**SET B**A picture containing text, logo, font, trademark

Description automatically generated

**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: 03-05-2023**

**Course Code & Title:** 18CSE382T Forensics and Incident Response **Duration:** 60 minutes

**Year & Sem: III Year / V Sem** **Max. Marks:** 30

**Course Articulation Matrix:**

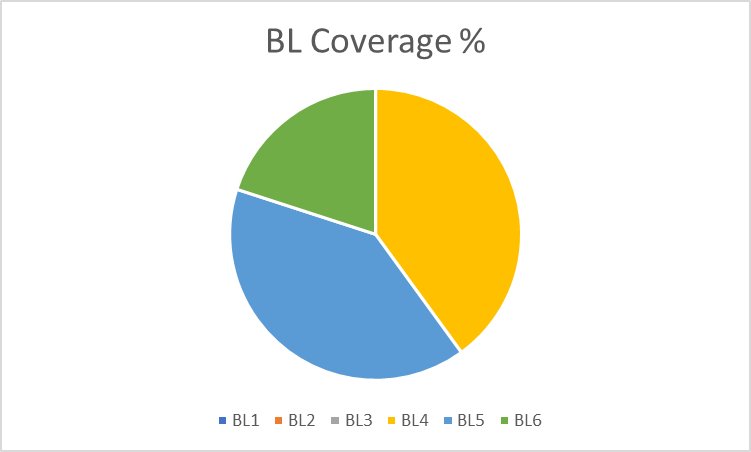
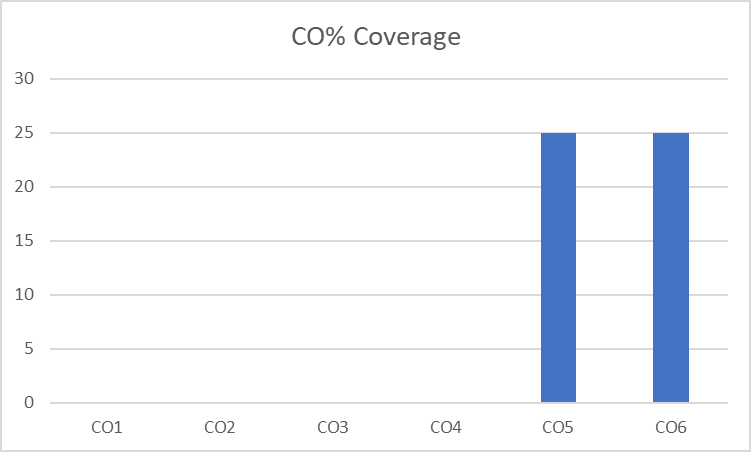
***CO 5; Understand the windows and linux investigation procedures.***

***CO 6: Introduce the report writing guidelines and principles***

| **S.No.** | **Course Outcome** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** | **PO11** | **PO12** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | **CO5** | H |  |  | H |  |  |  |  |  |  |  |  |
| 2 | **CO6** | H |  |  |  |  | H |  |  |  |  |  |  |

|  | **Part C (3\*10=30**) | **Marks** | **BL** | **CO** | **PO** | **PI Code** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Why corporate investigations are typically easier than law enforcement investigations. Recommend the process of investigations and justify the solutions.  **(OR)** | 10 | 5 | 3 | 2 | **1.6.1** |
| 2 | Elaborate in detail about the legal process to conduct computer investigation for potential criminal violations of law | **10** | **4** | **5** | **4** | **5.5.1** |
| 3 | Generalize the idea behind using the following tools in forensics.   1. Exploring windows registry 2. Examining the windows registry.   **(OR)** | **10** | **5** | **6** | **6** | **1.6.1** |
| 4 | Analyze about the types of forensic tools and how tasks performed by forensic tools.sd | **10** | **4** | **4** | **1** | **2.6.3** |
| 5. |  | **10** | **6** | **5,6** | **4,6** | **5.5.3** |

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



**Approved by the Scrutiny**