Course Plan

First: Course Information

Course No.: 1506754	Course Title: Digital Forensics	Credit Hours: 3	Theoretical: 3	Practical: 0
Prerequisite No. and Title:		Section No.:	Lecture Time:	
Level in JNQF	9			

Type Of Course:	☐ *Obligatory University Requirement* ☐ *Elective University Requirement* ☐ *Obligatory Faculty Requirement* ☐ *Elective Faculty Requirement* ■ *Obligatory Specialization Requirement* ☐ *Elective Specialization Requirement* ☐ *Ancillary course*
Type of Learning:	■ *Face-to-Face Learning* ☐ *Blended Learning (2 Face-to-Face + 1 Asynchronous)* ☐ *Online Learning (2 Synchronous+ 1 Asynchronous)*

Second: Instructor's Information

Course Coordinator:		
Name:	Academic Rank:	
Office Number:	Extension Number:	Email:
Course Instructor:		
Name:	Academic Rank:	
Office Number:	Extension Number:	Email:
Office Hours:	Sunday Monday Tuesday Wednesday Thursday	

Third: Course Description

This course covers methods and procedures for locating and recovering damaged or deleted digital data, and accessing tracking information, such as web history, cookies, and cache. It also sheds light on how the attacks originate on the Internet. This course is also concerned with identifying system vulnerabilities, communication ports, and encryption methods. In addition, this course highlights the topic of incident monitoring and response.

Fourth: Course Objectives

1. Introducing the student to the concepts, theories, principles and practices of digital forensics.
2. Developing the student's ability to deal with digital evidence.
3. Guiding the student to leverage evidence acquisition and validation, methodologies used in digital forensics.
4. Expanding the student's skills of digital evidence handling, examination of file systems, graphics file investigation, network and email investigation, legal, professional and ethical issues.
5. Providing the student with the skills of current development and tools in the field.

Fifth: Learning Outcomes

Level descriptor according to (JNQF)	CILOs Code	CILOs If any CLO will not be assessed in the course, mark NA.	Associated PILOs Code Choose one PILO for each CILO*	Assessment method Choose at least two methods
Knowledge	**K1**	Provide the students with the advanced uses of computer security and digital forensics.	**PK1**	• Mid-term Exam • Final Exam • Research
	K2	Describe the methods used to store data locally on a computer, remotely on the Internet, and in general on the local computer and the Internet.	**PK2**	• Mid-term Exam • Final Exam • Research
	K3	Demonstrate of methodologies and techniques used to manipulate with digital evidence.	**PK3**	• Mid-term Exam • Final Exam • Research
	K4	Describe the role of digital forensics in criminal investigations.	**PK4**	• Mid-term Exam • Final Exam • Research
Skills	**S1**	Evaluate an appropriate evidence handling process and digital forensics tools to plan and carry out a digital forensic investigation, from data gathering and validation to evidence discovery, analysis, validation, and presentation..	**PS1**	• Mid-term Exam • Final Exam • Research
	S2	Discover an existing report template, write a report of an analysis of digital evidence for a digital crime case	**PS2**	• Mid-term Exam • Final Exam • Research
	S3	Examine some hypothetical and actual case scenarios, review and synthesize existing industry best practices for the processing	**PS3**	• Mid-term Exam • Final Exam • Research

		of digital evidence.		
	S4	Conduct independent research to better comprehend a certain topic or stay current with field developments.	**PS4**	• Mid-term Exam • Final Exam • Research
Competencies	**C1**	Utilize different techniques for dealing with digital evidence.	**PC3**	• Mid-term Exam • Final Exam • Research
	C2	Develop effective communication skills with the students in the proper way to deliver the required skills and providing them with knowledge about digital forensics, techniques and tools.	**PC4**	• Mid-term Exam • Final Exam • Research

*CILOs: Course Intended Learning Outcomes; PILOs: Program Intended Learning Outcomes; For each CILO, the PILO could be the same or different.

Sixth: Learning Resources

Main Reference:	Guide to Computer Forensics and Investigations: Processing Digital Evidence			
Author: Bill Nelson, Amelia Phillips, Christopher Steuart	Issue No.: 6th	Print:	Publication Year: 2019	
Additional Sources and Websites:	- Research Papers - Computer Forensics and Digital Investigation with EnCase Forensic v7, Suzanne Widup, McGraw-Hill Education, 1st Edition 2014, ISBN-10: 0071807918 | ISBN-13: 978- 007180791 - Computer Forensics: Investigating Data and Image Files (CHFI), EC-Council, Course Technology, 2nd Edition 2016, ISBN-10: 1305883497 | ISBN-13: 978-1305883499 - Computer Forensics: Investigating Network Intrusions and Cybercrime, EC-Council, Course Technology, 2nd Edition 2016, ISBN-10: 1305883500 | ISBN-13: 978-1305883505 - Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet, Eoghan Casey, Academic Press, 3rd Edition 2017, ISBN-10: 0128103280 | ISBN-13: 978-0128103289 - An Introduction to Computer Security: the NIST Handbook, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf Access on June 29, 2022 - Who is the OWASP Foundation?, http://www.owasp.org/index.php/ Main_Page Access on June 29, 2022 - Cybersecurity, http://www.windowsecurity.com/whitepaper/ Access on June 29, 2022 - Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage (CHFI), EC-Council, Course Technology, 2nd Edition 2016, ISBN-10: 1305883489 | ISBN-13: 978-1305883482 - Computer Forensics: Investigation Procedures and Response (CHFI), EC-Council, Course Technology, 2nd Edition 2016, ISBN-10: 1305883470 | ISBN-13: 978-1305883475			
Teaching Type:	■ Classroom ■ Laboratory ☐ Workshop ■ MS Teams ■ Moodle			

