Indraprastha College for Women
University of Delhi

Work Plan for ODD SEMESTER – 2026

Course Name:	BA(P)
Paper Title:	Cyber Forensic
Unique Paper Code:	
Semester:	7th
Faculty:	Dr. Manju Bala
Year:	2026-27

Work Plan

Unit No.	Learning Objective	Lecture No.	Topics to be Covered
Unit 1: Digital Forensics :	By the end of this Unit, students will be able to: 1. Understand the principles and legal aspects of digital forensic investigations. 2. Collect, preserve, and verify digital evidence using standard forensic practices. 3. Create forensic disk images and perform evidence analysis using search and hashing techniques. 4. Apply networking knowledge to investigate network-related incidents. 5. Prepare professional forensic reports that meet legal and technical standards.	Lec1	Introduction to digital forensics
		Lec 2	Legal considerations
		Lec 3	recognising and collecting digital evidence
		Lec 4	hash values and file hashing,
		Lec 5	creating disk images,
		Lec 6	keyword and grep searches
		Lec 7	network basics
		Lec 8	reporting and peer review, digital forensics report.
Unit2: Windows OS Forensics :	By the end of this Unit, students will be able to: 1. Analyze Windows disk partition schemes and file systems to locate and recover digital evidence.	Lec 9	File systems – FAT, NTFS,
		Lec 10	windows registry forensics
		Lec 11	examining the Windows registry
		Lec 12	NTUser.Dat

	2. Examine Windows Registry artifacts to reconstruct user activities and system events. 3. Interpret Registry hive files, including NTUser.dat, SAM, Software, System, USRClass.dat, and AmCache, to support forensic investigations. 4. Apply Windows forensic techniques to identify user actions, system configurations, and application execution. 5. Document and present forensic findings in a structured and legally defensible manner.	Lec 13	Hive File Analysis,
		Lec 14	SAM Hive file,
		Lec 15	Software Hive file,
		Lec 16	System Hive File,
		Lec 17	USRClass.dat Hive File,
		Lec 18	AmCache Hive File
Unit 3: Evidence Recovery :	By the end of this unit, students will be able to: 1. Recover deleted and formatted data using standard forensic methods and tools. 2. Perform timeline analysis to reconstruct user activities and system events. 3. Extract and analyze internet, temporary, cache, and swap file artifacts for forensic investigations. 4. Use industry-standard forensic tools such as **EnCase Forensic Edition** and **Forensic Toolkit (FTK)** to acquire, analyze, and validate digital evidence. 5. Cross-validate forensic findings using multiple tools and conduct data recovery in accordance with legal, ethical, and professional standards.	Lec 19	Introduction to Deleted File Recovery Formatted Partition
		Lec 20	Recovery Data Recovery Tools Complete time line analysis of computer files based on file creation,
		Lec 21	File modification and file access, Recover Internet Usage Data, Recover Swap Files/Temporary Files/Cache Files Introduction to Encase Forensic Edition,
		Lec 22	Forensic Tool Kit (FTK),
		Lec 23	Use computer forensics software tools to cross-validate findings in computer evidence Data Recovery Procedures and Ethics
Unit 4: Investiga	By the end of this module, students will be able to:	Lec 24	Introduction to Cyber Forensic Investigation,

tion:	1. Explain the stages and methodologies of cyber forensic investigations. 2. Collect, preserve, recover, and analyze digital evidence using forensic tools and accepted procedures. 3. Conduct e-mail and IP-based investigations to identify sources of cyber incidents. 4. Apply encryption, decryption, and password recovery techniques relevant to forensic investigations while adhering to legal and ethical requirements. 5. Perform forensic investigations in compliance with search, seizure, documentation, and evidence handling standards to produce legally defensible findings.	Lec 25	Investigation Tools,
		Lec 26	Digital Evidence Collection, Evidence Preservation
		Lec 27	E-Mail Investigation, E-Mail Tracking, IP Tracking,
		Lec 28	E-Mail Recovery Encryption and Decryption Methods Search
		Lec 29	and Seizure of Computers
		Lec 30	Recovering deleted evidence Password Cracking.
Unit 5: Cyber Crimes and Cyber Laws:	By the end of this unit, students will be able to: 1. Explain the concepts of cyber crimes, Information Technology laws, and the legal framework governing cyberspace. 2. Analyze cyber offences, including hacking, fraud, software piracy, and intellectual property violations, from legal and technical perspectives. 3. Evaluate the legal aspects of e-commerce, including electronic contracts, jurisdiction, Electronic Data Interchange (EDI), and digital evidence. 4. Apply cryptographic concepts such as dual-key encryption and digital signatures to understand secure electronic transactions. 5. Interpret relevant national	Lec 31	Introduction to IT Laws & Cyber Crimes,
		Lec 32	Internet, Hacking, Cracking, Viruses,
		Lec 33	Software Piracy, Intellectual Property, Legal System of Information Technology,
		Lec 34	Understanding Cyber Crimes in context of Internet,
		Lec 35	IPC sections - 43, 65, 66A - 66F, 67, 67A, 67B, 72 [3] [5]
		Lec 36	Indian Penal Law & Cyber Crimes Fraud Hacking Mischief
		Lec 37	International law E-Commerce-Salient Features On-Line Contracts,
		Lec 38	Mail Box rule Privities of contract Jurisdiction,
		Lec 39	Electronic Data Interchange,
		Lec 40	issues Security and Evidence in E-Commerce: Dual Key encryption, signatures, security issues.

	and international cyber laws to address cyber crime investigations and ensure legal compliance in digital environments.		

Unit	Contents/Syllabus
I	Digital Forensics: Introduction to digital forensics, legal considerations, recognising and collecting digital evidence, preservation of evidence, hash values and file hashing, creating disk images, keyword and grep searches network basics reporting and peer review, digital forensics report.
II	Windows OS Forensics: Disk partition schema File systems – FAT, NTFS, windows registry forensics, examining the Windows registry, ex-FAT NTUser.Dat Hive File Analysis, SAM Hive file, Software Hive file, System Hive File, USRClass.dat Hive File, AmCache Hive File
III	Evidence Recovery: Introduction to Deleted File Recovery Formatted Partition Recovery Data Recovery Tools Data Recovery Procedures and Ethics, 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 Introduction to Encase Forensic Edition, Forensic Tool Kit (FTK), Use computer forensics software tools to cross-validate findings in computer evidence
IV	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
V	Cyber Crimes and Cyber Laws: Introduction to IT Laws & Cyber Crimes, Internet, Hacking, Cracking, Viruses, Software Piracy, Intellectual Property, 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 Jurisdiction of Contracts in E-Commerce, Electronic Data Interchange, issues Security and Evidence in E-Commerce: Dual Key encryption, signatures, security issues.

S. No.	Name of Authors/Books/Publishers
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

Paper Components			
Credits	**Lecture (L)**	**Tutorial (T)**	**Practical (P)**
Assessment Scheme			
S.No.	**Component**	**Marking Scheme**	**Total Marks**
1	Internal Assessment		**30**
	Assignment	12	
	Class Test	12	
	Attendance	6	
2.	Continuous Assessment (**Tutorial)**		NA
	• Activity 1		
	• Activity 2		
	• Attendance		
3.	Practical		40
	• Continuous Assessment	20	
	• End Term Written/Practical Exam	10	
	• Viva	10	
4.	End Semester Examination		90