SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

IV SEMESTER

CY3461 - BASICS OF CYBER FORENSICS

Regulation – 2023

Academic Year 2025 – 2026

(EVEN SEMESTER)

Prepared by

Mr.G. Avinesh Kumar,

Assistant Professor (O.G) / CYS

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203.

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

SUBJECT: CY3461 - BASICS OF CYBER FORENSICS

SEM / YEAR: IV SEM / II Year

UNIT – I : INTRODUCTION TO DIGITAL FORENSICS

Introduction Digital Forensics - Preparing for Digital Investigations - Maintaining Professional Conduct - Preparing a Digital Forensics Investigation - Understanding Data Recovery Workstations and Software - Conducting an Investigation.

PART – A

Q.No	Questions	BT Level	Competence
1.	Define digital forensics	BTL 1	Remembering
2.	What are the four primary stages of the digital forensic process?	BTL 1	Remembering
3.	How does digital forensics differ from traditional forensics?	BTL 2	Understanding
4.	What are two examples of digital devices that can hold evidence?	BTL 1	Remembering
5.	What is the importance of planning before conducting a digital investigation?	BTL 2	Understanding
6.	Mention two essential tools needed for preparing a digital investigation.	BTL 2	Understanding
7.	What is the purpose of a digital forensics toolkit?	BTL 1	Remembering
8.	Why is documenting the investigation plan crucial in digital forensics?	BTL 1	Remembering
9.	Define the chain of custody in digital forensics.	BTL 2	Understanding
10.	Mention two ethical responsibilities of a digital forensic examiner.	BTL 2	Understanding
11.	Why is confidentiality important in digital forensics investigations?	BTL 1	Remembering
12.	What is meant by impartiality in digital forensics?	BTL 2	Understanding
13.	What is a write blocker, and why is it used?	BTL 1	Remembering
14.	List two challenges faced when preparing a digital investigation.	BTL 1	Remembering
15.	What is the role of evidence integrity in a forensic investigation?	BTL 1	Remembering
16.	Mention two considerations when selecting tools for a digital investigation.	BTL 2	Understanding
17.	What is a data recovery workstation?	BTL 2	Understanding
18.	Name two software tools commonly used for data recovery.	BTL 1	Remembering
19.	What is the purpose of a hash value in verifying data integrity?	BTL 2	Understanding
20.	Why are imaging tools important in data recovery?	BTL 1	Remembering
21.	What is the role of a forensic acquisition tool in an investigation?	BTL 2	Understanding

PART – B

1.	Explain the importance of digital forensics in modern investigations. Provide examples of cases where digital forensics plays a crucial role. (16)	BTL 3	Applying
2.	What are the key challenges faced by digital forensic investigators when dealing with digital evidence? (16)	BTL 4	Analyzing
3.	Describe the different branches of digital forensics (e.g., network forensics, mobile forensics, etc.) and their significance in investigations. (16)	BTL 3	Applying
4.	Discuss the difference between live forensics and dead forensics. In which situations is each method used? (16)	BTL 3	Applying
5.	Outline the steps involved in preparing for a digital forensic investigation. What tools and resources are necessary? (16)	BTL 4	Analyzing

