Parul University

FACULTY OF ENGINEERING AND TECHNOLOGY

BACHELOR OF TECHNOLOGY

# DIGITAL FORENSICS & INCIDENT RESPONSE LABORATORY (303105396)

6TH Semester

Computer Science & Engineering Department

Cyber Security

# Lab Manual

ERP NO.:2303031260160

**Faculty of Engineering & Technology (FET)**

**Parul Institute of Engineering & Technology (PIET)**

**Department of Computer Science & Engineering**

# ***CERTIFICATE***

This is to certify that Mr./Ms. **NIMMANA MONIKA** has completed all the practical of the subject on his/her own and is submitting the lab manual with proper formatting as per the given instructions. His/Her work is found satisfactory and hence, he/she has successfully completed the term-work submission of DIGITAL FORENSICS & INCIDENT RESPONSE LABORATORY (303105396).

Date of Submission: _____

**Student's Signature** **Subject Faculty's Signature**

**HoD's Signature**

ERP NO.:2303031260160

# PRACTICAL ASSESSMENT TABLE

| SR. NO. | PRACTICAL TITLE | PAGE NO. | | MARKS (10) | SIGN |
|---|---|---|---|---|---|
| | | FROM | TO | | |
| 1 | Setting up a DFIR lab. | | | | |
| 2 | Non-Volatile Disk imaging using FTK Imager. | | | | |
| 3 | Analyzing the Physical image using Autopsy to extract evidence. | | | | |
| 4 | Analyzing the Live running OS using Autopsy to extract evidence without Imaging. | | | | |
| 5 | Creating RAM dumps using Dump-IT and FTK. | | | | |
| 6 | Analyzing the RAM Dump using Volatility Framework to extract evidence. | | | | |
| 7 | Setup SIEM tool and upload the extracted logs from windows system. | | | | |
| 8 | Installing wire shark and creating PCAP files for analysis. Application of wire shark search filters. | | | | |
| 9 | Network malware logs analysis CTF (using Wire-shark). | | | | |
| 10 | Windows security logs analysis (using SPLUNK). | | | | |

ERP NO.:2303031260160

# PRACTICAL 1

**AIM :** Setting up a DFIR lab.

To maximize the credibility of your law enforcement organization and crack more cases, it's important to meet the industry's strictest computer forensics lab requirement standards and upgrade it when an upgrade is due. But apart from budget considerations, getting the project rolling can be a slow start due to getting lost in all the information that's out there and not knowing where to begin.
To outline the process for you, we're going to list the necessary functions of digital forensic lab, examine its purpose, and cover all the questions you should ask to arrange a perfect digital forensic lab set up in an easy to follow step-by-step manner.

**Step 1: Get acquainted with the purpose of a digital forensic lab.**

Prior to determining the right digital forensic lab set up for your needs, it's essential to cover the basics. So What is a digital forensic lab??
At its very core, a digital forensics lab is a central space to analyze evidence. It's where a certified digital forensic examiner extracts and inspects evidence from various types of digital devices based on which to prosecute the perpetrator of the crime.
With its help, you will be able to:

- Improve the accuracy of the investigation.
- Solve more cases in less time.
- Increase the reputation of your law enforcement organization.
- Secure more opportunities for career advancement and promotion due to the outstanding work.

**Step 2: Determine the primary focus of your department**

Depending on what your department specializes in, you should pick the kind of digital forensic lab equipment that best compliments your work.

1. What types of digital evidence do you usually process?

That's where the majority of your budget should go. Due to the increase in efficiency, you will be able to solve more cases in record time, so in essence, the investment will pay for itself.

2. Say, you're more of a nice department that specializes in a certain area of digital forensics (for example mobile forensics). Then, the digital forensics equipment you end up going with should reflect that.

3. However, What if your objective is to become an all-in-one digital forensics service provider?

In that case, you need the kind of digital forensic lab setup that can handle anything you throw at it. A well-rounded digital forensic lab should be able to handle various types of operating systems, file systems, and databases, including:

- Mobile OS: Android, Ios.
- Computer OS: Windows, Linux, Mac.
- Disk Format: NTFS, FAT32.
- Database: MySQL, SQLServer, SQLite

**Step 3: Consider the physical limitations, the space, and the location you have available.**

Unless you'll be moving your operations to a whole new location, you're going to have to work with what you've got.

