SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

VIII SEMESTER-FINAL YEAR

1923804 – Cybercrime Investigations and Law Enforcement

Regulation – 2019

Academic Year: 2025 – 2026 (EVEN)

Prepared by

Mr. S.Giridharan, Assistant Professor / CYS

SRM VALLIAMMAI ENGINEERING COLLEGE
SRM Nagar, Kattankulathur-603203
DEPARTMENT OF CYBER SECURITY

QUESTION BANK

SUBJECT : 1923804 – Cybercrime Investigations and Law Enforcement

SEM / YEAR : VIII SEMESTER/ FINAL YEAR

UNIT -I INTRODUCTION

Introduction and Overview of Cyber Crime – Nature and Scope of Cyber Crime – Types of Cyber Crime: Social Engineering – Categories of Cyber Crime – Property Cyber Crime

UNIT –I [PART-A]

Q.No	Question	Competence	Level
1	What is cyber crime?	Remembering	BTL1
2	List the different types of cyber crimes?	Remembering	BTL1
3	Define ransomware attack.	Remembering	BTL1
4	Suggest some hacking techniques used by attackers.	Evaluating	BTL5
5	List the most powerful tools used in hacking.	Applying	BTL3
6	What is cyber terrorism?	Remembering	BTL1
7	Identify and explain two primary motivations that drive individuals to engage in cyber crime activities.	Analysing	BTL4
8	What are the preventive measures against cyber crimes?	Understanding	BTL2
9	Discuss the potential consequences of cyber crime for businesses.	Understanding	BTL2
10	Explain the term "malware" and its role in cyber crime.	Understanding	BTL2
11	What is the scope of Cyber Crime?	Creating	BTL6
12	What is Social Engineering attack?	Remembering	BTL1
13	What are the causes of Social Engineering attacks?	Understanding	BTL2
14	List the mitigation steps that can be taken against Social Engineering attacks.	Remembering	BTL1
15	What are the general categories of cybercrime?	Applying	BTL3
16	List the techniques used to perform Social Engineering attacks.	Applying	BTL3
17	Classify the different types of cyber criminals involved in cyber crime.	Analysing	BTL4
18	Difference between Cyber Crime and Conventional Crimes.	Evaluating	BTL5
19	Difference between virus and worm.	Analysing	BTL4
20	What role does social engineering play in various categories of cybercrime?	Creating	BTL6
21	What is the potential impact of cybercrimes on a global scale?	Understanding	BTL2
22	How do organizations learn from past incidents to enhance their security posture?	Evaluating	BTL5
23	Assess the financial impact of a recent cyber incident on affected businesses.	Applying	BTL3
24	Analyze a recent high-profile cybercrime case.	Analysing	BTL4

UNIT –I [PART-B]

Q.No	Question		Marks	Competence	Level
1	-	Classify and explain various types of cyber crimes and provide examples for each category and discuss the evolving nature of cyber threats.	13	Remembering	BTL1
2	A	Trace the evolution of cyber crime from its early stages to the	07	Evaluating	BTL5

		present day.			
	B	Discuss the preventive measures to overcome the cyber attacks and its measures.	06		
3	**-**	Analyze various social engineering techniques and provide detailed explanations of each technique, along with real-world examples.	13	Understanding	BTL2
4	**-**	Examine the tools and techniques used in cyber crime with its preventive measures.	13	Understanding	BTL2
5	**-**	Explain the role of email attachments in the spread of viruses.	13	Applying	BTL3
6	**A**	What is cyber crime? Discuss the motivation and techniques used by the cyber criminals.	07	Analysing	BTL4
	B	Define Social Engineering attack. List the tools and techniques used in Social Engineering attacks.	06		
7	**A**	Discuss the major cyber crimes that are happening frequently in cyberspace.	07	Remembering	BTL1
	B	List the preventive measures that can be taken against those Cyber attacks.	06		
8	**-**	Identify the impact of cyber security against cyber crime in the corporate world.	13	Analysing	BTL4
9	**-**	Discuss the technology development in Cyber Crime.	13	Remembering	BTL1
10	**A**	Discuss the types of cyber attacks on Mobile Phone.	07	Remembering	BTL1
	B	Discuss how it affects the Mobile users privacy along with its preventive measures.	06		BTL1
11	**-**	Can you provide examples of real-world incidents where social engineering was a key component of the attack?	13	Understanding	BTL2
12	**-**	Analyze a recent high-profile cybercrime case. What challenges were faced in attributing the crime to specific actors, and how were these challenges addressed or mitigated?	13	Applying	BTL3
13	**-**	What ethical considerations should be taken into account when developing strategies to combat cybercrime?	13	Applying	BTL3
14	**-**	What is the economic impact of cybercrime within each category on businesses and individuals?	13	Creating	BTL6
15	**-**	What role does the identification and exploitation of weaknesses play in the execution of cybercrimes?	13	Understanding	BTL2
16	**-**	Examine the legal outcomes of recent cybercrime cases	13	Analysing	BTL4
17	**-**	Evaluate the response of organizations to known vulnerabilities that were exploited in cyber attacks.	13	Evaluating	BTL5
UNIT -I[PART-C]					
1		Identify and explain various types of cybercrimes in the real-world with its preventive measures.	15	Evaluating	BTL5
2		Analyze the role of social engineering in cyber crimes. Discuss how attackers exploit human psychology to manipulate individuals and gain unauthorized access to systems.	15	Creating	BTL6
3		Explain in detail about the modes and methods of performing Cyber Crimes.	15	Evaluating	BTL5

