Module Descriptor

Title	Digital Forensic Analysis		
Session	2025/26	**Status**	Published
Code	COMP09107	**SCQF Level**	9
Credit Points	20	**ECTS (European Credit Transfer Scheme)**	10
School	**Computing, Engineering and Physical Sciences**		
Module Co-ordinator	Dr Babak Habibnia		

Summary of Module

This module aims to provide both broad and specialized knowledge of the fundamental principles of digital forensics, focusing on its application in computer crime scene investigations. Students will learn a systematic and impartial approach to the preservation and extraction of all digital evidence.

Learning Objectives

- Practical Knowledge: Gain practical knowledge about hardware and operating systems.
- Theoretical Foundations: Learn principles, theories, and technical skills for analysing and evaluating digital evidence using forensic tools and techniques.
- Case Study Application: Reinforce learning through practical case studies to achieve a comprehensive understanding of the subject matter.

Ethical and Professional Integration

Throughout the curriculum, ethical and professional issues will be integrated into the learning experience. This approach fosters a strong understanding of the importance of ethical conduct and professionalism, preparing students to be responsible practitioners in their future careers.

Development of Graduate Attributes

This module will work to develop key 'I am UWS' Graduate Attributes in students, ensuring that those who complete the module are:

Universal Attributes

- Critical Thinker
- Ethically minded
- Research-minded

Work Ready Attributes

- Problem-Solver
- Effective Communicator
- Ambitious

Successful Attributes

- Autonomous
- Resilient
- Driven

Key Topics

- Practical issues related to hardware and operating systems.
- Principles, theories, and technical skills for analyzing and evaluating digital evidence.
- Hands-on experience with forensic tools and techniques through various practical case studies.

This module prepares students for a successful career in digital forensics, equipping them with the necessary skills, knowledge, and ethical framework to excel in the field.

Module Delivery Method	**On-Campus**[1] ☒	**Hybrid**[2] ☒	**Online**[3] ☐	**Work -Based Learning**[4] ☐
Campuses for Module Delivery	☐ Ayr ☒ Dumfries	☒ Lanarkshire ☒ London ☐ Paisley	☐ Online / Distance Learning ☒ Other (specify) WTU	

Terms for Module Delivery	Term 1	☒	Term 2	☐	Term 3	☐
Long-thin Delivery over more than one Term	Term 1 – Term 2	☐	Term 2 – Term 3	☐	Term 3 – Term 1	☐

Learning Outcomes	
L1	Demonstrate a critical understanding of the principal theories, concepts, and principles of digital forensics, focusing on the significance of operating system artefacts as digital evidence. This includes articulating foundational theories, exploring key concepts such as chain of custody and data integrity, and analyzing how operating system artefacts can reconstruct user activity and system events, ultimately applying these principles in practical forensic investigations;
L2	Utilize forensic tools for the collection and analysis of digital evidence, while critically evaluating these tools and techniques to validate results. This involves applying various forensic software and methodologies to ensure accurate data retrieval, assessing the effectiveness and reliability of the tools used, and implementing validation techniques to confirm the integrity and authenticity of the collected evidence;

[1] Where contact hours are synchronous/ live and take place fully on campus. Campus-based learning is focused on providing an interactive learning experience supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus contact hours will be clearly articulated to students.

[2] The module includes a combination of synchronous/ live on-campus and online learning events. These will be supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus and online contact hours will be clearly articulated to students.

[3] Where all learning is solely delivered by web-based or internet-based technologies and the participants can engage in all learning activities through these means. All required contact hours will be clearly articulated to students.

