

6E7194

Total No. of Questions : 22

Total No. of Pages : 04

Roll No. : .....

**6E7194**

**B. Tech. VI-Sem. (Main/Back) Exam. May - 2025**

**Computer Sc. & Engg. (Cyber Security)**

**6CCS5-11 Cyber Forensic**

**Time: 3 Hours**

**Maximum Marks: 70**

**Instructions to Candidates :**

**Attempt all ten questions from Part-A, five questions out of seven questions from Part-B and three questions out of five questions from Part-C.**

*Schematic diagrams must be shown wherever necessary. Any data you feel missing suitably be assumed and stated clearly. Units of quantities used / calculated must be stated clearly.*

*Use of following supporting material is permitted during examination.*

*(Mentioned in Form No. 205)*

1. ....

2. ....

**PART-A**

**[10×2=20]**

**(Answer should be given up to 25 words only)**

**All questions are compulsory.**

**Q.1. Explain about hacking in brief.**

**Q.2. What do you understand by data seizure ?**

- Q.3. Explain privacy role in security.
- Q.4. What do you understand by Information Security.
- Q.5. Differentiate between adware and spyware ?
- Q.6. What do you mean by Metadata and its usage in Digital Forensics ?
- Q.7. Explain about IDS and IPS in brief.
- Q.8. What is the use of honey pots ?
- Q.9. What are the precautions to be taken for acquisition of digital evidence ?
- Q.10. Explain the need of sanitization of system.

**PART-B**

[5×4=20]

**(Analytical / Problem solving questions)**

**Attempt any 05 questions.**

- Q.1. What is the requirement of encryption ? Also explain its various methods for implementing. <https://www.rtuonline.com>
- Q.2. Explain about the basic practices to avoid any issue with biometric security systems.
- Q.3. Explain the role of chain of custody in evidence collection.
- Q.4. Explain about the file formats use in the digital evidence analysis.
- Q.5. What are various agencies being involved in solving the digital cyber crime including digital forensics ?

- Q.6. Explain the working of Public key infrastructure.
- Q.7. Explain common techniques used in investigating web attacks.

**PART-C**

[3×10=30]

**(Descriptive / Analytical / Problem solving / Design questions)**

**Attempt any 03 questions.**

- Q.1. Explain about all of the stages in digital evidence acquisition.
- Q.2. What are the best practices used for the security of a corporate environment with respect to firewall ?
- Q.3. What do you mean by an artifact ? Explain in detail.
- Q.4. Explain the terms mentioned below :
- (i) Brute force Method [3]
  - (ii) SQL Injection [3]
  - (iii) DoS and DDoS Attack [4]
- Q.5. Explain the role of timestamp in any digital evidence and also explain how an integrity can be maintained in the process of seizures.

----- x -----