|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Roll No. |  |  |  |  |  |  |  |  |  |  |  |  |



**PRESIDENCY UNIVERSITY**

**Bengaluru**

|  |
| --- |
| **End - Term Examinations – JANUARY 2025** |
| **Date:** 08 – 01- 2025 **Time:** 09:30 am – 12:30 pm |

|  |  |  |
| --- | --- | --- |
| **School:** SOCSE | **Program:** B.Tech- CCS | |
| **Course Code:** CSE2037 | **Course Name:** Cyber Forensics | |
| **Semester**: Vth | **Max Marks**: 100 | **Weightage**: 50% |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CO - Levels** | **CO1** | **CO2** | **CO3** | **CO4** |
| **Marks** | **24** | **24** | **26** | **26** |

**Instructions:**

1. *Read all questions carefully and answer accordingly.*
2. *Do not write anything on the question paper other than roll number.*

**Part A**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Answer ALL the Questions. Each question carries 2marks. 10Q x 2M=20M** | | | | |
| **1** | Describe Computer Fraud and Abuse Act. | **2 Marks** | **L1** | **CO1** |
| **2** | Define Modus Operandi. | **2 Marks** | **L1** | **CO1** |
| **3** | Describe a residual slack. | **2 Marks** | **L2** | **CO2** |
| **4** | Summarize file allocation table. | **2 Marks** | **L2** | **CO2** |
| **5** | Summarize benefits of cyber forensics. | **2 Marks** | **L2** | **CO3** |
| **6** | Generalize stages involved in traffic analysis in wireless networks. | **2 Marks** | **L2** | **CO3** |
| **7** | Describe organized crime. | **2 Marks** | **L2** | **CO3** |
| **8** | Illustrate factors that affect data back-up in recovery. | **2 Marks** | **L3** | **CO4** |
| **9** | Interpret Hearsay. | **2 Marks** | **L3** | **CO4** |
| **10** | Illustrate examples of Windows-based recovery tools. | **2 Marks** | **L3** | **CO4** |

**Part B**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Answer the Questions Total 80 Marks.** | | | | | |
| **11.** | **a.**  **b.** | Identify levels of certainty in digital forensics.  Describe equivocal forensic analysis. | **10 Marks**  **10 Marks** | **L1**  **L1** | **CO1**  **CO1** |
| **or** | | | | | |
| **12.** | **a.**  **b.** | Describe Trademarks and trade secrets.  Identify steps to conduct a complete and competent digital investigation. | **10 Marks**  **10 Marks** | **L1**  **L1** | **CO1**  **CO1** |
|  |  |  |  |  |  |
| **13.** | **a.**  **b** | Discuss file carving with Windows.  Describe ways of dealing with password protection and encryption. | **10 Marks**  **10 Marks** | **L2**  **L2** | **CO2**  **CO2** |
| **or** | | | | | |
| **14.** | **a.**  **b.** | Describe SSD.  Discuss structure of optical media disk formats. | **10 Marks**  **10 Marks** | **L2**  **L2** | **CO2**  **CO2** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **15.** | **a.**  **b.** | Describe characteristics of contemporary definitions of organized crime.  Explain stages involved in mobile forensics. | **10 Marks**  **10 Marks** | **L2**  **L2** | **CO3**  **CO3** |
| **Or** | | | | | |
| **16.** | **a.**  **b.** | Explain steps involved in disk forensics.  Summarize examples of Modus Operandi behaviors related to computer and Internet services. | **10 Marks**  **10 Marks** | **L2**  **L2** | **CO3**  **CO3** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **17.** | **a.**  **b.** | Explain steps involved in method of collection of digital evidence.  Interpret the Chain of Custody. | **10 Marks**  **10 Marks** | **L3**  **L3** | **CO4**  **CO4** |
| **Or** | | | | | |
| **18.** | **a.**  **b.** | Demonstrate role of data back-up in recovery.  Interpret rules of evidence | **10 Marks**  **10 Marks** | **L3**  **L3** | **CO4**  **CO4** |

**\*\*\*\*\* BEST WISHES \*\*\*\*\***