**SET B**

**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: 2021-22 (ODD)**

**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**  **(10 x 1 = 10 Marks)**  **Instructions: Answer all** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Q. No** | **Question** | **Marks** | **BL** | **CO** | **PO** | **PI Code** |
| **1** | \_\_ is a less structured attorneys cannot be forced to release verbal reports address the areas of the investigation yet to be completed.   1. Verbal reports 2. Written report. 3. Peripheral 4. Oral deposition | **1** | **2** | **2** | **1** | 2.5.1 |
| **2.** | In obtaining a warrant, an investigator must convince the judge on all the following points except: \_\_   1. Evidence of a crime is in existence. 2. A crime has been committed. 3. The owner or resident of the place to be searched is likely to have committed the crime. 4. The evidence is likely to exist at the place to be searched | **1** | **1** | **2** | **1** | 2.5.1 |
| **3.** | Rules created by the US supreme Court that govern how evidence can be used in both civil and criminal cases.   1. Federal rules of evidence Act 2. Federal rules of evidence (FRE) 3. Rules of evidence 4. Central processing Unit (CPU) | **1** | **1** | **2** | **1** | 1.7.1 |
| **4** | Private networks can be a richer source of evidence than the Internet because:  a. They retain data for longer periods of time.  b. Owners of private networks are more cooperative with law enforcement.  c. Private networks contain a higher concentration of digital evidence.  d. Nobody can be harmed by crime on the Internet | **1** | **2** | **3** | **1** | 2.7.1 |
| **5** | Identify the method which is not a data acquisition\_\_   1. Live acquisition 2. Logical Acquisition 3. Sparse Acquisition 4. Vendor acquisition | **1** | **2** | **2** | **1** | 1.6.1 |
| **6** | Which file is a sequence of bytes organized to blocks understandable by the system linker?   1. Object file 2. Source file 3. Executable file 4. Text file | **01** | **2** | **4** | **1** | 1.6.1 |
| **7** | \_\_ mounts, When a file system can be mounted over another file system that is remotely mounted not in local.   1. Recursive 2. Cascading 3. Trivial 4. Exhibits | **1** | **1** | **4** | **1** | 1.6.1 |
| **8** | Mounting of fil system indicates \_\_\_   1. Creating a file system 2. Deleting a file system 3. Attaching portion of file system to the directory structure 4. Removing portion of file system from the directory structure | **01** | **01** | **4** | **1** | 1.6.2 |
| **9** | Smallest addressable storage unit on the hard drive disk?   1. cylinder 2. row 3. sector 4. track | **1** | **1** | **4** | **1** | 1.7.2 |
| **10** | Independent organizational structure that allows the user to store and retrieve data is called \_\_   1. file system 2. files 3. file slack 4. file system area | 1 | 1 | 4 | 1 | 1.6 |



**SET B**

**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.***

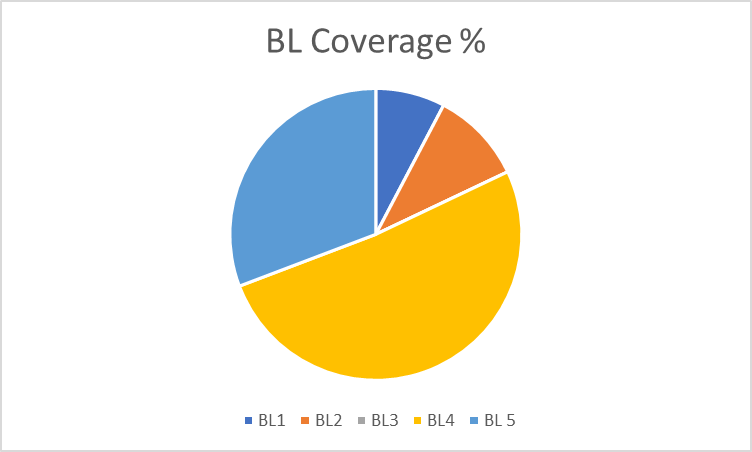
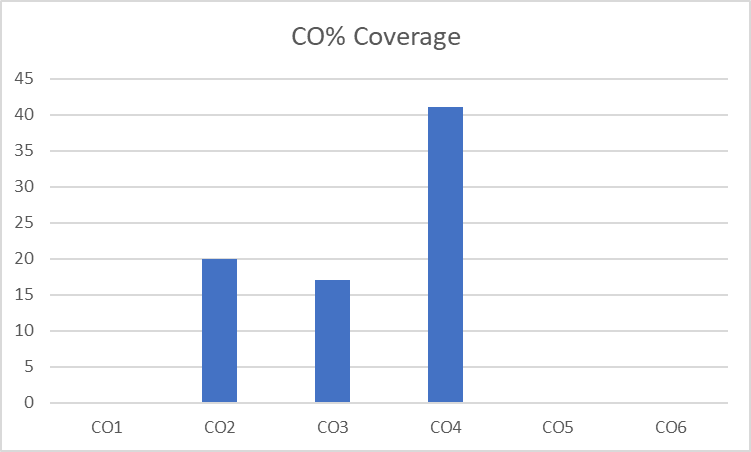
***CO 3: Gain knowledge on how scientific evidence collection/extraction during investigation.***

***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: Randomly selected four questions. Answer for four Questions** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| 11 | Analyze briefly about the forensic duplication and investigation. | 4 | 4 | 2 | 2 | **2.6.3** |
| 12 | What is an evidence custody form? What information does it contain? | 4 | 2 | 3 | 1 | **2.6.4** |
| 13 | List out the file system types and its characteristics | 4 | 2 | 4 | 1 | **5.6.1** |
| 14 | Explain in detail about how the understanding of file system plays a crucial role in cyber forensics | 4 | 4 | 4 | 1 | **2.6.3** |
| 15 | List out the steps involved in examining NTFS disk. | 4 | 4 | 4 | 1 | **5.6.1** |
|  | **Part C (2\*12=24**) |  |  |  |  |  |
| 16 | Explain the following terms   1. bit stream image 2. chain of custody 3. Evidence custody form   **(OR)** | 12 | 5 | 3 | 2 | **1.6.1** |
| 17 | Point out the features of forensic duplication and the investigation and also outline the challenges forensic examiners face when preparing and processing investigation including the ideas and questions they must consider. | 12 | 4 | 2 | 2 | 5..5.1 |
| 18 | Explain in detail about the following terms   1. Disk partitions (6) 2. FAT Disks (6)   **(OR)** | 12 | 4 | 4 | 1 | **1.6.1** |
| 19 | Generalize about NTFS data stream and encryption file system and NTFS Compressed files | 12 | 4 | 4 | 1 | 2.6.3 |

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



**Approved by the Scrutiny**