
Marshall A., Digital Forensics - Digital Evidence in Criminal Investigation, 2008, John Wiley and Sons
Jones K,J., Bejtlich R., Rose C.W., Real Digital Forensics, 2006, Addison Wesley.
Carrier, B., File System Forensic Analysis. 2005, Addison Wesley

View reading list on Talis Aspire

Research element

There is a strong emphasis on the development, growth and enhancement of individual research skills so as to provide participants with the high level research knowledge, skills and competencies needed to undertake an independent, original piece of research. The module content draws upon

and highlights research within the domain and the module assessment requires participants to perform further research before preparing a response to the assessment task.

Interdisciplinary

Although the module is largely dedicated towards the development of discipline-specific technical, professional and analytical skills, there is a small emphasis on the interdisciplinary nature of the subject. An incident investigation can be requested in any domain and this module highlights and demonstrates this by drawing on investigations within accounting firms, high-tech industries and public bodies.

International

The module is designed for an international cohort and may be taught anywhere in the world. Learning materials and examples will be drawn from a range of disciplines, cultures and countries covering the whole range of subjects and disciplines taught in WMG. Judicial process varies between countries and this module emphasises this throughout by drawing on examples of how the legal process applies in different countries as well as examples of investigations that involve multiple judiciaries.

Subject specific skills

Investigate digital artefacts against a realistic brief, preserving, analysing and interpreting the evidence

Apply scientific techniques and use scientific terminology appropriately in the context of digital forensic analysis.

Transferable skills

Critical thinking, ethical values, professionalism

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Tutorials	20 sessions of 1 hour (13%)
Online learning (independent)	50 sessions of 1 hour (33%)
Assessment	70 hours (47%)
Total	150 hours

Private study description

No private study requirements defined for this module.

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time
Coursework	80%	60 hours
Typically, a digital investigation of an incident resulting in a 'court style' report.		
In class test	20%	10 hours
An end of module in class test which tests key concepts relating to either the theoretical content, the practical content, or both		

Assessment group R

	Weighting	Study time
Assessed work as specified by department	100%	
100% Assignment		

Feedback on assessment

Written feedback provided with the mark via tabula.

Availability

Anti-requisite modules

If you take this module, you cannot also take:

- WM046-10 Digital Forensics

Courses

This module is Core optional for:

- Year 1 of TWMA-H6C7 Postgraduate Taught Cyber Security Engineering