

Module 39 Digital Forensics & Investigative Techniques

Module title	Digital Forensics & Investigative Techniques
Module NFQ level (only if an NFQ level can be demonstrated)	8
Module number/reference	BSCH-DFIT
Parent programme(s)	Bachelor of Science (Honours) in Computing Science
Stage of parent programme	Award stage
Semester (semester1/semester2 if applicable)	Semester 2
Module credit units (FET/HET/ECTS)	ECTS
Module credit number of units	5
List the teaching and learning modes	Direct, Blended
Entry requirements (statement of knowledge, skill and competence)	Learners must have achieved programme entry requirements.
Pre-requisite module titles	BSCH-CH, BSCH-OSD, BSCH-DNA
Co-requisite module titles	None
Is this a capstone module? (Yes or No)	No
Specification of the qualifications (academic, pedagogical and professional/occupational) and experience required of staff (staff includes workplace personnel who are responsible for learners such as apprentices, trainees and learners in clinical placements)	Qualified to as least a Bachelor of Science (Honours) level in Computer Science or equivalent and with a Certificate in Training and Education (30 ECTS at level 9 on the NFQ) or equivalent.
Maximum number of learners per centre (or instance of the module)	60
Duration of the module	One Academic Semester, 12 weeks teaching
Average (over the duration of the module) of the contact hours per week	3
Module-specific physical resources and support required per centre (or instance of the module)	One class room with capacity for 60 learners

Analysis of required learning effort		
	Minimum ratio teacher / learner	Hours
Effort while in contact with staff		
Classroom and demonstrations	1:60	36
Monitoring and small-group teaching		
Other (specify)		
Independent Learning		
Directed e-learning		
Independent Learning		54
Other hours (worksheets and assignments)		35
Work-based learning – learning effort		
Total Effort		125

Allocation of marks (within the module)					
	Continuous assessment	Supervised project	Proctored practical examination	Proctored written examination	Total
Percentage contribution	50%			50%	100%

Module aims and objectives

This module introduces the learner to the concepts of computer forensics and investigative techniques. They encounter various techniques used in digital forensic investigations and the tools required for these investigations. Learners also gain an exposure to the practical digital evidence gathering process. Current trends in computer forensics, such as network and cloud forensics are introduced using academic papers. Several investigative techniques will be covered, providing learners with a solid understanding of how to reason about evidence and hypotheses. Given a set of information, evidence, and hypotheses, how does an investigator make sense of it. How is sense made from an information set and how are better predictions made and investigative leads generated? There are many methods, from hard logical inferences to less formal structured analytic techniques.

Minimum intended module learning outcomes

On successful completion of this module, the learner will be able to:

1. Apply digital forensics principles and procedures
2. Discuss the importance of the integrity of digital evidence
3. Evaluate common digital forensic investigative methods and associated tools
4. Identify where to locate digital evidence across a range of devices
5. Critique the state-of-the-art digital forensic techniques and methodologies

6. Implement the most common approaches to digital forensic investigation.
7. Reason about evidence and hypotheses..

Rationale for inclusion of the module in the programme and its contribution to the overall MIPLOs

Digital forensics is a growing discipline. Understanding concepts from this module will not only provide a solid foundation in terms of job prospects, it will solidify many general computer science concepts. In terms of investigations, the learner will discover many useful techniques for making sense of a set of evidence and hypotheses that will be applicable in any environment.

Appendix 1 of the programme document maps MIPLOs to the modules through which they are delivered.

Information provided to learners about the module

Learners receive a programme handbook to include module descriptor, module learning outcomes (MIMLO), class plan, assignment briefs, assessment strategy, and reading materials.

Module content, organisation and structure

Digital forensics

- What is evidence?
- What is digital forensics?
- Importance of evidential integrity – chain of custody, documentation etc...

Forensic Examination of Computers and Digital Media

- Operating Systems
- Mobile devices
- Data sets (such as emails)
- Network forensics and packet analysis

Reverse engineering

- Common approaches
- Case studies

Investigative techniques

- Overview of how to investigate
- How to reason about evidence and hypotheses
- Common approaches to investigations
- Basic overview of formal logics (Bayesian, propositional, etc...)

- Alternatives to formal logic and how they are relevant in modern forensic casework

Module teaching and learning (including formative assessment) strategy

The module is delivered through a series of lectures. The emphasis is on developing knowledge and understanding in context.

Assessment is divided into three elements. The continuous assessment consists of a presentation on a prescribed and a comprehensive report on the same topic. These assess the learner's understanding in specific areas of the syllabus. Finally, there is an end of semester exam that tests the learners understanding of the theoretical material.

Timetabling, learner effort and credit

The module is timetabled as one 3-hour lecture per week.

There are 36 contact hours made up of 12 lectures delivered over 12 weeks with classes taking place in a classroom. The learner will need 54 hours of independent effort to further develop the skills and knowledge gained through the contact hours. An additional 35 hours are set aside for learners to work on assignments that must be completed for the module as a part of the continuous assessment.

Work-based learning and practice-placement

There is no work based learning or practice placement involved in the module.

E-learning

The college VLE is used to disseminate notes, advice, and online resources to support the learners. The learners are also given access to Lynda.com as a resource for reference.

Module physical resource requirements

Requirements are for a classroom for 60 learners equipped with a projector.

