R0799	Sub. Code 556101

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2023

First Semester

Cyber Forensics

INTRODUCTION TO CYBER FORENSICS

(CBCS – 2023 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the objective questions by choosing the correct options.

1. Which transport layer protocol is commonly associated with secure, encrypted communication over the internet, ensuring data confidentiality and integrity? (CO1, K2)

   (a) SMTP (Simple Mail Transfer Protocol)

   (b) FTP (File Transfer Protocol)

   (c) TLS (Transport Layer Security)

   (d) ICMP (Internet Control Message Protocol)

2. Which term is often used to describe individuals with limited technical skills who use pre-written scripts and tools to launch cyberattacks without fully understanding the underlying technology? (CO1, K2)

   (a) Black Hat Hackers

   (b) Gray flat Hackers

   (c) White Hat Hackers

   (d) Script Kiddies

3. Which type of cybercrime involves fraudulently acquiring sensitive information, such as credit card numbers or login credentials, through deceptive emails or websites? (CO2, K2)

(a) Identity Theft (b) Phishing

(c) Cyberbullying (d) Hacking

4. What is the key characteristic that distinguishes the deep web from the surface web? (CO2, K2)

(a) It contains illegal content and activities

(b) It is not indexed by search engines

(c) It requires special software like Tor to access

(d) It is only accessible to government agencies

5. Which web browser artifact contains information about websites a user has visited and the date and time of those visits? (CO3, K3)

(a) Cookies (b) Bookmark file

(c) History file (d) Cache files

6. Which of the following is NOT a common method used by forensics tools for password recovery? (CO3, K3)

(a) Dictionary attacks

(b) Brute force attacks

(c) Rainbow tables

(d) Social engineering

7. Which of the following is an example of a forensic tool used for the acquisition of social media evidence? (CO4, K4)

(a) Antivirus software

(b) Video editing software

(c) Social media management platform

(d) Facebook data scraper

8. Which of the following is a common feature of a forensic imager? (CO4, K4)

(a) Real-time data analysis

(b) Data destruction capabilities

(c) Encryption of evidence copies

(d) Network intrusion detection

9. What legal principle allows for exceptions to the hearsay rule in admitting certain types of digital evidence? (CO5, K5)

(a) The Hearsay Exception

(b) The Authentication Principle

(c) The Best Evidence Rule

(d) The Expert Witness Rule

10. Which type of digital evidence is more likely to be challenged for authenticity in court? (CO5, K5)

(a) Email messages (b) Encrypted files

(c) CCTV footage (d) Printed documents

Part B ($5 \times 5 = 25$)

Answer **all** the questions not more than 500 words each.

11. (a) Explain the concept of a Local Area Network (LAN) and its key components. (CO1, K2)

Or

(b) Outline cybercrime against a nation. (CO1, K2)

12. (a) Explain the distinctions between copyright and trademark-related offenses. (CO2, K2)

Or

(b) Compare the consensus mechanisms of Bitcoin and Ethereum. (CO2, K2)

13. (a) Identify the key legal and ethical considerations that digital forensic experts must adhere to when conducting database forensics investigations. (CO3, K4)

Or

(b) Develop and explain a comprehensive evidence collection procedure for digital forensics investigations. (CO3, K3)

14. (a) Generate a list of five key best practices for the secure handling and preservation of digital evidence in a forensic investigation. (CO4, K3)

Or

(b) Examine the key features and functionalities of Autopsy's timeline analysis tool, and discuss how it can be utilized in a digital forensic investigation. (CO4, K4)

15. (a) Assess the role of digital forensics in verifying e-signatures. (CO5, K4)

Or

(b) Explain the key characteristics of evidence used to assess the legal recognition of digital signatures in the context of the law. (CO5, K5)

Part C (5 × 8 = 40)

Answer **all** the questions not more than 1000 words each.

