	L	T	P	
CS414: Cyber Forensics	**3**	**1**	**0**	**Nil**

Course Objective: To introduce various techniques related to cyber forensics

S. No.	Course Outcomes (CO)
CO1	Describe TCP/IP, cyber attacks, cyber security, and types of cyber forensics.
CO2	Use tools and techniques for live data collection, registry analysis, and file auditing in Windows.
CO3	Apply tools and methods for data collection, log analysis, and process management in Unix/Linux systems.
CO4	Recover deleted files, analyze network traffic, and use forensic and ethical hacking tools.
CO5	Create detailed reports on forensic investigations, including evidence recovery and analysis using various tools.

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)	**12**

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	**12**
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	**12**
	Total	**48**