

Course Code: 20MCA267
Course Name: CYBER FORENSICS

Max. Marks: 60

Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks.

Marks

- | | | |
|----|--|-----|
| 1 | List any three private sector computer crimes. | (3) |
| 2 | Describe the different types of storage formats used for storing collected digital evidence. | (3) |
| 3 | Analyse how deleted data in solid state storage devices possess a challenge for investigation? | (3) |
| 4 | What happens when someone empty the Recycle Bin in NTFS ? | (3) |
| 5 | What is a data fork and a resource fork? | (3) |
| 6 | Differentiate between soft link and hard link. | (3) |
| 7 | How the forensics acquisition method in mobile differs from that in computer system? | (3) |
| 8 | Define the DiD strategy for protection. | (3) |
| 9 | Explain different roles of a forensics examiner | (3) |
| 10 | What are the different types of reports? | (3) |

PART B

Answer any one question from each module. Each question carries 6 marks.

Module I

- | | | |
|----|---|-----|
| 11 | Briefly describe the procedures for the following corporate investigations. | (6) |
| | a. Internet Abuse Investigations | |
| | b. E-mail Abuse Investigation | |
| | c. Industrial espionage investigations | |

OR

- | | | |
|----|---|-----|
| 12 | Describe the Evidence custody form. What is its importance? | (6) |
|----|---|-----|

Module II

- 13 Differentiate between FAT and NTFS file system (6)

OR

- 14 Illustrate Windows Registry organizations and functions of Registry HKEYs (6)

Module III

- 15 Illustrate the File structures in Ext4 Linux file system (6)

OR

- 16 Explain data acquisition and validation tools/commands available in Linux (6)

Module IV

- 17 Describe the importance and steps in the Standard operating procedure for network forensic. (6)

OR

- 18 Describe the hardware components inside a mobile phone and explain the different information stored in SIM. (6)

Module V

- 19 Describe the structure of a forensic report? (6)

OR

- 20 List out the factors the courts have used in determining whether to disqualify an Expert. (6)