16. (a) Explain the fundamental principles and mechanisms that ensure network security at the transport layer. (CO1, K2)

Or

(b) Outline the key tools frequently employed in cybercrime, delineating their distinct purposes and functionalities. (CO1, K2)

17. (a) Summarize Cybercrime against Individuals. (CO2, K3)

Or

(b) Illustrate the concepts of Ransomware. (CO2, K2)

18. (a) Identify and briefly describe the primary components and procedures involved in email forensics. (CO3, K4)

Or

(b) Develop an explanation of how the ext family of file systems, including ext2, ext3, and ext4, is critical in digital forensics. (CO3, K3)

19. (a) Examine the procedures and tools used in the acquisition of evidence from live systems, and discuss the ethical and legal implications surrounding this practice in digital forensics. (CO4, K5)

Or

(b) Operate WinHex to demonstrate how to locate and recover deleted files from a hard drive image in a digital forensic scenario. (CO4, K4)

20. (a) Explain the challenges associated with the admissibility and presentation of digital evidence in court. (CO5, K4)

Or

(b) Explain, through a case study, the impact of the convergence of cybercrime and traditional property crime on modern criminal investigations. (CO5, K5)

———————

R0800	Sub. Code 556102

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2023

First Semester

Cyber Forensics

CYBERCRIME ISSUES AND INVESTIGATION

(CBCS – 2023 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the following objective questions by choosing the correct options.

1. Which of the following is not a cybercrime? (CO1, K3)

   (a) Denial of Service

   (b) Man in the Middle

   (c) Malware

   (d) AES

2. What is the primary motivation for many cybercriminals? (CO1, K3)

   (a) Political activism

   (b) Financial gain

   (c) Personal revenge

   (d) Technological curiosity

3. In a legal context, what does the term "chain of custody" refer to? (CO2, K2)

(a) A document listing all the witnesses in a trial

(b) A series of court hearings related to a Case

(c) A systematic record of the handling and storage of evidence

(d) The order in which witnesses are called to testify in court

4. Which of the following best describes the role of a prosecuting attorney in a cybercrime case? (CO2, K2)

(a) Representing the government in criminal proceedings

(b) Analyzing network vulnerabilities

(c) Negotiating settlements with hackers

(d) Conducting cybersecurity risk assessments

5. Which legal concept is central to determining the legality of intercepting Wi-Fi transmissions in many jurisdictions? (CO3, K4)

(a) Digital encryption

(b) Informed consent

(c) User authentication

(d) Data encryption keys

6. Which of the following is an example of volatile data that live forensics investigators may collect during network analysis? (CO3, K4)

(a) Archived email logs

(b) Registry entries

(c) RAM contents

(d) System log files

7. What type of information can be obtained from a network service provider? (CO4, K5)

(a) Personal medical records

(b) Call and text message logs

(c) Credit card numbers

(d) Social media passwords

8. What is the primary challenge in mobile forensics when dealing with encrypted devices? (CO4, K5)

(a) Speed of data extraction

(b) Lack of available tools

(c) High cost of forensic software

(d) Breaking through encryption barriers

9. Which of the following is NOT a common form of cybercrime related to financial fraud? (CO5, K6)

(a) Phishing attacks

(b) Ransomware attacks

(c) Insider trading

(d) Credit card fraud

10. What is the primary goal of financial fraud investigations? (CO5, K6)

(a) To protect the rights of the accused

(b) To recover stolen funds and assets

(c) To promote financial innovation

(d) To increase banking regulations

Part B (5 × 5 = 25)

Answer **all** the questions not more than 500 words each.

11. (a) Identify the challenges law enforcement agencies face when prioritizing evidence in a complex cybercrime investigation. (CO1, K4)

Or

(b) Describe the key milestones in the evolution of computer crime from the 1970s to the present day. (CO1, K3)

12. (a) Difference between Civil and Criminal Cyber Cases. (CO2, K3)

Or

(b) Describe the primary responsibilities and challenges faced by a cybercrime investigator when handling a case involving a data breach. (CO2, K2)

13. (a) Examine the role of communication protocols in the Hacker Defender programs functionality. (CO3, K4)

Or

(b) Explain the concept of a "reasonable expectation of privacy" in the context of the Fourth Amendment as it applies to WLANs. (CO3, K4)

14. (a) Write a brief note on Call Detail Record. (CO4, K3)

Or

(b) Explain the challenges in extraction of Forensic evidence from communication devices. (CO4, K5)

15. (a) Compile the investigation of ATM withdrawal and Online Transaction Cases. (CO5, K5)

Or

(b) Elaborate the investigation of Bank to Bank Transfer and Transactions involving Cheques. (CO5, K6)

Part C $(5 \times 8 = 40)$

Answer **all** the questions not more than 1000 words each.