6.	Explain the significance of evidence preservation during the preparation phase. What are the consequences of improper preservation? (16)	BTL 3	Applying
7.	Discuss the factors to consider when planning a digital investigation. How do you ensure accuracy and efficiency? (16)	BTL 4	Analyzing
8.	Describe the components of a standard digital forensics toolkit. Provide examples of software and hardware tools used. (16)	BTL 4	Analyzing
9.	What is the chain of custody, and why is it critical to maintain during digital investigations? Explain with an example. (16)	BTL 4	Analyzing
10	Discuss the ethical responsibilities of a digital forensic investigator. Why is Impartiality and confidentiality important? (16)	BTL 4	Analyzing
11.	Explain how digital forensic professionals can avoid conflicts of interest and maintain professional integrity. (16)	BTL 3	Applying
12.	What are the legal implications of mishandling digital evidence? Discuss the role of professional conduct in ensuring evidence admissibility in court. (16)	BTL 3	Applying
13.	Explain the importance of using write blockers during the acquisition process. How do write blockers ensure evidence integrity? (16)	BTL 3	Applying
14.	Discuss the role of evidence imaging in digital forensics. How does creating a forensic image help in investigations? (16)	BTL 3	Applying
15.	What is the significance of proper documentation when preparing for a digital forensic investigation? What details should be included in the report? (16)	BTL 4	Analyzing
16.	Describe the challenges faced during the preparation stage of an investigation. How can investigators overcome these challenges? (16)	BTL 4	Analyzing
17.	What is a data recovery workstation? Explain its components and the role it plays in digital investigations. (16)	BTL 3	Applying
18	Describe two software tools used for recovering lost or deleted data. How do these tools work? (16)	BTL 4	Analyzing
19	Explain the process of recovering data from damaged or corrupted storage devices. What challenges can arise during this process? (16)	BTL 3	Applying
20	What is a hash value, and why is it critical when verifying the integrity of recovered data? Explain with an example. (16)	BTL 4	Analyzing

UNIT – II : PROCESSING CRIME AND INCIDENT SCENES

Identifying Digital Evidence – Collecting Evidence in Private-Sector Incident Scenes Preparing for a Search- Securing a Digital Incident or Crime Scene- Seizing Digital Evidence at the Scene - Storing Digital Evidence- Reviewing a Case.

PART – A

Q.No	Questions	BT Level	Competence
1.	Define digital evidence.	BTL 1	Remembering
2.	Mention two characteristics of admissible digital evidence.	BTL 2	Understanding
3.	List two common types of digital evidence found in cybercrime investigations.	BTL 1	Remembering
4.	What are two challenges faced when collecting evidence in private-sector incident Scenes?	BTL 2	Understanding
5.	Why is identifying digital evidence important in an investigation?	BTL 2	Understanding
6.	Name two tools used to identify hidden digital evidence.	BTL 1	Remembering
7.	Differentiate between private-sector and public-sector investigations.	BTL 1	Remembering
8.	Name two examples of evidence commonly found in private-sector incident scenes.	BTL 1	Remembering
9.	Why is a search warrant often not required in private-sector incident investigations?	BTL 2	Understanding

10.	How can investigators ensure the integrity of evidence collected in a private-sector Environment?	BTL 1	Remembering
11.	List two items an investigator must carry when preparing for a digital evidence Search.	BTL 1	Remembering
12.	Mention two ways to minimize evidence contamination during a search.	BTL 1	Remembering
13.	What is the significance of a search warrant in digital evidence collection?	BTL 2	Understanding
14.	What is the first step when securing a digital crime scene?	BTL 2	Understanding
15.	List two methods to prevent tampering with evidence at a digital crime scene.	BTL 1	Remembering
16.	Why is it important to document the condition of the scene before starting the investigation?	BTL 2	Understanding
17.	Mention two challenges investigators face in securing a digital crime scene.	BTL 1	Remembering
18.	What are two precautions to take when handling live digital devices at a crime Scene?	BTL 2	Understanding
19.	What is the purpose of labeling seized digital evidence?	BTL 2	Understanding
20.	Name two precautions when seizing storage devices to avoid data loss.	BTL 1	Remembering
21.	List two tools used to create forensic images of seized digital evidence.	BTL 1	Remembering
22.	Why is maintaining a chain of custody essential for seized evidence?	BTL 2	Understanding
23.	Mention two examples of volatile data that should be collected first during seizure.	BTL 2	Understanding
	PART – B		
1	Explain the concept of digital evidence and its role in modern investigations. (16)	BTL 4	Analyzing
2	Discuss the key challenges investigators face in identifying digital evidence. (16)	BTL 4	Analyzing
3	Describe the process of identifying volatile and non-volatile digital evidence. (16)	BTL 3	Applying
4	Explain the importance of metadata in identifying digital evidence. (16)	BTL 4	Analyzing
5	How does the scope of investigations in private-sector incident scenes differ from public-sector cases? (16)	BTL 3	Applying
6	Outline the procedures for collecting evidence in private-sector environments Without violating employee privacy. (16)	BTL 3	Applying
7	Discuss the legal implications of evidence collection in private-sector Investigations. (16)	BTL 4	Analyzing
8	Describe the challenges of handling encrypted data during evidence collection in private-sector cases. (16)	BTL 3	Applying
9	Explain the importance of working with internal teams, such as IT departments, during private-sector evidence collection. (16)	BTL 4	Analyzing
10	Explain the significance of obtaining search warrants in digital evidence Investigations. (16)	BTL 2	Understanding
11	Discuss the role of risk assessment and contingency planning in preparing for a search. (16)	BTL 4	Analyzing
12	Describe the ethical considerations involved in preparing for a digital evidence search. (16)	BTL 3	Applying
13.	Explain the importance of securing a digital crime scene to preserve evidence integrity. (16)	BTL 4	Analyzing