Reading lists and other information resources

Recommended Text

Heuer, R.J., Pherson, R.H. (2015) *Structured Analytic Techniques for Intelligence Analysis*. Thousand Oaks: CQ Press

Secondary Reading

Graves, M. W. (2014) *Digital Archaeology: The Art and Science of Digital Forensics*, Upper Saddle River: Addison-Wesley

Specifications for module staffing requirements

For each instance of the module, one lecturer qualified to at least Bachelor of Science (Honours) in Computer Science or equivalent, and with a Certificate in Training and Education (30 ECTS at level 9 on the NFQ) or equivalent.. Industry experience would be a benefit but is not a requirement.

Learners also benefit from the support of the programme director, programme administrator, learner representative and the Student Union and Counselling Service.

Module Assessment Strategy

The assignments constitute the overall grade achieved, and are based on each individual learner's work. The continuous assessments provide for ongoing feedback to the learner and relates to the module curriculum.

No.	Description	MIMLOs	Weighting
1	Assignment Learners are asked to submit a dissertation on a (different) topic related to recent technologies and trends in the field of digital forensics/investigative techniques.	1-7	25%
2	Presentation Each learner will be asked to prepare a short presentation regarding the topic covered in no.1 Presentation will be short, 5-10 minutes.	1-7	25%
3	Written exam that tests the theoretical aspects of the module.	1-7	50%

All repeat work is capped at 40%.

Sample assessment materials

Note: All assignment briefs are subject to change in order to maintain current content.

Digital Forensics and Investigative Techniques

Assignment

25% - Overall

In a world where viewing and storage of images of dinosaurs is illegal, you are given an image of a machine suspected of being involved in a crime ([img.e01](#)). Your task is to analyse the image in a forensically sound manner and write a letter of findings.

Any forensic tool may be used however a virtual machine running a clean OS is recommended.

Your letter of findings should answer:

1. Was this machine involved in the crime?
2. If so, explain what happened.
3. What evidence do you have to support?

[15 marks]

Using an appropriate structured analytic technique, reason about and present the above case. Provide this information in your letter.

[10 marks]

GRIFFITH COLLEGE DUBLIN

**QUALITY AND QUALIFICATIONS IRELAND
EXAMINATION**

Digital Forensics and Investigative Techniques

Lecturer(s):

External Examiner(s):

Date: XXXXX

Time: XXXXXXX

**THIS PAPER CONSISTS OF FOUR QUESTIONS
ALL QUESTIONS TO BE COMPLETED
ALL QUESTIONS CARRY EQUAL MARKS**

[BASICS]

What are the three stages of the digital forensic process?

[5 marks]

What is evidence?

[5 marks]

Explain chain of custody using an example.

[5 marks]

Explain the trend in digital forensics moving away from full disk imaging of storage media.

[5 marks]

An investigator receives a USB storage device and is asked to report on its contents. Explain the steps the investigator should take to prevent evidence spoliation.

[5 marks]

Total (25 marks)

[Forensic Examination]

What is the Windows Registry, and name an appropriate tool to aid in its examination?

[5 marks]

Why is ascertaining a time zone important during an investigation?

[5 marks]

What is file carving? Provide an example of any tool that performs file carving.

[5 marks]

Indicate what and how many hits the follow regex will match for in the string "00 0F FF FE"?

`/F{1,2}/g`

[10 marks]

Total (25 marks)

[Reverse engineering]

What is reverse engineering?

[5 marks]

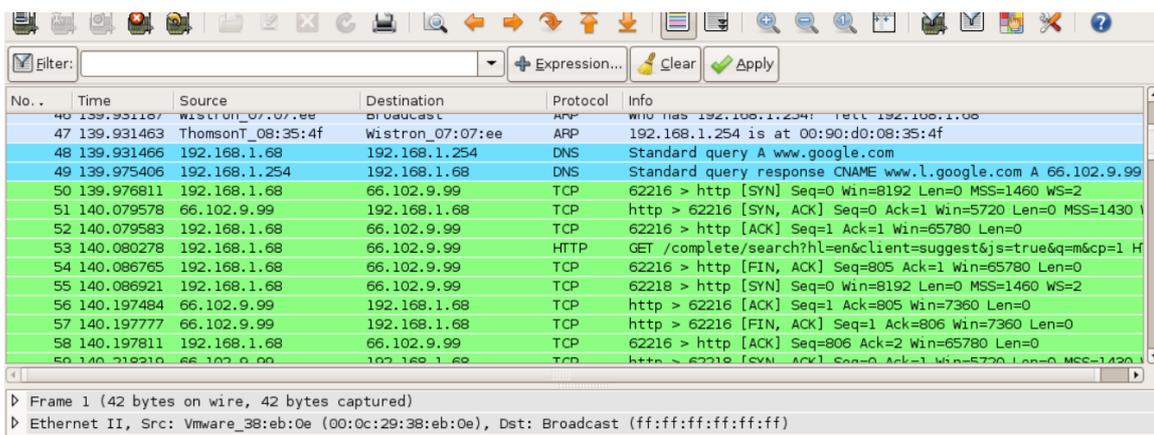
How can we limit the information in *Procmon* to be more relevant to an executable "test.exe"?

[5 marks]

Name two packet capturing and analysis applications.

[5 marks]

What has the following packet capturing application captured?



The screenshot shows a Wireshark packet capture interface. The packet list pane displays the following data:

No.	Time	Source	Destination	Protocol	Info
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
59	140.212210	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430

The packet details pane shows the selected packet (No. 47) as:

- Frame 1 (42 bytes on wire, 42 bytes captured)
- Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

[10 marks]

[Investigative Techniques]

What is a hypothesis?

[5 marks]

List three techniques to reason about a set of information?

[5 marks]

Given the simple morphological analysis (MA) model:



And the CCA values:



Assuming a tick (✓) indicates consistency, who was not at the scene of the crime?

[15 marks]