16. (a) Discuss common misconceptions and myths about cybercrime. Provide detailed explanations for each myth. (CO1, K3)

Or

(b) Explain the components and elements involved in computer crime. (CO1, K3)

17. (a) Explain the Keys to Effective Testimony. (CO2, K3)

Or

(b) Summaries the Role of Law Enforcement Officers. (CO2, K2)

18. (a) Discuss the legal implications of unauthorized eavesdropping on Wi-Fi networks, including relevant laws and potential consequences for individuals or entities involved. (CO3, K4)

Or

(b) Examine the Legal complexities surrounding the interception of Wi-Fi transmissions, specifically in cases involving encrypted file systems. (CO3, K5)

19. (a) Explain the laws and rules related to interception and monitoring under IT (Amendment) act, 2008. (CO4, K3)

Or

(b) Explain the Techniques involved in Mobile Forensics. (CO4, K5)

20. (a) Discuss in detail about Advance Fee Fraud. (CO5, K4)

Or

(b) Write a Case study on Sharing of morphed obscene contents through email and Facebook. (CO5, K6)

———————

R0801	Sub. Code 556103

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2023

First Semester

Cyber Forensics

ADVANCED DATABASE SECURITY

(CBCS – 2023 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the following objective questions by choosing the correct options.

1. Which of the following is a primary goal of web security risk analysis and best practices? (CO1, K2)

   (a) Ensuring 100% protection against all possible threats.

   (b) Identifying potential risks and vulnerabilities.

   (c) Achieving high web traffic and user engagement.

   (d) Reducing server response times.

2. Which of the following is a common method used for Multi-Factor Authentication (MFA) in web security? (CO2, K2)

   (a) Captcha verification

   (b) Username and password

   (c) Fingerprint recognition

   (d) Website URL

3. Why would a hacker use a proxy server? (CO2, K2)

(a) To create a stronger connection with the target

(b) To create a ghost server on the network

(c) To obtain a remote access connection

(d) To hide malicious activity on the network

4. Which of the following techniques is commonly used for subdomain enumeration in web security assessments? (CO2, K2)

(a) SQL Injection

(b) Cross-site Scripting (XSS)

(c) DNS Enumeration

(d) Phishing Attacks

5. Which of the following tools is used for purpose of data auditing for SQL Server only? (CO3, K4)

(a) ApexSQL (b) SQL Ninja

(c) SQL Audit (d) Idera

6. Prevention of access to the database by unauthorized users is referred to as : (CO3, K4)

(a) Reliability (b) Security

(c) Productivity (d) Integrity

7. Which of the following is used only for data entry and storage, and never for processing? (CO4, K5)

(a) Mouse

(b) Dumb terminal

(c) Micro computer

(d) Dedicated data entry system

8. Most backup and recovery commands in ———— are executed by server sessions. (CO4, K5)

(a) Backup Manager

(b) Recovery Manager

(c) Backup and Recovery Manager

(d) Database Manager

9. What is the primary purpose of encryption in mobile device security? (CO5, K5)

(a) To improve battery life

(b) To make the device run faster

(c) To protect data from unauthorized access

(d) To enhance Wi-Fi connectivity

10. In PELBAC, what is the primary goal? (CO5, K5)

(a) Maximize data sharing

(b) Protect user privacy

(c) Monitor user activities

(d) Optimize location accuracy

Part B ($5 \times 5 = 25$)

Answer **all** the questions not more than 500 words each.

11. (a) Explain how cryptography contributes to web security. (CO1, K2)

Or

(b) Express the relationship between cryptography and the patent system, and discuss their implications for innovation and security in a digital age. (CO1, K2)

12. (a) Explain how backups are useful in web privacy. (CO2, K2)

Or

(b) Summarise the steps and practices for securing web application. (CO2, K2)

13. (a) Explain data integrity for databases. (CO3, K4)

Or

(b) Examine the role of an access control model in XML databases. How does it ensure data security and integrity within an XML database system? (CO3, K4)

14. (a) Explain the concept of trustworthy records retention in security re-engineering for databases. (CO4, K3)

Or

(b) Explain the importance of regular testing and simulation in the context of damage recovery for data processing systems. (CO4, K5)

15. (a) Explain the concept of probabilistic databases in the context of Bayesian modeling. (CO5, K3)

Or

(b) Explain the key principles and mechanisms involved in privacy-enhanced location-based access control. (CO5, K5)

Part C (5 × 8 = 40)

Answer **all** the questions not more than 1000 words each.

