هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAAA

2023

TPG-153

Course Specification

(Postgraduate)

Course Title: **Digital Forensics**	
Course Code: CYBS60312	
Program: M.Sc. in Cybersecurity	
Department: **Department of Computer Science**	
College: **Faculty of Computing and Information**	
Institution: Al-Baha University	
Version: **1**	
Last Revision Date: **12 December 2023**	

Table of Contents

A. General information about the course: 3
B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods: 4
C. Course Content: 6
D. Students Assessment Activities: 6
E. Learning Resources and Facilities: 7
F. Assessment of Course Quality: 8
G. Specification Approval Data: 8

A. General information about the course:

1. Course Identification:

1. Credit hours: (3)

2. Course type

A.	☐University	☐College	☐Department	☐Track	
B.	☐ Required		☒ Elective		

3. Level/year at which this course is offered: (3/2)

4. Course general Description:

This course provides knowledge of forensics techniques and skills to apply them to investigation activities in a way that complies with the legal requirements. It presents an overview of the principles and practices of digital investigation. The objective of this class is to emphasize the fundamentals and importance of digital forensics. Students will learn different techniques and procedures that enable them to perform a digital investigation. This course focuses mainly on the analysis of physical storage media and volume analysis. It covers the major phases of digital investigation such as preservation, analysis and acquisition of artifacts that reside in hard disks and random-access memory. Students will work on project to setup and use of an investigator's laboratory, computer investigations using digital evidence controls, processing crime and incident scenes, performing data acquisition, computer forensic analysis, e-mail investigations, and image file recovery.

5. Pre-requirements for this course (if any)**:**

None

6. Pre-requirements for this course (if any)**:**

None

7. Course Main Objective(s):

Upon successful completion of the course, the student will be able:

1. **Describe students to conduct a digital investigation in an organized and systematic way.**

2. **Infer theoretical and practical knowledge, as well as current research on Digital Forensics.**
3. **Upon completion of the course, students can apply open-source forensics tools to perform digital investigation and understand the underlying theory behind these tools.**
4. **Transform the digital investigation observations into forensic report.**

2. Teaching Mode: (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	26	80%
2	E-learning	7	20%
3	Hybrid □ Traditional classroom □ E-learning		
4	Distance learning		

3. Contact Hours: (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	33
2.	**Laboratory/Studio**	-
3.	**Field**	-
4.	**Tutorial**	-
5.	**Others (specify)……**	-
	Total	33

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods:

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	**Describe the importance of Digital forensics and its use in solving cases**		**Lectures Assignments Group Discussion**	**Assignment Midterm exams Final Exam**

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
	related to Cybercrime			
1.2	Recognize the Techniques, Procedures, and protocols required in digital investigation and collecting digital evidence		Lectures Assignments Group Discussion	Assignment Midterm exams Final Exam
…				
2.0	**Skills**			
2.1	Illustrate legal and regulation issues related to digital forensics and investigation according to the legislation, regulations, instructions and decisions in the Kingdom.		Lectures Assignments Group Discussion	Assignment Midterm exams Final Exam
2.2	Analyze digital crime and incident scenes		Lectures Assignments Group Discussion	Assignment Midterm exams Final Exam
2.3	Solve a given cyber investigation problem using digital forensics techniques and tools.		Lectures Assignments Group Discussion	Assignment Quiz Project Final Exam
2.4	Manage the digital forensic investigation reports		Lectures Assignments Group Discussion	Assignment Project Final Exam
3.0	**Values, autonomy, and responsibility**			
3.1	Participate in groups collaboratively.		Team-based learning	Report, presentation, and Class Discussions

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
3.2				
...				

