**Lab-11: Static Acquisition with DEFT**

**Course Name**: FRS301-Digital Forensics

**Student Name**: Nguyễn Trần Vinh – SE160258

**Instructor Name**: Lê Tiến Dũng

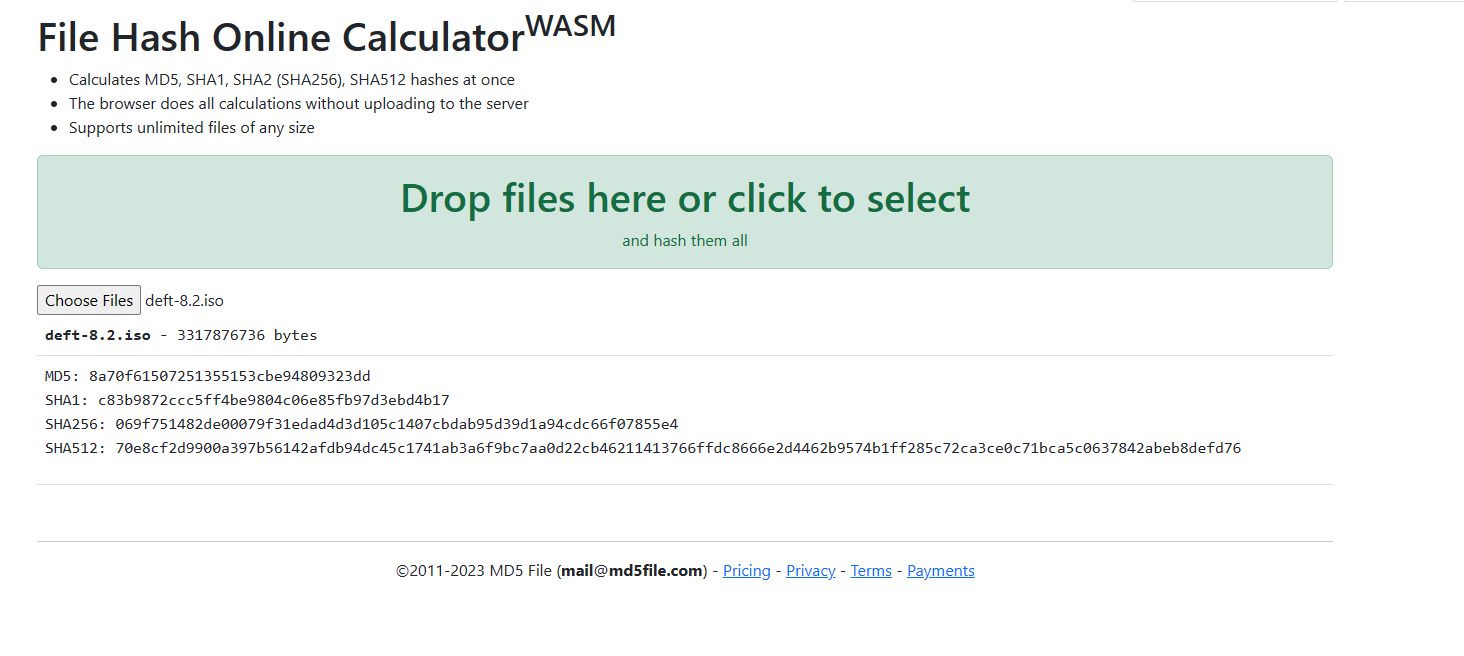
