**Module Descriptor**

| | | | |
|---|---|---|---|
| **Title** | Advanced Digital Forensic Analysis | | |
| **Session** | 2025/26 | **Status** | Published |
| **Code** | COMP10073 | **SCQF Level** | 10 |
| **Credit Points** | 20 | **ECTS (European Credit Transfer Scheme)** | 10 |
| **School** | **Computing, Engineering and Physical Sciences** | | |
| **Module Co-ordinator** | Dr Babak Habibnia | | |

**Summary of Module**

Module Overview: Advanced Digital Forensic Analysis

This module provides students with a comprehensive understanding of the essential theories, concepts, and principles necessary for investigating digital crime incidents effectively.

Key Areas of Focus:

1. Advanced Specialist Knowledge

- Network Forensics: Techniques for analyzing and interpreting network traffic.
- Memory Analysis: Methods for examining volatile memory to extract evidence.
- Malware Forensics: Strategies for dissecting malware to understand its functionality and impact.
- Embedded Systems: Investigating digital devices integral to modern technology.

2. Practical Case Studies

- Evaluation of real-world applications of forensic techniques.
- Hands-on experiences reinforcing theoretical knowledge.

3. Evolving Landscape of Digital Crime

- Exploration of emerging threats in digital crime.
- Forensic strategies used by law enforcement and government agencies.

4. Digital Forensic Investigation Procedures

- Insight into the steps involved in conducting a digital forensic investigation through case studies and hypothetical scenarios.

5. Ethical and Professional Responsibilities

- Emphasis on the ethical and professional standards required in the field.
- Integration of ethical considerations throughout the curriculum to prepare responsible practitioners.

Independent Learning and Collaboration

- Continuous Development: Encouraging students to stay updated with the latest advancements.

- Independent Learning Style: Guidance on developing an inquiry-based approach to knowledge.

- Collaborative Learning: Opportunities to share findings through seminars and online discussions, fostering peer interaction and collaboration.

Key Topics

- Principles, Theories, and Technical Skills: Focus on analyzing and evaluating digital evidence.

- Guided Activities: Exercises designed to enhance understanding and application of forensic techniques.

Development of Graduate Attributes

The module aims to develop key attributes aligned with the “I am UWS” framework:

- Universal Attributes
- Critical Thinker: Ability to analyze complex scenarios critically.
- Ethically Minded: Commitment to ethical practices in forensic investigations.
- Research-Minded: Engagement in research to inform and enhance practice.
- Work Ready Attributes
- Problem-Solver: Developing innovative solutions to forensic challenges.
- Effective Communicator: Proficiency in articulating findings and insights clearly.
- Ambitious: Drive for personal and professional growth.
- Successful Attributes
- Autonomous: Ability to work independently and take initiative.
- Resilient: Capacity to handle challenges and adapt to change.
- Driven: Motivation to achieve excellence in the field.

This module is designed to equip students with the necessary skills and knowledge to navigate the complexities of digital crime investigation. By integrating ethical considerations and fostering both independent and collaborative learning, students will be well-prepared to become responsible, effective practitioners in the field of digital forensics.

| **Module Delivery Method** | **On-Campus**[1] | **Hybrid**[2] | **Online**[3] | **Work -Based Learning**[4] |
|---|---|---|---|---|
| | ☒ | ☒ | □ | □ |

[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

| | | | |
|---|---|---|---|
| **Campuses for Module Delivery** | □ Ayr<br>□ Dumfries | ☒ Lanarkshire<br>□ London<br>☒ Paisley | □ Online / Distance Learning<br>□ Other (specify) |

| | | | | | | |
|---|---|---|---|---|---|---|
| **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** | Digital forensics is grounded in key theories and principles:<br>1. Chain of Custody ensures the integrity and admissibility of evidence in court.<br>2. Digital Evidence Theory emphasizes the importance of preserving data in its original state.<br>3. Incident Response Frameworks offer structured approaches for managing cybersecurity incidents.<br>4. Forensic Analysis Models provide systematic methods for evidence collection and reporting.<br>5. Legal and Ethical Principles govern data privacy and ensure responsible practices.<br>A solid understanding of these concepts is crucial for conducting effective and credible forensic investigations. |
| **L2** | Critical Analysis and Evaluation of Forensic Evidence:<br>1. Source Verification ensures the credibility of evidence from digital devices and logs.<br>2. Data Integrity checks for tampering using hashing algorithms.<br>3. Contextual Analysis examines the circumstances under which data was collected.<br>4. Corroboration strengthens evidence by cross-referencing multiple sources.<br>5. Legal Considerations ensure compliance with data privacy laws and evidence admissibility.<br>6. Expert Interpretation provides deeper insights through specialized knowledge.<br>This structured approach is vital for ensuring accurate and reliable conclusions in forensic investigations. |
| **L3** | Digital Forensic Analysis Process:<br>1. Planning: Define objectives, determine the scope, and gather necessary resources.<br>2. Development: Create a forensic strategy and establish protocols for evidence handling.<br>3. Execution: Acquire data using forensic tools, analyze it, and document findings.<br>4. Formal Documentation: Compile a comprehensive report that summarizes methods, findings, and includes relevant evidence.<br>This structured approach ensures thorough, accurate, and legally sound digital forensic analysis. |
| **L4** | Legal and Ethical Requirements in Forensic Evidence Collection<br>Legal Requirements: |