4	Discuss the new trend in cyber crime and compare the methods and techniques used in conventional crime with the cyber crime.	15	Creating	BTL6
5	How does the digital environment contribute to the anonymity of cybercriminals?	15	Creating	BTL6

UNIT -II CYBER CRIME ISSUES

Unauthorized Access to Computers – Computer Intrusions – White collar Crimes – Viruses and Malicious Code – Internet Hacking and Cracking – Virus Attacks – Software Piracy – Intellectual Property – Mail Bombs – Exploitation – Stalking and Obscenity in Internet – Digital laws and legislation – Law Enforcement Roles and Responses.

UNIT-II [PART-A]

Q.No	Question	Competence	Level
1	Define unauthorized access to computers and explain why it is considered a cyber crime.	Remembering	BTL1
2	Name two common methods used by cybercriminals to gain unauthorized access to computers.	Remembering	BTL1
3	Define computer intrusions.	Understanding	BTL2
4	Define a computer virus and explain how it differs from other types of malicious code.	Creating	BTL6
5	What is software piracy?	Remembering	BTL1
6	What is white collar crime and who is involved in it?	Understanding	BTL2
7	Define the term mail bomb.	Remembering	BTL1
8	Differentiate internet hacking and internet cracking.	Understanding	BTL2
9	What are the 4 types of Intellectual Property?	Understanding	BTL2
10	Outline two cybersecurity measures that organizations can implement to protect against computer intrusions.	Analysing	BTL4
11	List the types of viruses.	Applying	BTL3
12	Define Intellectual Property.	Analysing	BTL4
13	What are the effects of mail bombing?	Creating	BTL6
14	What is internet hacking?	Applying	BTL3
15	Classify the types of tools used in internet hacking.	Applying	BTL3
16	What are the techniques used in computer intrusion?	Evaluating	BTl5
17	List the White Collar crimes.	Analysing	BTL4
18	What are the motivations behind performing unauthorized access into computers?	Evaluating	BTL5
19	What is stalking and obscenity on the internet?	Analysing	BTL4
20	What is the primary goal of exploitation?	Remembering	BTL1
21	Are there cultural or legal variations in the definition of obscenity?	Understanding	BTL2
22	How do digital copyright laws impact the rights and revenues of content creators in the online environment?	Applying	BTL3
23	How is digital evidence collected, preserved, and presented in legal proceedings?	Remembering	BTL1
24	What factors contribute to variations in response times?	Evaluating	BTL5

UNIT -II [PART-B]

Q.No		Question	Marks	Competence	Level
1	**A**	Explain the role of phishing attacks in facilitating unauthorized access.	08	Remembering	BTL1
	B	Provide an example of a phishing technique used for unauthorized access.	05		