**Lab Due Date**: 3/3/2023

**What You Need for This Project**

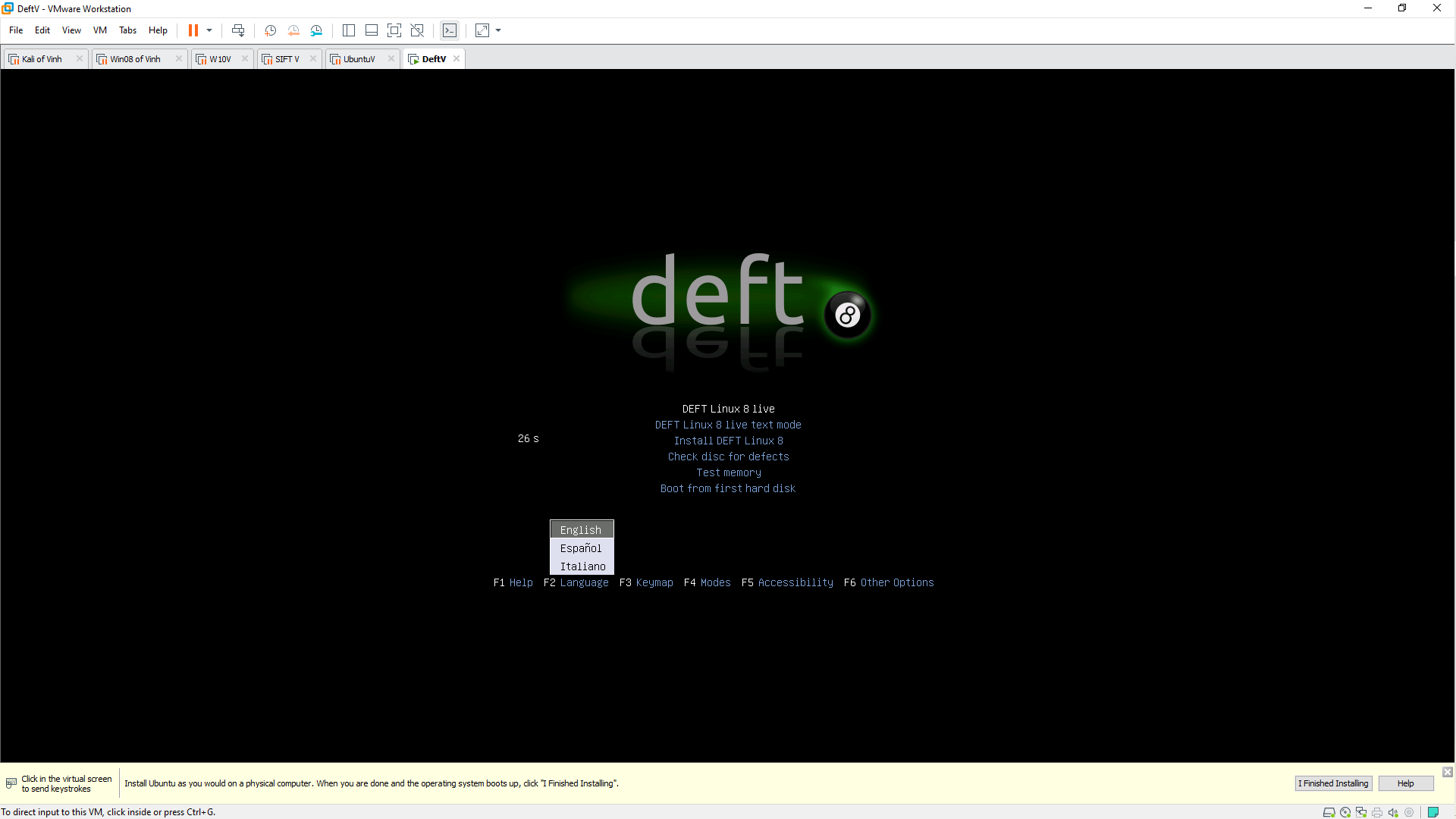
* VMware Player

**Downloading DEFT**

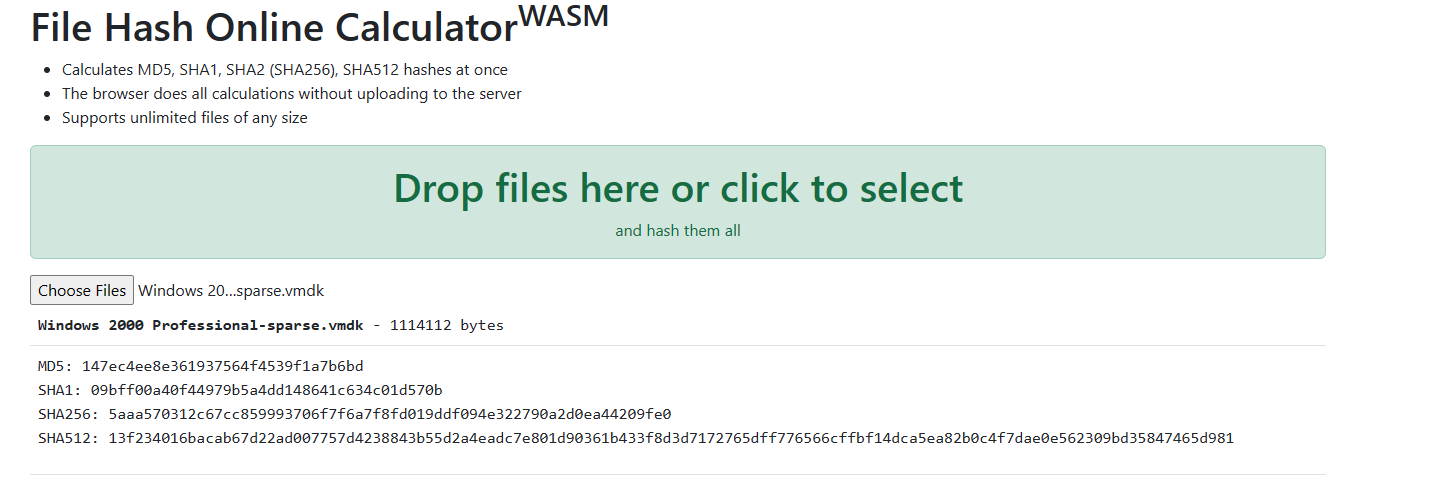
