Guidelines for Cyber Forensics (NEP UGCF 2022)

Discipline Specific Elective Semester VII

(Effective from Academic Year 2025-26)

S.No.	Unit	Chapter Section/Page	References	Hours
1.	**Digital Forensics:**			
	Introduction to digital forensics, legal considerations, recognising and collecting digital evidence, preservation of evidence, hash values and file hashing, creating disk images,	Ch-1 (pg 1-16)	[3]	
	keyword and grep searches	Ch - 5 (pg 119-120)	[2]	
	network basics	Ch- 7 (Sec 7.10)	[1]	
	reporting and peer review, digital forensics report.	Ch-15 (pg 459-464)	[3]	
2.	**Windows OS Forensics:**			
	Disk partition schema	Ch - 3(pg 52-53)	[2]	
	File systems – FAT, NTFS, windows registry forensics, examining the Windows registry,	Ch-2	[3]	
	ex-FAT	Ch- 6 (pg 209-210)	[1]	
	NTUser.Dat Hive File Analysis, SAM Hive file, Software Hive file, System Hive File, USRClass.dat Hive File,	Ch - 4 (pg 78-84)	[2]	
	AmCache Hive File	To be done in practicals as lab exercises		
3.	**Evidence Recovery:**			
	Introduction to Deleted File Recovery	Ch - 7 (Sec 7.5)	[1]	
	Formatted Partition	pg 52-53	[2]	

	Recovery Data Recovery Tools	 Ch- 9 (Sec 9.5 (autopsy tool))	 [1]	
	Data Recovery Procedures and Ethics	Ch - 8 (Sec 8.2.2)	[1]	
	Complete time line analysis of computer files based on file creation, File modification and file access, Recover Internet Usage Data, Recover Swap Files/Temporary Files/Cache Files	Ch-2	[3]	
	Introduction to Encase Forensic Edition, Forensic Tool Kit (FTK),	To be done in practicals as lab exercises		
	Use computer forensics software tools to cross-validate findings in computer evidence	Ch - 7 (Sec 7.3)	[1]	
4.	**Investigation:** Introduction to Cyber Forensic Investigation, Investigation Tools, Digital Evidence Collection, Evidence Preservation E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery Encryption and Decryption Methods Search and Seizure of Computers Recovering deleted evidence Password Cracking.	 Ch - 5 (Sec 5.2.4, 5.2.5) Ch - 6 (Sec 6.1.1, 6.1.2) Ch- 5 (Sec 5.10.9 – 5.10.12) Ch- 7 (Sec 7.8) Ch- 8 (Sec 8.2.3) Ch - 7 (Sec 7.5) Ch - 7 (Sec 7.9)	 [1]	
5.	**Cyber Crimes and Cyber Laws:** Introduction to IT Laws & Cyber Crimes, Internet, Hacking, Cracking, Viruses, Software Piracy, Intellectual Property,	 Ch-1 (before notable data breaches)	 [3]	

	Legal System of Information Technology, Understanding Cyber Crimes in context of Internet,Indian Penal Law & Cyber Crimes Fraud Hacking Mischief International law E-Commerce-Salient Features On-Line Contracts, Mail Box rule Privities of, Contracts Jurisdiction issues in E-Commerce, Electronic Data Interchange, Security and Evidence in E-Commerce: Dual Key encryption, Digital signatures, security issues.	IPC sections - 43, 65, 66A - 66F, 67, 67A, 67B, 72 Ch- 14 (Sec 14.5) Refer to online resources	[5] [1]	

References:

1. Dejey, S. Murugan, Cyber Forensics, Oxford University Press, 2018.
2. C. Altheide & H. Carvey, Digital Forensics with Open Source Tools, Syngress, 2011. ISBN: 9781597495868.
3. Niranjan Reddy, Practical Cyber Forensics. An Incident-Based Approach to Forensic Investigations, Apress, 2019 (Available on DU eLibrary).
4. Marjee T. Britz, Computer Forensics and Cyber Crime: An Introduction, Pearson Education, 2013.
5. https://www.indiacode.nic.in/handle/123456789/1999?sam_handle=123456789/1362

Additional References:

1. "Computer Forensics: Investigating Network Intrusions and Cybercrime" by Cameron H.
2. Malin, Eoghan Casey, and James M. Aquilina Online Course Management System: https://esu.desire2learn.com/
3. Computer Forensics, Computer Crime Investigation by John R., Vacca, Firewall Media, New Delhi.
4. Computer Forensics and Investigations by Nelson, Phillips, Enfinger, Steuart, CENGAGE Learning

5. Real Digital Forensics by Keith J.Jones, Richard Bejitlich, Curtis W.Rose , Addison-Wesley, Pearson Education

Suggested Practicals

1. Study of Network-Related Commands (Windows)
2. Study of Network-related Commands(Linux)
3. Analysis of Windows registry
4. Capture and analyse network packets using Wireshark. Analyse the packets captured.
5. Creating a Forensic image using FTK Imager/ Encase Imager: creating a forensic image, checking the integrity of data, and analysing the forensic image
6. Using System internal tools for network tracking and process monitoring, do the following:
    a. Monitor live processes
    b. Capture RAM
    c. Capture TCP/UDP packets
    d. Monitor the Hard disk
    e. Monitor Virtual Memory
    f. Monitor Cache Memory

Note: The following tools/e-resources may be used for the above practicals:

• Wireshark • COFEE Tool • Magnet RAM Capture • RAM Capture • NFI Defragger • Toolsley • Volatility