Seventh: Course Structure

Lecture Date	Course Intended Teaching Outcomes (CILOs)	Topics	Teaching Procedures*	Teaching Methods**	References***
Week 1	C2, K1	An Overview of Digital Forensics	Face-to-Face	Lecturing	Textbook-ch1
Week 2	C2, K1	• Preparing for Digital Investigations	Face-to-Face	Lecturing, Research Assignments	Textbook-ch1, Research Papers

		• Cyber Crime Investigations Case studies Research Topic			
Week 3	S1, K2, K3, K4	• The Investigator's Office and Laboratory • Digital Investigations Process Research Process-1	Face-to-Face	Lecturing, Research Assignments	Textbook-ch2
Week 4	S1, K2, K3, K4	• Storage in Digital Evidence • Recovering Data from a Windows Hard Disk Research Process-2	Face-to-Face	Practice, Lecturing, Research Assignments	Textbook-ch3
Week 5	S1, K2, K3, K4	• File System Research Process-3	Face-to-Face	Practice, Lecturing, Research Assignments	Textbook-ch3, ch4, ch5
Week 6	S2, K2, K3, K4	• Data Acquisition and methods Research Process-4	Face-to-Face	Practice, Lecturing, Research Assignments	Textbook-ch3
Week 7	S2, K2, K3, K4	• Anti-Forensics Techniques Research Process-5	Face-to-Face	Practice, Lecturing, Research Assignments	Research Papers
Midterm Exam					
Week 8	S3, K2, K3, K4	• Operating Systems Forensics • Forensics Software and Hardware Tools • Linux and Mac Forensics Research Process-6	Face-to-Face	Practice, Lecturing, Research Assignments	Textbook-ch3, ch4, ch5, ch6, ch7
Week 9	S3, K2, K3, K4	• Virtual Machine Forensics • Network Forensics Research Process-7	Face-to-Face	Lecturing	Textbook-ch10

Week 10	S1, K2, K3, K4	• Investigating Web Attacks Research Process-8	Face-to-Face	Lecturing	Research Papers
Week 11	S2, K2, K3, K4	• E-mail and Social Media Investigations • Mobile Device Forensics Research Process-9	Face-to-Face	Practice, Assignments	Textbook-ch11, ch12
Week 12	C1, C2, S3, S4, K1	• Cloud Forensics • IoT Forensics Research Process-10	Face-to-Face	Lecturing	Textbook-ch12, ch13
Week 13	C1, C2, S3, S4, K1	• Forensics Report Writing and Presentation Revision	Face-to-Face	Lecturing	Textbook-ch14, Research Papers
Week 14	C1, C2, S3, S4, K1	• Operating Systems Forensics • Forensics Software and Hardware Tools • Linux and Mac Forensics Research Process-6	Face-to-Face	Practice, Lecturing, Research Assignments	Textbook-ch3, ch4, ch5, ch6, ch7
Final Exam					

*Teaching procedures: (Face-to-Face, synchronous, asynchronous).   ** Teaching methods: (Lecture, video….).
*** Reference: (Pages of the book, recorded lecture, video….)

Eighth: Assessment Methods

Methods	Online Learning	Blended Learning	Face-To-Face Learning	Specific Course Output to be assessed **If any CILO will not be assessed in the course, mark NA.									
				K1	K2	K3	K4	S1	S2	S3	S4	C1	C1
First Exam													
Second Exam													
Mid-term Exam			30		✓		✓	✓	✓	✓			✓
Participation													
Asynchronous Activities													
Quizzes													
Assignments/ Research			30	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Group presentation													
Final Exam			40	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Total out of 100			100										

Ninth: Course Policies

- All course policies are applied to all teaching patterns (online, blended, and face-to-face Learning) as follows:
  a. Punctuality.
  b. Participation and interaction.
  c. Attendance and exams.
- Academic integrity: (cheating and plagiarism are prohibited).

Approval	Name	Date	Signature
Head of Department			
Faculty Dean			