WM3E5-15 Cyber Forensics

20/21

Department
WMG
Level
Undergraduate Level 3
Module leader
Harjinder Lallie
Credit value
15
Module duration
11 weeks
Assessment
100% coursework
Study locations
University of Warwick main campus, Coventry Primary
Distance or Online Delivery

Description

Introductory description

Cyber security teams are routinely called on to investigate incidents ranging from the downtime of critical resources such as servers and networks, to complex cyber-attacks which lead to loss of resource, reputational damage and potential fines. Digital investigation is the process of identifying and analysing the causes of incidents and providing a robust and comprehensive response and explanation to stakeholders on the cause of an incident and the steps that can be taken to mitigate against it occurring again in the future.
The endpoint of a digital investigation is often a report which must clearly, cogently and convincingly attribute the root cause of the incident, whilst at the same time be easily understood by lay audiences which range from members of a court to chief executives in an organisation. This ability to organise important information and present it professionally and clearly is a key skill within the cyber security domain.

Module aims

This module outlines the steps that an investigator must follow in a wide range of incidents and equips participants with the skills required to apply scientific techniques and industry standard tools to a digital investigation and present convincing results.
The module draws on case studies of example incidents which require investigation. Participants

perform an investigation through the stages of evidence analysis and report writing. Throughout this process, participants are introduced to the range of tools available during an investigation and issues relating to the admissibility of evidence produced by these tools. Participants gain a thorough understanding of how the mode of investigation differs between different types of investigation, for instance corporate and criminal investigations.
Participants are made acutely aware of the importance of drawing the correct inference from digital evidence and the significant challenges faced by investigators, namely that digital data 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 and its structure may be unclear.

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, negative / absence and positive / presence findings. Valid inferences, testing of nonstandard techniques in novel situations. Analysing memory forensics, analysing network forensics. Anti-forensics.
- Presentation. Eyewitness, expert witness testimony, responsibility.
- Incident response and management. Preparation, trusted toolset; issues, maintaining power vs cutting power, transmitting devices, live systems, encrypted storage.
- Intrusion detection methods. intrusion response, management and handling; intrusion analysis, monitoring and logging.
- Judicial systems. Jurisdiction (national vs international context), agencies; cyberspecific issues, geolocale 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:

- Demonstrate the ability to apply digital forensic tools and techniques to solve given problems.
- Investigate digital artefacts against a realistic brief, preserving, analysing and interpreting the evidence.
- Evaluate, the capability to perform incident management and incident response.
- Understand the complexities of jurisdiction in the cyber domain.

Indicative reading list

Carvey, H. A. (2007) Windows forensic analysis: DVD toolkit. Burlington, MA: Syngress Pub. Available at: https://ebookcentral.proquest.com/lib/warw/detail.action?docID=328624.
Casey, E. (2010) Handbook of digital forensics and investigation. Amsterdam: Academic. Available at: http://encore.lib.warwick.ac.uk/iii/encore/record/C__Rb3102958.
Choo, K.-K. R. and Dehghantanha, A. (eds) (2017) Contemporary digital forensic investigations of cloud and mobile applications. Amsterdam: Syngress is an imprint of Elsevier. Available at: http://encore.lib.warwick.ac.uk/iii/encore/record/C__Rb3102957.
Lallie, H.S., 2020. Dashcam forensics: A preliminary analysis of 7 dashcam devices. Forensic Science International: Digital Investigation, 33, p.200910.
Lallie, H. and Benford, D. (2011) 'Challenging the Reliability of iPhone - Geo-tags', The International Journal of Forensic Computer Science, 6(1), pp. 59–67. doi: 10.5769/J201101004.
Lallie, H. S. (2012) 'An Overview of the Jumplist Configuration File in Windows 7', Journal of Digital Forensics, Security and Law, 7(1), pp. 15–28. Available at: https://0-search-proquest-com.pugwash.lib.warwick.ac.uk/docview/1356584414?accountid=14888.

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.

Subject specific skills

Participants will demonstrate:

- an understanding of assessing the business impact of an incident.
- an understanding of disaster recovery planning and the importance of business continuity policy.
- the ability to conduct and manage a digital investigation.
- an awareness of the auditing and the importance of security controls

Transferable skills

Communication
Teamwork and working effectively with others

Critical thinking
Problem solving
Professionalism

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (6%)
Tutorials	12 sessions of 1 hour (8%)
Practical classes	10 sessions of 1 hour (6%)
Work-based learning	32 sessions of 1 hour (20%)
Private study	54 hours (34%)
Assessment	40 hours (25%)
Total	158 hours

Private study description

15 hours of private study

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 Report	60%	25 hours	Yes (extension)
Participants will be provided an investigation brief and typically provided with a 'digital forensic image' (a bit for bit copy of a suspect's hard disk). Participants will be required to conduct an investigation and report on the results.			
Coursework	40%	15 hours	Yes (extension)
Participants will be provided with an incident outline. Participants will be required to outline how			

	Weighting	Study time	Eligible for self-certification

an organisation should respond to the given incident, providing very clear advice to colleagues at C or E level.

Feedback on assessment

Feedback will be given as appropriate to the assessment type:
– verbal formative feedback on lab activities
– written summative feedback on post module assessment.

Availability

Courses

This module is Optional for:

- DWMS-H652 Undergraduate Digital and Technology Solutions (Data Analytics) (Degree Apprenticeship)
  - Year 3 of H652 Digital and Technology Solutions (Data Analytics) (Degree Apprenticeship)
  - Year 4 of H652 Digital and Technology Solutions (Data Analytics) (Degree Apprenticeship)
- DWMS-H653 Undergraduate Digital and Technology Solutions (Network Engineering) (Degree Apprenticeship)
  - Year 3 of H653 Digital and Technology Solutions (Network Engineering) (Degree Apprenticeship)
  - Year 4 of H653 Digital and Technology Solutions (Network Engineering) (Degree Apprenticeship)
- DWMS-H654 Undergraduate Digital and Technology Solutions (Software Engineering) (Degree Apprenticeship)
  - Year 3 of H654 Digital and Technology Solutions (Software Engineering) (Degree Apprenticeship)
  - Year 4 of H654 Digital and Technology Solutions (Software Engineering) (Degree Apprenticeship)