Title:	Incident Response & Forensics APPROVED
Long Title:	Incident Response & Forensics

Module Code:	COMP9038	**Duration:**	1 Semester

Credits:	10
NFQ Level:	Expert
Field of Study:	Computer Science
Valid From:	Semester 1 - 2019/20 (September 2019)
Module Delivered in	2 programme(s)
Module Coordinator:	Sean McSweeney
Module Author:	VINCENT RYAN
Module Description:	Computer misuse in organisations typically fall into two general categories. Either a computer is leveraged to commit a crime or itself is a target for crime. This module will focus on the computer itself as the victim of crime and the examination of computer systems that have been remotely attacked, which is commonly referred to as Incident Response (IR). As part of this module data acquisition and recovery techniques will be examined to support forensic investigations and the tools, policies and procedures that are useful in the field of IR.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
LO1	Discuss the main technical approaches and challenges associated with IR.
LO2	Investigate the current legal frameworks and data privacy laws relevant to the field of IR.
LO3	Develop an Incident Response (IR) plan for an organisation with the aim of improving a firm's security posture.
LO4	Gather static data from a computer or storage device with the aim of preserving evidence.
LO5	Acquire volatile memory and data using advanced tools and techniques.
LO6	Interpret data collected as part of a forensic investigation.
LO7	Analyse the main exploitation mitigation techniques for modern day operating systems.

Pre-requisite learning
Module Recommendations *This is prior learning (or a practical skill) that is strongly recommended before enrolment in this module. You may enrol in this module if you have not acquired the recommended learning but you will have considerable difficulty in passing (i.e. achieving the learning outcomes of) the module. While the prior learning is expressed as named CIT module(s) it also allows for learning (in another module or modules) which is equivalent to the learning specified in the named module(s).*
Incompatible Modules *These are modules which have learning outcomes that are too similar to the learning outcomes of this module. You may not earn additional credit for the same learning and therefore you may not enrol in this module if you have successfully completed any modules in the incompatible list.*
No incompatible modules listed
Co-requisite Modules
No Co-requisite modules listed
Requirements *This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed. You may not enrol on this module if you have not acquired the learning specified in this section.*
Students should have a very good knowledge of Operating Systems, and be comfortable while working at the command line in both a Windows and Linux environment.

Module Content & Assessment

Indicative Content
Incident Response Incident Response theory. Challenges associated with IR. Lifecycle of Incident Responce, Policies, Procedures, Tools and commands useful in various OS's, WMIC, Powershell, SysInternals Tools. Planning for an IR: Pre-Incident Preparation, Scoping an Incident, Remediation. Acquiring data from many systems.
EDiscovery Laws relating to the capture of static and dynamic data. EDiscovery issues. Laws related to monitoring communications and traffic data during an incident. Disclosure of stored communications and documents. EU and Global legal frameworks.
Data Acquisition Imaging, dd, dc3dd, FTK, hardware, software, volatile data, imaging live and dead systems, chain of custody.
File Systems FAT, NTFS, exFAT, ext2/3, ext4, superblock, timings, filesystem storage, metadata, inodes.
Windows Internals The Registry, Typical Windows Processes such as lsass, winlogin, explorer, svchost.
Forensic Analysis Data Carving, Timeline Analysis, supertimelines, unallocated data, slack space, Host Block Area, Windows Registry Keys, restore points, ShellBags,Finding evidence of file opening/download/execution, physical location, external device usage, browser usage, account login/logout.
Memory Forensics Acquiring a memory image, hibernation files and crash dumps, memory dump formats, Processes and drivers in memory, event logs, registry, network artefacts in memory, kernel forensics, locating malware and code injection, use of volatility and/or rekall.
Exploitation Mitigation EMET, Stack canaries, DEP, ASLR, SEHOP, Control Flow Guard, Null Pointer Dereference, Isoltae Heap, Deferred Free.
Other Topics Forensic analysis of Smartphones, USB sticks, Counter Forensics.

