Module Specification (AQD007)

	Part One: ABOUT THE MODULE		
1a	Module title	Digital Investigation and E-Discovery	
1b	Subject	BSc (Hons) Computer Networking and IT Security	
1c	Location(s) module is offered	Islington College	
1d	Courses Module is available on	On-Campus	
2	Module code	**CC6011NI**	
3	Module level and credit rating	**Level 6**	30
4	School	School of Computing and Digital Media	
5	Teaching period	*Year Long (30 Weeks)*	
6	Mode of attendance	*Day*	
7	Module prerequisites and corequisites	*None*	
8	Module description		
	Digital crimes are becoming far more sophisticated and harder to fight against. Therefore, the need for educating cybersecurity, investigation, and e-Discovery professionals is more critical than ever - there is a large talent gap for people with these skills. It is imperative to explore advanced detective and preventive technology in combating the ever-changing digital and cybercrimes. This module provides knowledge of how to detect and prevent digital crimes and cyber incident at both law enforcement and corporate level. In this module, students are also prepared for their career as a professional working in Cyber security and notably the digital investigation and e-discovery domains. It provides students with practical knowledge and skills needed to succeed in the external exam from the certification of CompTIA Security+.		
9	Module learning outcomes		
	On successful completion of the module students will be able to: LO1. identify and apply major developments in the digital crime investigation and E-discovery field; LO2. demonstrate an understanding of how advances in digital technology are related to criminal behaviour; LO3. appreciate the relationships between the advances in digital technology such as encryption, data hiding techniques and obstruction and their retrieval; LO4. evaluate and select appropriate tools and techniques for the detection and prevention of digital crime and e-discovery; LO5. perform a digital forensic analysis using suitable the appropriate investigation tools and approaches on different types of crime, platforms and contexts; LO6. Understand the e-discovery landscape through the Electronic Discovery Reference Model (EDRM) and notably Identification, Preservation, Collection, Processing, Review & Analysis, Production and Presentation LO6. be familiar with the different approaches that can be applied to real-time cybercrime investigation at law enforcement level and e-discovery at corporate level; LO7. be prepared for the CompTIA Security+ certification exam.		

10	Indicative syllabus – *for full details see section C in module booklet*
	• Introduction and reviews of new digital crime, cyber threat and digital assets misuse. [LO1, LO2, LO3] • Investigating digital crime using the appropriate resources and approaches for both law enforcement and corporate e-discovery; including data detection, recovery, processing, and validation. Preserving critical data and perform targeted, remote collections in context of e-discovery. [LO3, LO4, LO6] • Detecting Data Exfiltration and Unauthorized Browsing using E-discovery approach; detecting Insider Threats and Advanced Persistent Threats. [LO3, LO4, LO5] • data-hiding detection and investigation techniques for selected media types and approaches; digital watermarking and media signature, detecting copying. [LO3, LO5] • Steganography in different types of media such as textual data, images, audio, and streaming media. [LO6] • Data mining security, associated crime detection, and criminal behaviour. LO4, LO5, LO6] • Real-time analytical techniques for detecting security events on active systems and networks (e.g. intrusion and exfiltration detection). [LO4, LO5, LO6] • preparing for the CompTIA Security+ examination which includes ▪ Network security ▪ Compliance and operational security ▪ Threats and vulnerabilities ▪ Application, data and host security ▪ Access control and identity management. [LO7]
11	Indicative bibliography and key on-line resources
	Reading List: https://londonmet.rl.talis.com/lists/C466DB21-50AE-0B12-76BC-AAFCE872C859.html?edit&version=v1&lang=en&login=1 Textbooks: Core Text: • **Andrew Staniforth (2017) Handbook of Cyber Crime Investigation. Oxford University Press, ISBN13: 9780191035791** • **Mark Surguy, Weightmans (2018) E-Discovery: An Introduction to Digital Evidence ISBN: 9781787421721** • **David L. Prowse (2017) CompTIA Security+ SY0-501 Cert Guide (4th Edition) (Certification Guide), Pearson** Other Texts: • Casey, E. (2010) Digital evidence and computer crime, Third edition: forensic science, computers and the Internet, Academic Press. • Jones, K.J., Bejtlich, R., and Rose, C.W. (2006) Real Digital Forensics. Addison-Wesley. • Steve Anson, Steve Bunting, Ryan Johnson, and Scott Pearson, 2012, Mastering Windows Network Forensics and Investigation, SYBEX • Michael Gregg, Build Your Security LAB a field guide for network testing, 2008, Wiley • Cox, I.J., Miller, M., and Bloom, J. (2007) Digital Watermarking and Steganography, Morgan Kaufmann Publishers

