澳門理工大學
Universidade Politécnica de Macau
Macao Polytechnic University

FACULTY OF APPLIED SCIENCES

BACHELOR OF SCIENCE IN COMPUTING

LEARNING MODULE OUTLINE

Academic Year	2025/2026	Semester	2
Module Code	COMP402		
Learning Module	Computer Forensics		
Pre-requisite(s)	Nil		
Medium of Instruction	English		
Credits	3	Contact Hours	45 hrs
Instructor	Wilson Ho	Email	kcho@mpu.edu.mo
Office	A216, Chi-Un building	Office Phone	85996586

MODULE DESCRIPTION

Computer forensics is the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. This module enables students to draw on an array of methods for discovering and analysing data that resides in a computer system, or recovering deleted, encrypted, or damaged file information. This module will also provide students with the necessary skills to identify an intruder’s footprints and to properly gather the necessary evidence.

MODULE INTENDED LEARNING OUTCOMES (ILOS)

On completion of this learning module, students will be able to:

M1.	Tell basics concepts of digital forensic science; (EA2p)
M2.	Develop an understanding of the rules of evidence and the importance of the chain of custody; (ET1p, ET5p)
M3.	Organize and analyze computer forensic evidence. (EA2p, ET5p, EP3p, EP8p)
M4.	Apply a number of different computer forensic tools to extract and analyze digital evidence. (ET1p, ET5p, EP8p)

These ILOs aims to enable students to attain the following Programme Intended Learning Outcomes (PILOs):

PILOs	M1	M2	M3	M4
P1. Select and apply proven methods, tools and techniques to the effective and efficient implementation of information systems;				

P2. Evaluate computer systems in a local area network, and understand the additional requirements for connection to other networks through wide area networks;				
P3. Be competent in system development in the Internet and the web platform;				
P4. Work independently to design and implement a relational database, with an emphasis on how to organise, maintain and retrieve information from a DBMS;				
P5. Acquire essential knowledge in specific fields of computing disciplines including multimedia, security and artificial intelligence;	✓	✓	✓	✓
P6. Acquire the perceptive skills needed to understand information presented in the form of UML diagram, flow chart or other industry standard formats;				
P7. Understand the need for and use of the necessary mathematical techniques;				
P8. Work independently to develop an understanding of, and the knowledge and skills associated with the general support of computer systems and networks;	✓	✓	✓	✓
P9. Work as an effective member of a team in the analysis, design and development of software systems;				
P10. Use project planning and management techniques in systems development;				
P11. Understand the fundamental and operational issues of computer systems in business environments;				
P12. Equip with adequate written, oral communication and interpersonal skills;				
P13. Build the capacity and desire for lifelong learning and to learn advanced and emerging technologies on one's own;				
P14. (For Enterprise Information Systems specialisation) Gain an in-depth understanding of the information technology related to enterprise information systems, with an emphasis on development of such systems to support business processes;	✓	✓	✓	✓
P15. (For Gaming Technology specialisation) Acquire the general and advanced knowledge of current technologies and operating environment in the gaming industry;				
P16. (For Computer Education specialization) Acquire the general and practical knowledge of computer education and its practicing environment in secondary education.				

MODULE SCHEDULE, COVERAGE AND STUDY LOAD

Week	Content Coverage	Contact Hours
1	1. Understanding the Digital Forensics Profession and Investigations	4.5
	1.1 An overview of Digital Forensics	
	1.2 Preparing for Digital Investigations	
	1.3 Maintaining Professional Conduct	
	1.4 Preparing a Digital Forensics Investigation	
	1.5 Procedures for Private-Sector High-Tech Investigations	
	1.6 Understanding Data Recovery Workstations and Software	
	1.7 Conducting an Investigation	
2	2. Report Writing and Testimony for Digital Investigations	3
	2.1 Understanding the Importance of Reports With a View to Testifying	
	2.2 Guidelines for Writing Reports	
	2.3 Generating Report Findings and Writing the Digital Forensics Report	
	2.4 Preparing for Testimony	
	2.5 Testifying in Court and Depositions	
3	3. The Investigator’s Laboratory and Digital Forensics Tools	3
	3.1 Understanding Forensics Lab Accreditation Requirements	
	3.2 Determining the Physical Requirements for a Computer Forensics Lab	
	3.3 Selecting a Basic Forensic Workstation	
	3.3 Building a Business Case for Developing a Forensics Lab	
	3.4 Evaluating Digital Forensics Tools	
	3.5 Digital Forensics Software Tools	
	3.6 Digital Forensics Hardware Tools	
	3.7 Validating and Testing Forensics Software	
4	4 Data Acquisition	4.5
	4.1 Understanding Storage Formats for Digital Evidence	
	4.2 Acquisition Planning	
	4.3 Contingency Planning for Image Acquisitions	

