**SET A**

**SRM Institute of Science and Technology**

**College of Engineering and Technology**

**School of Computing**

**Department of Networking and Communications**

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

**Academic Year: 2022-23 (Even)**

**Test: CLA-T2** **Date: 03-04-2023**

**Course Code & Title:** 18C**S**C385T Forensics and Incident Response **Duration:** 100 minutes

**Year & Sem: III Year / V Sem** **Max. Marks:** 50

**Course Articulation Matrix:**

***CO 2: Understand the purpose and usage of various forensic tools.***

***CO 3: Gain knowledge on how scientific evidence collection/extraction during investigation.***

***CO 4: Acquire knowledge on file systems and its inner workings.***

| **S.No.** | **Course Outcome** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** | **PO11** | **PO12** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | **CO2** | H | H |  |  | H |  |  |  |  |  |  |  |
| 2 | **CO3** | H |  |  |  |  |  |  |  |  |  |  |  |
| 3 | **CO4** | H |  |  |  |  |  |  |  |  |  |  |  |

| **Part – A**  **(10x 1 = 10 Marks)**  **Instructions: Answer all** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Q. No** | **Question** | **Marks** | **BL** | **CO** | **PO** | **PI Code** |
| **1** | An attorney asking a digital investigator to fin vin supporting a particular line of inquiry is an example of \_\_\_   1. Influencing the examiner 2. Due diligence 3. Quid Pro Que 4. Voir dire | **1** | **2** | **2** | **1** | **1.7.1** |
| **2.** | The First US law to address computer crime is called \_\_   1. Computer Fraud and Abuse Act(CFAA) 2. Florida Computer Crime ACT 3. Computer Abuse Act 4. Weapon or Tool Design to Commit Act | **1** | **1** | **2** | **1** | 1.6.1 |
| **3.** | Regarding the admissibility of evidence which of the following is not a consideration \_\_\_   1. Relevance 2. Authenticity 3. Best Evidence 4. Nominally Prejudicial | **1** | **1** | **3** | **1** | 2.5.1 |
| **4** | Volatile data during the incidence is a part of \_\_\_   1. Host based data collection. 2. Hardware based data Collection. 3. Software Based data Collection. 4. IDS based data Collection | **1** | **2** | **2** | **1** | 1.6.1 |
| **5** | While creating an evidence report in incident response method which one is not the report type?   1. Writing formal Report 2. Written Informal Report 3. Manual report 4. High risk documents | **1** | **2** | **3** | **1** | 1.7.1 |
| **6** | Identify which one is not the data categories of the file system \_\_   1. FAT 2. GFS 3. NTFS 4. RFS | **1** | **1** | **4** | **1** | 1.6.1 |
| **7** | Mapping of file system is managed by \_\_   1. File Metadata 2. Page table 3. Virtual Memory 4. File System | **1** | **1** | **4** | **1** | 1.6.1 |
| **8** | In the past the method for expressing an option has been to frame a \_\_\_ question based on available factual evidence.   1. Hypothetical 2. Nested 3. Challenging 4. Contradictory | 1 | 2 | 4 | 1 | 2.5.1 |
| **9** | This is the table contains information about the cluster that are setup by the file system is called  \_\_   1. File name area 2. File to file 3. File allocation table 4. File system area | 1 | 1 | 4 | 1 | 1.6.1 |
| **10** | The unused space in a file allocation block or memory page that may hold residual data is called \_\_\_\_   1. Slack space 2. Shrink space 3. Data space 4. File space | 1 | 1 | 4 | 1 | 1.6.1 |