Assessment Breakdown	%
Course Work	100.00%

Course Work

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	An example assignment that may be set as part of this assessment may be to discuss the field of IR bearing in mind the legal frameworks and data privacy laws relevant to the field.	1,2,3	30.0	Week 5
Project	Given log file data the student may be expected to gather static and volatile data using well known tools and techniques with the aim of perserving evidence that may form part of an forensic investigation.	4,5,6	30.0	Week 10
Project	This project will evaluate the student's understanding of the exploitation mitigation techniques that may be employed in modern operationg systems. The student may be explected to peform a memory extraction on patched and unpatched operating systems and a comparative analysis of the resulting data.	4,5,7	40.0	Sem End

No End of Module Formal Examination

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

The institute reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	4.0	Every Week	4.00
Lab	Lab to support learning outcomes.	2.0	Every Week	2.00
Independent Learning	Independent learning	8.0	Every Week	8.00
			Total Hours	14.00
			Total Weekly Learner Workload	14.00
			Total Weekly Contact Hours	6.00

Workload: Part Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	4.0	Every Week	4.00
Lab	Lab to support learning outcomes.	2.0	Every Week	2.00
Independent Learning	Independent learning	8.0	Every Week	8.00
			Total Hours	14.00
			Total Weekly Learner Workload	14.00
			Total Weekly Contact Hours	6.00

Module Resources

Recommended Book Resources

- **Jason Luttgens, Matthew Pepe, Kevin Mandia 2014, *Incident Response and Computer Forensics, Third Edition* [ISBN: 9780071798686]**

Supplementary Book Resources

- **Bill Nelson and Christopher Steuart 2018, *Guide To Computer Forensics And Investigations*, 6th Ed., CENGAGE [ISBN: 9781337568944]**
- **Philip Polstra 2015, *Linux Forensics*, CreateSpace Independent Publishing Platform [ISBN: 1515037630]**
- **Chet Hosmer 2014, *Python Forensics: A workbench for inventing and sharing digital forensic technology*, Syngress [ISBN: 0124186769]**
- **Michael Hale Ligh, Jamie Levy, Aaron Walters, Andrew Case 2014, *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*, Wiley [ISBN: 1118825098]]**
- **Kieth Jones, Richard Betjlich 2012, *Real Digital Forensics, Volume 2*, Addison-Wesley [ISBN: 032168477X]**
- **Harlan Carvey 2011, *Windows Registry Forensics*, Syngress [ISBN: 1597495808]**
- **Eoghan Casey 2011, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Third Edition Ed., Academic Press [ISBN: 0123742684]**
- **Andrew Hoog 2011, *Android Forensics*, Syngress [ISBN: 1597496510]**
- **Bill Nelson, Amelia Phillips, Christopher Steuart 2010, *Lab Manual for Nelson/Phillips/Steuart's Guide to Computer Forensics and Investigations* [ISBN: 1435498852]**
- **Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard 2010, *Malware Analyst's Cookbook and DVD*, Wiley [ISBN: 0470613033]**
- **Brian Carrier 2005, *File system forensic analysis*, Addison-Wesley Upper Saddle River, NJ [ISBN: 0321268172]**

Recommended Article/Paper Resources

- **Wilkinson S, Haagman D. 2010, *Good practice guide for computer-based electronic evidence*, Association of Chief Police Officers**
- **Grance, Tim, Karen Kent, and Brian Kim 2004, *Computer security incident handling guide*, NIST Special Publication**
- **CREST *Cyber Security Incident Response Guide***
  http://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide.pdf

Other Resources

- **website: *forensics blog*, SANS**
  http://computer-forensics.sans.org
- **Website: *Journey into IR***
  http://journeyintoir.blogspot.ie/
- **CD-ROM: *Live CD for Forensics***
  http://www.caine-live.net/
- **CD_ROM: *Live CD for Forensics***
  http://www.deftlinux.net/
- **CD_ROM: *Live CD for Forensics*, SANS**
  http://www.sans.org/sift-kit/essential.p hp
- **website: *forensics articles***
  http://www.forensickb.com/
- **website: *COMPUTER FORENSIC RESOURCES***
  http://www.evestigate.com/COMPUTER%20FOR ENSIC%20RESOURCES.htm
- **RFC: Network Working Group 2002, *RFC 3227 - Guidelines for Evidence Collection and Archiving***
- **Website: Computer Incident Response Center Luxembourg*Recommendations for Readiness to Handle Computer Security Incidents***
  https://www.circl.lu/pub/tr-22/

Module Delivered in

Programme Code	Programme	Semester	Delivery
CR_KINSE_9	Master of Science in Cybersecurity	1	Mandatory
CR_KINSY_9	Postgraduate Diploma in Science in Cybersecurity	1	Mandatory