Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S6 (R,S) Examinations April 2026 (2019 Scheme)

Course Code: CCT304

Course Name: CYBER FORENSICS

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks. Marks

1 What are the key legal considerations involved in conducting a Cyber forensic investigation? (3)

2 List any six physical requirements of a Cyber forensics Lab? (3)

3 Name any three software tools and three hardware tools used in computer forensics investigations. (3)

4 Explain any three disadvantages of conducting private forensic investigations with suitable examples. (3)

5 Define Locard's exchange principle? How is it important and applicable in cyber forensics field? (3)

6 Explain the term Drive-by Download. How does it pose a threat to computer security? (3)

7 The IT Act 2000 is often called the "Cyber Law of India." Explain its main objective and mention any two offences covered under this Act? (3)

8 How can cybercrimes affect individuals and organizations? Give suitable examples? (3)

9 Define the following terms: (3)

(i) Trail Obfuscation (ii) Spoofing (iii) Data Remanence (iv) Degaussing

10 Identify the open-source tool used to permanently erase data from storage devices such as USB drives. Explain how it works? (3)

PART B

Answer one question from each module, each carries 14 marks.

Module I

11 a) Explain the process of forensic investigation in a Cyber forensic case and illustrate it with a neat diagram. (7)

b) Explain the steps followed in the forensic protocol for acquiring evidence during a Cyber forensic investigation. (7)

OR

12 a) Explain the different storage formats for digital evidence and discuss how to determine the best acquisition method during a Cyber forensic investigation. (8)

b) A company suspects one of its employees is leaking confidential data and hires an investigator to find the source. Differentiate between private and public investigations and state which type applies in this case? (6)

Module II

13 a) Analyse the major challenges faced in cyber forensic investigations and explain how these challenges impact the process of collecting, preserving, and presenting digital evidence in court? (8)

b) Explain the main HKEYs in the Windows Registry and describe the function of each? (6)

OR

14 a) Apply your knowledge of cyber forensics to explain any two types and give an example of how each can be used in a real digital investigation? (8)

b) Explain the concept of Whole Disk Encryption (WDE) and discuss its importance in digital forensics. List any four open-source tools used for WDE? (6)

Module III

15 a) Explain the different types of volatile information in live response systems. Also, discuss the tools used to obtain volatile information from Windows-based systems? (8)

b) Explain the role of network forensic analysis tools in cyber investigations. Describe how Wireshark can be used to capture and analyze network traffic? (6)

OR

16 a) Explain the concept of rootkits in cyber forensics. Discuss their types and describe various techniques and tools used for rootkit detection? (7)

b) Explain the process of live response data collection in Windows systems. Discuss the types of data collected and the tools used in this process? (7)

Module IV

17 a) Write down the significance of the IT Act, 2000, along with all amendments made in 2008? (7)

b) What is cybercrime? Explain any cybercrime with a sample case study and analysis tools? (7)

OR

18 a) Analyze how social media platforms can be both a tool for communication and a medium for cybercrimes. Discuss preventive measures and forensic approaches used to investigate such incidents? (7)

b) What measures should be taken to protect ICT and prevent the misuse of the Internet? (7)

Module V

19 a) Explain the concepts of data wiping and data shredding in digital forensics. Discuss how these techniques differ and their importance in secure data disposal? (7)

b) Explain the concept of trail obfuscation in cyber forensics. Discuss the various techniques used by attackers to hide their digital traces and the forensic methods used to detect such activities? (7)

OR

20 a) Explain how steganography and cryptography are applied in digital forensics to secure, conceal, and analyze digital evidence. Discuss any one suitable tool and its forensic use? (8)

b) Explain anti-forensic detection techniques used to uncover hidden data in image files. Illustrate your answer with a suitable case study and identify a tool commonly used for such detection. (6)

******