2	**-**	Discuss the challenges in attributing computer intrusions to specific nation-states.	13	Analysing	BTL4
3	**A**	Explain the connection between unauthorized access and data breaches.	7	Understanding	BTL2
	B	Explain the importance of strong and unique passwords in preventing unauthorized access.	6		
4	**-**	Discuss how insider threats can contribute to unauthorized access in a workplace environment.	13	Understanding	BTL2
5	**-**	Define social engineering and explain how it can be used to facilitate unauthorized access.	13	Applying	BTL3
6	**-**	Define unauthorized access. List the techniques used to gain unauthorized access and its preventive measures.	13	Applying	BTL3
7	**-**	Discuss the various aspects of software piracy and its impact and preventive measures on the software industry.	13	Understanding	BTL2
8	**A**	What is internet hacking? Discuss the techniques and tools used in internet hacking.	6	Creating	BTL6
	B	What is internet cracking? Discuss the techniques and tools used in internet cracking.	7		
9	**-**	Explain the concept of mail bombing. Discuss the motives behind mail bombing and its impact on individuals, organizations and network systems.	13	Applying	BTL3
10	**-**	Discuss White collar crimes and analyze the challenges associated with investigating White-collar crimes.	13	Analysing	BTL4
11	**A**	How do intellectual property laws balance the protection of rights with fostering innovation and competition?	6	Evaluating	BTL5
	B	Can you provide examples of successful cases where digital content creators have been able to enforce their intellectual property rights?	7		
12	**-**	Name some common targets that cyber attackers aim to exploit during the exploitation phase.	13	Remembering	BTL1
13	**-**	What measures can individuals take to protect themselves from online stalking?	13	Remembering	BTL1
14	**A**	How is digital evidence handled and evaluated in legal proceedings?	6	Evaluating	BTL5
	B	Can you provide examples of cases where digital evidence played a critical role in legal outcomes?	7		
15	**-**	How is law enforcement response time measured in emergency situations, and what factors contribute to variations in response times?	12	Understanding	BTL2
16	**-**	How are obscenity laws applied to content on the internet?	13	Remembering	BTL1
17	**-**	What ethical considerations should be taken into account when conducting exploitation in penetration testing?	13	Analysing	BTL4
UNIT -II [PART-C]					
1	**-**	Provide a detailed analysis of common methods and techniques used by attackers for unauthorized access to computer systems.	15	Evaluating	BTL5
2	**-**	Analyze how ransomware functions as a form of	15	Creating	BTL6

		unauthorized access. Discuss the motivations behind ransomware attacks and their impact on victims.			
3	**A**	Define software piracy and its types.	5	Evaluating	BTL5
	B	Define Mail Bombing and explain how it operates.	5		
	C	What is White-collar crimes and the motive behind it?	5		
4	**-**	Discuss internet hacking and internet cracking. Analyze the evolving landscape of Cyber security and its countermeasures employed against internet hacking and cracking.	15	Creating	BTL6
5	**-**	How effectively do laws regulate digital speech on social media platforms without infringing on free expression?	15	Evaluating	BTL5

UNIT –III INVESTIGATION

Introduction to Cyber Crime Investigation – Investigation Tools – Discovery – Digital Evidence Collection – Evidence Preservation – E–Mail Investigation – Tracking – IP Tracking – E–Mail 116 Recovery – Hands on Case Studies – Encryption and Decryption Methods – Search and Seizure of Computers – Recovering Deleted Evidences – Password Cracking.

UNIT-III [PART-A]

Q.No	Question	Competence	Level
1	Define Cyber Crime Investigation and explain its significance in the digital age.	Remembering	BTL1
2	What are the key tools used in Cyber Crime Investigation, and how do they aid in the process?	Remembering	BTL1
3	Describe the process of digital evidence discovery and its role in cyber crime cases	Analysing	BTL4
4	Explain the importance of proper digital evidence collection in cyber crime investigations.	Remembering	BTL1
5	Discuss the methods and techniques involved in preserving digital evidence for legal purposes.	Understanding	BTL2
6	How does email investigation contribute to solving cyber crime cases, and what role do emails play as evidence?	Analysing	BTL4
7	Discuss the procedures and tools used in tracking IP addresses during a cyber crime investigation.	Understanding	BTL2
8	Elaborate on the challenges associated with preserving digital evidence in a rapidly evolving technological landscape.	Understanding	BTL2
9	Provide examples of hands-on case studies in cyber crime investigation and highlight key learnings.	Applying	BTL3
10	Explain the steps involved in the recovery of deleted emails as part of a cyber crime investigation.	Evaluating	BTL5
11	How can investigators ensure the admissibility of digital evidence in a court of law?	Applying	BTL3
12	Discuss the legal aspects and challenges associated with search and seizure of computers in cyber crime cases.	Remembering	BTL1
13	Elaborate on the techniques employed in password cracking during cyber crime investigations.	Understanding	BTL2
14	Explain the significance of chain of custody in the handling of digital evidence during investigations.	Creating	BTL6
15	Discuss the ethical considerations and privacy concerns related to cyber crime investigations.	Creating	BTL6
16	What role does encryption play in cyber crime, and how can investigators decrypt encoded information?	Applying	BTL3

