H9DFA: Digital Forensics and Auditing

Module Code:	H9DFA
Long Title	Digital Forensics and Auditing APPROVED
Title	Digital Forensics and Auditing
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	5
Module Coordinator:	Simon Caton
Module Author:	Simon Caton
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	

Learning Outcomes	
On successful completion of this module the learner will be able to:	
#	**Learning Outcome Description**
LO1	Critically analyse what a digital investigation is, the sources of digital evidence, along with potential challenges and limitations of forensics.
LO2	Evaluate and assess how data collection is accomplished whilst ensuring the integrity of the original and forensics copy.
LO3	Appropriate and correct use of toolsets and processes to support legal requirements for use of seized data as part of a review or investigation.
LO4	Use search criteria, keywords and other techniques to determine whether events or activities have been performed by individuals, systems and/or entities.

Dependencies
Module Recommendations
No recommendations listed
Co-requisite Modules
No Co-requisite modules listed

Entry requirements	

H9DFA: Digital Forensics and Auditing

Module Content & Assessment

Indicative Content
Basic Principles and methodologies for digital forensics • Design systems with forensic needs in mind • Rules of Evidence – general concepts and differences between jurisdictions and Chain of Custody • Search and Seizure of evidence: legal and procedural requirements
Digital Evidence methods and standards • Techniques and standards for Preservation of Data • Legal and Reporting Issues (including Criminal Justice Act 2011) • The role of an expert witness
System Forensics • Operating Systems Forensics • Web & Network Forensics • Mobile Device Forensics
Auditing • Identification and application of framework criteria (e.g. ISO 27001, PCI DSS) • Identifying the area of concern to maintain impartiality & consistency • Contractual obligations / limitations: right to investigate or audit • Challenges: Privacy, collusion, encryption
Attack detection and investigation • Anti-forensics techniques used by attackers

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

Assessments

Full Time

Coursework

Assessment Type:	Project	**% of total:**	50
Assessment Date:	n/a	**Outcome addressed:**	2,3,4
Non-Marked:	No		

Assessment Description:
A technical project that within the context of a financial investigation scenario.

End of Module Assessment

Assessment Type:	Terminal Exam	**% of total:**	50
Assessment Date:	End-of-Semester	**Outcome addressed:**	1,2,4
Non-Marked:	No		

Assessment Description:
The examination will be a minimum of two hours in duration and may include a mix of: short answer questions, vignettes, essay based questions and case study based questions. Marks will be awarded based on clarity, appropriate structure, relevant examples, depth of topic knowledge, and evidence of outside core text reading.

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.

H9DFA: Digital Forensics and Auditing

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	Every Week	24.00
Tutorial	No Description	24	Every Week	24.00
Independent Learning Time	No Description	77	Every Week	77.00
			Total Weekly Contact Hours	48.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	24	Every Week	24.00
Tutorial	No Description	24	Every Week	24.00
Independent Learning Time	No Description	77	Every Week	77.00
			Total Weekly Contact Hours	48.00

Module Resources

Recommended Book Resources

John Sammons. (2015), Digital Forensics: Threatscape and Best Practices, Syngress, p.182, [ISBN: 9780128045268].

Delena D. Spann. (2013), Fraud Analytics: Strategies and Methods for Detection and Prevention, 1. John Wiley & Sons, p.176, [ISBN: 9781118230688].

Nabar, Shubha U et al.. (2008), A survey of query auditing techniques for data privacy". In: Privacy-Preserving, Springer.

Cox, Arthur. Litigation & Dispute Resolution Briefing..

Supplementary Book Resources

B. Nelson et al.. (2015), Guide to Computer Forensics and Investigations, 5. Delmar Cengage Learning, [ISBN: 1285060032].

Albert J. Marcella, Frederic Guillossou, Fredrick Guillossou.. (2012), Cyber forensics: from Data to Digital Evidence, Chichester; John Wiley & Sons, [ISBN: 1118273664].

Sunder Gee.. (2015), Fraud and fraud detection: A Data Analytics Approach, Wiley, p.336, [ISBN: 1118779657].

Recommended Article/Paper Resources

Arthur Cox. Litigation & Dispute Resolution Briefing.,
http://www.arthurcox.com/wp-content/uplo ads/2014/01/Arthur-Cox-The-Criminal-Just ice-Act-2011-September-2011.pdf

Shubha U. Nabar, Krishnaram Kenthapadi, Nina Mishra, Rajeev Motwani. (2008), A Survey of Query Auditing Techniques for Data Privacy, Privacy-Preserving Data Mining, 2008, 415-431.

This module does not have any other resources

Discussion Note:	