**SET A**

**SRM Institute of Science and Technology**

**College of Engineering and Technology**

**School of Computing**

**Department of Networking and Communications**

SRM Nagar, Kattankulathur – 603203, Chengalpattu District, Tamilnadu

**Academic Year: 2022-23 (Even)**

**Test: CLA-T2** **Date: 03-03-2023**

**Course Code & Title:** 18C**S**C385T Forensics and Incident Response **Duration:** 100 minutes

**Year & Sem: III Year / V Sem** **Max. Marks:** 50

**Course Articulation Matrix:**

***CO 2: Understand the purpose and usage of various forensic tools.***

***CO 3: Gain knowledge on how scientific evidence collection/extraction during investigation.***

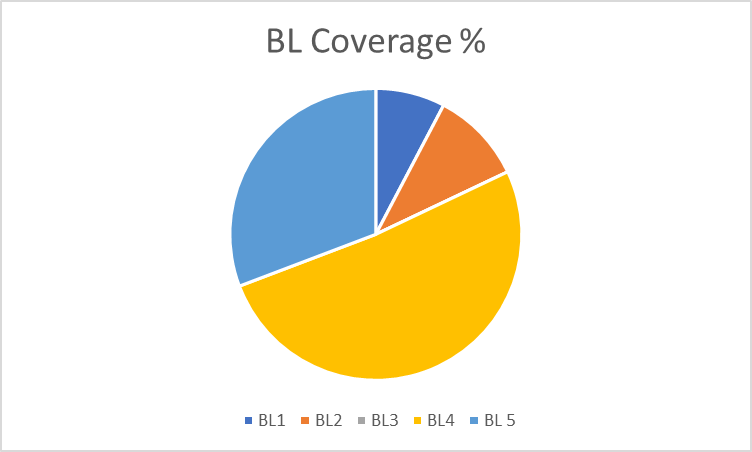
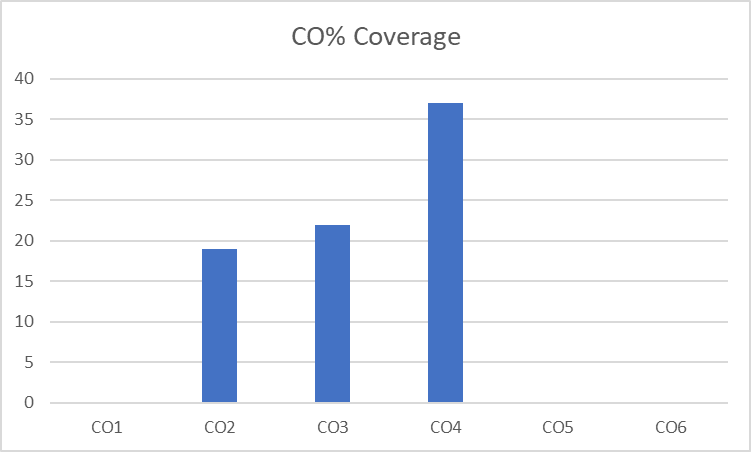
***CO 4: Acquire knowledge on file systems and its inner workings.***

| **S.No.** | **Course Outcome** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** | **PO11** | **PO12** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | **CO2** | H | H |  |  | H |  |  |  |  |  |  |  |
| 2 | **CO3** | H |  |  |  |  |  |  |  |  |  |  |  |
| 3 | **CO4** | H |  |  |  |  |  |  |  |  |  |  |  |

| **Part – B**  **( 4\*4 = 16 Marks)**  **Instructions: Answer any 4 Questions** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **11** | **Illustrate acquiring data with dd command and dcfldd in linux?** | **4** | **4** | **2** | **2** | **2.6.3** |
| **12** | **Explain about Evidence handling and specify the report format in detail.** | **4** | **2** | **3** | **1** | **2.6.4** |
| **13** | **Assess data FTK imager detail and list out some applications** | **4** | **4** | **4** | **5** | **5.6.1** |
| **14** | **Show how to recover the deleted files in FAT system and brief it** | **4** | **4** | **4** | **1** | **2.6.3** |
| **15** | **Show how the digital evidence stored and explain it?** | **4** | **4** | **3** | **1** | **5.6.1** |
| **Part – C**  **( 2\*12 = 24 Marks)** | | | | | | |
| **16** | Analyze and write short notes on   1. Forensic Duplication 2. Forensic Investigation   (OR) | **12** | **5** | **2** | **2** | **1.6.1** |
| **17** | What is digital evidence? State and explain task that investigators perform when working with digital evidence | **12** | **4** | **3** | **2** | 5..5.1 |
| **18** | Summarize the steps involved in examining NTFS disk and explain it.  (OR) | **12** | **5** | **4** | **1** | **1.6.1** |
| **19** | Illustrate in detail on FAT32 file system and its directory structure in detail. | **12** | **4** | **4** | **1** | 2.6.3 |

**\*Program Indicators are available separately for Computer Science and Engineering in AICTE examination reforms policy.**

**Course Outcome (CO) and Bloom’s level (BL) Coverage in Questions**



**Approved by the Scrutiny**