

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK



VII SEMESTER

OCY101- CYBER FORENSIC AND INVESTIGATION

Regulation – 2023

Academic Year 2026 – 2027 (ODD SEMESTER)

Prepared by

**MS. C. JESIFICA CINTHAMANI, Assistant
Professor (O.G) / CYS**



SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)
SRM Nagar, Kattankulathur – 603 203.

DEPARTMENT OF CYBER SECURITY



QUESTION BANK

SUBJECT: OCY101-CYBER FORENSIC AND INVESTIGATION

SEM / YEAR : VII Sem / IV Year

UNIT – I : INTRODUCTION TO CYBER FORENSICS

Computer Forensics Fundamentals – Types of Computer Forensics Technology– Types of Computer Forensics Systems – Vendor and Computer Forensics Services.

PART – A

Q.No	Questions	BT Level	Competence
1.	Define Computer Forensics.	BTL 1	Remembering
2.	What are the main objectives of computer forensics?	BTL 1	Remembering
3.	List any four applications of computer forensics.	BTL 2	Understanding
4.	What is meant by digital evidence?	BTL 1	Remembering
5.	State any two principles of computer forensics.	BTL 2	Understanding
6.	What are the different types of computer forensics technology?	BTL 1	Remembering
7.	Define disk forensics.	BTL 1	Remembering
8.	What is network forensics?	BTL 1	Remembering
9.	What is database forensics?	BTL 1	Remembering
10.	What is mobile device forensics?	BTL 1	Remembering
11.	What are the different types of computer forensics systems?	BTL 1	Remembering
12.	What is a stand-alone computer forensics system?	BTL 1	Remembering
13.	What is the purpose of a portable computer forensics system?	BTL 1	Remembering
14.	Differentiate between hardware-based and software-based forensic systems.	BTL 2	Understanding
15.	What are the essential features of a computer forensics system?	BTL 1	Remembering
16.	Who are computer forensics vendors?	BTL 2	Understanding
17.	Name any four popular computer forensics tools/vendors.	BTL 2	Understanding
18.	What services are provided by computer forensics vendors?	BTL 1	Remembering
19.	Why is a write blocker used in computer forensics?	BTL 2	Understanding
20.	What is the importance of maintaining the chain of custody in computer forensics?	BTL 1	Remembering

PART – B

1.	Explain the fundamentals of Computer Forensics. Discuss its objectives, importance, scope, and applications in detail. (16)	BTL 3	Applying
2.	Describe the Computer Forensics Investigation Process with a neat diagram, explaining each phase involved. (16)	BTL 4	Analyzing
3.	Discuss the various types of Computer Forensics Technology. Explain their features, applications, advantages, and limitations. (16)	BTL 4	Analyzing
4.	Explain Disk Forensics, Network Forensics, Database Forensics, and Mobile Device Forensics with suitable examples. (16)	BTL 3	Applying
5.	Compare different Computer Forensics Technologies based on their purpose, tools used, and areas of application. (16)	BTL 3	Applying