**Checking the Hash Value of the DEFT ISO File**

****

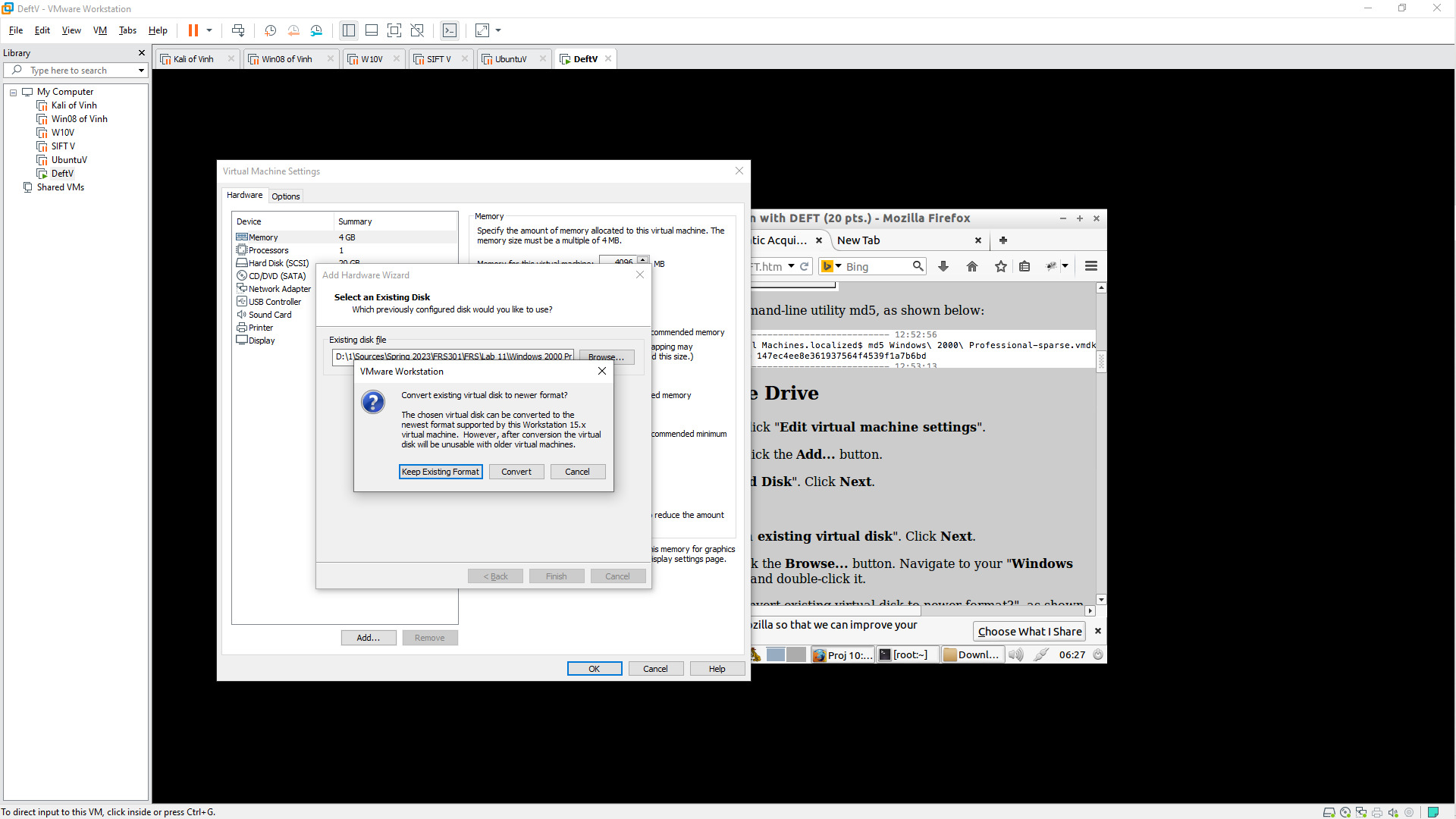
