No of Pages : 2 Course Code : 18XWO2

Roll No:
(To be filled in by the candidate)

**PSG COLLEGE OF TECHNOLOGY, COIMBATORE - 641 004**

**SEMESTER EXAMINATIONS, MAY 2022**

**MSc - SOFTWARE SYSTEMS Semester : 8**

**18XWO2 COMPUTER FORENSICS**

**Time : 3 Hours** **Maximum Marks : 100**

**INSTRUCTIONS:**

1. Answer **ALL** questions. Each question carries 20 Marks.
2. Subdivision (a) carries 3 marks each, subdivision (b) carries 7 marks each and subdivision (c) carries 10 marks each.
3. Course Outcome : Table

| Qn.1 | CO.1 | Qn.2 | CO.2 | Qn.3 | CO.3 | Qn.4 | CO.4 | Qn.5 | CO.5 |
|---|---|---|---|---|---|---|---|---|---|

1. a) In the digital era, computers become more prevalent in businesses and the employers must safeguard critical business information. An unfortunate concern today is the possibility that data could be damaged, destroyed, or misappropriated by a discontented individual. If an employer has decided to terminate such an employee from the organization, what security measures must be taken by an employer to protect himself from false charges made by the employee?

   b) i) A person working in an organization has typed the organization's business secrets in a word document and sold it to another company and erased the contents of the file and deleted the file. How will a forensic specialist collect evidence against him? (3)

   ii) A cybercriminal hides a message in a word document and changes the extension of the file as .jpg. How will the forensic analyst read the content in the word document? (4)

   c) How will you recover multimedia files that are stored either on storage devices or in computer memory using the file carving approach?

2. a) Imagine a case where we suspect that someone installed a key logger or removed confidential information with a USB drive. How would we find evidence that a USB storage device was inserted and used?

   b) i) In an organization, an e-mail is sent from a branch office to a head office. How will the authenticity of the e-mail message be verified by the head office? (3)

   ii) On receiving an email, how will the forensic analyst identify if any part of the email message is deleted? (4)

**No of Pages : 2** **Course Code : 18XWO2**

c) Explain the steps carried out by a computer forensic specialist to investigate and collect evidence about the online activities carried out by a suspect before the capture of the system. Also, list the steps to find artifacts or evidence of nearly all the suspect's activity in the browser and its associated directories and databases.

3. a) A forensic specialist has a memory dump of the suspect system. How will he look for any malware running in the memory of the suspect system?

b) i) An employee fired from an organization has stored a file in an encrypted format. To collect evidence against the fired employee, the investigator has to decrypt the file to find the contents of the file? How will the investigator achieve this? (3)

ii) You suspect a process running in the memory to be malicious. To conform this, how do you extract the process from the memory and identify if it is actually malicious or benign? (4)

c) How will you analyze the memory of a compromised system to identify the picture of the events that occurred during an attack?

4. a) How will a forensic investigator identify if the attacker has visited facebook by analysing the network traffic?

b) i) A forensic investigator had received a file by an email. What are the different steps to be followed to identify if it is a suspicious file based on its purpose and functionality? (3)

ii) In recent days, the attacker sends malware by changing a bit to evade the antivirus based on file signature hash value. How can such malwares be identified using file signature analysis? (4)

c) How can you identify intrusion by inspecting the network traffic and individual packets?

5. a) How will a forensic investigator identify the username and password of an android phone in clear text?

b) You have a mobile phone for forensic analysis. How will you track the places where the mobile phone is carried?

c) Explain the various techniques involved to circumvent passcode and obtain root access in an android device.

**/END/**

**FD/JU**