- This involves measuring the space you have available and making sure it's suitable for high-end digital forensics lab equipment.
- Visualize the big picture of how everything will go together and don't forget to leave enough room for maintenance and upgrades further down the road.

**Essential Elements :**

Your digital forensic lab setup should include the following essential elements:

- Basic Sector: Case acceptance, IT infrastructure, Evidence storage.
- Functionality Sector: Computer Division, Mobile devices Division, Video division, Audio division, Database division, Data recovery division.
- Processing Sector: Storage medium repair division, Digital analysis & display division.
- Output Sector: Report generation division, Conference center division

**Environment factor :**

Before going further, you should remind that what you're looking for is an environment that is clean, cool, and available – the last thing you want is to risk that the evidence ends up damaged due to unsuitable environmental factors.

**Implementation location :**

If you find out you need a new central base of operations, consider moving to a place where most of your clients/visitors/ users come from. This will greatly reduce the time it takes for evidence samples to reach your lab and thus make the investigation process as efficient as possible.

**Safety & Security :**

Furthermore, there are several safety and security considerations to have in mind when choosing the optimal space.

Make sure only those cleared to have access can enter the premises. Since you'll be working with sensitive data, every third-party contractor could be a potential malicious insider, so think twice before letting somebody inside.
Due to similar reasons, make sure the computer screens are not facing the windows – someone could be spying from the outside of the building, so keep the confidential data safe.

**Step 4: Assess your existing equipment.**
After that, before investing in an entirely new set of digital forensics equipment and gear, assess your current one to see if there's anything that can be repurposed always make sense. However, if the current gear you're working with is really old, it's probably better to give it a complete overhaul – a digital forensic lab set up that is older might not be up to the task of handling modern digital forensics challenges.
Either way, the computer you're going to be using should be dedicated to digital forensics purposes exclusively. Ideally, you should have a dedicated machine for every task–one for mobile forensics, one for computer forensics, and so on.
When it comes to the sheer processing power of your computer forensics lab equipment, the most spaced up computer should be reserved for evidence processing and analysis – the one for acquisition and administrative tasks always comes second. If you have some extra monitors lying around from your old digital forensic lab set up, think about re-using them. In fact, you can even use them to create a dual-monitor setup for extra screen real estate and heightened productivity.

**Step 5: Determine your software needs.**
Software is one of the most essential parts of any digital forensic lab setup, hence it's also one of the most substantial expenses you can expect to cover.

**Free open-source forensic tools are an option?**
Unless, of course, you're planning to wing it by relying on open-source digital forensic tools exclusively. That, however, can have its fair share of drawbacks, the most notable of which is a steep learning curve, lack of support, hidden malware, data loss, and simply not being up to the modern day's digital forensics challenges.
As a general rule of thumb, you get what you pay for. If nothing else, paid digital forensics software is the superior choice due to the support that you get. As you probably know already, during an investigation, time is of the essence, and you simply cannot afford to lose any of it by having to stumble over technical hurdles.

**Choose the digital forensic software properly and wisely.**
When choosing your digital forensics software provider, give preference to the ones that have specialized in serving the digital forensics niche exclusively rather than developing a general type of software solutions.

Keep in mind that, these should be designed to preserve the integrity of the evidence and make sure it stands in court.
Above all else, your digital forensics software of choice should have the features you need to support your workflow and the digital forensics field your department specializes in.

