

Welcome & Administrative Matters

MSCS 630: Cybercrime Investigation and Digital Evidence

Dr. Mouatez Karbab



أكاديمية جوعان بن جاسم للدراسات الدفاعية
Joaan Bin Jassim Academy for Defence Studies

October 1, 2026



Outline

- 1 Course
- 2 Learning Materials
- 3 Methodology
- 4 Assessment and Grading
- 5 Course Schedule



Outline

- 1 Course
- 2 Learning Materials
- 3 Methodology
- 4 Assessment and Grading
- 5 Course Schedule



Course Information

Course:	Cybercrime Investigation and Digital Evidence
Code:	MSCS 630
Program:	Master of Science in Cyber Defense
Type:	Compulsory
Credit:	3
Hours:	Thursdays 8:00-11:00
Room:	Lab Room
Webpage:	https://courses.karbab.net/mscs630/
Instructor:	Dr. ElMouatez Billah Karbab
Email:	mouatez@karbab.net



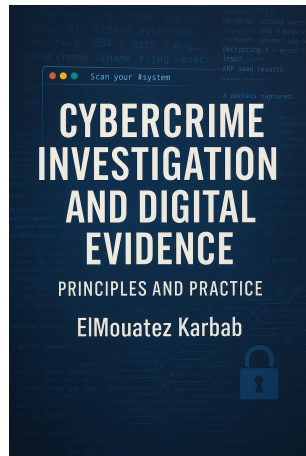
Outline

- 1 Course
- 2 Learning Materials**
- 3 Methodology
- 4 Assessment and Grading
- 5 Course Schedule



Learning Materials

- **Mandatory Textbook:** Karbab, E. (2026). *Cybercrime Investigation and Digital Evidence*. (<https://books.karbab.net/cybercrime-investigation/>)
- **Optional:** Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.
- **Optional:** Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and Digital Forensics: An Introduction*. Routledge.



Outline

- 1 Course
- 2 Learning Materials
- 3 Methodology**
- 4 Assessment and Grading
- 5 Course Schedule



Methodology

- Activities Process
- Educational Process
 - ① **Learner Engagement**
 - ② **Violation of intellectual and moral rights**
 - ③ **Cases of late delivery or non-delivery of duties**
 - ④ **Conduct**

Outline

- 1 Course
- 2 Learning Materials
- 3 Methodology
- 4 Assessment and Grading
- 5 Course Schedule



Assessment and Grading

Assessment Tool	Timing	Grade
Participation	During The Semester	15
Labs	During The Semester	15
Project	Submission on Week 13	30
Final Exam	Week 15	40
Total		100



Outline

- 1 Course
- 2 Learning Materials
- 3 Methodology
- 4 Assessment and Grading
- 5 Course Schedule**



Course Schedule I

This schedule is tentative and subject to change at the instructor's discretion.

Week	Topic	Readings
Week 1	Defining Cybercrime in the 2026 Landscape Cybercrime Ecosystems Lab: Network Forensics Analysis of a DDoS Attack	Chapter 1 Chapter 2
Week 2	Legal and Regulatory Frameworks Ethics, Privacy, and Professional Responsibility Lab: Investigating a Business Email Compromise (BEC) Scam	Chapter 3 Chapter 4
Week 3	Foundational Concepts of Digital Evidence Evidence Acquisition and Preservation Lab: Establishing Evidence Integrity and Chain of Custody	Chapter 5 Chapter 6
Week 4	Forensic Lab Infrastructure and Toolkits Lab: Validating a Forensic Tool Function Final Project Proposal Due	Chapter 7
Week 5	File System and Operating System Forensics Lab: NTFS File Recovery and Data Carving	Chapter 8
Week 6	Foundations and Practice of Memory Forensics Lab: Initial Triage of a Compromised Windows System	Chapter 9



Course Schedule II

Week	Topic	Readings
Week 7	Network Forensics and Encrypted Traffic Analysis Lab: Intelligence from Encrypted Traffic (TLS/JA3)	Chapter 10
Week 8	Log Analysis for Incident Response Lab: Web Server Log Triage with Command-Line Tools	Chapter 11
Week 9	Mobile, IoT, and Cloud Forensics Lab: Analysis of an Android Logical Backup	Chapter 12
Week 10	Malware Analysis and Reverse Engineering Lab: Introductory Reverse Engineering with Ghidra	Chapter 15
Week 11	Investigating the Dark Web and Cryptocurrency Lab: Public Blockchain Analysis - Tracing Illicit Funds	Chapter 16
Week 12	Forensics for IoT, ICS, and Operational Technology Lab: Embedded Device Firmware Reverse Engineering	Chapter 17
Week 13	Insider Threat Investigations Lab: Enterprise Log and Network Traffic Analysis for Anomaly Detection Final Project Due	Chapter 20
Week 14	OSINT and Threat Intelligence Integration Lab: Mapping Malicious Infrastructure from an Indicator of Compromise (IOC)	Chapter 22
Week 15	Final Exam	



Thank You!