**Creating a New Virtual Machine**

****

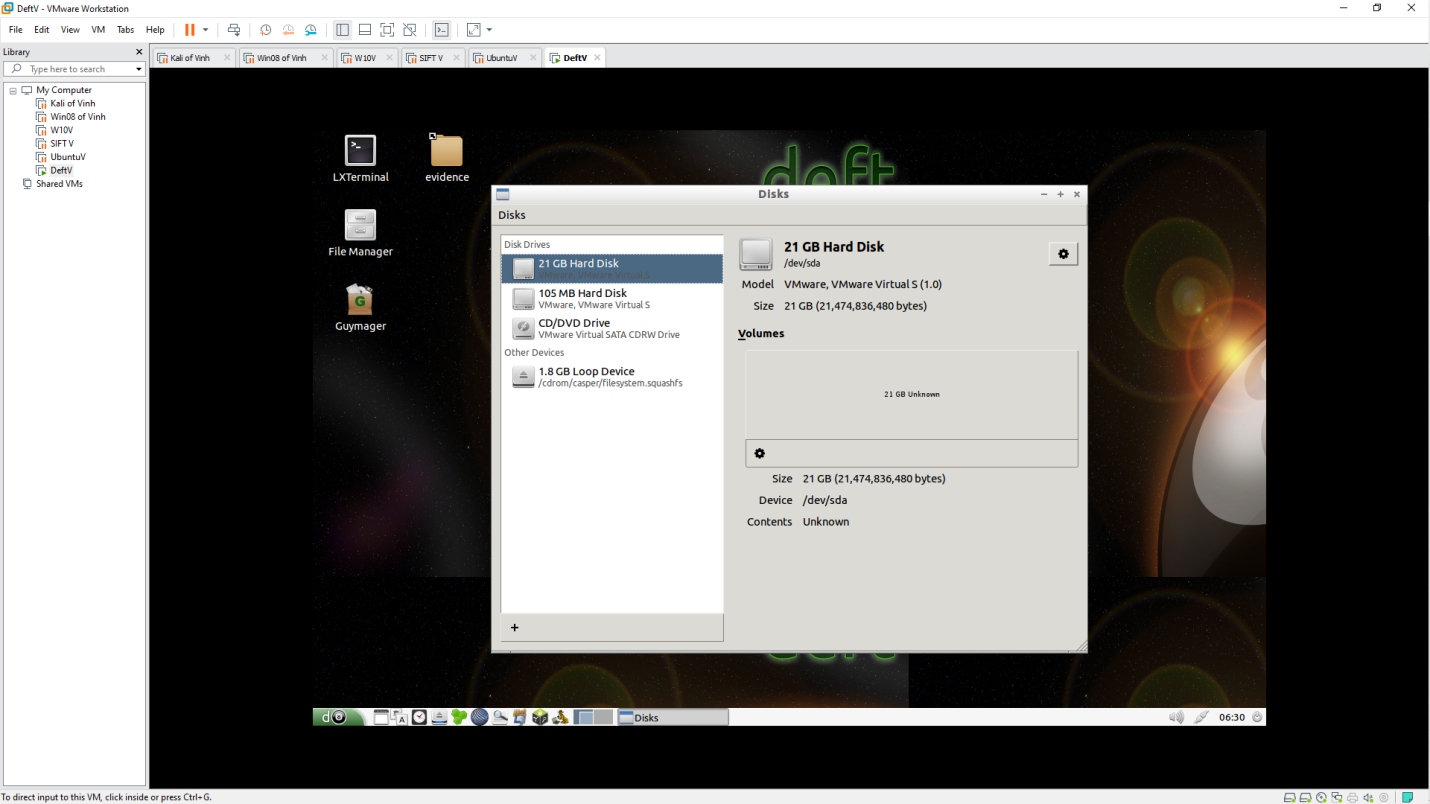
