QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**2024/2025**		**University Specialization**		**Cybersecurity**
Course No.	**0133325**		**Course name**		**Data Analytics**
Credit Hours	**3**		**Prerequisite Co-requisite**		**0133212**
Course type	☐ MANDATORY UNIVERSITY REQUIREMENT	☐ UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY MANDATORY REQUIREMENT	☐ Support course family requirements	☐ ✓ **Mandatory requirements** ☐ Elective 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	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

The course entails a scientific examination of data analytics in the field of cybersecurity, with a particular focus on its application in cybercrime investigations. It provides an overview of cybercrime types and the challenges faced by investigators, emphasizing the importance of digital evidence collection. The course also details the roles and responsibilities of forensic investigators. In addition, this course highlights the centrality of operating systems in cybercrimes and instructs students on the collection and analysis of both volatile and non-volatile data in Windows systems, including memory and registry analysis, browser history examination, and the analysis of Windows OS files, metadata, and logs.

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)	"CHFI Computer Hacking Forensic Investigator Certification" by Charles Brooks			
Supporting websites				
The physical environment for teaching	☐ ✓**Class room**	☐ labs	☐ **Virtual educational platform**	☐ Others
Necessary equipment and	**Data show, Computer**			

software	
Supporting people with special needs	
For technical support	**E-learning and Open Educational Center. Computer Center**

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

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Basic Knowledge about data analytics in digital forensics.	**PLO2**
K2	Knowledge about different phases of forensic investigation process.	**PLO2**
K3	Knowledge about different types of digital evidences and the rules of digital evidence.	**PLO2**
K4	Explain some techniques on how to Examine Windows volatile (e.g., running processes) and non-volatile data (e.g. OS registry, Explorer cache)	**PLO2**
	Skills	
S1	Perform a good cycle of analytics on the collected data by Windows OS using some tools such as OS Forensic.	**PLO7**
S2	Being able to perform some techniques (e.g., hashing) on evidence resources or sensors to assure the legitimacy of collected digital evidence.	**PLO7**
S3	Perform or run several windows commands and utilities (e.g., netstat, ipconfig) to collect analytics data needed for forensic investigation process.	**PLO8**
	Competences	
C1	Independently manage tasks related to data analytics in context of digital forensic process.	**PLO12**

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	Types of Cyber Crimes, Challenges that cybercrime present to investigator.	Lectures	Lecture Notes
2	Digital Evidences, Sources of Digital Evidences	Lectures	Lecture Notes
3	Computer Forensics Pre-investigation phase, Computer Forensics Pre-investigation phase	Lectures	Lecture Notes
4	Computer Forensics Pre-investigation phase_2, Computer Forensics Pre-investigation phase_2	Lectures	Lecture Notes
5	Computer Forensics investigation phase_1, Computer Forensics investigation phase_1	Lectures	Lecture Notes
6	Computer Forensics investigation phase_2, Computer Forensics investigation phase_2	Lectures	Lecture Notes
7	Computer Forensics investigation phase_2, Computer Forensics investigation phase_2	Lectures	Lecture Notes
Midterm Exam (30%)			
9	OS forensic- collecting volatile information, OS forensic- collecting volatile information	Lectures	Lecture Notes
10	OS forensic- collecting non-volatile information, OS forensic- collecting non-volatile information	Lectures	Lecture Notes
11	Windows memory analysis, Windows memory analysis	Lectures	Lecture Notes
12	Windows registry analysis_1, Windows registry analysis_1	Lectures	Lecture Notes
13	Windows registry analysis_2 Windows registry analysis_2	Lectures	Lecture Notes
14	Explorer Cache, Cookies and history analysis	Lectures	Lecture Notes
15	Explorer Cache, Cookies and history analysis	Lectures	Lecture Notes

Final Exam (40%)

*** 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 : Volatile & Non-Volatile Evidence Collection (PBL)

Task / Activity	Reference	Expected Results
Identify volatile digital evidence sources	OS Forensic – Collecting Volatile Information	Clear list of volatile data
Collect volatile system information (RAM, processes, network)	OS Forensic – Collecting Volatile Information	Successfully captured live evidence
Preserve volatile data using forensic tools	OS Forensic – Collecting Volatile Information	Forensically sound data acquisition
Identify non-volatile evidence sources	OS Forensic – Collecting Non-Volatile Information	Clear storage artifacts identified
Collect non-volatile files, logs, and artifacts	OS Forensic – Collecting Non-Volatile Information	Proper evidence acquisition
Verify integrity of collected evidence	OS Forensic Principles	Evidence authenticity maintained
Prepare forensic documentation	PBL Documentation	Structured investigation report

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			