	4.4 Using Acquisition Tools	
	4.5 Validating Data Acquisitions	
	4.6 Performing RAID Data Acquisitions	
	4.7 Using Other Forensics Acquisition Tools	
5	5 Processing Crime and Incident Scenes	3
	5.1 Identifying Digital Evidence	
	5.2 Collecting Evidence at Private-Sector Incident Scenes	
	5.3 Processing Law Enforcement Crime Scenes	
	5.4 Preparing for a Search	
	5.5 Securing a Computer Incident or Crime Scene	
	5.6 Seizing Digital Evidence at the Scene	
	5.7 Archival Storage and Transportation of Digital Evidence	
	5.8 Obtaining a Digital Hash	
	5.9 Employee Compliance Investigations	
6	6 Working with Microsoft File Systems and the Windows Registry	3
	6.1 Understanding File Systems	
	6.2 Exploring Microsoft File Structures	
	6.3 Examining FAT Disks	
	6.4 Exploring NTFS Disks	
	6.5 Understanding Whole Disk Encryption	
	6.6 Understanding the Windows Registry	
	6.7 Windows Forensics Artifacts	
7	7 Linux and Macintosh File Systems	3
	7.1 Examining Linux File Structures	
	7.2 Understanding Macintosh File Structures	
	7.3 Using Linux Forensics Tools	
8	8 Media Files and Digital Forensics	3
	8.1 Media Files	
	8.2 Data Compression and Obfuscation	

	8.3 Additional Data-Hiding Techniques	
	8.4 Digital Evidence Validation and Discrimination	
	8.5 Examination Planning	
9	9 Virtual Machine Forensics and Live Acquisitions Forensics	3
	9.1 An Overview of Virtual Machine Forensics	
	9.2 Performing Live Acquisitions	
	9.3 Remote Acquisition Tools	
10	10 Network Forensics	3
	10.1 Network Forensics Overview	
	10.2 Exploring Common Network Forensics Tools	
	10.3 Investigating Virtual Networks	
	10.4 Researching and Investigating Types of Attacks	
11	11 Cloud Forensics and the Internet of Anything	3
	11.1 An Overview of Cloud Computing	
	11.2 Technical Challenges in Cloud Forensics	
	11.3 Conducting a Cloud Investigation	
	11.4 An Overview of the Internet of Things, the Internet of Anything, and the Internet of Everything Technologies Supporting the Growth of the Internet of Things	
	11.5 Categories of the Internet of Anything	
12	12 Mobile Device Forensics	3
	12.1 Understanding Mobile Devices and Cellular Networks	
	12.2 Mobile Device Evidence Sources	
	12.3 Mobile Device Security	
	12.4 Seizing and Securing Mobile Devices	
	12.5 Mobile Device Evidence Extraction and Examination	
	12.6 Mobile Device Forensics Tools	
13	13 E-mail and Social Media Investigations	3
	13.1 Exploring the Role of E-mail in Investigations	
	13.2 Exploring the Client and Server Roles in Email	
	13.3 Investigating E-mail Crimes and Violations	

	13.4 Understanding Email Servers and Server Logs	
	13.5 Using Specialized Email Forensics Tools	
14	14 e-Discovery	3
	14.1 Overview of e-Discovery, Rules, and Policies	
	14.2 The Impact of Case Law on e-Discovery	
	14.3 EDRM and e-Discovery Case Flow	
	14.4 Common e-Discovery Tools	

TEACHING AND LEARNING ACTIVITIES

In this learning module, students will work towards attaining the ILOs through the following teaching and learning activities:

Teaching and Learning Activities	M1	M2	M3	M4
T1. Lectures	✓	✓	✓	✓
T2. In-class exercises	✓	✓	✓	✓

ATTENDANCE

Attendance requirements are governed by the Academic Regulations Governing Bachelor's Degree Programmes of the Macao Polytechnic University. Students who do not meet the attendance requirements for the learning module shall be awarded an 'F' grade.

ASSESSMENT

In this learning module, students are required to complete the following assessment activities:

Assessment Activities	Weighting (%)	AHEP3 LOs	ILOs to be Assessed
A1. Assignments	40%	EA2p, ET5p, EP3p, EP8p	M1, M2, M3, M4
A2. Test	20%	EA2p, ET1p, ET5p	M1, M2, M3,
A3. Examination	40%	EA2p, ET1p, ET5p	M1, M2, M3

The assessment will be conducted following the University's Assessment Strategy (see www.mpu.edu.mo/teaching_learning/en/assessment_strategy.php). Passing this learning module indicates that students will have attained the ILOs of this learning module and thus acquired its credits.

Students with an overall score of less than 35 in the coursework must take the re-sit examination even if the overall score for the module is 50 or above.

Students with a score of less than 35 in the final examination must take the re-sit examination even if the overall score for the module is 50 or above.

Students with an overall final grade of less than 35 are NOT allowed to take the re-sit examination.

REQUIRED READINGS

1. Nelson, B., Phillips, A., & Steuart, C. (2025). *Guide to Computer Forensics and Investigations* (7th ed.). Cengage Learning.

REFERENCES

1. Oettinger, W. (2020). *Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence*. Packt Publishing.
2. Tamma, R. (2020). *Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices* (4th ed.). Packt Publishing.

STUDENT FEEDBACK

At the end of every semester, students are invited to provide feedback on the learning module and the teaching arrangement through questionnaires. Your feedback is valuable for instructors to enhance the module and its delivery for future students. The instructor and programme coordinators will consider all feedback and respond with actions formally in the annual programme review.

ACADEMIC INTEGRITY

The Macao Polytechnic University requires students to have full commitment to academic integrity when engaging in research and academic activities. Violations of academic integrity, which include but are not limited to plagiarism, collusion, fabrication or falsification, repeated use of assignments and cheating in examinations, are considered as serious academic offenses and may lead to disciplinary actions. Students should read the relevant regulations and guidelines in the Student Handbook which is distributed upon the admission into the University, a copy of which can also be found at www.mpu.edu.mo/student_handbook/.