

Course Code: 20MCA267**Course Name: CYBER FORENSICS**

Max. Marks: 60

Duration: 3 Hours

PART A*Answer all questions, each carries 3 marks.*

Marks

- | | | |
|----|---|-----|
| 1 | How cyber crime related to cyber forensics? | (3) |
| 2 | What do you mean by 'Forensic Copy'? | (3) |
| 3 | Write down the different steps involved in boot sequence? | (3) |
| 4 | Mention any six Windows Registry terminology. | (3) |
| 5 | Compare hard and soft links. | (3) |
| 6 | Figure out resource and data fork in a Macintosh operating system file. | (3) |
| 7 | Point out three methods of mobile forensics process. | (3) |
| 8 | List down any six uses of Wireshark tool. | (3) |
| 9 | What are the different types of reports in cyber forensics? | (3) |
| 10 | Which are the factors that courts have used in determining whether to disqualify an expert? | (3) |

PART B*Answer any one question from each module. Each question carries 6 marks.***Module I**

- | | | |
|----|--|-----|
| 11 | Explain the various steps involved in cyber forensics investigation. | (6) |
|----|--|-----|

OR

- | | | |
|----|--|-----|
| 12 | Illustrate the areas of cyber forensics. | (6) |
|----|--|-----|

Module II

- | | | |
|----|-----------------------------------|-----|
| 13 | How SSD differ from HDD? Explain. | (6) |
|----|-----------------------------------|-----|

OR

- | | | |
|----|---|-----|
| 14 | Mention any one computer hardware encryption program. Explain | (6) |
|----|---|-----|

Module III

- 15 Differentiate between HFS & HFS+ file systems. (6)

OR

- 16 (a) What are the information contained in an inode, when a file or directory is created on a UNIX file system? (3)
(b) How inode pointers works in LINUX file system? (3)

Module IV

- 17 Explain smartphone specific hardware options. (6)

OR

- 18 Discuss mobile forensics tools. (6)

Module V

- 19 Write down cyber forensics report structure. (6)

OR

- 20 List and explain the steps involved in generating forensics report using Autopsy tool. (6)
