Macao Polytechnic University

Faculty of Applied Sciences

Bachelor of Science in Computing

Module Outline

Academic Year 2022/2023 Semester 2

Learning Module	Computer Forensics			**Class Code**	COMP402
Pre-requisite(s)	Nil				
Medium of Instruction	English			**Credit**	3
Lecture Hours	39 hrs	**Lab/Practice Hours**	6 hrs	**Total Hours**	45 hrs
Instructor	Wilson Ho		**E-mail**	kcho@mpu.edu.mo	
Office	A216, Chi-Un Building, Main Campus		**Telephone**	8599-6586	

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.

Learning Outcomes

After completing the learning module, students will be able to:

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

Content

1. Understanding the Digital Forensics Profession and Investigations (4.5 hours)
    - 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. The Investigator's Office and Laboratory (3 hours)
    - 2.1 Understanding Forensics Lab Accreditation Requirements
    - 2.2 Determining the Physical Requirements for a Computer Forensics Lab
    - 2.3 Selecting a Basic Forensic Workstation
    - 2.4 Building a Business Case for Developing a Forensics Lab
3. Data Acquisition (3 hours)
    - 3.1 Understanding Storage Formats for Digital Evidence
    - 3.2 Determining the Best Acquisition Method
    - 3.3 Contingency Planning for Image Acquisitions
    - 3.4 Using Acquisition Tools
    - 3.5 Validating Data Acquisitions
    - 3.6 Performing RAID Data Acquisitions
    - 3.7 Using Remote Network Acquisition Tools
    - 3.8 Using Other Forensics Acquisition Tools

4. Processing Crime and Incident Scenes (3 hours)
    4.1 Identifying Digital Evidence
    4.2 Collecting Evidence in Private-Sector Incident Scenes
    4.3 Processing Law Enforcement Crime Scenes
    4.4 Preparing for a Search
    4.5 Securing a Computer Incident or Crime Scene
    4.6 Seizing Digital Evidence at the Scene
    4.7 Storing Digital Evidence
    4.8 Obtaining a Digital Hash
    4.9 Reviewing a Case
5. Working with Windows and CLI Systems (3 hours)
    5.1 Understanding File Systems
    5.2 Exploring Microsoft File Structures
    5.3 Examining NTFS Disks
    5.4 Understanding Whole Disk Encryption
    5.5 Understanding the Windows Registry
    5.6 Understanding Microsoft Startup Tasks
    5.7 Understanding Virtual Machines
6. Current Digital Forensics Tools (3 hours)
    6.1 Evaluating Computer Forensics Tool Needs
    6.2 Computer Forensics Software Tools
    6.3 Computer Forensics Hardware Tools
    6.4 Validating and Testing Forensics Software
7. Linux and Macintosh File Systems (3 hours)
    7.1 Examining Linux File Structures
    7.2 Understanding Macintosh File Structures
    7.3 Using Linux Forensics Tools

8. Recovering Graphics Files (3 hours)
    8.1 Recognizing a Graphics File
    8.2 Understanding Data Compression
    8.3 Locating and Recovering Graphics Files
    8.4 Identifying Unknown File Formats
    8.5 Understanding Copyright Issues with Graphics
9. Digital Forensics Analysis and Validation (4.5 hours)
    9.1 Determining What Data to Collect and Analyze
    9.2 Validating Forensic Data
    9.3 Addressing Data-Hiding Techniques
10. Virtual Machine Forensics Live Acquisitions and Network Forensics (3 hours)
    10.1 An Overview of Virtual Machines Forensics
    10.2 Performing Live Acquisitions
    10.3 Network Forensics Overview
11. E-mail and Social Media Investigations (3 hours)
    11.1 Exploring the Role of E-mail in Investigations
    11.2 Exploring the Roles of the Client and Server in E-mail
    11.3 Investigating E-mail Crimes and Violations
    11.4 Understanding E-mail Servers
    11.5 Using Specialized E-mail Forensics Tools
12. Mobile Device Forensics (3 hours)
    12.1 Understanding Mobile Device Forensics
    12.2 Understanding Acquisition Procedures for Mobile Devices

13. Cloud Forensics (3 hours)

13.1 An Overview of Cloud Computing

13.2 Legal Challenges in Cloud Forensics

13.3 Technical Challenges in Cloud Forensics

13.4 Acquisitions in the Cloud

13.5 Conducting a Cloud Investigation

13.6 Tools for Cloud Forensics

14. Report Writing for High-Tech Investigations (3 hours)

14.1 Understanding the Importance of Reports

14.2 Guidelines for Writing Reports

14.3 Generating Report Findings with Forensics Software Tools

Teaching Method

Lectures, lab practice and tutorials

Attendance

Attendance requirements are governed by the "Academic Regulations Governing Bachelor's Degree Programmes" of Macao Polytechnic Institute. Students who do not meet the attendance requirements for the module will not be permitted to sit the final or re-sit examination and shall be awarded an 'F' grade.

Assessment

This learning module is graded on a 100 point scale, with 100 being the highest possible score and 50 being the passing score.

	Item	Description	AHEP3 LO	Percentage
1.	Assignment(s)	Home-based exercises	EA2p, ET5p, EP3p,EP8p	40%
2.	Test	Knowledge assessment	EA2p, ET1p, ET5p	20%
3.	Examination	3-hour written examination	EA2p, ET1p, ET5p	40%
			Total Percentage:	100%

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.

Teaching Material

Textbook(s)

1. Nelson, B., Phillips, A., & Steuart, C. (2018). *Guide to Computer Forensics and Investigations* (6th ed.). Course Technology.

Reference

Reference book(s)

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.