Journals:

- International Conference on IT Security Incident Management & IT Forensics, Proceedings/International Conference on IT Security Incident Management & IT Forensics, Los Alamitos, Calif. IEEE Computer Society
- IEEE transactions on information forensics and security, IEEE Signal Processing Society, 2006 Quarterly
- Digital forensics magazine [electronic resource], TR Media, Quarterly, Began with Issue 01 (Nov. 2009)
- Digital investigation, ScienceDirect (Online service), Kidlington & Elsevier, eJournal/eMagazine

Websites:

- https://www.cybersecuritychallenge.org.uk/
- https://www.gov.uk/government/policies/cyber-security
- https://digital-forensics.sans.org/
- https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/ediscovery-toolkit
- http://student.londonmet.ac.uk/weblearn/

Electronic Databases:

- WorldCat.org

Social Media Sources: N/A

Other: None

12 What is the balance of independent study and scheduled teaching activity within the module?

- A process of personal development planning takes place throughout the course to help students to think about and make sense of what is being learnt and why, plan ahead and relate to what has been learned and their own future.
- Students will be expected and encouraged to produce such as reflective commentaries and graduation statements on the learning activities and tasks that they carry out to complete their work.
- Students are invited to include PDP via learning journals, case books, annotated sketchbooks, and/or blog environment.

NOTE: 1 credit = 10 hours' learning (i.e. 30 credits should total 300 hours)

Method	*Description*	*Learning hours*
Scheduled Learning & Teaching	Lectures/Tutorials/Workshops/ Drop-ins	90 hours
Guided independent study	Self-study	139 hours
Assessment preparation/delivery	Research, Solution Design, Development and Reporting/Documenting. Exam Review and Revision.	71 hours
Placement/study abroad		
TOTAL LEARNING HOURS FOR THE MODULE		300 hours

13a Description of assessment items.

Students are assessed by two compulsory assessments [LO1-7] and an optional assessment [LO7] which is organised externally by the CompTIA, a leading provider of

	vendor-neutral certifications in the world. The first compulsory assessment [LO1-6] is an assignment based on the successful completion of a series of workshop tasks. It will allow students to demonstrate their awareness and technical skills in the contexts in the prevention and detection of digital crimes. Students will produce a technical report (about 1500 words in total) detailing with their findings of an investigation into an area relating new technology crimes, their detection and prevention, as well as the knowledge and skills necessary for handling digital evidence. The second compulsory assessment [LO7], 1-hour exam, is designed to assess the practical knowledge and skills needed to succeed in the CompTIA Security+ certification exam, which will provide students with the confidence and competence in the external CompTIA Security+ accreditation exam.

13b	*Description of assessment component*		*Assessment weighting*	*Qualifying marks and conditions*	*Qualifying sets*	*Week due*	Learning outcome/s
	Course work	CW (1500 words) - online submission (Individual)	50%	N/A	N/A	12	LO1-LO6
	Unseen Exam	2-hour unseen exam designed for CompTIA Security+ certification	50%	N/A	N/A	30	LO1-LO6

Part Two: SCHOOL USE		
14	Nominated External Examiner at time of approval	
15	Nominated Module Leader at time of approval	

Part Three: OFFICIAL USE AND CODES – *responsibility for completion is as indicated*		
16	Original date of validation (AQD)	
17	Revision date (specify cohort) (AQD)	
18	Module specification version number (AQD)	
19	SITS Mark Scheme (Student Journey)	
20	Subject Standards Board Name (Student Journey)	