[4] Learning activities where the main location for the learning experience is in the workplace. All required contact hours, whether online or on campus, will be clearly articulated to students

L3	Plan, undertake, and report on a thorough digital forensic analysis by developing a structured approach that includes defining the scope of the investigation, applying appropriate forensic methodologies, and systematically documenting each step of the process. This outcome emphasizes the importance of clear reporting, ensuring that findings are presented in a coherent and comprehensive manner, suitable for both technical and non-technical audiences, while adhering to legal and ethical standards in digital forensics;
L4	Explain the legal and ethical requirements for gathering forensic evidence and conduct forensic examinations in an ethical, legal, and professional manner. This includes understanding relevant laws and regulations governing digital forensics, adhering to best practices for evidence collection and preservation, and maintaining integrity and objectivity throughout the examination process. Emphasizing the importance of ethical conduct, this outcome prepares students to navigate complex legal landscapes while ensuring that their forensic practices uphold professional standardsr;
L5	Critically reflect on forensic literature and quality information sources by evaluating the credibility, relevance, and applicability of various academic and professional resources in the field of digital forensics. This involves analyzing current research, methodologies, and best practices, while distinguishing between reliable sources and misinformation. By fostering a critical perspective, students will enhance their ability to make informed decisions and contribute to the ongoing development of knowledge within the discipline.

Employability Skills and Personal Development Planning (PDP) Skills	
SCQF Headings	**During completion of this module, there will be an opportunity to achieve core skills in:**
Knowledge and Understanding (K and U)	**SCQF 9** • Comprehensive Knowledge: Gain a thorough understanding of the scope and defining characteristics of digital forensics, including its main areas and boundaries. • Critical Understanding: Develop a critical understanding of the principles, key theories, concepts, and terminology associated with digital forensics
Practice: Applied Knowledge and Understanding	**SCQF 9** • Application of Techniques: Utilize key skills, techniques, and practices related to digital forensics effectively in various scenarios. • Routine Methods of Inquiry: Engage in routine methods of inquiry to investigate and analyze digital evidence systematically. • Adaptability in Contexts: Practice in a range of contexts that incorporate a degree of unpredictability, enhancing problem-solving abilities and adaptability in real-world situations.
Generic Cognitive skills	**SCQF 9** • Critical Analysis: Undertake critical analysis, evaluation, and synthesis of ideas, concepts, information, and issues within the field of digital forensics. • Problem Identification: Identify and analyze routine professional problems and issues related to digital forensics practices. • Informed Judgements: Draw on a diverse range of sources to inform judgments and decision-making processes in the context of digital forensics.

Communication, ICT and Numeracy Skills	**SCQF 9** • Diverse Skill Application: Utilize a wide range of skills to support established practices in digital forensics. • Information Presentation: Present or convey information about relevant topics to informed audiences, both formally and informally, ensuring clarity and engagement. • Data Interpretation and Evaluation: Interpret, use, and evaluate data effectively, drawing meaningful conclusions to support forensic investigations and analyses.
Autonomy, Accountability and Working with Others	**SCQF 9** • Autonomy and Initiative: Exercise autonomy and initiative in various activities related to digital forensics, demonstrating self-direction and proactive engagement. • Ethical and Professional Management: Manage complex ethical and professional issues following established ethical codes and practices, ensuring integrity and accountability in all forensic activities.

Prerequisites	**Module Code** COMP08074	**Module Title** Operating Systems
	Other	
Co-requisites	**Module Code**	**Module Title**

Learning and Teaching
In line with current learning and teaching principles, a 20-credit module includes 200 learning hours, normally including a minimum of 36 contact hours and maximum of 48 contact hours. This module adopts a hands-on, active learning approach, utilizing a variety of complementary methods, including lectures, seminars, practical sessions, research on current developments, and case studies. Learning Framework • Introduction of Topics: Core subjects will be introduced in lectures and further explored through guided inquiry and problem-based learning activities. • Theoretical Reinforcement: Theoretical concepts will be reinforced through the critical analysis and discussion of case studies in tutorials, designed to elaborate on both theoretical and laboratory content. • Real-World Application: Students will navigate real-world scenarios through structured inquiry-based learning, enhancing their practical skills. Directed Learning • Directed learning activities will strengthen understanding of essential theories and contextualize knowledge within the discipline. Industry Engagement • An industry lecture series will present insights from practitioners across various sectors, highlighting current practices, approaches, and challenges in the field. Independent Learning • As the subject area is continually evolving, students are expected to stay updated through independent study. They will be encouraged to develop an independent learning style,

acquiring and applying knowledge through personal inquiry, supported by guided activities and exercises.