16. (a) Explain the major parts of web security problems. (CO1, K2)

Or

(b) Summarise Online Cryptographic Protocols and Systems. (CO1, K2)

17. (a) Explain privacy-protecting techniques for choosing a good service provider. (CO2, K3)

Or

(b) Explain the essential physical security measures to protect servers and maintain web privacy. (CO1, K2)

18. (a) Examine the differences between discretionary access control and mandatory access control. (CO3, K4)

Or

(b) Examine the key security challenges and strategies for protecting data warehouses and OLAP systems in a modern enterprise environment. (CO3, K4)

19. (a) Explain the purpose and key steps involved in damage quarantine within a data processing system. (CO4, K3)

Or

(b) Explain the concept of database watermarking in detail, including its purposes, types, and potential benefits. (CO4, K5)

20. (a) Discuss the role of Bayesian methods in enhancing data quality and privacy in database publishing. (CO5, K5)

Or

(b) Explain how database-driven websites play a pivotal role in efficiently enforcing security and privacy policies in mobile applications. (CO5, K5)

———————

R0802	Sub. Code 556104

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2023

First Semester

Cyber Forensics

CRYPTOGRAPHY AND NETWORK SECURITY

(CBCS – 2023 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the following objective questions by choosing the correct option.

1. In affine block cipher systems if f(m)=Am + t, what is f(m1+m2+m3) ? (CO1, K2)

   (a) f(m1) + f(m2) + f(m3) + t

   (b) f(m1) + f(m2) + f(m3) + 2t

   (c) f(m1) + f(m2) + f(m3)

   (d) 2(f(m1) + f(m2) + f(m3))

2. What are the allowable values of word size in bit for RC5 algorithm. (CO1, K1)

   (a) 16, 32 (b) 16, 32, 64

   (c) 8, 16, 32 (d) 16, 32, 48

3. How many primitive roots are there for 25? (CO2, K1)

(a) 4 (b) 5

(c) 7 (d) 8

4. What is the general equation for elliptic curve systems? (CO2, K1)

(a) $y^3 + b\_1xy + b\_2y = x^3 3 + a\_1x^2 + a\_2x + a\_3$

(b) $y^3 + b\_1x + b\_2y = x^2 + a\_1x^2 + a\_2x + a\_3$

(c) $y^2 + b\_1xy + b\_2y = x^3 + a\_1x^2 + a\_2$

(d) $y^2 + b\_1xy + b\_2y = x^3 + a\_1x^2 + a\_2x + a\_3$

5. Message authentication code is also known as (CO3, K4)

(a) key code

(b) hash code

(c) keyed hash function

(d) message key hash function

6. S/MIME is abbreviated as ————. (CO3, K4)

(a) Secure/Multimedia Internet Mailing Extensions

(b) Secure/Multipurpose Internet Mailing Extensions

(c) Secure/Multimedia Internet Mail Extensions

(d) Secure/Multipurpose Internet Mail Extensions

7. ———— is a set of conventions and rules set for communicating two or more devices residing in the same network? (CO4, K3)

(a) Security policies

(b) Protocols

(c) Wireless network

(d) Network algorithms

8. ———— infects the executables as well as the boot sectors. (CO4, K3)

(a) Non-resident Virus

(b) Boot Sector Virus

(c) Polymorphic Virus

(d) Multipartite Virus

9. CRD in Mobile Forensic stands for (CO5, K3)

(a) Call Details Records

(b) Call Data Records

(c) Compact Disk Rewritable

(d) Compact Disk Readers

10. What do we call the pieces of information in a quantum computer? (CO5, K5)

(a) Bits (b) Qubits

(c) Bytes (d) Qubytes

Part B $(5 \times 5 = 25)$

Answer **all** the questions not more than 500 words each.

11. (a) Summaries Security Services. (CO1, K3)

Or

(b) Compare Symmetric and Asymmetric Key Cryptography. (CO1, K2)

12. (a) What is Diffie-Hellman Key Exchange? Discuss with an example. (CO2, K1)

Or

(b) Describe Two way Hash Functions. (CO2, K1)

13. (a) Generate simple Certificate using x.509 Certificate Framework. (CO3, K3)

Or

(b) Examine the Operations Pretty Good Privacy. (CO3, K4)

14. (a) Discover the types of security threats faced when using the Web. (CO4, K4)

Or

(b) Identify the basic techniques to eliminate the guessable passwords. (CO4, K3)

15. (a) Explain the significance of conducting a network security audit in an organization. (CO5, K4)

Or

(b) Determine the primary purpose of stenography in modern communication and information security. Provide an example. (CO5, K5)

Part C (5 × 8 = 40)

Answer **all** the questions not more than 1000 words each.