17	Elaborate on the role of artificial intelligence and machine learning in cyber crime investigations.	Remembering	BTL1
18	Explain the methods used in recovering deleted evidence from digital devices during an investigation.	Understanding	BTL2
19	Analyze the evolving nature of cyber threats and the corresponding adaptations required in cyber crime investigation techniques.	Evaluating	BTL5
20	Discuss the role of public-private partnerships in combating cyber crimes.	Remembering	BTL1
21	Describe the role of forensic experts in cyber crime investigations and their responsibilities.	Applying	BTL3
22	How does password cracking contribute to uncovering critical information in digital forensics?	Evaluating	BTL5
23	Discuss the impact of technological advancements on the field of cyber crime investigation.	Analysing	BTL4
24	How does international cooperation enhance the effectiveness of cyber crime investigations?	Analysing	BTL4

UNIT -III [PART-B]

Q.No		**Question**	**Marks**	**Competence**	**Level**
1	**-**	Define cybercrime investigation and delineate the steps involved.	13	Remembering	BTL1
2	**A**	Explain about password cracking and its types.	07	Evaluating	BTL5
	B	Give tools involved in password cracking	06	Analysing	BTL4
3	**-**	Analyze the phases involved in cybercrime investigations.	13	Understanding	BTL2
4	**-**	Examine the challenges in the acquisition of digital evidence, emphasizing the importance of maintaining the integrity during an investigation.	13	Evaluating	BTL5
5	**-**	Present a comprehensive overview of the tools and methodologies employed in cybercrime investigations, substantiating your discussion with examples derived from real-world cases.	13	Understanding	BTL2
6	**-**	Evaluate the methodologies and technologies applied in the identification and tracking of cybercriminals.	13	Remembering	BTL1
7	**A**	Explain the recent cyber-attacks.	07	Applying	BTL3
	B	Who are cybercriminals and explain their types and motives	06		
8	**-**	Explain the process of email recovery in the context of cybercrime investigations. Explain its challenges involved.	13	Understanding	BTL2
9	**-**	Investigate various encryption and decryption techniques employed in cybercrime.	13	Remembering	BTL1
10	**A**	Illustrate the phases of investigation.	07	Analysing	BTL4
	B	Describe the collection phase in details	06		
11	**-**	Explore techniques and tools used in the recovery of deleted evidence. Provide illustrative case studies to underscore instances of successful recovery.	13	Creating	BTL6
12	**A**	Define cybercrime investigation.	07	Remembering	BTL1
	B	Explain the types of cyber investigation.	06		
13	**-**	Describe Password cracking. Examine password cracking methodologies and tools.	13	Understanding	BTL2
14	**-**	Define digital evidence and expound the steps involved in its collection.	13	Creating	BTL6

15	-	Illustrate in detail on email investigations, encompassing methodologies, tools.	13	Applying	BTL3
16	-	Discuss about search and seizure of computers	13	Analysing	BTL4
17	-	Explain the tools used in cybercrime investigations.	13	Applying	BTL3

UNIT -III [PART-C]

1	Define the cybercrime investigation and outline the sequential steps integral to its execution.	15	Evaluating	BTL5
2	Elaborate on the intricacies of email recovery within the context of cybercrime investigations, including the challenges inherent in the process.	15	Creating	BTL6
3	Investigate the techniques and tools employed in the recovery of deleted evidence, supported by illustrative case studies highlighting successful recovery instances.	15	Creating	BTL6
4	Break down the various phases encompassed in the investigation of cybercrimes, providing a detailed analysis of each.	15	Evaluating	BTL5
5	Provide an explanation of the diverse tools utilized in cybercrime investigations, elucidating their roles and functionalities in the investigative process.	15	Evaluating	BTL5

