جامعـة الـزيتـونـــة الأردنيــة

Al–Zaytoonah University of Jordan

كلية العلوم وتكنولوجيا المعلومات

Faculty of Science and Information Technology

	" عراقة وجودة" "Tradition and Quality"

Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

QF01/0408-4.0E

Study plan No.	**2024/2025**	**University Specialization**	**Cybersecurity**
Course No.	**0133427**	**Course name**	**Digital Forensics Investigations**
Credit Hours	**3**	**Prerequisite Co-requisite**	**Software Security**
Course type	□ MANDATORY UNIVERSITY REQUIREMENT □ UNIVERSITY ELECTIVE REQUIREMENTS	□ FACULTY MANDATORY REQUIREMENT □ Support family course requirements	□ Elective requirements □ ✓**Mandatory requirements**
Teaching style	□ **Full online learning**	□ ✓Blended learning	□ Traditional learning
Teaching model	□ 2Synchronous: 1asynchronous	□ 2 face to face : 1synchronous	□ **3 Traditional**

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	**Academic rank**	**Office No.**	**Phone No.**	**E-mail**	
Dr. Seraj Fayyad	**Assistant Professor**	**114**		**s.fayyad@zuj.edu.jo**	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	CHFI Computer Hacking Forensic Investigator Certification", by Charles Brooks
Supportive learning resources (Books, databases, periodicals, software, applications, others)	- Digital Forensics and Incident Response: Incident Response Techniques and Procedures, Gerard Johansen, 2017 - Practical Digital Forensics, Richard Boddington, 2016
Supporting websites	https://www.eccouncil.org/
The physical environment for teaching	☐ **Class room** ☐ labs ☐ **Virtual educational platform** ☐ Others
Necessary equipment and software	Tools and software required for conducting digital forensic tasks, along with platforms used for digital forensic activities.
Supporting people with special needs	
For technical support	**E-learning and Open Educational Center. Computer Center**

Security Department

Course learning outcomes (S= Skills, C= Competences K= Knowledge,)

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Basic Knowledge about functions of log management infrastructure.	**MK2**
K2	Gain a good knowledge about web application digital forensic and indication of web attack.	**MK2**
K3	Knowledge about different tools that could be used in digital forensics such as sniffing tools (e.g., ominpeek)	
K4	Gain a good knowledge about SQL server digital forensic.	
K5	Being able to differentiate between different functions of log management infrastructure.	
	Skills	
S1	Examine the Router, IDS, Firewall, DHCP logs.	**MK1**
S2	Investigate SQL injection and XSS injection scripts including possible obfuscations techniques.	**MK3**
S3	Investigate active logs of SQL server and being able to identify changes performed on a given table.	
	Competences	

C1	Independently manage tasks related to digital forensic of web, SQL server, and network.	

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	**Fully electronic learning**	**Blended learning**	**Traditional Learning (Theory Learning)**	**Traditional Learning (Practical Learning)**
First exam	0	**0**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation / practical applications	0	**0**	0	0
Asynchronous interactive activities	%30	**%30**	%30	%30
final exam	%40	**%40**	%40	%40

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc, which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	**Subject**	**learning style***	**Reference ** **
1	Network Forensic and Logs and Events Correlations	Face to Face in Lab	
2	Log Management infrastructure Functions	Face to Face in Lab	
3	Log Management infrastructure Functions_2	Face to Face in Lab	
4	Challenges of log Management	Face to Face in Lab	
5	Centralized of logging and Ensure Log File authenticity	Face to Face in Lab	
6	Analysis of Router logs and Firewall logs	Face to Face in Lab	
7	Analysis of IDS logs,	Face to Face in Lab	
8	Analysis of IDS and DHCP logs	Face to Face in Lab	
9	Investigation of Network Traffic, Wireshark and Omnipeek tools	Face to Face in Lab	

10	Web attacks ,	Face to Face in Lab	
11	Web attack indications	Face to Face in Lab	
12	Web attacks ,forensic challenges	Face to Face in Lab	
13	Investigating IIS ,Investigating Apache logs	Face to Face in Lab	
14	Investigating Web attacks ,Web attacks Investigation tools	Face to Face in Lab	
15	Data storage in MSSQL ,Collecting SQL trace file	Face to Face in Lab	
16	Collecting Active Transaction Logs Database forensic using SQL server management Studio	Face to Face in Lab	

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**

**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

This activities was designed using the **Project-Based Learning (PBL)**

Project 1: Web Attack Detection & Forensic Analysis Lab

Task / Activity	Reference	Expected Results
Set up a vulnerable web server (OWASP Juice Shop) and generate attack logs. Analyze IIS/Apache logs to identify SQLi, XSS, and path traversal attack patterns using command-line tools (grep, awk) and Log Parser Lizard.	OWASP Top 10, Apache/IIS Log Format Documentation, Web Forensics Case Studies	A detailed incident report correlating log entries to specific OWASP attacks, with identified IoCs and a timeline of the attack sequence.

Project 2: SQL Server Attack Investigation & Evidence Collection

Task / Activity	Reference	Expected Results
Simulate a SQL injection attack on a test MSSQL database. Configure and collect a SQL Server Profiler trace, analyze transaction logs for malicious data manipulation, and extract forensic artifacts from database storage files.	Microsoft SQL Server Forensic Analysis Whitepapers, Database Security Best Practices, SQL Server Profiler Documentation	A comprehensive forensic report containing the malicious SQL query, extracted database evidence, and a validated method for collecting and preserving SQL trace files as evidence.

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

Week	Task / activity	Reference	Expected results
1			
2			
3			
4			
5			
6			
7			
8			