16. (a) Explain Security Attacks in detail. (CO1, K3)

Or

(b) Summarise DES Algorithm with example. (CO1, K2)

17. (a) Explain the Security of RSA Algorithm. (CO2, K3)

Or

(b) Explain in detail about Digital Signature. (CO2, K2)

18. (a) Compare Kerberos V4 and V5. (CO3, K4)

Or

(b) Simplify the process of creating and implementing an effective IP security policy for a small to medium-sized organization. (CO3, K4)

19. (a) Develop a concise overview of how SSL/TLS encryption helps protect sensitive data during online transactions. Explain the key cryptographic techniques. (CO4, K3)

Or

(b) Identify and elaborate on three distinct types of firewalls used in network security. (CO4, K4)

20. (a) Interpret the fundamental principles and steps involved in implementing the ECC algorithm within a Java application to provide secure encryption and digital signatures. (CO5, K5)

Or

(b) Evaluate DNA Cryptography. (CO5, K5)

———————

R0803	Sub. Code 556105

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2023

First Semester

Cyber Forensics

INFORMATION AND WEB SECURITY

(CBCS – 2023 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the following objective questions by choosing the correct options.

1. ———— involves maintaining data accuracy and completeness and protecting system components. (CO3, K1)

   (a) Data confidentiality

   (b) Data integrity

   (c) Authentication

   (d) Authorization

2. ———— is an agency within the U.S. Commerce Department's Technology Administration. (CO3, K1)

   (a) SANS (b) Burton Group

   (c) NIST (d) CERT

3. ———— is a special form of attack using which hacker's exploit – human psychology. (CO2, K1)

(a) Cross Site Scripting

(b) Insecure network

(c) Reverse Engineering

(d) Social Engineering

4. A ———— is a software bug that attackers can take advantage to gain unauthorized access in a system. (CO1, K1)

(a) System error (b) Bugged system

(c) Security bug (d) System virus

5. Controls that are intended to ensure that attacks are unsuccessful is analogous to ———— in dependability engineering. (CO3, K1)

(a) Fault avoidance (b) Fault tolerance

(c) Fault Recovery (d) Fault detection

6. Which of the following qualifies as best DR (Disaster Recovery) site? (CO4, K1)

(a) DR site in the same campus

(b) DR site in the same city

(c) DR site in the same country

(d) DR site in a different country

7. A ———— firewall is basically a router with a special set of filters that determines whether each packet is allowed to crass over a network boundary. (CO4, K1)

(a) Packet filtering

(b) Proxy firewall

(c) Network Address Translation

(d) Virtual Private Networks

8. Which of the following is not a computer-based identification technique? (CO5, K1)

(a) Password-based systems

(b) Physical tokens

(c) Tamper-proofing the document

(d) Biometrics

9. Passwords can be intercepted as they move through the Internet. This interception is performed by programs known as (CO4, K1)

(a) Password bases

(b) Password sniffers

(c) Password rotation

(d) Password keepers

10. ———— is a information-gathering tool which gives information regarding the operating system of a web server? (CO3, K1)

(a) NsLookup (b) Traceroute

(c) Whois (d) Netcraft

Part B (5 × 5 = 25)

Answer **all** the questions not more than 500 words each.

11. (a) Discuss the overview of security. (CO1, K3)

Or

(b) Elaborate the characteristics of security patterns in detail. (CO3, K2)

12. (a) Differentiate between risks, threats and vulnerabilities. (CO2, K3)

Or

(b) Explain the importance of countermeasures in security attack. (CO4, K5)

13. (a) List and explain the professional ethics. (CO3, K2)

Or

(b) Write short notes on steps in the change management process. (CO3, K2)

14. (a) What is cryptography? Explain the roles of cryptography. (CO4, K2)

Or

(b) Describe the cryptography and the patent system. (CO4, K3)

15. (a) Define cookie. Explain the cookie protocol with an example. (CO5, K2)

Or

(b) Explain the different types of firewalls. (CO5, K2)

Part C ($5 \times 8 = 40$)

Answer **all** questions not more than 1000 words each.