UNIT –IV DIGITAL FORENSICS

Introduction to Digital Forensics – Forensic Software and Hardware – Analysis and Advanced Tools – Forensic Technology and Practices – Forensic Ballistics and Photography – Face, Iris and Fingerprint Recognition – Audio Video Analysis – Windows System Forensics – Linux System Forensics – Network Forensics

UNIT -IV [PART-A]

Q.No	Question	Competence	Level
1	Explain digital forensics.	Remembering	BTL1
2	What are the key differences between traditional forensics and digital forensics?	Remembering	BTL1
3	Describe the challenges associated with collecting and preserving digital evidence.	Understanding	BTL2
4	Discuss the role of forensic software in digital investigations.	Remembering	BTL1
5	Name and explain three common forensic hardware tools used in digital investigations.	Analysing	BTL4
6	How does write-blocking technology contribute to the integrity of digital evidence?	Applying	BTL3
7	Outline the steps involved in the analysis phase of digital forensics.	Remembering	BTL1
8	Provide examples of advanced digital forensic tools and their applications.	Analysing	BTL4
9	What challenges might investigators face when dealing with encrypted data during digital forensic analysis?	Understanding	BTL2
10	How does the use of artificial intelligence impact digital forensic practices?	Analysing	BTL4
11	Explain the importance of chain of custody in digital forensics investigations.	Remembering	BTL1
12	Discuss the ethical considerations in the field of digital forensics.	Understanding	BTL2
13	What role does forensic ballistics play in criminal investigations?	Creating	BTL6
14	How can photography be utilized in digital forensics, particularly in crime scene documentation?	Creating	BTL6
15	Compare and contrast face, iris, and fingerprint recognition	Evaluating	BTL5

	technologies in forensic applications.		
16	Discuss the limitations and potential biases associated with biometric recognition systems.	Applying	BTL3
17	Explain the challenges involved in analyzing audio and video evidence in digital forensics.	Applying	BTL3
18	How can deep learning algorithms be employed in audio-video forensics?	Remembering	BTL1
19	Describe the key differences in conducting forensics on Windows and Linux systems.	Understanding	BTL2
20	What are the common artifacts investigators look for in Windows system forensics?	Analysing	BTL4
21	Define network forensics and its importance in investigating cybercrimes.	Applying	BTL3
22	Discuss the role of log analysis in network forensics.	Evaluating	BTL5
23	List the tools used in digital forensics.	Understanding	BTL2
24	Explain about iris and face recognition.	Evaluating	BTL5

UNIT -IV [PART-B]

Q.No		**Question**	**Marks**	**Competence**	**Level**
1	**A**	Describe Open-source forensic software.	6	Understanding	BTL2
	B	Describe Commercial forensic software.	7		
2	**-**	Define digital forensics investigation. Illustrate its steps involved.	13	Remembering	BTL1
3	**-**	Compare and contrast the advantages and disadvantages of open-source and commercial forensic software.	13	Remembering	BTL1
4	**-**	Illustrate Digital forensic investigation process with diagrammatic representation.	13	Applying	BTL3
5	**-**	What is digital forensic Analysis and explain the Advanced Tools used.	13	Analysing	BTL4
6	**A**	How does face recognition support digital forensics	7	Understanding	BTL2
	B	How does fingerprint recognition support digital forensics	6		
7	**A**	Explain the techniques and challenges involved in audio video analysis in digital forensics.	6	Evaluating	BTL5
	B	Explain the tools used in audio video analysis in digital forensics.	7		
8	**A**	Describe the key differences in conducting digital forensics on Linux systems.	6	Remembering	BTL1
	B	Describe the key differences in conducting digital forensics on windows systems.	7	Understanding	BTL2
9	**A**	Illustrate in detail about Network forensic.	8	Applying	BTL3
	B	Explore the tools used in network forecsics	5		
10	**-**	Illustrate the Forensic Software and Hardware	13	Creating	BTL5
11	**-**	Discuss the challenges associated with preserving and analyzing network-based digital evidence.	13	Remembering	BTL1
12	**-**	Describe about Forensic Technology and its Practices	13	Applying	BTL3
13	**-**	What role does forensic ballistics play in criminal investigations, and how is it applied in the digital realm?	13	Creating	BTL6
14	**-**	Discuss the use of photography in digital forensics, highlighting key considerations for capturing and	13	Analysing	BTL4