C. Course Content:

No	List of Topics	Contact Hours
1.	Digital Forensics Terminologies	3
2.	Legal Compliance: Applicable Laws, Affidavits, Testimony, Testifying, Case Law and Chain of Custody	6
3.	Investigatory Process	6
4.	Acquisition and Preservation of Evidence: Write-blocking, Imaging Procedures, Live Forensics, Analysis and Authentication of Evidence (Hashing), File Recovery	6
5.	Analysis of Evidence: Root Cause Analysis, Metadata and File Carving	6
6.	Reporting and Presentation of Results: Timeline and Attribution	3
	Email and Database Forensics	3
Total		33

D. Students Assessment Activities:

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignments	Every two weeks	5%
2.	Report, presentation, and Class Discussions	Week 10	5%
3.	Midterm Exam	Within the 6th Week	20%
4.	Quizzes	Week 8	10%
5.	Project	Week 11	10%
6.	Final Exam	Week 13	50%

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

E. Learning Resources and Facilities:

1. References and Learning Resources:

Essential References	□ B. Nelson, A. Phillips, and C. Steuat, Guide to Computer Forensics and Investigations, 6th Ed, Cengage, 2019. □ Joakim Kävrestad, Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications, Springer, 2018, ISBN-10: 331996318X □ Mike Sheward, Hands-on Incident Response and Digital Forensics, 2018, ISBN-10: 1780174209 □ Jason Wayne,Cybercrime and Digital Forensics, Clanrye International, 2018, ISBN-10: 1632407256 □ Sherri Davidoff, Jonathan Ham Network Forensics: Tracking Hackers Through Cyberspace, Prentice Hall, 2012
Supportive References	• Computer Forensic Training Center Online http://www.cftco.com/ • Computer Forensics World http://www.computerforensicsworld.com/ • Digital Forensic Magazine http://www.digitalforensicsmagazine.com/ The Journal of Digital Forensics, Security and Law http://www.jdfsl.org/ • Journal of Digital Forensic Practice http://www.tandf.co.uk/15567281 • DOJ Computer Crime and Intellectual Property Section - http://www.usdoj.gov/criminal/cybercrime/searching.html • Electronic Crime Scene Investigation: A Guide for First Responders - http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm and related publications at http://nij.ncjrs.org/publications/pubs_db.asp • CERIAS Forensics Research (http://www.cerias.purdue.edu/research/forensics/) • Scientific Working Group on Digital Evidence (http://ncfs.org/swgde/index.html) • DoD Cybercrime Center (http://www.dc3.mil) • National Criminal Justice Reference Service - http://www.ncjrs.gov/app/publications/alphalist.aspx • Digital Forensics Research Workshop (http://www.dfrws.org/) • National White Collar Crime Center (http://www.nw3c.org/) • The IACIS® Forensic Computer Security-related organizations : CERT, SANS, CIS, CASPR, CSI, CIAO, DRII, ISSA, IATFF, I2SF, NIAP, CSRC, OWASP
Electronic Materials	• Access to the Saudi Digital Library (SDL). • Using the learning management system of the university – Rafid System (https://lms.bu.edu.sa/). • https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=90 • ACM Transactions on Computing Education (TOCE) – http://toce.acm.org/ • ACM (Association for Computer Machinery) Curricula Recommendations – • http://www.acm.org/education/curricula-recommendations
Other Learning Materials	

2. Educational and Research Facilities and Equipment Required:

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	• A classroom or lecture hall with whiteboard for 25 students. • A laboratory with 25 computers.
Technology equipment (Projector, smart board, software)	All students shall have • A laptop or access to a desktop computer with access to a programming development tool • High speed Internet connection • Power outlets for student's laptop plug-in
Other equipment (Depending on the nature of the specialty)	• The laboratory should have computers with programming development tools. • SANS SIFT, ProDiscover Forensic, Volatility Framework. • The Sleuth Kit (+Autopsy), CAINE, Xplico, X-Ways Forensic.

F. Assessment of Course Quality:

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students - Program Leaders	Indirect
Effectiveness of students assessment	Program Leaders	Indirect
Quality of learning resources	Students	Indirect
The extent to which CLOs have been achieved	Peer reviewers	Direct
Reviewing course effectiveness and planning for improvement.	Program Leaders - Faculty	Direct

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval Data:

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	