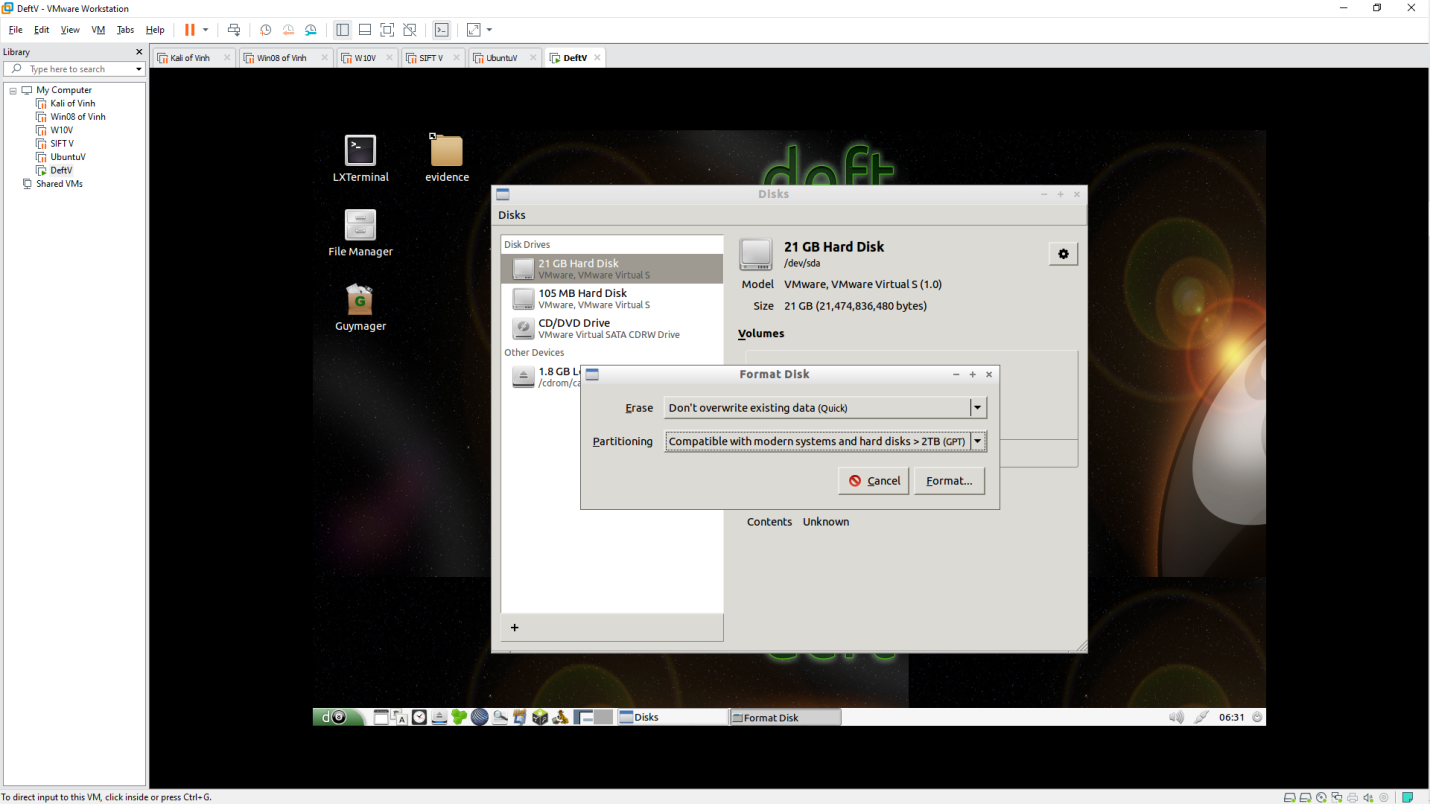
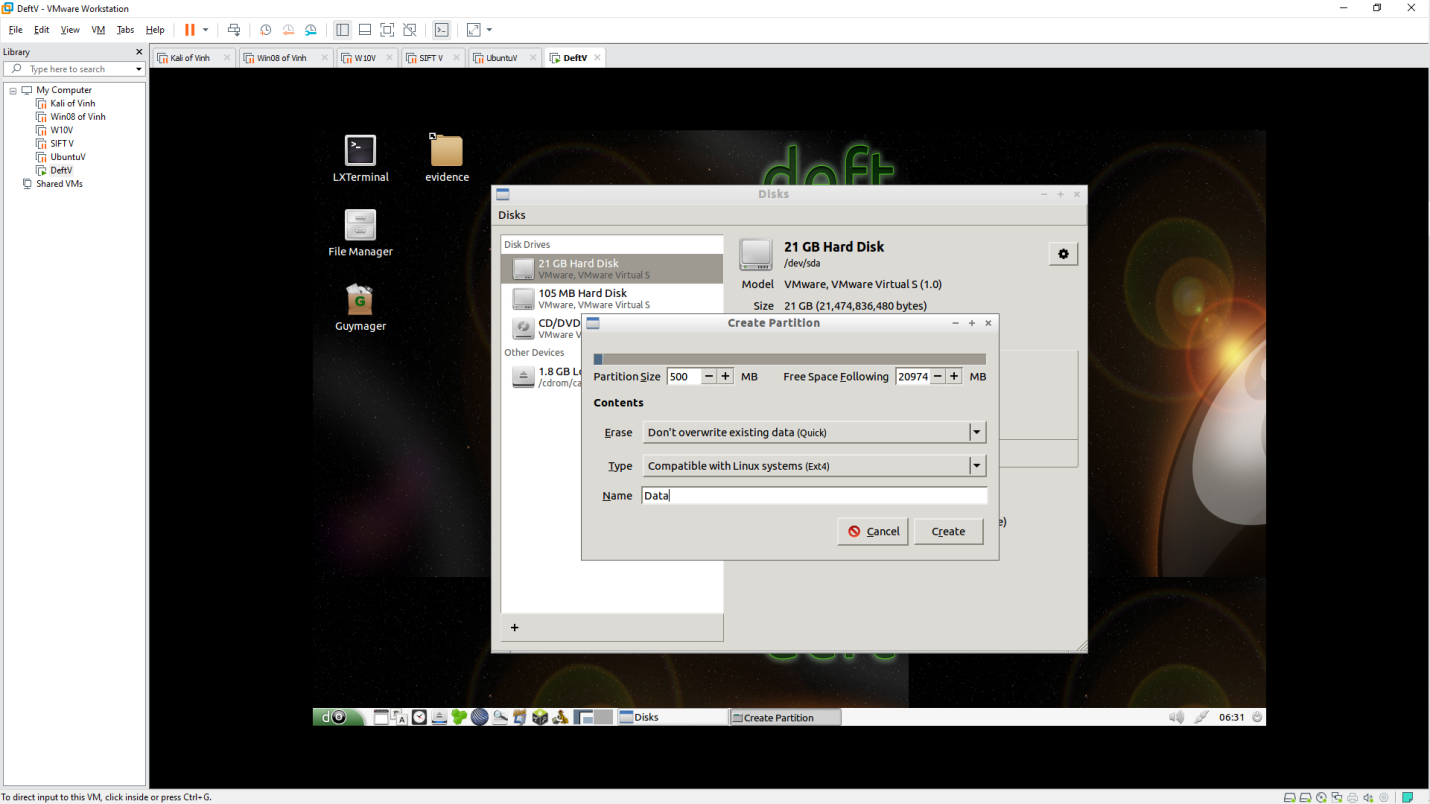
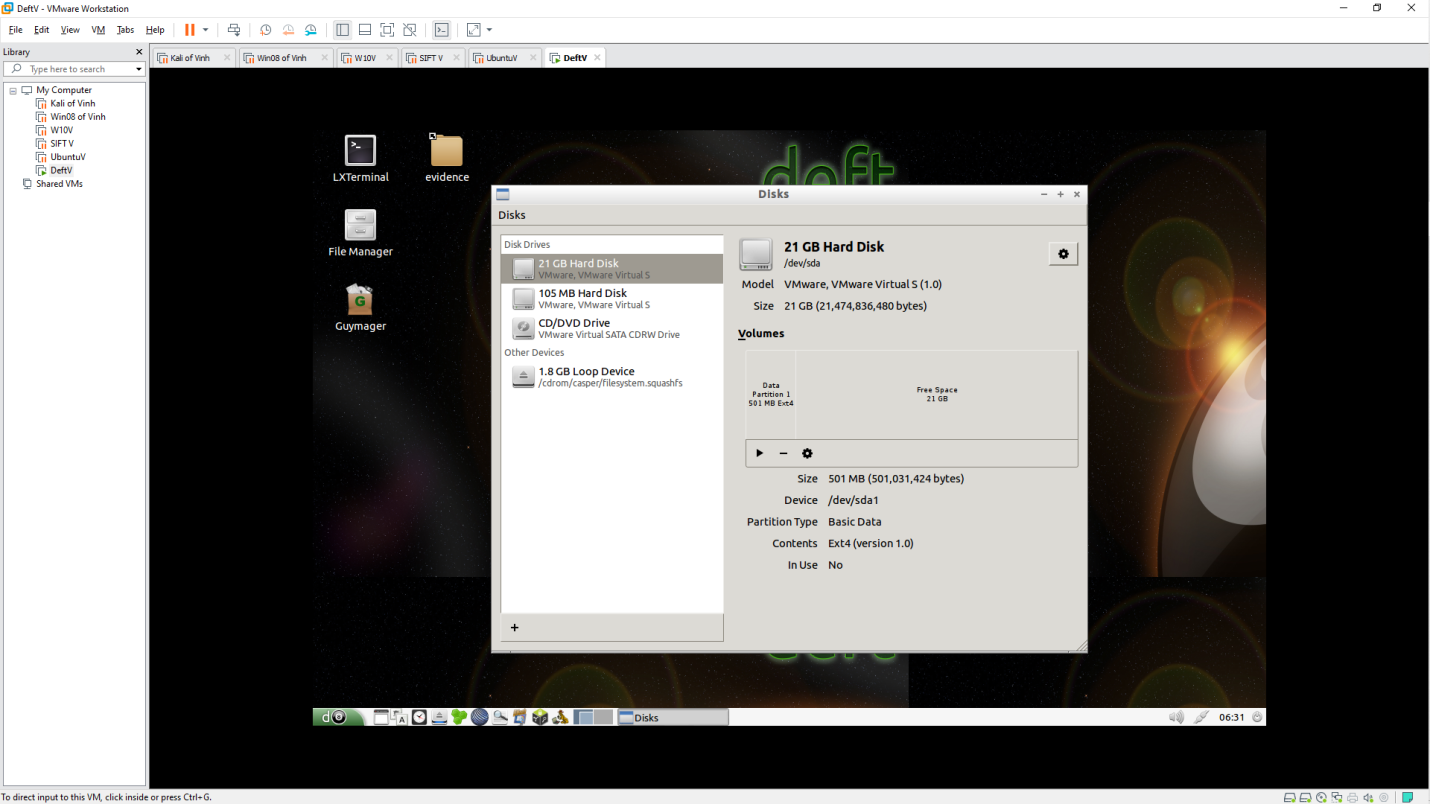