		analyzing digital images.			
15	-	Compare and contrast face, iris, and fingerprint recognition technologies in digital forensics.	13	Analysing	BTL4
16	-	Discuss the privacy and security implications of using biometric data in forensic investigations.	13	Understanding	BTL2
17	-	What is network forensics, and how does it contribute to investigating cybercrimes?	13	Remembering	BTL1
UNIT -IV [PART-C]					
1	-	Define digital forensic analysis and elucidate the advanced tools utilized in the process.	15	Evaluating	BTL5
2	-	Examine the pros and cons of both open-source and commercial forensic software, highlighting the distinctions between the two	15	Creating	BTL6
3	-	Provide a definition of a digital forensics investigation and outline the steps integral to its execution.	15	Evaluating	BTL5
4	-	Depict the landscape of forensic software and hardware, illustrating their applications in digital investigations.	15	Creating	BTL6
5	-	Explain the concept of network forensics and its role in the examination of cybercrimes.	15	Evaluating	BTL5

UNIT -V LAWS AND ACTS

Laws and Ethics – Digital Evidence Controls – Evidence Handling Procedures – Basics of Indian Evidence ACT IPC and CrPC – Electronic Communication Privacy ACT – Legal Policies.

[PART-A]

Q.No	Question	Competence	Level
1	What is the purpose of laws in society?	Remembering	BTL1
2	Define ethical principles and provide an example of how they influence decision-making.	Remembering	BTL1
3	What is the difference between a law and an ethical guideline?	Analysing	BTL4
4	Explain the concept of legal liability and its significance in relation to ethics	Understanding	BTL2
5	What are digital evidence controls, and why are they important in the context of digital investigations?	Understanding	BTL2
6	Name three common types of digital evidence controls used to ensure the integrity and authenticity of digital evidence.	Creating	BTL6
7	Explain the concept of chain of custody in digital forensics and its significance in preserving the admissibility of digital evidence	Remembering	BTL1
8	What role does encryption play in digital evidence controls, and how does it impact the handling and storage of digital evidence?	Applying	BTL3
9	Discuss the challenges associated with maintaining the integrity of digital evidence in the face of rapidly evolving technology and changing data storage formats.	Understanding	BTL2
10	What are digital evidence controls, and why are they important in the context of digital investigations?	Remembering	BTL1
11	Name three common types of digital evidence controls used to ensure the integrity and authenticity of digital evidence.	Understanding	BTL2
12	Explain the concept of chain of custody in digital forensics and its significance in preserving the admissibility of digital evidence.	Evaluating	BTL5

13	What role does encryption play in digital evidence controls, and how does it impact the handling and storage of digital evidence?	Analysing	BTL4
14	Discuss the challenges associated with maintaining the integrity of digital evidence in the face of rapidly evolving technology and changing data storage formats.	Remembering	BTL1
15	How can conflicts arise between legal requirements and ethical considerations, and how can they be resolved?	Applying	BTL3
16	What are digital evidence controls, and why are they important in the context of digital investigations?	Applying	BTL3
17	Name three common types of digital evidence controls used to ensure the integrity and authenticity of digital evidence.	Creating	BTL6
18	Explain the concept of chain of custody in digital forensics and its significance in preserving the admissibility of digital evidence.	Analysing	BTL4
19	What role does encryption play in digital evidence controls, and how does it impact the handling and storage of digital evidence?	Evaluating	BTL5
20	Discuss the challenges associated with maintaining the integrity of digital evidence in the face of rapidly evolving technology and changing data storage formats.	Evaluating	BTL5
21	Discuss the challenges and debates surrounding the ECPA in the context of modern technology and digital privacy concerns	Understanding	BTL2
22	What is the Electronic Communications Privacy Act (ECPA), and what is its primary objective?	Remembering	BTL1
23	Explain the key provisions of the ECPA that protect the privacy of electronic communications.	Analysing	BTL4
24	What are the main differences between Title I and Title II of the ECPA?	Applying	BTL3

UNIT -V [PART-B]