14	What are the steps to document and photograph a digital incident scene Before starting an investigation? (16)	BTL 3	Applying
15.	Discuss the role of a first responder in securing a digital incident or crime scene. (16)	BTL 3	Applying
16.	Explain how investigators can ensure that no digital evidence is tampered with during the securing process. (16)	BTL 4	Analyzing
17.	Describe the procedures for seizing digital evidence at a crime scene while maintaining its admissibility in court. (16)	BTL 3	Applying
18.	Explain the significance of the chain of custody when handling seized digital Evidence. (16)	BTL 4	Analyzing
19.	Discuss how forensic imaging is used to preserve the integrity of seized digital evidence. (16)	BTL3	Applying
20.	Explain how to prioritize the collection of volatile data during evidence seizure. (16)	BTL4	Analyzing
21.	Explain the legal and procedural requirements for long-term storage of digital evidence. (16)	BTL4	Analyzing

UNIT – III : ANALYSIS AND VALIDATION

Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition –Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics.

PART – A

Q.No	Questions	BT Level	Competence
1.	Define data discrimination is done by using Hash Values.	BTL 1	Remembering
2.	Give some legal and illegal purposes for using steganography.	BTL 1	Remembering
3.	Analyze whether password recovery is included in all the computer forensic tools is used or not. Why?	BTL 2	Understanding
4.	Show the guidelines for identifying steganography files.	BTL 1	Remembering
5.	List the general procedures used for most Computer Forensics Investigations.	BTL 2	Understanding
6.	Give the methods for Steganalysis Attack.	BTL 1	Remembering
7.	Classify the Compression techniques used in Computer Forensics	BTL 1	Remembering
8.	Interpret Bit Shifting with an example.	BTL 1	Remembering
9.	Point out the Shareware Programs for Remote Acquisitions.	BTL 2	Understanding
10.	What is the purpose of PUK (Pin Unlock Key)?	BTL 2	Understanding