6.	Explain the different Types of Computer Forensics Systems with their architecture, features, advantages, and disadvantages. (16)	BTL 3	Applying
7.	Discuss the design and working of Standalone, Portable, and Distributed Computer Forensics Systems. (16)	BTL 4	Analyzing
8.	Explain the hardware and software requirements of a Computer Forensics System with suitable illustrations. (16)	BTL 3	Applying
9.	Discuss the role of Computer Forensics Systems in digital crime investigations and legal proceedings. (16)	BTL 4	Analyzing
10.	Explain the importance of evidence acquisition, preservation, analysis, and reporting in computer forensic investigations. (16)	BTL 3	Applying
11.	Discuss the role of Computer Forensics Vendors in digital investigations. Explain the services they provide with suitable examples. (16)	BTL 4	Analyzing
12.	Explain the features and applications of popular Computer Forensics Tools such as EnCase, FTK, Autopsy, and X-Ways Forensics. (16)	BTL 3	Applying
13.	Compare commercial and open-source Computer Forensics Tools with respect to cost, functionality, and usability. (16)	BTL 5	Evaluating
14.	Explain the various Computer Forensics Services offered by vendors, including incident response, forensic analysis, expert testimony, and training. (16)	BTL 3	Applying
15.	Discuss the importance of Chain of Custody and evidence handling procedures in computer forensic investigations. (16)	BTL 4	Analyzing
16.	Explain the legal, ethical, and technical challenges involved in Computer Forensics. (16)	BTL 3	Applying
17.	Discuss the role of computer forensics in investigating cybercrimes such as hacking, identity theft, insider attacks, and financial fraud. (16)	BTL 4	Analyzing
18.	Explain how Computer Forensics Technology assists organizations in preventing, detecting, and investigating cyber incidents. (16)	BTL 3	Applying
19.	Compare different Computer Forensics Systems and Technologies based on their applications, advantages, limitations, and performance. (16)	BTL 5	Evaluating
20.	Describe the complete workflow of a Computer Forensics Investigation, starting from incident identification to final reporting, highlighting the technologies, systems, and vendor services involved. (16)	BTL 4	Analyzing
21.	Discuss the design and working of Standalone, Portable, and Distributed Computer Forensics Systems. (16)	BTL 4	Analyzing
22.	Explain the hardware and software requirements of a Computer Forensics System with suitable illustrations. (16)	BTL 3	Applying

UNIT – II: COMPUTER FORENSIC EVIDENCE AND CAPTURE

Data Recovery – Evidence Collection and Data Seizure-Duplication and Preservation of Digital Evidence-Computer Image Verification and Authentication.

PART – A

Q.No	Questions	BT Level	Competence
1.	Define data recovery.	BTL 1	Remembering
2.	What are the objectives of data recovery in computer forensics?	BTL 1	Remembering
3.	List any four methods of data recovery.	BTL 2	Understanding
4.	What is evidence collection in digital forensics?	BTL 1	Remembering
5.	Define data seizure.	BTL 1	Remembering

6.	State any two guidelines for collecting digital evidence.	BTL 2	Understanding
7.	What is the importance of the chain of custody during evidence collection?	BTL 1	Remembering
8.	What precautions should be taken while seizing a computer system?	BTL 1	Remembering
9.	Define duplication of digital evidence.	BTL 1	Remembering
10.	What is a forensic image?	BTL 1	Remembering
11.	Differentiate between disk cloning and disk imaging.	BTL 2	Understanding
12.	Why is digital evidence duplicated instead of analyzing the original media?	BTL 2	Understanding
13.	What is the purpose of preserving digital evidence?	BTL 1	Remembering
14.	List any four methods used to preserve digital evidence.	BTL 2	Understanding
15.	What is computer image verification?	BTL 1	Remembering
16.	What is the role of hash values in image verification?	BTL 1	Remembering
17.	Name any two hash algorithms used for evidence authentication.	BTL 2	Understanding
18.	Define authentication of digital evidence.	BTL 1	Remembering
19.	Why is evidence integrity important in computer forensics?	BTL 2	Understanding
20.	Mention the purpose of MD5 or SHA-256 in forensic investigations.	BTL 2	Understanding

