Roll No											

PRESIDENCY UNIVERSITY

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

Presidency University Act, 2013 of the Karnataka Act No. 41 of 2013 | Established under Section 2(f) of UGC Act, 1956
Approved by AICTE, New Delhi | Approved By BCI
Bengaluru

Even Semester End Term Examination, May / June 2026

Date: 22/05/2026		**Time: 09.30 AM - 12.30 PM**
Course Code: PGL3025	**Course Name: Cyber Crime and Digital Forensics**	
Semester: Second Semester	**Max. Marks: 100**	**Weightage: 50%**

CO - Levels	CO1	CO2	CO3	CO4	CO5
Marks	24	24	54	36	42

PART A: Answer Following Questions. 20 M

Qn.No	Questions	M	CO	BT
1	What is hacking? Distinguish between ethical hacking and illegal hacking.	2	CO1	BT1
2	State the meaning and two main objectives of the Information Technology Act, 2000.	2	CO2	BT1
3	What is a Denial of Service (DoS) attack? How does it differ from a DDoS attack?	2	CO1	BT1
4	What is digital evidence? Give three examples of digital evidence that can be produced in court.	2	CO3	BT1
5	Name any two types of jurisdiction relevant in cybercrime cases and explain each briefly.	2	CO2	BT1
6	What is the significance of Section 79A of the IT Act, 2000 in the context of digital forensics?	2	CO3	BT2
7	What is multi-factor authentication (MFA) and how does it enhance cyber security?	2	CO4	BT1
8	Explain the meaning of "encryption" and distinguish between symmetric and asymmetric encryption.	2	CO4	BT1
9	What is the role of CERT-In in India's cyber security framework?	2	CO4	BT1
10	What is a deepfake and how does it pose a legal and social threat in the context of cybercrime?	2	CO5	BT2

PART B: Answer Any 1 Following Questions. 10 M

PTO (Please Turn Over)

Qn.No	Questions	M	CO	BT
11	Explain the types of cybercrime classified by target crimes against individuals, property, and organizations, with examples of each and their legal consequences under Indian law.	10	CO1	BT2
12	Discuss the current and emerging trends in cybercrime, including ransomware-as-a-service, cryptocurrency-based payments, and AI-generated phishing attacks, and their impact on detection and prosecution.	10	CO1	BT3

PARTC: Answer Any 1 Following Questions. 10 M				
Qn.No	**Questions**	**M**	**CO**	**BT**
13	Explain the ethical and legal issues arising from government surveillance and monitoring in cyberspace with reference to the right to privacy recognized in Justice K.S. Puttaswamy v. Union of India (2017) and Section 69A of the IT Act.	10	CO2	BT3
14	Discuss the significance of digital forensics in criminal investigations, explaining its basic methodologies and the legal standards for admissibility of digital evidence in Indian courts.	10	CO2	BT2

PART D: Answer Any 1 Following Questions. 10 M				
Qn.No	**Questions**	**M**	**CO**	**BT**
15	Explain the legal foundation for handling digital evidence in India under the Bharatiya Sakshya Adhiniyam, 2023 and IT Act, 2000, including the certification requirements and how judicial precedents have shaped the law.	10	CO3	BT3
16	Discuss the role of cyber awareness and training in building an organization's human firewall against social engineering attacks, with reference to the behavioral and institutional dimensions of cybercrime prevention.	10	CO3	BT2

PART E: Answer Any 1 Following Questions. 15 M				
Qn.No	**Questions**	**M**	**CO**	**BT**
17	A 16-year-old girl receives friend requests from a stranger on Instagram. After weeks of chatting, the stranger convinces her to share personal photographs. The stranger then uses these photographs to blackmail her, demanding money and more images. The girl's parents report the matter to the police. Analyze the legal provisions applicable to cyber offences involving minors, along with the role of digital forensic investigation and jurisdictional challenges in such cases.	15	CO3	BT4
18	A journalist is investigating political corruption and uses an anonymous blogging platform to publish leaked government	15	CO3	BT4

	documents. The government issues a blocking order under Section 69A of the IT Act to take down the blog. The journalist challenges the order, arguing it violates freedom of speech. Analyze the conflict between government regulation of online content and the fundamental right to freedom of speech in India.			

PART F: Answer Any 1 Following Questions. 15 M				
Qn.No	**Questions**	**M**	**CO**	**BT**
19	A financial crime investigation team seizes a suspect's smartphone, which is password protected. The forensic examiner uses a commercial unlocking tool to bypass the password and extracts call records, banking apps, and deleted messages. The suspect argues that forced extraction violates his right against self-incrimination under Article 20(3) of the Constitution. Evaluate the constitutional validity of compelled access to digital devices and the admissibility of such evidence in court.	15	CO4	BT5
20	A multinational company operating in India discovers that an employee has been exfiltrating trade secrets by sending encrypted files to a competitor's server located abroad. The company's IT security team identifies the breach through log analysis. The company wants to preserve evidence and pursue legal action. Explain a digital forensic and incident response plan for handling a cyber breach, focusing on evidence preservation and legal compliance.	15	CO4	BT5

PART G: Answer Any 1 Following Questions. 20 M				
Qn.No	**Questions**	**M**	**CO**	**BT**
21	The AIIMS Delhi ransomware attack (2022) resulted in the encryption of critical patient data, forcing the hospital to operate manually for weeks. The attack was attributed to a foreign nation-state sponsored group. The malware exploited vulnerabilities in the hospital's outdated server infrastructure. CERT-In led the response, and law enforcement initiated an investigation. Digital forensic analysis identified the malware strain and traced communication logs to servers abroad.	20	CO5	BT5
22	An Indian law firm discovers that its client files, including confidential communications protected by attorney-client privilege, have been accessed by an unknown party through a spear-phishing attack on a senior partner's email account. The breach is discovered three weeks after it occurred. The firm must notify affected clients, preserve evidence, assess its legal liability, and implement	20	CO5	BT5

	preventive measures, all while maintaining confidentiality obligations. Critically analyze the legal and ethical obligations of a law firm in handling cyber incidents, including issues of evidence preservation and confidentiality.			

PTO (Please Turn Over)