**Step 6: Cover your hardware needs.**
Without the proper computer forensics lab equipment, it's impossible to stay on top of crime in your area. When your clients/visitors/users come to you, they want to see that the fate of the investigation rests in good hands.
To make a convincing case, double-check the computer forensics lab requirement list that's in effect in your local area. For starters, be on the lookout for the following standards as a sign of confidence:

- Risk management (ISO 31000)
- Information security management (ISO 27000)
- Occupational health safety (OHSAS 18000)
- Environmental management system (ISO 14000)

Apart from the run-of-the-mill digital forensics equipment such as workstations, monitors, evidence storage, large displays, intelligent tables & chair, and similar, it's a good idea to cover all your bases and have a well-rounded base of operations from where you'll be conducting your investigation.
Besides, as optional hardware, you could look into them specifically, which includes :

- Microscopes
- Spectrometers
- Chromatographs
- Fume hoods

**Step 7. Pick your digital forensic lab provider.**
Finally, the last step is to do your due diligence and pick a trustworthy provider that's most suitable for guaranteeing all the necessary functions of a digital forensic lab. You deserve a solution that won't leave you hanging, the kind that inspires you to do your best digital forensics work without any technical obstacles.
Ask yourself: what brand of digital forensics lab do the top law enforcement agencies rely on? Whatever they use, it's probably for a good reason. Don't be afraid to shop around and see what's getting the best reviews and what meshes with your law enforcement organization.

# PRACTICAL 1

**AIM :** Non-Volatile Disk imaging using FTK Imager.

Non-volatile disk imaging using **FTK Imager**, a forensic acquisition tool developed by **AccessData**, is the process of creating an exact bit-by-bit copy of a storage device such as a hard disk, SSD, or USB drive for digital forensic investigations. This imaging captures all data present on the disk including active files, deleted files, unallocated space, slack space, and file system metadata without altering the original evidence. The primary objective is to preserve the integrity and authenticity of digital evidence so that analysis can be performed on the image rather than the original device. FTK Imager supports multiple image formats such as RAW (dd) and E01 and generates cryptographic hash values (MD5, SHA-1, or SHA-256) during acquisition to verify data integrity. Matching hash values before and after imaging confirm that the evidence has not been modified, making the forensic image legally admissible. Thus, FTK Imager plays a vital role in maintaining chain of custody and ensuring reliable evidence preservation in digital forensics.

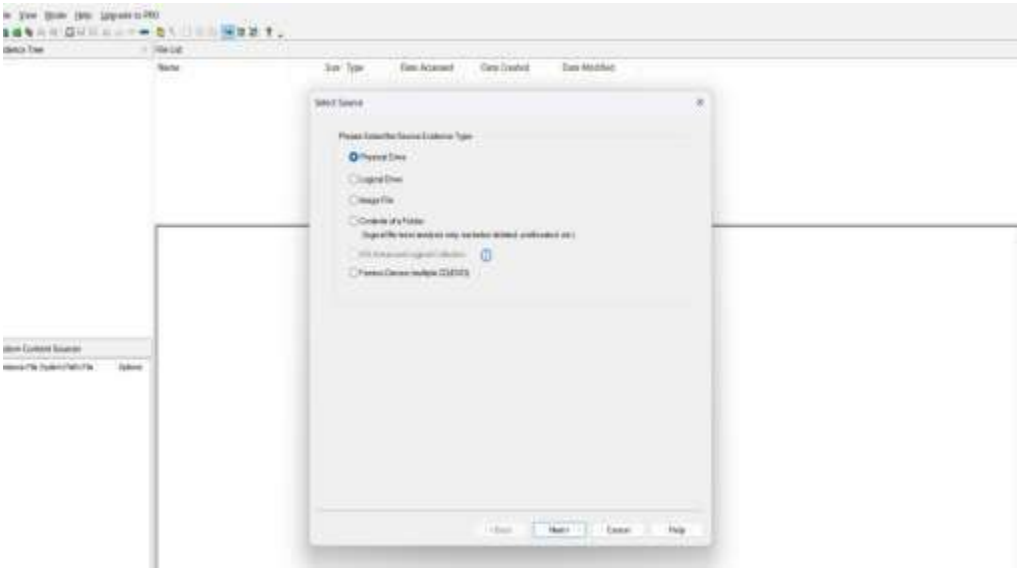
**STEPS :**

1) Install FTK Imager.

