H9FRED: Forensics and eDiscovery

Module Code:	H9FRED
Long Title	Forensics and eDiscovery APPROVED
Title	Forensics and eDiscovery
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	5
Module Coordinator:	Vanessa Ayala-Rivera
Module Author:	Vikas Sahni
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	PhD/Master's degree in a computing 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	Demonstrate in-depth critical awareness and interpretation of laws, compliance requirements, methods and procedures used in digital forensics investigations.
LO2	Carry out a forensic investigation of operating systems, mobile devices and networks, critically analyse the evidence and document the findings in a report.
LO3	Compare, evaluate and use forensic tools to forensically analyse digital devices.
LO4	Carry out an eDiscovery engagement across multiple platforms making use of various electronic discovery tools.
LO5	Critically analyse the results of an eDiscovery review, prepare production sets, write reports, and appraise the concepts for information retrieval and enterprise search technologies.

Dependencies

Module Recommendations

No recommendations listed

Co-requisite Modules

No Co-requisite modules listed

Entry requirements	Programme entry requirements must be satisfied.

H9FRED: Forensics and eDiscovery

Module Content & Assessment

Indicative Content
Introduction to Digital Forensics Introduction to the module. Principles of forensics, need of digital forensics, background to digital forensics, Computer crime. Scenarios of digital forensics investigations. Steps of digital forensics methodology. Categories of incidents.
Digital Evidence: Best Practices Sources of digital evidence and the investigation process. Evidence handling rules. ACPO principles of computer related evidence. Chain of custody. Need to maintain extensive documentation. Digital forensics report writing, typical parts, letter of findings, affidavits.
Forensic Tools Types of computer forensic tools, various tasks performed by forensic tools and its details. Drive imaging. Password cracking tools. Forensic workstation, choosing the forensic toolkit. Validating and testing forensic software, using NIST tools.
Windows Forensics Importance of operating system forensics. Relevant windows data structures. History of the windows registry, registry editor key, registry information. Tracking user activity by analysing shellbags and quick access/Recent Files Review bitlocker encryption and location of recovery keys.
Network Forensics Basics of network forensics When to apply network forensics. Key elements in communication. Network trace. Key concepts to interpret a network trace. IP and MAC addresses and networking infrastructure. Show how session keys (perfect forward secrecy) encryption/decryption works with RSA .Public Key encryption. Explain the role of deep packet inspection and web application firewalls in a network.
Mobile Device Forensics Mobile devices, mobile phones in crime, collecting a phone for analysis, data recovered from a mobile phone. Components of mobile phone. Accessing the data from a mobile phone. Tools used for mobile forensic analysis.
Linux Forensics Linux shell, linux boot sequence. Filesystems and disk/directory Encryption techniques. Important directories and sub-directories. File deletion in linux. Find Recently accesses/modified/changed files Log analysis /var/log/*
Introduction to Electronic Discovery What is discovery, how is conventional discovery different to eDiscovery. What is electronic discovery. Common challenges of electronic discovery. Examine Microsoft Purview or Gcloud Vault , eDiscovery platforms.
Enterprise Search Discuss Full-text search, Faceting, Nearest-Neighbour/Clustering. Highlighting of hits. Rich document handling. Document fields and schema design.
Electronic Discovery Reference Model Discussing various phases of Electronic discovery reference model in detail. Information governance. Deduplication, keyword searching, technology assisted review (TAR), email threading, textual near duplicate identification.
Electronic Discovery Processes Approaches to eDiscovery. Forms of electronically stored information. What constitutes evidence and what is metadata. Selecting an eDiscovery tool. Significance of quality assurance in eDiscovery practices. Email archiving/journaling.
Revision, catch-up and formative feedback n/a

Assessment Breakdown	%
Coursework	100.00%

Assessments

Full Time

Coursework

Assessment Type:	CA 1	**% of total:**	40
Assessment Date:	n/a	**Outcome addressed:**	1,2,3
Non-Marked:	No		

Assessment Description:
Practical work will be conducted throughout the semester to assess the learner's knowledge on forensic procedures, acquisition methods, analysis of computer data and eDiscovery processes making use of various forensic and eDiscovery tools.

Assessment Type:	Formative Assessment	**% of total:**	Non-Marked
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4,5
Non-Marked:	Yes		

Assessment Description:
Formative assessment will be provided on the in-class individual or group activities. Feedback will be provided in written or oral format, or on-line through Moodle. In addition, in class discussions will be undertaken as part of the practical approach to learning.

Assessment Type:	CA 2	**% of total:**	60
Assessment Date:	n/a	**Outcome addressed:**	4,5
Non-Marked:	No		

Assessment Description:
A terminal assessment that will assess learner's knowledge and analytical skills regarding enterprise search and eDiscovery rules, processes, and platforms. Students will conduct practical activities using various tools and write a report on their work.

No End of Module Assessment

No Workplace Assessment

Reassessment Requirement

Coursework Only
This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Reassessment Description
The reassessment strategy for this module will consist of an assessment that will evaluate all learning outcomes.

H9FRED: Forensics and eDiscovery

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Independent Learning	Independent learning	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Workload: Blended

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	12	Per Semester	1.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Directed Learning	Directed e-learning	12	Per Semester	1.00
Independent Learning	Independent learning	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	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Independent Learning	Independent learning	89	Per Semester	7.42
			Total Weekly Contact Hours	3.00

Module Resources

Recommended Book Resources

G. Johansen. (2020), Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd edition. Packt Publishing.

Justin Seitz,Tim Arnold. (2021), Black Hat Python, Python Programming for Hackers and Pentesters, 2nd Ed. No Starch Press, p.216, [ISBN: 978-1718501126].

Supplementary Book Resources

Harlan Carvey. (2016), Windows Registry Forensics, 2nd Ed. Syngress, p.216, [ISBN: 978-0128032916].

Nipun Jaswal. (2019), Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools, Packt Publishing, [ISBN: 978-1789344523].

This module does not have any article/paper resources

Other Resources

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

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

[Website], COMPUTER FORENSIC RESOURCES, http://www.evestigate.com/COMPUTER%20FOR ENSIC%20RESOURCES.htm.

[Website], Security Journals/Whitepapers https://securityjournaluk.com/.

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

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

[Website], AI Powered Search. https://livebook.manning.com/book/ai-pow ered-search/about-this-meap/v-9/.

[Website], Guide: Good Practice Discovery Guide - CLAI, https://clai.ie/wp-content/uploads/2021/ 10/CLAI-Good-Practice-Discovery-Guide-v2 _0.pdf.

[Website], Relativity One Discovery User Guide. https://help.relativity.com/RelativityOn e/Content/index.htm.

[Website], Microsoft Purview, Microsoft365 eDiscovery. https://learn.microsoft.com/en-us/micros oft-365/compliance/ediscovery?view=o365- worldwide.

[Website], Apache Lucene Solr https://github.com/mikeroyal/Apache-Luce ne-Solr-Guide.

[Website], Autopsy Sleuth Kit. https://www.sleuthkit.org/autopsy/.

[Website], Nist forensic sample images. https://cfreds.nist.gov/.

[Website], Linux forensics cheatsheet http://www.security-hive.com/post/linux- forensics-the-complete-cheatsheet.

Discussion Note:	