11.	How will you generalize the modes of Protection?	BTL 2	Understanding
12.	Define any three standard procedures used in Network Forensics.	BTL 2	Understanding
13.	Examine whether all the e-mail headers contain the same type of information.	BTL 1	Remembering
14.	Decide the roles of Client and Servers in E-mail investigations.	BTL 1	Remembering
15.	Give the e-mail storage format available in Novell Evolution.	BTL 1	Remembering
16.	Analyze how the Router logs can be used to verify the types of E-mail data?	BTL 2	Understanding
17.	Decide whether you need a search warrant to retrieve information from a system server.	BTL 2	Understanding
18.	Mention the four places where mobile device information might be used.	BTL 2	Understanding
19.	What are the SIMCon's features?	BTL 2	Understanding
20.	Create steganography. Isolate a mobile device from incoming signals and in what way it is related to MVNO (Mobile Virtual Network Operator?	BTL 1	Remembering
21.	What is scope creep?	BTL 2	Understanding
22.	Define file manipulation.	BTL 2	Understanding
23.	Infer the use of Key escrow?	BTL 2	Understanding
	PART – B		
1	Discuss how will you validate the forensic data using: (i) Validating the hexadecimal (8) (ii) Validating with Computer Forensics Programs(8)	BTL 4	Analyzing
2	Examine in detail the techniques used for Addressing Data Hiding.(16)	BTL 3	Applying
3	Describe the process of performing remote acquisition in detail(16)	BTL 4	Analyzing
4	Explain the following terms in detail:- (i) Securing a Network (8) (ii) Performing Live Acquisitions(8)	BTL 3	Applying
5	Generalize the roles of the following term in investigations:- (i) Network Forensics(6) (ii) Cell Phone Device Forensics(6) (iii) Order of Volatility(4)	BTL 4	Analyzing
6	Explain briefly about the following terms in detail:- (i) Examining and copying E-mail Messages(8) (ii) Copying an E-mail Message(8)	BTL 3	Applying
7	Describe the process of investigating email crimes and violation.(16)	BTL 4	Analyzing
8	Describe in detail about using specialized E-mail Forensics Tools.(16)	BTL 4	Analyzing
9	Examine the following e-mail server logs: (i) UNIX E-mail server Logs (8) (ii) Microsoft E-mail Server Logs(8)	BTL 3	Applying
10	Analyze how mobile devices play a crucial role in forensics by : (i) Basics of mobile Forensics(6) (ii) Inside Mobile Devices(6) (iii) Inside PDAs(4)	BTL 3	Applying
11	Describe in detail about the steps involved in securing a network.(16)	BTL 4	Analyzing

12	Briefly explain how the following roles are applied in investigations:- (i) E-mail in investigations(8) (ii) E-mail in Client and Server(8)	BTL 4	Analyzing
13	Give a brief description of the following data-hiding techniques: (i) Hiding Partitions(6) (ii) Bit-Shifting (6) (iii) Marking Bad Clusters(4)	BTL 3	Applying
14	Explain in detail about validating and testing Forensics Software.(16)	BTL 3	Applying
15.	Explain the basic steps for all computer forensics investigations.(16)	BTL 3	Applying
16.	What are data hiding techniques in forensics? Explain.(16)	BTL 4	Analyzing
17.	Explain the four methods of acquiring data for forensics analysis?(16)	BTL 4	Analyzing
18.	Develop Standard Procedures for Network Forensics and explain the working of any one network tool.(16)		
19.	To analyze e-mail evidence, an investigator must be knowledgeable about an e-mail server's internal operations. True or False? Justify your answer with suitable use cases.(16)	BTL 6	Creating
20.	When acquiring a mobile device at an investigation scene, you should leave it Connected to a PC so that you can observe synchronization as it takes place. True or False? Justify your answer.(16)	BTL 5	Evaluating
21.	Explain about Validating Forensic Data.(16)	BTL 5	Evaluating

UNIT-IV E-MAIL AND SOCIAL MEDIA INVESTIGATIONS

Role of E-mail in Investigations – Roles of the Client and Server in E-mail – Investigating E- mail Crimes and Violations-
Understanding E-mail Server- E-mail Forensics Tools - Social Media Forensics on Mobile Devices Performing.

PART – A

Q.No	Questions	BT Level	Competence
1.	How can e-mails serve as digital evidence in investigations?	BTL 1	Remembering
2.	Mention two types of crimes where e-mails are commonly used as evidence.	BTL 1	Remembering
3.	What are two advantages of using e-mail evidence in investigations?	BTL 2	Understanding
4.	Define the term "header analysis" in the context of e-mail investigations.	BTL 1	Remembering
5.	How does IP address tracking assist in e-mail investigations?	BTL 1	Remembering
6.	What is the role of an e-mail client in sending and receiving messages?	BTL 1	Remembering
7.	List two functions of an e-mail server.	BTL 2	Understanding
8.	Differentiate between IMAP and POP3 protocols in e-mail communication.	BTL 2	Understanding
9.	What is the purpose of the SMTP protocol in e-mail systems?	BTL 2	Understanding
10.	How do clients and servers work together to ensure reliable e-mail delivery?	BTL 2	Understanding
11.	Mention two common types of e-mail crimes.	BTL 2	Understanding
12.	Why is the analysis of e-mail headers important in investigating e-mail violations?	BTL 1	Remembering
13.	List two techniques used to trace the origin of phishing e-mails.	BTL 2	Understanding
14.	What role does a spam filter play in preventing e-mail crimes?	BTL 2	Understanding
15.	Name two challenges faced during the investigation of e-mail crimes.	BTL 1	Remembering
16.	What is an e-mail server, and why is it critical in forensic investigations?	BTL 2	Understanding
17.	Mention two types of e-mail servers commonly used in organizations.	BTL 1	Remembering
18.	Name two tools used for e-mail forensics and their primary functions.	BTL 1	Remembering
19.	What is the primary objective of social media forensics?	BTL 1	Remembering