## 2) Creating a Disk Manager.

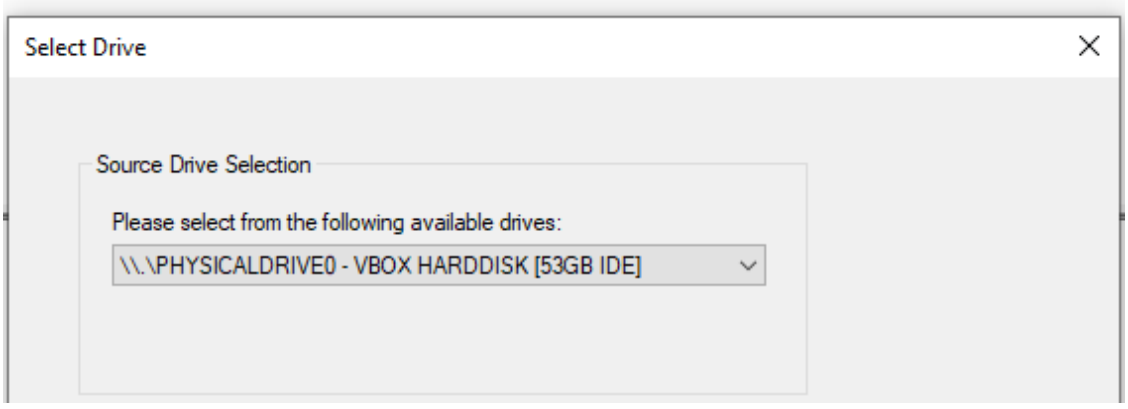
**Go to "File" option and click on "Create Disk Image"**

**Select the source evidence type**

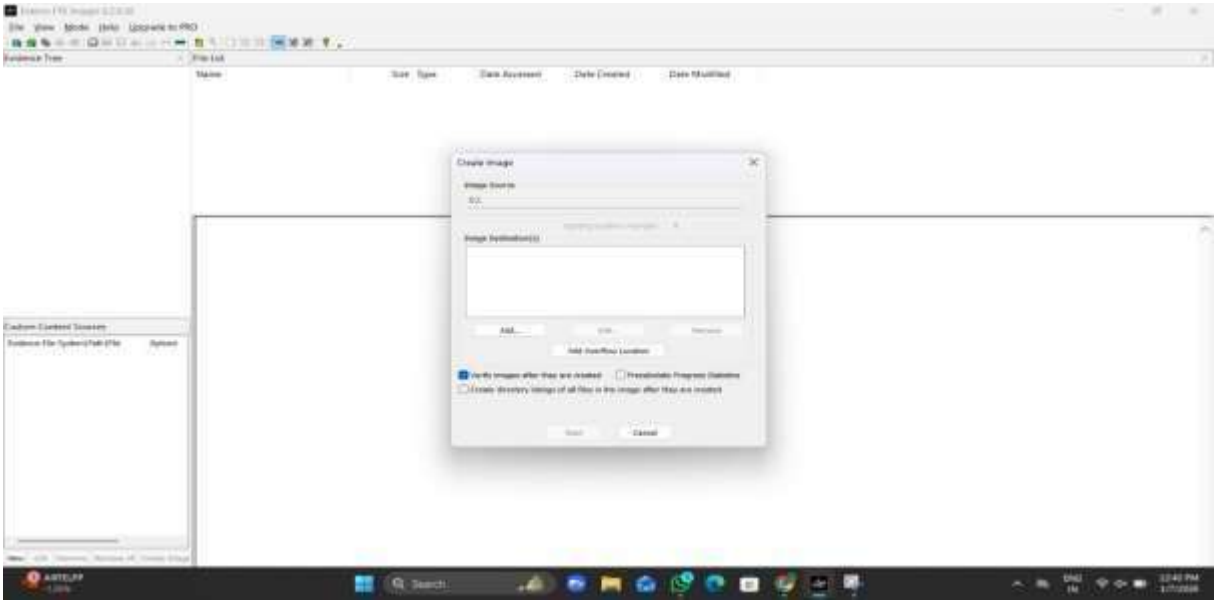


- Physical Drive: A physical drive refers to the hardware unit within a computer, laptop, or server. It is a data storage device that can store and retrieve digital information. Example: HDD, SSD, Pendrive.
- Logical Drive: A logical drive is a virtual tool that creates usable storage capacity on one or more physical hard drives in an operating system. The drive is referred to as "virtual" because it doesn't physically exist. Example: Local Disk (C:\, D:\)
- Image File: A forensic image (forensic copy) is a bit-by-bit, sector-by-sector direct copy of a physical storage device, including all files, folders and unallocated, free and slack space.
- Contents of a folder: Only file analysis is done
- Ferrico Device: use it for imaging CD/DVD's