Q.No		**Question**	**Marks**	**Competence**	**Level**
1	**A**	Explain the concept of digital evidence controls comprehensively.	08	Remembering	BTL1
	B	Discuss the main objectives of digital evidence controls and the specific measures used to ensure the integrity, authenticity, and admissibility of digital evidence in the context of digital investigations.	05		
2	**-**	Discuss the relationship between laws and ethics. How do they intersect, and what are the key differences between the two? Provide examples to illustrate your points.	13	Analysing	BTL4
3	**-**	Explore the challenges that arise when ethical considerations conflict with existing laws or legal frameworks. Discuss the potential consequences of such conflicts and propose approaches for resolving them.	13	Understanding	BTL2
4	**A**	Identify and discuss some of the common challenges and threats associated with maintaining the integrity and security of digital evidence.	06	Understanding	BTL2
	B	Propose the strategies and best practices that can be implemented to mitigate these risks and enhance the	07	Remembering	BTL1

		effectiveness of digital evidence controls.			
5	**-**	Ethics can sometimes inform the creation and amendment of laws. Provide examples of historical or contemporary instances where ethical considerations influenced the development of legal frameworks or led to significant legal reforms.	13	Understanding	BTL2
6	**A**	Outline the key principles and steps involved in establishing and maintaining an unbroken chain of custody for digital evidence.	08	Applying	BTL3
	B	Discuss the potential implications and consequences of a compromised chain of custody on the admissibility and credibility of digital evidence in legal proceedings.	05		
7	**-**	Compare and contrast the specific challenges and considerations associated with handling each type of evidence. Discuss the best practices, techniques, and technologies that can be employed to overcome these challenges and ensure effective evidence handling in each case.	13	Remembering	BTL1
8	**A**	Describe in detail the step-by-step process involved in evidence handling procedures, from the initial collection of evidence at a crime scene to its presentation in court.	06	Evaluating	BTL5
	B	Discuss the significance of each step and the specific measures that should be taken to maintain the chain of custody, preserve the integrity of physical and digital evidence, and ensure its admissibility in legal proceedings.	07		
9	**-**	In what ways does the Electronic Communications Privacy Act (ECPA) balance the interests of privacy and law enforcement/security in the digital age?	13	Remembering	BTL1
10	**-**	In what ways can businesses navigate the balance between profit maximization and ethical responsibility within the confines of existing legal frameworks, and what role should regulations play in ensuring ethical business practices?	13	Analysing	BTL4
11	**-**	What are the ethical considerations surrounding the use of emerging technologies, such as artificial intelligence or genetic engineering, and how should legal frameworks adapt to address these ethical concerns?	13	Understanding	BTL2
12	**-**	How do cultural differences influence the interpretation and implementation of laws and ethical principles across various societies, and what challenges does this pose in creating globally applicable standards?	13	Analysing	BTL4
13	**-**	What are the primary challenges in enforcing and complying with its regulations in today's evolving digital landscape?	13	Evaluating	BTL5
14	**A**	What are the key provisions and protections offered by the Electronic Communications Privacy Act (ECPA)?	07	Applying	BTL3
	B	How have technological advancements since its enactment impacted the interpretation and application of these provisions?	06		
15	**-**	What are the key provisions and protections offered by	13	Creating	BTL6

		the Electronic Communications Privacy Act (ECPA)?			
16	**-**	How have technological advancements since its enactment impacted the interpretation and application of these provisions?	13	Applying	BTL3
17	**-**	How does the Electronic Communications Privacy Act (ECPA) govern the interception and access of electronic communications by government entities, service providers, and third parties?	13	Understanding	BTL2
UNIT-V[PART-C]					
1		Discuss the relationship between laws and ethics. How do they intersect, and what are the key differences between the two? Provide examples to illustrate your points.	15	Creating	BTL6
2		Compare and contrast the specific challenges and considerations associated with handling each type of evidence. Discuss the best practices, techniques, and technologies that can be employed to overcome these challenges and ensure effective evidence handling in each case.	15	Creating	BTL6
3		Ethics can sometimes inform the creation and amendment of laws. Provide examples of historical or contemporary instances where ethical considerations influenced the development of legal frameworks or led to significant legal reforms.	15	Evaluating	BTL5
4		What are the key provisions and protections offered by the Electronic Communications Privacy Act (ECPA)?	15	Evaluating	BTL5
5		How does the Electronic Communications Privacy Act (ECPA) govern the interception and access of electronic communications by government entities, service providers, and third parties?	15	Creating	BTL6