20.	List two challenges faced during social media forensics on mobile devices.	BTL 1	Remembering

PART-B			
1.	Discuss the significance of e-mails in uncovering digital evidence during criminal investigations.(16)	BTL 3	Applying
2.	Explain the types of e-mail metadata that are essential for forensic analysis.(16)	BTL 4	Analyzing
3.	Examine the process of ensuring the authenticity and integrity of e-mails Used as evidence. (16)	BTL 4	Analyzing
4.	Explore the interaction between e-mail clients and servers in transmitting and storing messages. (16)	BTL 4	Analyzing
5.	Assess the vulnerabilities in client-server communication that cybercriminals exploit. (16)	BTL 3	Applying
6.	Describe the role of protocols like SMTP, IMAP, and POP3 in e-mail communication.(16)	BTL 3	Applying
7.	Examine the steps involved in investigating phishing, spoofing, and Business e-mail compromise cases. (16)	BTL 3	Applying
8.	Discuss the importance of e-mail headers in tracing the source of malicious Communications. (16)	BTL 3	Applying
9.	Evaluate the tools and techniques for recovering deleted e-mails during an Investigation. (16)	BTL 4	Analyzing
10.	Explain the legal and ethical considerations in accessing and analyzing suspect e-mails(16)	BTL 3	Applying
11.	Analyze the role of service providers in aiding investigations of e-mail-related crimes. (16)	BTL 3	Applying
12.	Describe the architecture of e-mail servers and its relevance in forensic investigations. (16)	BTL 3	Applying
13.	Explore the types of logs and data stored on e-mail servers that assist in investigations(16)	BTL 4	Analyzing
14.	Discuss the risks associated with misconfigured e-mail servers in facilitating cybercrimes(16)	BTL 3	Applying
15.	Investigate the capabilities and limitations of popular e-mail forensic tools. (16)	BTL 6	Creating
16.	(i) Evaluate the impact of server misconfigurations, such as open relay exploitation, on the security of e-mail communications.(8) (ii) Explain how encryption mechanisms like SSL/TLS enhance the security of e-mail servers during data transmission.(8)	BTL 5	Evaluating
17.	Assess the effectiveness of tools in detecting anomalies in e-mail communication patterns. (16)	BTL 3	Applying
18.	Examine the processes for tracing the origin of spoofed e-mails using forensic tools. (16)	BTL3	Applying

UNIT V CLOUD FORENSICS

Overview of Cloud Computing - Legal Challenges in Cloud Forensics - Technical Challenges in Cloud Forensics - Standards and Training - Acquisitions in the Cloud – Cloud Investigation.

PART-A

Q.No	Questions	BT Level	Competence
1.	Define cloud computing.	BTL 1	Remembering
2.	List the three primary service models of cloud computing.	BTL 2	Understanding
3.	Differentiate between public and private cloud deployment models.	BTL 1	Remembering
4.	Name two examples of cloud service providers.	BTL 1	Remembering
5.	Explain the significance of jurisdiction in cloud forensics.	BTL 1	Remembering
6.	State two privacy laws that impact cloud forensic investigations.	BTL 1	Remembering
7.	Mention two legal constraints when acquiring evidence from the cloud.	BTL 2	Understanding