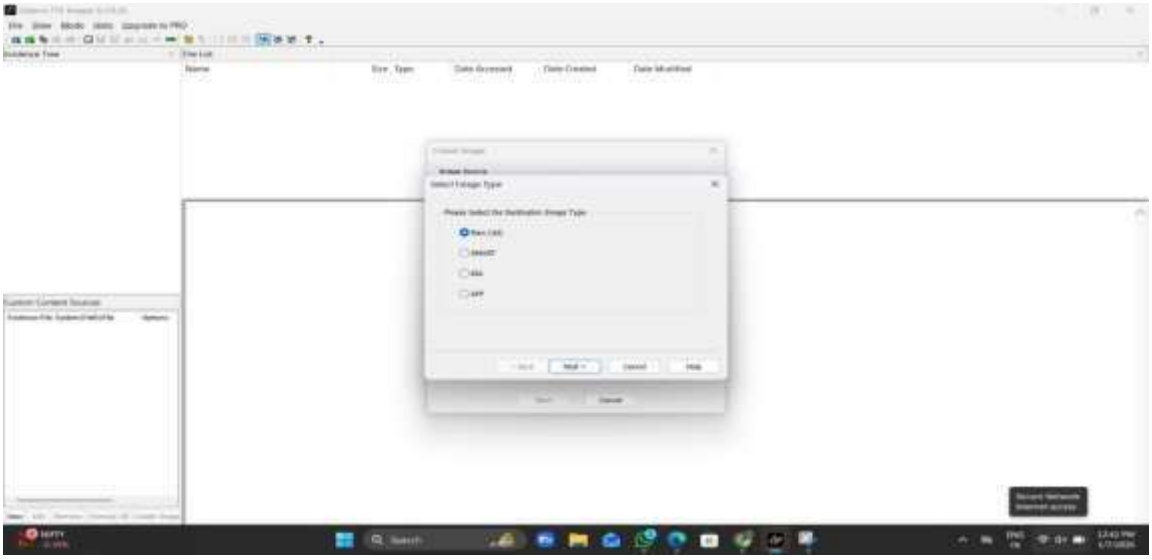
3) Select the Source Drive



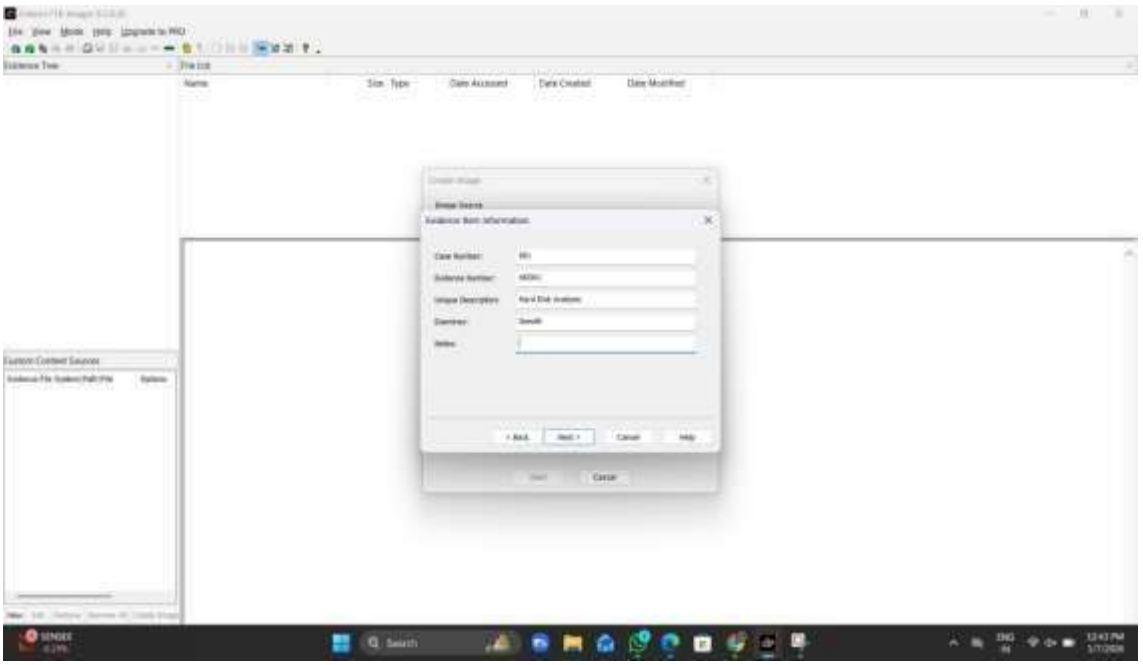
4) Now add the Image destination, i.e where the image must be saved