PART – B

1.	Explain the concept of Data Recovery and discuss the various techniques used to recover deleted, damaged, and lost digital data. (16)	BTL 3	Applying
2.	Describe the data recovery process in detail with suitable examples and applications in computer forensic investigations. (16)	BTL 4	Analyzing
3.	Explain the procedures involved in Evidence Collection during a digital forensic investigation. Discuss the best practices to ensure evidence integrity. (16)	BTL 3	Applying
4.	Discuss the steps involved in Data Seizure and explain the precautions that must be taken while seizing digital devices. (16)	BTL 4	Analyzing
5.	Explain the importance of the Chain of Custody in digital forensics. Describe the procedures followed to maintain it throughout an investigation. (16)	BTL 3	Applying
6.	Describe the methods of collecting, documenting, and handling digital evidence in computer forensic investigations. (16)	BTL 4	Analyzing
7.	Explain the process of Duplication of Digital Evidence. Compare disk imaging and disk cloning with suitable examples. (16)	BTL 3	Applying
8.	Discuss the various methods and tools used for creating forensic copies of digital evidence. (16)	BTL 4	Analyzing
9.	Explain the importance of Preservation of Digital Evidence and discuss the techniques used to prevent evidence contamination. (16)	BTL 3	Applying
10.	Describe the legal and technical challenges involved in the preservation of digital evidence. (16)	BTL 4	Analyzing
11.	Explain the concept of Computer Image Verification. Discuss the techniques used to verify the integrity of forensic images. (16)	BTL 3	Applying
12.	Describe the role of hashing algorithms in computer image verification. Explain the working of MD5 and SHA-256 with suitable examples. (16)	BTL 4	Analyzing
13.	Explain the process of Authentication of Digital Evidence and discuss its significance in legal proceedings. (16)	BTL 3	Applying
14.	Discuss the methods used to ensure the integrity, authenticity, and admissibility of digital evidence in court. (16)	BTL 4	Analyzing
15.	Explain the complete process of evidence acquisition, duplication, preservation, verification, and authentication in a computer forensic investigation. (16)	BTL 3	Applying

16.	Describe the role of forensic imaging tools in evidence acquisition and verification with suitable examples. (16)	BTL 4	Analyzing
17.	Discuss the challenges encountered in data recovery and digital evidence handling. Suggest appropriate solutions. (16)	BTL 4	Analyzing
18.	Explain the importance of forensic image verification in maintaining the reliability and credibility of digital evidence. (16)	BTL 3	Applying
19.	Discuss the legal, ethical, and procedural considerations involved in evidence collection, preservation, and authentication. (16)	BTL 4	Analyzing
20.	Illustrate a digital forensic case study describing the complete process from data recovery and evidence collection to forensic imaging, verification, authentication, and presentation of evidence in court. (16)	BTL 4	Analyzing

UNIT – III : COMPUTER FORENSIC ANALYSIS

Discovery of Electronic Evidence- Identification of Data – Reconstructing Past Events – Fighting against Macro Threats – Information Warfare Arsenal – Tactics Of the Military Tactics of Terrorist and Rogues – Tactics of Private Companies.

PART – A

Q.No	Questions	BT Level	Competence
1.	Define electronic evidence.	BTL 1	Remembering
2.	What is meant by the discovery of electronic evidence?	BTL 1	Remembering
3.	List any four sources of electronic evidence.	BTL 2	Understanding
4.	What is identification of data in digital forensics?	BTL 1	Remembering
5.	Why is data identification important in a forensic investigation?	BTL 2	Understanding
6.	Define reconstruction of past events.	BTL 1	Remembering
7.	What is the purpose of reconstructing past events in computer forensics?	BTL 1	Remembering
8.	List any four sources used to reconstruct past events.	BTL 2	Understanding
9.	What are macro threats in cyberspace?	BTL 1	Remembering
10.	Mention any four methods used to fight against macro threats.	BTL 2	Understanding
11.	What is meant by Information Warfare (IW)?	BTL 1	Remembering
12.	List any four components of the Information Warfare Arsenal.	BTL 2	Understanding
13.	What are the objectives of military information warfare?	BTL 1	Remembering
14.	Mention any four tactics used by the military in information warfare.	BTL 2	Understanding
15.	What is meant by the tactics of terrorists and rogues in cyberspace?	BTL 2	Understanding
16.	List any four cyber attack techniques commonly used by terrorists and rogue groups.	BTL 2	Understanding
17.	What are the objectives of cyber attacks carried out by private companies?	BTL 1	Remembering
18.	Mention any four tactics used by private companies in cyber competition.	BTL 1	Understanding
19.	Differentiate between military cyber tactics and terrorist cyber tactics.	BTL 2	Understanding
20.	What is the role of computer forensics in investigating information warfare incidents.	BTL 1	Remembering

