WM9C1-15 Digital Forensic Investigation

24/25

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

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:

- Critically evaluate relevant digital forensic characteristics of selected digital electronic devices
- Apply scientific techniques to investigate digital artefacts against a realistic brief
- Analyse evidence uncovered through an investigation
- Report on digital forensic evidence against a given legal context

Indicative reading list

Casey, E., 2011. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.
Choo, K.K.R. and Dehghantanha, A. eds., 2016. Contemporary Digital Forensic Investigations of Cloud and Mobile Applications. Syngress.
Nelson, B., Phillips, A. and Steuart, C., 2014. Guide to computer forensics and investigations. Cengage Learning.

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 in such a way that it can 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

Participants will develop an advanced applied understanding of how to manage a digital investigation regardless of whether it is a criminal or civil/corporate matter.

Transferable skills

Communication, teamwork, digital literacy, intercultural awareness, professionalism, organisational awareness

Study

Study time

Type	Required
Lectures	7 sessions of 1 hour (5%)
Practical classes	23 sessions of 1 hour (15%)
Online learning (independent)	60 sessions of 1 hour (40%)
Assessment	60 hours (40%)
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 A2

	Weighting	Study time
Digital investigation assessment	20%	12 hours

A timed closed book test which tests the ability to evaluate forensic characteristics of given devices/operating systems, and the ability to apply scientific reasoning during the course of an investigation.

Students resitting the in-class test will be given another opportunity to sit the test at a time within four weeks after the module has completed (as the test normally runs on the penultimate day of the original four week block). The multiple choice questions will be changed (question bank and cycling answers)

	Weighting	Study time
Practical investigation of a cyber crime incident	80%	48 hours

The coursework will involve the investigation of an incident to reveal the range and prevalence of digital evidence that can be extracted from a given device or devices.

The report is written for a law enforcement agency and will involve the practical examination of the device itself and the forensic examination of the evidenced created thereof using digital forensic tools.

Feedback on assessment

Feedback will be provided as annotated commentary within the submitted work. High level feedback will be provided on a standard WMG feedback sheet. Students will have an opportunity to get further feedback and support directly from the module tutor.

Availability

Courses

This module is Core for:

- MSc Cyber Security Management and MSc Cyber Security Engineering