Collaborative Learning

• Students will have opportunities to share their findings through seminar presentations and engage in online discussions with their peers, promoting a collaborative learning environment.

Overview

• This module equips students with the necessary skills and knowledge to effectively analyze and evaluate digital evidence, preparing them for success in the dynamic field of digital forensics.

Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture / Core Content Delivery	12
Tutorial / Synchronous Support Activity	12
Laboratory / Practical Demonstration / Workshop	24
Independent Study	152
Please select	
Please select	
TOTAL	200

Indicative Resources

The following materials form essential underpinning for the module content and ultimately for the learning outcomes:

• C. Altheide and H. Carvey (2011) Digital Forensics with Open Source Tools. Elsevier.

• K. Jones, R. Betjlich. (2012), Real Digital Forensics, Volume 2, Addison-Wesley. T.J. O'Connor. (2012), Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers, Syngress publisher.

• B. CArrier (2005), File System ForensicAnalysis.

• E. Casey. (2011), Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press.

• J. Seitz. (2009), Python Programming for Hackers and Reverse Engineers,.

• S. Anson, S. Bunting. (2007), Mastering Windows network forensic investigation, Wiley, Indianapolis, Ind.

• B. Nelson, A. Phillips, C. Steuart. (2009), Guide to Computer Forensics and Investigation.

(N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)

Attendance and Engagement Requirements

In line with the Student Attendance and Engagement Procedure, Students are academically engaged if they are regularly attending and participating in timetabled on-campus and online teaching sessions, asynchronous online learning activities, course-related learning resources, and complete assessments and submit these on time.

For the purposes of this module, academic engagement equates to the following:

The School of Computing, Engineering and Physical Sciences considers attendance and engagement to mean a commitment to attending, and engaging in, timetabled sessions. You will scan your attendance via the scanners each time you are on-campus and you will login to the VLE several times per week. Where you are unable to attend a timetabled learning session due to illness or other circumstance, you should notify the Programme Leader that you cannot attend. Across the School an 80% attendance threshold is set. If you fall below this, you will be referred to the Student Success Team to see how we can best support your studies.

Equality and Diversity
The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: UWS Equality, Diversity and Human Rights Code. Aligned with the University's commitment to equality and diversity, this module supports equality of opportunity for students from all backgrounds and learning needs. Using the VLE, material will be presented electronically in formats that allow flexible access and manipulation of content. This module complies with University regulations and guidance on inclusive learning and teaching practice. This module has lab-based teaching and as such you are advised to speak to the Module Co-ordinator to ensure that specialist assistive equipment, support provision and adjustment to assessment practice can be put in place, in accordance with the University's policies and regulations.
(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)

Supplemental Information

Divisional Programme Board	**Computing**
Overall Assessment Results	☐ **Pass / Fail** ☒ **Graded**
Module Eligible for Compensation	☒ **Yes** ☐ **No** **If this module is eligible for compensation, there may be cases where compensation is not permitted due to programme accreditation requirements. Please check the associated programme specification for details.**
School Assessment Board	Business & Applied Computing
Moderator	Raman Singh
External Examiner	M Davis
Accreditation Details	
Module Appears in CPD catalogue	☒ **Yes** ☐ **No**
Changes / Version Number	1.1

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1

Examination Record - Logbook (40%)
Assessment 2
A Practical Assessment - Analysis Report + Presentation (60%) - Students will be required to perform an appropriate forensic analysis based on a given scenario and raw data and required to present the outputs and findings in a formal written report.
Assessment 3
(N.B. (i) Assessment Outcomes Grids for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed. (ii) An indicative schedule listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Module Handbook.)

Component 1							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Logbook (practical)	☒	☒	☒	☒	☒	40	2

Component 2							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Report of pratical/field/analysis + Presentation	☒	☒	☒	☒	☐	60	8

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
	☐	☐	☐	☐	☐		
Combined total for all components						100%	10 hours

Change Control

What	**When**	**Who**
Attendance and Engagement and Equality and Diversity Statements	20/01/25	R Moffat