

CCY3003 Digital Forensics and Incident Response**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY2001	3	6	2	--	2	3

COURSE AIM

To get the students to:

- Develop a comprehensive understanding of the major forensic processes employed in the investigation of cybercrimes, including computer procedure analysis, digital evidence collection, analysis, recovery, and preservation.
- Acquire technical proficiency in critical areas, such as data imaging, hashing, file recovery techniques, file system fundamentals, and the identification of mismatched file types.
- Learn how to effectively report and present digital evidence using established methodologies.
- Explore the legal and technical dimensions of digital forensics and incident response, ensuring students are well-versed in both the practical and legal aspects of the field.

COURSE WEEKLY CONTENTS

1	Introduction to Digital Forensics and Incident Response
2	Computer System Fundamentals
3	Data Acquisition and Imaging
4	Data Hashing and Integrity Verification
5	File Recovery and Reconstruction
6	File System Analysis
7	Identification of Mismatched File Types
8	7th week Assessment
9	Evidence Handling and Preservation
10	Network Forensics
11	Memory Forensics
12	Incident Response Frameworks
13	12th week Assessment
14	Malware Analysis for Incident Response
15	Legal and Ethical Considerations

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7	←		30	MARKS		→	30
8 to 12	←		20	MARKS		→	20
1 to 15	←		10	MARKS		→	10
16 or 17			Final Exam				40

REFERENCES

Textbook	Johansen, Gerard, Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response, Packet Publisher
-----------------	---