Reg. No. \_\_\_\_\_\_\_\_\_\_\_\_\_



**End Semester Examination – Nov / Dec – 2019**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Code :** | **17CA2065** | **Duration :** | **3hrs** |
| **Sub. Name :** | **ADVANCED COMPUTER FORENSICS** | **Max. Marks :** | **100** |

**ANSWER ALL QUESTIONS (5 x 20 = 100 Marks)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No.** | **Sub Div.** | **Questions** | **Course**  **Outcome** | **Marks** |
| 1. | a. | Distinguish Computer Forensics and Data Recovery. | CO1 | 5 |
| b. | Describe how to prepare for computer investigations and explain the procedures that computing investigators commonly use in corporate high-tech investigations. | CO1 | 15 |
| **(OR)** | | | | |
| 2. | a. | Explain requirements for data recovery workstations and software. | CO3 | 10 |
| b. | Describe the investigation triad that makes up computing security. | CO1 | 5 |
| c. | Discuss the common mistakes that could be performed by the first  responders. | CO1 | 5 |
|  |  |  |  |  |
| 3. | a. | Describe Hard disk drive and explain the main components of hard disk drive. | CO1 | 12 |
| b. | Write a short note on data storage. | CO1 | 3 |
| c. | Distinguish backing storage and main memory. | CO2 | 5 |
| **(OR)** | | | | |
| 4. | a. | Explain how to use remote network acquisition tools. | CO3 | 5 |
| b. | Outline the causes of data loss with an example each. | CO3 | 5 |
| c. | Discuss the primary types of magnetic storage devices / media. | CO3 | 10 |
|  |  |  |  |  |
| 5. | a. | Write a short note on FAT file system. | CO4 | 5 |
| b. | Describe Steganography and explain in detail the techniques used in steganography with a chart. | CO4 | 15 |
| **(OR)** | | | | |
| 6. |  | Explain in detail how the windows registry works. | CO4 | 20 |
|  |  |  |  |  |
| 7. |  | Write a detailed note on chain of custody and explain the procedures to establish the chain of custody. | CO4 | 20 |
| **(OR)** | | | | |
| 8. |  | Explain the salient features of IT Amendment Act 2008. | CO5 | 20 |
|  | | **Compulsory**: |  |  |
| 9. |  | Outline the general four step procedures to be followed while collecting and analyzing the evidence. Customize the details to suit your situation as an investigator. | CO6 | 20 |