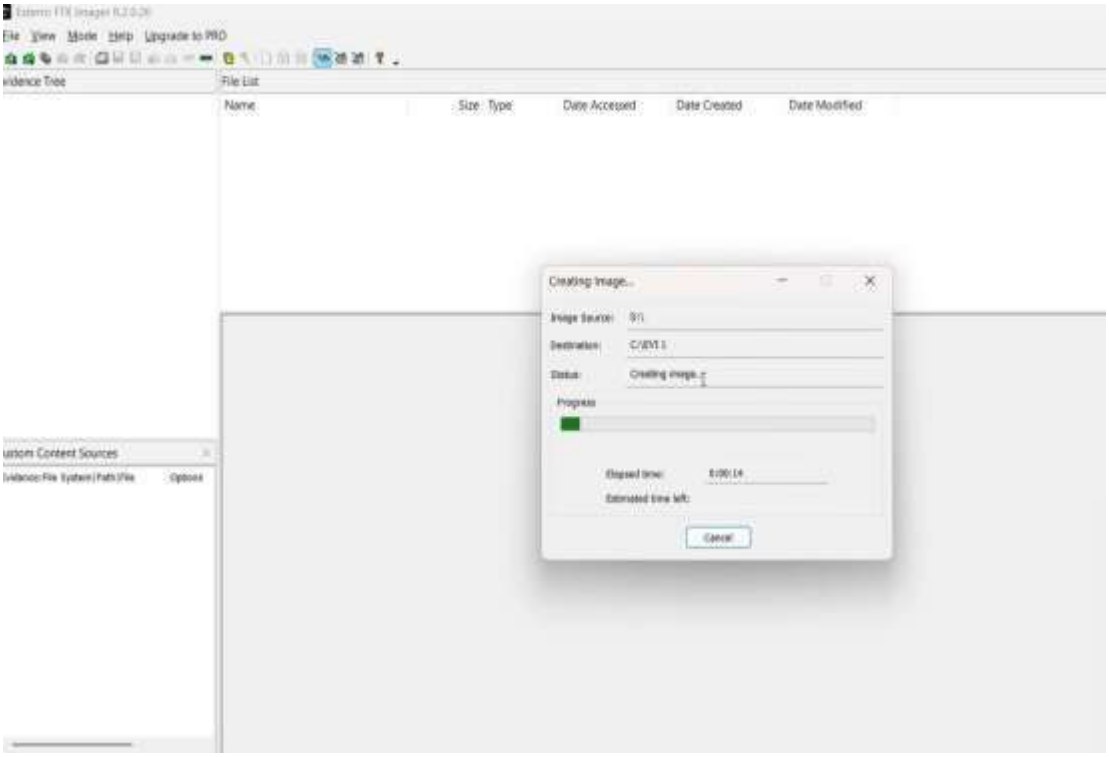
Raw is a bit-by-bit uncompressed copy of the original, while the other three alternatives are designed for use with a specific forensics program. We typically use Raw or E01, which is an EnCase forensic image file format.



5) Add the Evidence Item Information.



6) Select Image Destination and click on Finish.



7) The FTK Imager will now start to image the physical disk and will save in the destined folder.