**Imam Mohammad Ibn Saud Islamic University**

**College of Computer and Information Sciences**

**Computer Science Department**

|  |  |
| --- | --- |
| **Course Title:** | *Selected Topics in Cyber Security and Networks* |
| **Course Code:** | CS443 |
| **Course Instructor:** | Dr. Miled Tezeghdanti and Dr. Wojdan BinSaeedan |
| **Lab Assignment:** | How to Acquire Data |
| **Semester:** | 1st Semester, 2023 |
| **Due Date:** | Monday (2023-09-25( |
| **Marks:** | 10 |

|  |
| --- |
| **Instructions:**   1. There (1) question in (1) page. 2. Utilize the provided solution template that aligns with the assignment file. |

|  |  |  |
| --- | --- | --- |
| **Question** | **CLOs** | **Question Marks** |
| 1.1 | 2.1, 2.2 | 5 |
| 1.2 | 2.1, 2.2 | 5 |
| **Total** | | **10** |

**Scenario:**

|  |  |
| --- | --- |
| **Question 1:** | **[ ] / 10 Marks** |

In these exercises, we will go through the process of collecting the most important data from a live Windows system, to start initial analysis and imaging the whole system for further analysis and investigations. The scope of this lab is a hard disk drive with a Windows operating system installed on it.

**Goals:**

* Collect volatile data.
* Create a custom forensic image.
* Create a full system image.

**Recommend Tool:** AccessData FTK-Imager

**Tasks:**

**Tasks 1.1:** Dumping the system’s memory**:**

For this task, let’s assume that we want to dump the system’s memory (make a copy) so we can perform memory forensic investigations later. Use the FTK Imager tool to acquire the memory of the suspect’s machine. Compare the size of the memory image and the size of the actual system’s memory, and make sure they match!

**Tasks 1.2:** Creating a Custom Forensic Image

In this task, we will continue to use AccessData’s FTK Imager to create an image file of specific system files to use for analysis. Let’s assume that the suspect’s system that we want to gather information from already has an external drive. In a real-life scenario, the only difference will be that you will be plugging in your own USB thumb drive and running FTK-Imager from there.

In this task, create a custom image and make sure you gather the following:

* File System Files
* Windows Registry Files
  + SAM
  + SYSTEM
  + SOFTWARE
  + SECURITY
  + DEFAULT
* Recycle Bin Files
* Log Files (evtx, log, etc.)
* Link Files (.lnk)
* Prefetch and Cache Files (Prefetch, RecentFileCache.bcf)
* User Files
* Task Files

Finally, don’t forget to encrypt the data gathered.

**Submission:** You must submit:

1. A solution file that provides a comprehensive explanation and step-by-step instructions for completing all the tasks.
2. A OneDrive link to access a video recording that provides a comprehensive explanation and step-by-step instructions for completing all the tasks.