

Branch Name:	Bachelor of Technology (Computer Engineering / Information Technology)
Program Code:	ET103/ET105
Course Title:	Elective -V Theory: Digital Forensic & Incident Response
Course Code:	2ET1030708T
Pre-requisite Course:	Basic knowledge of Computer Networks, Operating Systems

Course Objectives: To understand the principles of digital forensics, cybercrime investigation, evidence handling, and incident response & develop skills in forensic analysis, malware investigation, reporting, use of modern forensic tools and technologies.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								Total (Marks)
					Theory (Marks)				Practical (Marks)				
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
3	3	-	-	3	24	60	16	40	-	-	-	-	100

Course Contents:

Unit No	Topics	Total Hours	Weightage (%)
1	Introduction to Digital Forensics: Introduction, Types of Forensic – Computer/ Digital forensic concept & goal, Computer forensic process, Benefits of computer forensics-uses of computer forensics, Role of Forensic Investigator, Forensic Readiness, Basics principles of forensic, Computer Forensic Investigation Process, Introduction to Computer Crime and process	6	15%
2	Incident Response: Introduction, Incident Response Lifecycle (NIST Framework), Preparation Phase, Incident Identification & Detection, Containment Strategies, Eradication & Recovery, Incident Documentation & Reporting	6	20%
3	Digital Evidence and First Responder Procedure: Introduction, First Responder Toolkit, Digital Evidence Collection & Preservation, Collection Issues facing computer forensics, Types of Investigation, Techniques of Digital Forensics, IT Act & Forensic Law	7	25%
4	Windows Forensics and File Recovery: Introduction, Major forensic areas in Windows, Volatile & Non-Volatile Information, Windows Registry, event log file, password storage., Recovering deleted files and partitions, Data organization in Windows - Anatomy of a disc drive, cache files and files in unallocated space, File carving and Event Logs	7	25%
5	Network Forensics: Introduction, Network Data collection methods, Network Components and their Forensic Importance, Forensic Tools, Password Cracking, Wireless Attacks	7	15%

Reference Books:

1. Learn Computer Forensic by William Oettinger
2. Practical Forensic Imaging by Bruce Nikkel
3. Digital Forensics Workbook Hands-on Activities in Digital Forensics by Michael K Robinson
4. Practical Guide to Digital Forensics Investigations by Darren Hayes

List of Open-Source Software/learning website:

1. NIST SP 800-101, 800-86 <https://csrc.nist.gov/publications/sp800>
2. ISO/IEC 27037, 27041 <https://www.iso.org/standard/44381.html>
3. <https://cyberdefenders.org/>
4. <https://nptel.ac.in/courses/128106006>

Course Outcomes (CO):

Course Outcomes	Description	Bloom's Taxonomy Level
CO1	Understand digital forensics, cybercrime, laws & ethics	Remember (1) Understand (2)
CO2	Collect, preserve, and document digital evidence	Apply (3)
CO3	Analyze file systems, memory, and storage devices	Analyze (4) Evaluate (5)
CO4	Perform network and malware forensics	Apply (3) Analyze (4)
CO5	Develop and implement incident response strategies to prepare reports	Evaluate (5) Create (6)

Mapping of CO with PO and PSO

Course Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)			
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3	PSO 4
CO1	H	M	-	-	L	M	-	H	-	-	-	M	M	L	L	H
CO2	M	H	-	H	H	-	-	M	-	M	-		H	M	L	M
CO3	M	H	-	H	H	-	-	-	-	-	-	L	H	M	M	L
CO4	M	H	M	H	H	-	-	-	-	-	-	L	H	H	H	L
CO5	M	H	H	H	H	L	-	-	M	M	M	M	H	H	H	M

H: High, M: Medium, L: Low