Cyber security Exercise 8 :

1. Perform Memory capture and analysis using FTK imager tool

***Aim:***

The aim of an FTK (Forensic Toolkit) image is to create a bit-by-bit copy of a digital storage device, such as a hard drive, USB drive, or other digital media, in a forensically sound manner. This means that the copy is an exact replica of the original, including all files, metadata, and unallocated space, ensuring that no data is altered or omitted during the copying process.

***purpose of creating an FTK image include:***

* FTK Imager is a tool for creating disk images and is absolutely free to use. It was developed by The Access Data Group. It is a tool that helps to preview data and for imaging
* You can also mount an image for a read-only view that will also allow you to view the contents of the forensic image exactly as the user saw it on the original drive.
* Ensuring that the original data remains unaltered for legal and investigative purposes.
* Allowing investigators to analyze the data without risking changes to the original evidence.
* Maintaining a documented process to demonstrate that the evidence has been handled in a secure and consistent manner.
* Providing a copy that can be used by multiple investigators simultaneously without compromising the integrity of the original data.
* Adhering to legal standards and procedures for digital evidence handling.
* FTK images are crucial in digital forensics for conducting thorough and reliable investigations.

***How to Download FTK image tool :***

To download the FTK Imager tool, follow these steps:

Visit the Official Website:

Step 1: Go to the [AccessData website](

https://www.exterro.com/ftk-product-downloads/ftk-imager-version-4-7-1

Step 2 : Look for the section where you can download FTK Imager. It is usually under the

product downloads or software downloads section.

Step 3 : Select FTK Imager

Find the FTK Imager tool from the list of available software and select it.

Step 4: Fill in the Required Information:

You may be required to fill out a form with your personal information, such as your

name, email address, and organization, to access the download link.

Step 5: Download the Installer:

After submitting the required information, you will be provided with a link to

download the FTK Imager installer. Click the link to download the file.

Step 6: Install FTK Imager:

Once the download is complete, run the installer and follow the on-screen instructions to

install FTK Imager on your computer.

Step 7: Launch FTK Imager:

After installation, you can launch FTK Imager from your Start menu or desktop shortcut.