H8DIGFOR: Digital Forensics

Module Code:	H8DIGFOR
Long Title	Digital Forensics APPROVED
Title	Digital Forensics
Module Level:	LEVEL 8
EQF Level:	6
EHEA Level:	First Cycle

Credits:	5

Module Coordinator:	Arghir Moldovan

Module Author:	Arghir Moldovan

Departments:	School of Computing

Specifications of the qualifications and experience required of staff	MSc and/or PhD degree in computer science or cognate discipline. May have industry experience also.

Learning Outcomes

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

#	Learning Outcome Description
LO1	Rationalise the ethics, legal situation, compliance requirements, methods and procedures used in forensics investigations.
LO2	Conduct a forensic investigation analysing evidence and understanding formats for stored data that can be retrieved from various systems and devices.
LO3	Apply specialist forensic tools to forensically analyse devices and investigate security breaches.

Dependencies

Module Recommendations

No recommendations listed

Co-requisite Modules

No Co-requisite modules listed

Entry requirements	See Section 4.2 Entry Procedures and Criteria for the programme.

H8DIGFOR: Digital Forensics

Module Content & Assessment

Indicative Content
Overview Introduction to digital forensics Principles of forensics, chain of custody Investigative steps and techniques, ethics and legalities
Forensics Labs Forensics Lab policies and setup Standard operating procedures Hardware and software requirements
Expert Testimony Role of an expert witness Ethics that apply to expert witnesses Rules expert witnesses are obliged to adhere to
Digital Evidence Sources of digital evidence Properties and principles of digital evidence Appropriate handling of evidence Procedures that need to be observed for digital evidence identification, acquisition and storage Forensic imaging techniques
Hardware Systems Hardware considerations: computer architecture, physics of different storage technologies, magnetic and solid-state storage media, partitioning and formatting, buffering, caching Data in ROM and RAM storage Other storage devices like photocopiers, cameras, smartphones, etc.
Forensic Analysis Analysis of different types of information that is stored Understanding formats for stored data, and how is used by specialist tools Manual review of media Cracking passwords Keyword searches Email and image analysis Internet history analysis
Operating Systems Forensics Operating systems and their tools File systems characteristics and analysis Windows forensics: Alternate Data Stream, Registry, Recycle Bin, System logs
Cloud Forensics Cloud forensics stakeholders Challenges in cloud forensics Acquisition and analysis of cloud forensic data
Network Forensics Differences in procedures for network forensics through the monitoring of network traffic Analysis of what data is on the network and identifying what the traffic is Logging of incidents

Assessment Breakdown	%
Coursework	50.00%
End of Module Assessment	50.00%

Assessments

Full Time

Coursework

Assessment Type:	Formative Assessment	**% of total:**	Non-Marked
Assessment Date:	n/a	**Outcome addressed:**	1,2,3
Non-Marked:	Yes		

Assessment Description:
Formative assessment will be provided on the in-class individual or group activities.

Assessment Type:	Continuous Assessment	**% of total:**	50
Assessment Date:	Week 11	**Outcome addressed:**	2,3
Non-Marked:	No		

Assessment Description:
The continuous assessment will focus on the practical aspects of digital forensics. Learners will be provided with one or more forensic disk images and they will be asked to conduct digital forensics testing activities through the application and usage of appropriate tools and techniques. Learners will have to document their findings in a report they will submit for assessment. Part of the continuous assessment may consist of a group-based research and presentation on a case where digital forensics played a crucial role towards solving the case.

End of Module Assessment

Assessment Type:	Terminal Exam	**% of total:**	50
Assessment Date:	End-of-Semester	**Outcome addressed:**	1,2
Non-Marked:	No		

Assessment Description:
Learners are required to complete a formal end-of-semester examination.

No Workplace Assessment

Reassessment Requirement

Repeat examination
Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.

Reassessment Description
The reassessment strategy for this module will consist of a written examination that will assess all learning outcomes.

H8DIGFOR: Digital Forensics

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	24	Per Semester	2.00
Tutorial	No Description	12	Per Semester	1.00
Independent Learning	No Description	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	24	Per Semester	2.00
Tutorial	No Description	12	Per Semester	1.00
Independent Learning	No Description	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Module Resources

Recommended Book Resources

Bill Nelson, Amelia Phillips, Christopher Steuart. (2019), Guide to Computer Forensics and Investigations, 6th Edition. Cengage Learning, p.688, [ISBN: 9781337568944].

Supplementary Book Resources

Keith J. Jones, Richard Bejtlich. (2011), Real Digital Forensics, Volume 2, Addison-Wesley Professional, p.448, [ISBN: 9780321684776].

Eoghan Casey. (2011), Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition. Academic Press, p.807, [ISBN: 978-0123742681].

John Sammons. (2014), The Basics of Digital Forensics, 2nd Edition. Syngress Press, p.200, [ISBN: 9780128016350].

Lei Chen, Hassan Takabi, Nhien-An Le-Khac. (2019), Security, Privacy, and Digital Forensics in the Cloud, John Wiley & Sons, p.360, [ISBN: 978-1119053286].

Recommended Article/Paper Resources

Various Articles, Digital Investigations,
http://www.journals.elsevier.com/digital -investigation

Various Articles, Digital Forensics Magazine,
http://www.digitalforensicsmagazine.com/

Other Resources

[Website], Live CD for Forensics,
http://www.caine-live.net/

[Website], forensics articles,
http://www.forensickb.com/

[Website], Forensic Focus,
http://www.forensicfocus.com

[Website], SANS,
http://www.sans.org

[Website], CISSP,
https://www.isc2.org/Certifications/CISS P

Discussion Note:	