



Cybercrime Investigation and Digital Evidence

MSCS 630 - Fall 2026

COURSE

Course:	Cybercrime Investigation and Digital Evidence
Code:	MSCS 630
Program:	Master of Science in Cyber Defense
Type:	Compulsory
Credits:	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

DESCRIPTION

This course provides a comprehensive and methodologically rigorous examination of the principles and practices of modern digital forensics and cybercrime investigation. Moving from foundational legal and ethical principles to the deep technical analysis of contemporary digital evidence sources, the curriculum is designed to equip students with the knowledge and practical skills required to conduct effective investigations in a rapidly evolving technological landscape. The course traces the evolution of digital crime, deconstructs the complex cybercrime ecosystem, and provides in-depth training on the forensic analysis of both traditional and emerging platforms, including cloud infrastructure, mobile devices, IoT, and cyber-physical systems. A significant emphasis is placed on practice-oriented learning, utilizing industry-standard open-source tools to prepare students for real-world challenges in law enforcement, corporate security, and incident response roles.

OBJECTIVES

Upon successful completion of this course, students will be able to:

- Critically analyze the modern cybercrime landscape, including attacker motivations, the Cybercrime-as-a-Service (CaaS) economy, and the governing legal and ethical frameworks.
- Master the complete forensic process for digital evidence, from forensically sound acquisition and preservation under a strict chain of custody to the in-depth analysis of file systems, operating system artifacts, and application data.
- Conduct advanced forensic analysis of volatile memory and network traffic to uncover transient evidence, reconstruct security incidents, and identify indicators of compromise.
- Apply specialized forensic techniques to a wide range of modern evidence sources, including Android and iOS devices, cloud infrastructure (IaaS, PaaS, SaaS), Internet of Things (IoT) devices, and cyber-physical systems such as vehicles and drones.
- Investigate complex, human-centric threats such as social engineering and insider attacks, and leverage Open-Source Intelligence (OSINT) to enrich forensic findings.
- Understand and counter the challenges posed by advanced adversary techniques, including counter-forensics, encryption, synthetic media (deepfakes), and dark web activities.
- Develop the core professional competencies required for a career in digital forensics, including critical thinking, effective technical reporting, preparation for expert testimony, and strategies for professional resilience.

LEARNING OUTCOMES

Upon completion of this course, students will be able to:

1. **Execute a Forensically Sound Evidence Workflow:** Acquire and preserve disk, memory, and network evidence under a strict chain of custody, applying write-blocking, hash verification, and documented tool validation on a working open-source forensic platform (SIFT Workstation, Autopsy).
2. **Analyze Host and System Artifacts:** Reconstruct user and attacker activity from file system structures (NTFS, ext4), operating system artifacts such as the Windows Registry and system logs, and volatile memory examined with the Volatility Framework.
3. **Reconstruct Incidents from Network and Log Evidence:** Correlate packet captures, encrypted traffic metadata (TLS/JA3), and server and application logs into a defensible incident timeline supported by identified indicators of compromise.

4. **Investigate Modern and Adversarial Evidence Sources:** Apply specialized techniques to mobile, cloud, IoT, and industrial control system evidence, and counter adversary tradecraft through malware reverse engineering with Ghidra, dark web and blockchain tracing, and the detection of counter-forensic activity.
5. **Communicate Findings to Legal and Organizational Audiences:** Produce court-admissible forensic reports and prepare for expert testimony, arguing conclusions within the legal and ethical constraints of admissibility, jurisdiction, and privacy.

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.

METHODOLOGY

This course includes lectures, discussions, practical applications, group activities, research, and academic reports. Learners contribute to the educational process by reading and analyzing research related to lecture topics and by enriching the discussion through critical evaluation of research and the proposed scientific materials. The course material, references and research readings will be provided to learners on the electronic platform. The weekly lectures give learners the opportunity to absorb the key concepts and discuss the readings. The learner is expected to contribute actively to the educational process and will evaluate various activities related to the course such as participation during lectures, critical discussion of research, theoretical and practical assignments.

ACTIVITIES PROCESS

- Learners are expected to participate actively in the classroom and in work teams, attending regularly and arriving and leaving on time, without using mobile phones or holding side conversations.
- All learners should take great care in completing and submitting requirements on time.
- All learners should treat additional weekly readings with great care to understand, analyze and develop their knowledge by looking for other sources.
- All learners must keep a course portfolio.

- Learners are expected to write down the necessary knowledge during the lecture.

EDUCATIONAL PROCESS

1. **Learner Engagement** Classroom participation and lecture attendance are required of every student at the Joaan Bin Jassim Academy for Defense Studies, and the student is expected to attend all lectures. If the student exceeds the permissible percentage of absence, which is 25%, they will receive a failure grade regardless of their performance. It is the student's responsibility to monitor their attendance. Attendance will be recorded starting from the first day of school, regardless of the period allocated for dropping and adding courses.
2. **Violation of intellectual and moral rights** Violation of intellectual and moral rights is considered academic abuse and may result in the loss of grades or failure. These violations include the following issues and apply to all learners' work:
 - Using the works, ideas, images, or words of any other person without their permission or without reference to the source.
 - Using someone else's name, sentence, paragraph, or article without using quotation marks.
 - Misuse of cited sources.
3. **Cases of late submission or non-submission of assignments**
 - A student who misses the exam, or does not submit the project or deliver a presentation on time, without permission or a medical excuse, will be graded on that component according to the rules of procedure of the Joaan Bin Jassim Academy for Defense Studies.
 - If a learner is unable to complete an assignment due to an acceptable excuse, they will receive an "incomplete" grade in that assessment and will be given another assessment or extension period.
4. **Conduct** The Academy expects learners to adhere to high standards of conduct in their interaction with course professors, their colleagues, and the academy community, according to the rules of procedure of the Joaan Bin Jassim Academy for Defense Studies.

ASSESSMENT AND GRADING

A number of different assessment tools will be used to measure the achievement of the aforementioned learning outcomes, including tests, classroom participation and labs.

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

Grading Scale:

Grade	Description	Percentage	Points Earned
A	Excellent	90-100	4.00
B+	Very Good (high)	85 to <90	3.50
B	Very Good	80 to <85	3.00
C+	Good (high)	75 to <80	2.50
C	Good	70 to <75	2.00
F	Fail	Less than 70	0.00
P+	Pass		
P	Pass		
I	Incomplete		
IP	Continuing course		
TC	Transfer Credit		
W	Withdrawal		
WF	Forced Withdrawal		
AU	Audit		

LEARNING AND RESEARCH RESOURCES

All students are required to register with the Qatar National Library (<https://www.qnl.qa/en>), which provides access to most international electronic databases across all scientific disciplines and languages. Relevant databases can be found at <https://qnl.libguides.com/az.php>, including "Dar Almandumah," "Al Manhal," and databases for theses and dissertations in Arabic. The library also offers access to renowned databases such as Taylor & Francis, ProQuest, Military Database, JSTOR, and Sage Journals.

COURSE SCHEDULE

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
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	