8.	List two ways investigators ensure compliance with legal requirements in Cloud forensics.	BTL 2	Understanding
9.	State two reasons why multi-tenancy complicates cloud forensics.	BTL 2	Understanding
10.	Mention two issues caused by the lack of physical access to cloud servers during investigations.	BTL 2	Understanding
11.	Identify two challenges in ensuring the chain of custody for cloud-based evidence.	BTL 1	Remembering
12.	List two difficulties in analyzing encrypted data stored in the cloud.	BTL 1	Remembering
13.	Name two tools commonly used for cloud forensic investigations.	BTL 1	Remembering
14.	Mention two international standards relevant to cloud forensics.	BTL 2	Understanding
15.	Identify two organizations involved in setting cloud forensic standards.	BTL 2	Understanding
16.	List two benefits of standardized procedures in cloud forensic Investigations.	BTL 2	Understanding
17.	Name two challenges in implementing uniform training programs for cloud forensic investigators.	BTL 1	Remembering
18.	Define the term "live acquisition" in cloud forensics.	BTL 1	Remembering
19.	State two methods used to collect volatile data from cloud environments.	BTL 2	Understanding
20.	Identify two differences between logical and physical acquisitions in the cloud.	BTL 2	Understanding
21.	Mention two challenges in collecting logs from cloud service providers.	BTL 2	Understanding
22	List two best practices for acquiring evidence in cloud forensic Investigations.	BTL 1	Remembering
	PART-B		
1.	Discuss the characteristics of cloud computing as defined by the NIST framework. (16)	BTL 3	Applying
2.	Explain the differences between IaaS, PaaS, and SaaS cloud service models with examples. (16)	BTL 3	Applying
3.	Describe how virtualization technology supports the functioning of cloud computing. (16)	BTL 4	Analyzing
4.	Examine the impact of cloud scalability and elasticity on modern business operations. (16)	BTL 3	Applying
5.	Evaluate how data jurisdiction impacts the collection of evidence in cloud environments. (16)	BTL 5	Evaluating
6.	Explain the challenges of obtaining legal consent for accessing multi-tenant cloud environments. (16)	BTL 3	Applying
7.	Analyze the legal implications of data residency requirements on cross-border investigations. (16)	BTL 4	Analyzing
8.	Discuss the importance of service level agreements (SLAs) in addressing legal challenges in cloud forensics. (16)	BTL 3	Applying
9.	(i) Discuss how the lack of physical access to cloud infrastructure affects forensic investigations. (8) (ii) Evaluate the limitations of traditional forensic tools in acquiring evidence from virtualized environments. (8)	BTL 3	Applying
10.	Examine the challenges posed by multi-tenancy in isolating and preserving evidence(16)	BTL 3	Applying
11.	Analyze the technical difficulties in reconstructing events from log data stored in distributed cloud systems. (16)	BTL 4	Analyzing
12.	Discuss the importance of establishing standardized procedures in cloud forensics. (16)	BTL 1	Remembering
13.	(i) Analyze the challenges in developing universal cloud forensic standards across jurisdictions. (8) (ii) Evaluate the need for specialized training to handle unique challenges in live cloud acquisitions.(8)	BTL 5	Evaluating
14.	Explain the role of certifications and training programs in Improving cloud forensic expertise. (16)	BTL 3	Applying

15.	Discuss the differences between live and static acquisitions in cloud forensics and their respective use cases. (16)	BTL 3	Applying
17.	Elaborate on client/server application program TELNET. (16)	BTL 6	Creating
18.	(i) Analyze the challenges of acquiring volatile memory data from virtual machines in the cloud.(8) (ii) Examine the limitations of snapshot-based acquisitions in capturing real-time cloud activities.(8)	BTL 4	Analyzing
19.	Explain the process of collecting log data from cloud service providers during an investigation. (16)	BTL 3	Applying
20.	Explain the steps involved in a cloud forensic investigation, from evidence identification to reporting. (16)	BTL 3	Applying
21.	Discuss how investigators address anti-forensic techniques used by criminals in cloud environments. (16)	BTL 4	Analyzing