PART – B

1.	Explain the concept of Discovery of Electronic Evidence and discuss its significance in digital forensic investigations. (16)	BTL 3	Applying
2.	Describe the various sources and types of electronic evidence. Explain the procedures for identifying, collecting, and preserving electronic evidence. (16)	BTL 4	Analyzing
3.	Discuss the process of Identification of Data in computer forensics. Explain the techniques used to locate and classify digital evidence. (16)	BTL 4	Analyzing
4.	Explain the methods used for identifying relevant digital data from computers, storage devices, networks, and cloud environments. (16)	BTL 3	Applying
5.	Describe the concept of Reconstructing Past Events in digital forensics. Explain the techniques used to recreate user activities and system events. (16)	BTL 4	Analyzing
6.	Discuss the role of system logs, file systems, browser history, registry entries, and metadata in reconstructing past events. (16)	BTL 4	Analyzing
7.	Explain the concept of Macro Threats in cyberspace. Discuss the major cyber threats affecting governments, organizations, and individuals. (16)	BTL 3	Applying
8.	Describe the various strategies and technologies used to fight against macro threats with suitable examples. (16)	BTL 4	Analyzing
9.	Explain the concept of Information Warfare (IW). Discuss its objectives, characteristics, and importance in modern cyber warfare. (16)	BTL 3	Applying
10.	Discuss the different components of the Information Warfare Arsenal and explain their roles in cyber operations. (16)	BTL 4	Analyzing
11.	Explain the tactics employed by military organizations in information warfare. Discuss their objectives, strategies, and cyber defense mechanisms. (16)	BTL 3	Applying
12.	Describe the various cyber attack techniques used by terrorists and rogue organizations. Explain how digital forensics helps investigate such attacks. (16)	BTL 4	Analyzing
13.	Discuss the objectives and methods adopted by terrorists and rogue groups in conducting cyber attacks. (16)	BTL 4	Analyzing
14.	Explain the cyber tactics employed by private companies in protecting information assets and maintaining competitive advantage. (16)	BTL 3	Applying
15.	Compare the information warfare tactics of military organizations, terrorists, rogue groups, and private companies with suitable examples. (16)	BTL 5	Evaluating
16.	Discuss the role of computer forensics in investigating information warfare incidents involving military, terrorist, and corporate environments. (16)	BTL 4	Analyzing
17.	Explain the legal, ethical, and technical challenges involved in the discovery and analysis of electronic evidence. (16)	BTL 3	Applying
18.	Describe the complete process of electronic evidence discovery, data identification, event reconstruction, and evidence reporting in a forensic investigation. (16)	BTL 4	Analyzing
19.	Discuss the role of digital forensics in combating cyber terrorism, cyber espionage, and information warfare. (16)	BTL 4	Analyzing
20.	Illustrate a case study involving a cyber attack, explaining how electronic evidence was discovered, data was identified, past events were reconstructed, and forensic analysis was used to determine the attack tactics and support legal proceedings. (16)	BTL 4	Analyzing

UNIT-IV INVESTIGATION			
Arsenal – Surveillance Tools – Hackers and Theft of Components –Contemporary Computer Crime- Identity Theft and Identity Fraud – Organized Crime &Terrorism – Avenues Prosecution and Government Efforts – Applying the First Amendment to Computer Related Crime-The Fourth Amendment and other Legal Issues.			
PART – A			
Q.No	Questions	BT Level	Competence
1.	Define computer crime.	BTL 1	Remembering
2.	What is meant by a surveillance tool in computer investigations?	BTL 1	Remembering
3.	List any four surveillance tools used in digital investigations.	BTL 2	Understanding
4.	What is meant by the term arsenal in the context of cyber investigations?	BTL 1	Remembering
5.	Who is a hacker?	BTL 2	Understanding
6.	What is meant by the theft of computer components?	BTL 1	Remembering
7.	List any four examples of contemporary computer crimes.	BTL 2	Understanding
8.	Define identity theft.	BTL 1	Remembering
9.	Differentiate between identity theft and identity fraud.	BTL 2	Understanding
10.	Mention any four methods used to commit identity theft.	BTL 2	Understanding
11.	What is the role of organized crime in cybercrime?	BTL 1	Remembering
12.	How is terrorism related to computer crime?	BTL 1	Remembering
13.	State any two government efforts to combat cybercrime.	BTL 2	Understanding
14.	What is meant by cybercrime prosecution?	BTL 1	Remembering
15.	What is the significance of the First Amendment in computer-related crime investigations?	BTL 1	Remembering
16.	What is the Fourth Amendment?	BTL 1	Remembering
17.	Why is the Fourth Amendment important in digital forensic investigations?	BTL 2	Understanding
18.	Mention any four legal issues involved in computer crime investigations.	BTL 2	Understanding
19.	What is the role of law enforcement agencies in investigating cybercrime?	BTL 1	Remembering
20.	State any two challenges faced during the investigation of computer-related crimes.	BTL 2	Understanding

