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



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

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Code :** | **17CA3006** | **Duration :** | **3hrs** |
| **Sub. Name :** | **DIGITAL FORENSICS** | **Max. Marks :** | **100** |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No.** | **Sub Div.** | **Questions** | **Course**  **Outcome** | **Marks** |
| 1. | a. | Write a note on digital forensics. | CO1 | 10 |
| b. | Elaborate the rules of digital forensics. | CO1 | 10 |
| **(OR)** | | | | |
| 2. | a. | Discuss the concepts of cyber crime and its types. | CO1 | 10 |
| b. | Prepare the Chain of Custody for the following case scenario:  “John was the chief of a Forensics Laboratory, which analyzed digital documents from various areas of forensic investigation, once they received confidential digital evidences as hard disk, pen drive mobile phone, pager, fitness band and digital siri related to a criminal case.” | CO5 | 10 |
|  |  |  |  |  |
| 3. | a. | Describe the process of Windows Forensics. | CO3 | 10 |
| b. | Discuss the MAC forensics process. | CO3 | 10 |
| **(OR)** | | | | |
| 4. | a. | Examine the given scenario: “Joseph and Buella are fellow co-artists who deliver coded messages to each other to communicate. Recently Buella was put in jail for stealing a rare and expensive diamond. The details of the theft were stored in Buella’s desktop.  The police did some research and found the system was in power off state, but they haven't been able to extract any evidence. Could you help the police to gather the evidence from the system?” | CO5 | 10 |
| b. | Elaborate any one recent cyber crime. | CO4 | 10 |
|  |  |  |  |  |
| 5. | a. | Explain the various networking devices in detail. | CO4 | 10 |
|  | b. | Identify the problem in the given scenario: “Anne was the chief of a Forensics Laboratory, which analyzed digital documents from various areas of forensic investigation, once they received confidential digital evidences as hard disk, pen drive and mobile phone related to a criminal case. Due to the urgency with which the case was to be solved, a person in the laboratory started analyzing the evidence without taking the copy of the file. An error occurred during the forensic process, due to which the entire file got corrupted and couldn’t be reconstructed.” Explain the process that should have been done before analyzing the original file so that loss of file could have been avoided. | CO4 | 10 |
| **(OR)** | | | | |
| 6. | a. | Elaborate the evidences that can be gathered from the devices such as router and switch. | CO5 | 10 |
| b. | Explain the general structure of Chain in detail. | CO1 | 10 |
|  |  |  |  |  |
| 7. | a. | Discuss the seizure issues related to digital crime. | CO3 | 10 |
| b. | Write a detailed note on digital sytems development model. | CO4 | 10 |
| **(OR)** | | | | |
| 8. | a. | Describe the internet protocol suite. | CO4 | 10 |
| b. | Discuss in brief any one Forensics Internet application. | CO5 | 10 |
|  | | **Compulsory**: |  |  |
| 9. | a. | Explain the Digital Forensics process. | CO1 | 10 |
| b. | Elaborate the ISO / OSI model. | CO4 | 10 |