Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module code	CONL723
Module title	Digital Forensics
Level	7
Credit value	15
Faculty	FAST
Module Leader	Leanne Davies
HECoS Code	100366
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
MSc Computer Science with Cyber Security	Core

Pre-requisites

Studied CONL701 Critical Research for Postgraduate Study

Breakdown of module hours

Learning and teaching hours	15 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	0 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	15 hrs
Placement / work based learning	0 hrs
Guided independent study	135 hrs
Module duration (total hours)	150 hrs

For office use only	
Initial approval date	17/6/21
With effect from date	28/06/21
Date and details of revision	
Version number	1

Module aims

This module will introduce students to the principles of digital forensics to gather and analyse evidence from computer systems and communications. Students will learn the techniques, technologies and tools required to gather information within practical environments, and effectively report the results for consideration within legal and commercial situations.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Select, justify and explain a range of digital forensics techniques and tools used to discover information within computer systems
2	Make informed judgements by critically evaluating the use of a variety of approaches to digital forensics.
3	Critically evaluate computer systems and networks to identify and analyse useful information in an ethically sound manner.
4	Use and adapt digital forensics techniques to analyse existing systems and retrieve pertinent information.
5	Reflect upon, document and evaluate digital forensics outcomes in a legal, ethical and commercial compliant manner.

Assessment

Indicative Assessment Tasks:

This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

Students will complete a portfolio analysing and applying their knowledge of digital forensics. The portfolio may include written submissions, quizzes, discussions and practical based activities.

Word Count equivalent: 3000 words

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1-5	Portfolio	100%

Derogations

None

Learning and Teaching Strategies

The overall learning and teaching strategy is one of guided independent study requiring ongoing student engagement. Online material will provide the foundation of the learning resources, requiring the students to login and engage on a regular basis throughout the eight-week period of the module. There will be a mix of suggested readings, discussions and

interactive content containing embedded digital media and self-checks for students to complete as they work through the material and undertake the assessment tasks. The use of a range digital tools via the virtual learning environment together with additional sources of reading will also be utilised to accommodate learning styles. There is access to a helpline for additional support and chat facilities through Canvas for messaging and responding.

Indicative Syllabus Outline

1. Introduction to digital forensics
2. Acquiring digital evidence
3. Operating system forensics
4. Web and email forensics
5. Antiforensics techniques
6. Open source intelligence gathering
7. Reporting digital forensics

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads

Digital archaeology: the art and science of digital forensics: Graves, Michael

Other indicative reading

Årnes, A. (2017) *Digital Forensics.* Wiley-Blackwell.

Holt, T.J., Bossler, A.M., and Seigfried-Spellar, K.C. (2017) *Cybercrime and Digital Forensics: An Introduction*. 2nd ed. Routledge.

Sheward, M. (2018) *Hands-on Incident Response and Digital Forensics.* BCS, The Chartered Institute for IT.

Employability skills – the Glyndŵr Graduate

Each module and programme is designed to cover core Glyndŵr Graduate Attributes with the aim that each Graduate will leave Glyndŵr having achieved key employability skills as part of their study. The following attributes will be covered within this module either through the content or as part of the assessment. The programme is designed to cover all attributes and each module may cover different areas.

Core Attributes
Engaged
Enterprising
Ethical

Key Attitudes
Commitment
Curiosity
Resilience
Confidence
Adaptability

Practical Skillsets
Digital Fluency
Organisation
Critical Thinking
Communication