PART-B			
1.	Explain the concept of computer crime and discuss the different types of contemporary computer crimes with suitable examples. (16)	BTL 3	Applying
2.	Describe the various surveillance tools used in computer forensic investigations. Explain their features, applications, advantages, and limitations. (16)	BTL 4	Analyzing
3.	Discuss the role of surveillance tools in cybercrime investigation and evidence collection. (16)	BTL 4	Analyzing
4.	Explain the methods used by hackers to steal computer components, data, and information. Discuss preventive measures against such attacks. (16)	BTL 3	Applying
5.	Discuss the causes, techniques, impacts, and prevention of theft of computer components in organizations. (16)	BTL 4	Analyzing
6.	Explain the concept of identity theft and identity fraud. Discuss their types, methods, impacts, and preventive measures. (16)	BTL 3	Applying
7.	Describe the complete process of investigating an identity theft case using digital forensic techniques. (16)	BTL 4	Analyzing
8.	Discuss the various forms of organized cybercrime and explain the role of digital forensics in combating organized criminal activities. (16)	BTL 4	Analyzing

9.	Explain the relationship between cyber terrorism and computer crime. Discuss the objectives, attack methods, and countermeasures. (16)	BTL 3	Applying
10.	Discuss the role of government agencies and law enforcement organizations in preventing, investigating, and prosecuting cybercrime. (16)	BTL 4	Analyzing
11.	Explain the various avenues of prosecution available for computer-related crimes. Discuss the legal procedures followed during prosecution. (16)	BTL 3	Applying
12.	Describe the government initiatives and legal frameworks adopted to combat cybercrime at the national and international levels. (16)	BTL 4	Analyzing
13.	Explain the application of the First Amendment to computer-related crimes. Discuss its impact on freedom of speech in cyberspace. (16)	BTL 3	Applying
14.	Discuss the significance of the Fourth Amendment in digital forensic investigations. Explain how it governs search and seizure of electronic evidence. (16)	BTL 4	Analyzing
15.	Explain the legal procedures involved in search, seizure, collection, preservation, and presentation of digital evidence under the Fourth Amendment. (16)	BTL 3	Applying
16.	Discuss the various legal and ethical issues involved in computer crime investigations. (16)	BTL 4	Analyzing
17.	Compare the First Amendment and Fourth Amendment with respect to computer-related crime investigations. (16)	BTL 5	Evaluating
18.	Explain the challenges faced by investigators in handling contemporary computer crimes, including identity theft, cyber terrorism, and organized cybercrime. (16)	BTL3	Applying
19.	Discuss the importance of computer forensics in investigating hackers, organized crime, and cyber terrorism. Illustrate your answer with suitable examples. (16)	BTL 4	Analyzing
20.	Illustrate a case study involving a cybercrime investigation, explaining the use of surveillance tools, collection of digital evidence, legal issues, prosecution process, and the application of constitutional provisions. (16)	BTL 5	Evaluating

UNIT V COMPUTER FORENSIC INVESTIGATION CASES

Developing Forensic Capabilities – Searching and Seizing Computer Related Evidence –Processing Evidence and Report Preparation – Future Issues.

