Course code: Course Title	Course Structure			Pre-Requisite
SE415: Cyber Forensics	L	T	P	NIL
	3	1	0	

Course Objective: To introduce various techniques related to Cyber Forensics.

S. NO	Course Outcomes (CO)
CO1	Understand the fundamentals of cyber security, cyber-attacks, and digital forensics techniques.
CO2	Apply forensic techniques and data collection methods using built-in and freeware tools.
CO3	Analyze live data collection and forensic investigation techniques in Unix/Linux environments.
CO4	Utilize forensic tools and techniques to recover deleted files, analyze network traffic, and assess vulnerabilities

S.No.	Contents	Contact Hours
UNIT 1	**Introduction**: Review of TCP/IP and TCP, IP Header analysis, Introduction to Cyber World, Cyber-attacks and cyber security, Information warfare and cyber terrorism, Types of cyber-attacks, Cyber Crime and Digital Fraud, Overview of Types of computer forensics i.e. Media Forensics, Network forensics (internet forensics), Machine forensic, Email forensic (e-mail tracing and investigations)	10
UNIT 2	**Live Data collection and investigating windows environment**: windows Registry analysis, Gathering Tools to create a response toolkit (Built in tools like netstat, cmd.exe, nbtstat, arp, md5sum, regdmpetc and tools available as freeware like Fport, Pslistetc), Obtaining volatile Data (tools like coffee, Helix can be used) Computer forensics in windows environment, Log analysis and event viewer, File auditing, identifying rogue machines, hidden files and unauthorized access points	12
UNIT 3	**Live Data collection and investigating Unix/Linux environment** : /Proc file system overview , Gathering Tools to create a response toolkit (Built in tools like losetup , Vnode , netstat , df , md5sum , straceetc and tools available as freeware like Encase , Carboniteetc) Handling Investigations in Unix/Linux Environment: Log Analysis (Network, host, user logging details), Recording incident time/date stamps, Identifying rogue processes, unauthorized access points, unauthorized user/group accounts	10
UNIT 4	**Forensic tools and report generation**: Recovery of Deleted files in windows and Unix, Analyzing network traffic, sniffers, Ethical Hacking, Hardware forensic tools like Port scanning and vulnerability assessment tools like Nmap, Netscan etc. Password recovery (tools like John the ripper, L0phtcrack, and THC-Hydra), Mobile forensic tools and analysis of called data record Template for computer forensic reports	10
	TOTAL	42

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1.	Kevin Mandia, Chris Prosise, Matt Pepe, “Incident Response & Computer	2003

	Forensics", McGraw-Hill Osborne Media.	
2.	Bill Nelson, Amelia Phillips, Frank Enfinger, Christopher Steuart, "Guide to Computer Forensics and Investigations", Thomson Course Technology.	**2008**
3.	Eoghan Casey, "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet", Academic Press, 3rd Edition.	**2011**
4.	"File System Forensic Analysis", Brian Carrier , addition Wesley	**2005**