16. (a) Illustrate the various types of security taxonomies. (CO5, K4)

Or

(b) Describe the sources for security pattern mining in detail. (CO5, K4)

17. (a) Discuss the different malicious attacks. (CO2, K3)

Or

(b) Explain the common types of attacks with examples. (CO3, K2)

18. (a) Describe the system administration guide for disaster assessment and recovery. (CO4, K3)

Or

(b) Elaborate the software development models in detail. (CO3, K4)

19. (a) Discuss the three primary facets of the web security problem. (CO5, K3)

Or

(b) What is the need for identification? Explain the Computer-Based Identification Techniques with examples. (CO4, K3)

20. (a) How do you avoid spam and junk email? Explain. (CO5, K3)

Or

(b) Explain the following

(i) Whois

(ii) nsLookup

(iii) netcraft

(iv) web server fingerprinting. (CO4, K4)

———————

R0804	Sub. Code
	556501

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2023

First Semester

Cyber Forensics

Elective – FRAUDS AND COUNTER MEASURES

(CBCS – 2023 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the following objective questions by choosing the correct option.

1. What is the most common form of acquisition and payment fraud? (CO1, K1)
   (a) Kickbacks to customers
   (b) Collusive employee-vendor scheme
   (c) Paying ghost employees
   (d) Theft of cash

2. What is a concept of internal control? (CO3, K1)
   (a) Sales and accounts
   (b) Purchases and accounts payable
   (c) Capital expenditures
   (d) Separation of duties

3. Probably the most prevalent form of entity is the (CO2, K1)
   (a) Sole proprietorship
   (b) Partnership
   (c) Subsidiary
   (d) Corporation

4. What does ratio analysis use within the financial statement elements? (CO4, K1)

(a) Product lines (b) Trending

(c) Relationships (d) Vertical analysis

5. What is less likely to occur in an ethical corporate culture? (CO2, K1)

(a) Fraud (b) Obtaining clients

(c) Data mining (d) Forensic accounting

6. What is not a stage of money laundering? (CO3, K1)

(a) Absorption (b) Placement

(c) Layering (d) Integration

7. The goal of a criminal investigation is (CO1, K1)

(a) Surveillance

(b) Prosecution

(c) Reparation of damage

(d) Proving the truth

8. An ———— is a conversation with a purpose that has barriers that need to be broken down. (CO2, K1)

(a) Interview (b) Inference

(c) Interrogation (d) Ambush

9. What is the difference between a square and a rectangular matrix? (CO3, K2)

(a) The size of the table

(b) The ability to relate unmatched items

(c) The clarity

(d) The accuracy

10. What is the key to effective investigate management with inference models? (CO2, K1)

(a) A mixed mass of evidence

(b) A weighted mass of evidence

(c) A key list

(d) An inference chart

Part B ($5 \times 5 = 25$)

Answer **all** the questions not more than 500 words each.

11. (a) Describe the Categories of Occupational Fraud. (CO1, K2)

Or

(b) Explain the payroll fraud with an example. (CO3, K2)

12. (a) Write short notes on real estate limited partnership fraud scheme. (CO2, K3)

Or

(b) Discuss about the insurance claim fraud in detail. (CO4, K3)

13. (a) Illustrate the internal controls with an example. (CO3, K3)

Or

(b) What are the employee thefts? Explain. (CO5, K4)

14. (a) Discuss the 3Cs of investigative management in detail. (CO4, K3)

Or

(b) What is document? Explain the types of documents to expect. (CO4, K3)

15. (a) Write short notes on temporal analysis tools. (CO5, K3)

Or

(b) How do Constructing an Investigative Inference Chart? (CO3, K5)

Part C (5 × 8 = 40)

Answer **all** questions not more than 1000 words each.

16. (a) What is fraud? Explain the types of fraud in detail. (CO1, K3)

Or

(b) Illustrate the Sales and Accounts Receivable fraud with an example. (CO5, K4)

17. (a) Describe the business enterprises in the global environment. (CO2, K3)

Or

(b) Explain the popular financial ratios in detail. (CO3, K2)

18. (a) What is the importance of accounting professionals in the investigation? Explain. (CO3, K3)

Or

(b) Discuss the organized crime and business in detail. (CO4, K3)

19. (a) Explain the following. (CO4, K4)

(i) Case initiation

(ii) Case evaluation.

Or

(b) How are the documents collected from third parties? Explain. (CO4, K2)

20. (a) Describe the matrices and link diagrams used in associational analysis. (CO5, K3)

Or

(b) Discuss the role of the nontestimonial expert in detail. (CO3, K2)

———————