PART-A

Q.No	Questions	BT Level	Competence
1.	Define forensic capabilities in digital investigations.	BTL 1	Remembering
2.	What are the key components of developing forensic capabilities?	BTL 1	Remembering
3.	Mention any four requirements for a digital forensic lab.	BTL 2	Understanding
4.	What is meant by computer-related evidence?	BTL 1	Remembering
5.	State any two sources of computer-related evidence.	BTL 2	Understanding
6.	What is the purpose of searching digital evidence?	BTL 1	Remembering
7.	Define search and seizure in computer forensics.	BTL 2	Understanding
8.	List any four tools used for searching computer evidence.	BTL 2	Understanding
9.	What precautions should be taken during seizure of digital devices?	BTL 2	Understanding
10.	What is meant by evidence preservation?	BTL 1	Remembering
11.	Why is documentation important during evidence collection?	BTL 1	Remembering
12.	Define forensic imaging.	BTL 1	Remembering
13.	What is meant by processing of digital evidence?	BTL 1	Remembering
14.	List any four steps involved in evidence processing.	BTL 2	Understanding

15.	What is the role of a forensic investigator in report preparation?	BTL 1	Remembering
16.	What is a forensic report?	BTL 1	Remembering
17.	State any two important components of a forensic report.	BTL 2	Understanding
18.	Mention any four future challenges in computer forensics.	BTL 2	Understanding
19.	What are emerging issues in digital forensic investigations?	BTL 1	Remembering
20.	Why is continuous updating of forensic tools necessary?	BTL 5	Remembering
PART-B			
1.	Explain the concept of developing forensic capabilities and discuss the requirements for establishing a modern digital forensic laboratory. (16)	BTL 3	Applying
2.	Describe the essential components of a computer forensic infrastructure and explain their roles in investigations. (16)	BTL 4	Analyzing
3.	Discuss the steps involved in building effective digital forensic capabilities in law enforcement and corporate environments. (16)	BTL 4	Analyzing
4.	Explain the importance of standard operating procedures (SOPs) in digital forensic investigations. (16)	BTL 3	Applying
5.	Discuss the process of searching computer-related evidence and explain the techniques used for locating hidden or deleted data. (16)	BTL 4	Analyzing
6.	Describe the legal and technical procedures involved in seizing computer-related evidence. (16)	BTL 4	Analyzing
7.	Explain the guidelines to be followed during search and seizure of digital devices to ensure admissibility of evidence in court. (16)	BTL 3	Applying
8.	Discuss the challenges faced during the collection of computer-related evidence and suggest solutions. (16)	BTL 4	Analyzing
9.	Explain the role of forensic imaging tools in searching and seizing digital evidence. (16)	BTL 3	Applying
10.	Elaborate the step-by-step process of evidence acquisition, preservation, and documentation in computer forensics. (16)	BTL 4	Analyzing
11.	Explain the importance of processing digital evidence in a forensic investigation and describe the stages involved. (16)	BTL 3	Applying
12.	Discuss various methods used for analyzing and processing digital evidence from storage devices and networks. (16)	BTL 4	Analyzing
13.	Describe the process of forensic report preparation and explain the key elements of a good forensic report. (16)	BTL 4	Analyzing
14.	Discuss the importance of documentation and reporting standards in digital forensic investigations(16)	BTL 4	Analyzing
15.	Explain how forensic investigators ensure accuracy, reliability, and integrity while preparing reports. (16)	BTL 3	Applying
16.	Discuss the major future challenges in digital forensics, including encryption, cloud computing, and AI-based crimes. (16)	BTL 4	Analyzing
17.	Explain the impact of emerging technologies on the future of computer forensic investigations. (16)	BTL 3	Applying
18.	Discuss how cybercrime evolution is shaping future requirements for forensic tools and techniques. (16)	BTL 4	Analyzing
19.	Explain the role of data filtering, recovery, and reconstruction during evidence processing. (16)	BTL 3	Applying
20.	Illustrate a complete forensic investigation workflow, starting from evidence search and seizure to processing, analysis, and report preparation, including future considerations. (16)	BTL 5	Analyzing