| | |
|---|---|
| | 1. Admissibility: Collect evidence in compliance with legal standards to ensure its admissibility in court.<br>2. Chain of Custody: Maintain a documented chain of custody to preserve the integrity of evidence.<br>3. Search Warrants: Secure the necessary legal permissions before accessing data.<br>Ethical Requirements:<br>1. Privacy Considerations: Respect privacy rights and comply with data protection laws.<br>2. Informed Consent: Obtain consent from individuals involved when applicable.<br>3. Integrity: Conduct examinations objectively and report findings truthfully.<br>Forensic Examinations:<br>1. Standard Protocols: Follow established methodologies to ensure consistency and reliability.<br>2. Documentation: Record all steps and findings throughout the examination process.<br>3. Professional Standards: Stay up-to-date with legal and ethical guidelines in the field. |
| **L5** | Critical Evaluation of Forensic Literature:<br>1. Relevance and Scope: Focus on current trends and methodologies in digital forensics.<br>2. Quality of Sources: Prioritize peer-reviewed journals for credible and authoritative information.<br>3. Consistency of Findings: Compare studies to identify consistent results and methodological rigor.<br>4. Reliability of Information: Examine data sources and author credentials to assess trustworthiness.<br>5. Emerging Trends: Evaluate literature on new technologies and future research directions.<br>This approach ensures reliance on robust evidence and methodologies, supporting effective forensic practice. |

| **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 10**<br>This approach ensures reliance on strong evidence and methodologies, fostering effective forensic practices. Legal and ethical guidelines maintain responsible investigations, while key terminology like digital evidence, forensic images, and hashing aids in communication and documentation. Reporting standards and presentation protocols ensure proper documentation for court. Theoretical frameworks such as digital evidence and incident response theories guide practices, with concepts like attribution and data integrity bolstering evidence credibility. Emerging technologies like cloud computing and IoT, alongside cybersecurity integration, are shaping digital forensics. Ongoing research and collaboration between academia, industry, and law enforcement drive the discipline forward, enhancing investigative effectiveness. |

| | |
|---|---|
| **Practice: Applied Knowledge and Understanding** | **SCQF 10**<br>Digital forensics uses advanced techniques to investigate digital evidence, including data recovery, forensic imaging, and network analysis. Key methods involve file carving, bit-by-bit imaging, packet sniffing, and malware reverse engineering. Memory forensics helps recover active processes from RAM, while cryptography and hashing maintain data integrity and facilitate access to encrypted information. Legal and ethical practices, such as ensuring chain of custody, are vital for preserving evidence credibility. Strong reporting skills are crucial for presenting findings in court. Mastery of these techniques ensures effective, legally sound investigations. |
| **Generic Cognitive skills** | **SCQF 10**<br>Digital forensics addresses complex issues like data breaches and cybercrime by clearly defining problems and breaking them into manageable parts. Professionals analyze attack methods and legal implications, offering tailored solutions through creative problem-solving, particularly with challenges like encrypted data. Staying current with research and collaborating with peers is crucial for improving knowledge and practices. In scenarios with limited data, assessing the reliability of sources and exercising informed judgment are key. Effective digital forensics depends on critical thinking, creativity, and analytical skills to navigate challenges and enhance investigative outcomes. |
| **Communication, ICT and Numeracy Skills** | **SCQF 10**<br>Digital forensics utilizes advanced techniques such as data recovery, forensic imaging, malware analysis, and network forensics to uncover and preserve digital evidence. Mastery of these skills allows practitioners to tackle complex cases while adhering to legal and ethical standards. Effective communication is key when presenting specialized information to both expert and lay audiences, requiring professionals to tailor their language to the audience's level of understanding. Evaluating data from various sources is also crucial, as practitioners must assess its reliability and draw conclusions that support investigations. This blend of technical expertise and clear communication ensures that forensic findings are presented accurately and persuasively. |
| **Autonomy, Accountability and Working with Others** | **SCQF 10**<br>In digital forensics, exercising autonomy and initiative is crucial for effectively managing investigations and tackling complex challenges. Professionals often work independently, making critical decisions about their analyses and the tools they use. This autonomy allows them to adapt to evolving situations, implement innovative solutions, and respond quickly to emerging threats.<br>Equally important is handling complex ethical and professional issues. Practitioners must navigate legal constraints, privacy concerns, and the potential implications of their findings. Upholding ethical standards, such as maintaining the chain of custody and ensuring data integrity, is vital for preserving the credibility of their work. By exercising sound judgment and adhering to ethical guidelines, professionals balance investigative demands with their responsibilities to the law and society. This combination of initiative and ethical management is essential for successful outcomes in digital forensics. |

| | | |
|---|---|---|
| **Prerequisites** | **Module Code**<br>COMP09107 | **Module Title** Digital Forensic Analysis |

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

**Indicative Resources**

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

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

- Cory Altheide and Harlan Carvey. (2011) Digital Forensics with Open Source Tools (1st Ed.). Syngress Publishing.
- Gerard Johansen. (2017) Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents. Packt Publishing.
- David Watson. (2013) Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements. Syngress Publishing.

- Cory Altheide and Harlan Carvey. (2011) Digital Forensics with Open Source Tools (1st Ed.). Syngress Publishing.
- Gerard Johansen. (2017) Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents. Packt Publishing.
- David Watson. (2013) Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements. Syngress Publishing.

**(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**<br>**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** | 1.07 |

| **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.<br>(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 | 10 |

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

**Change Control**

| **What** | **When** | **Who** |
|---|---|---|
| Attendance and Engagement and EDI statements updated | 20/01/2025 | F Valentine |
| | | |
| | | |

|  |  |  |
|---|---|---|
|  |  |  |