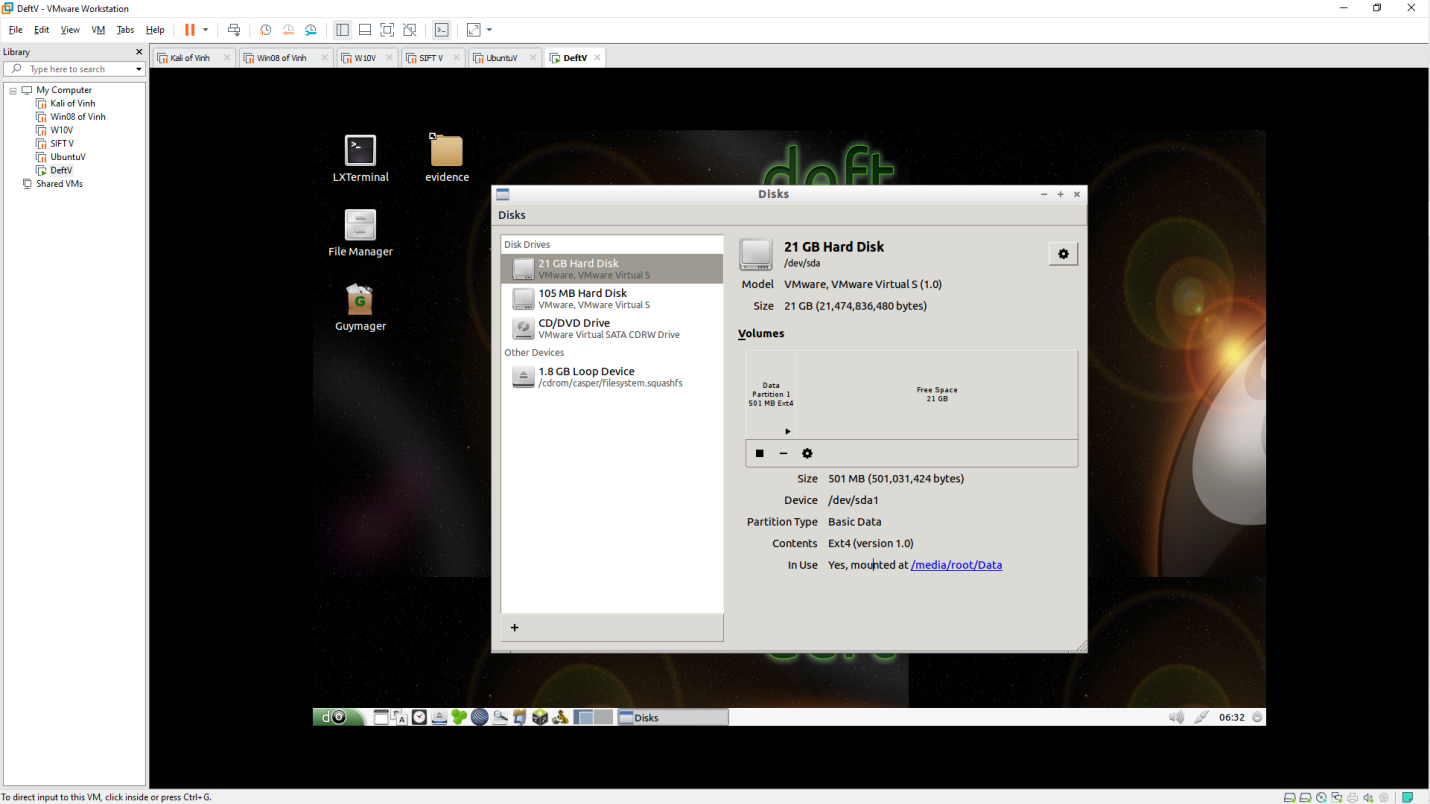
**Preparing the Evidence Drive**

****

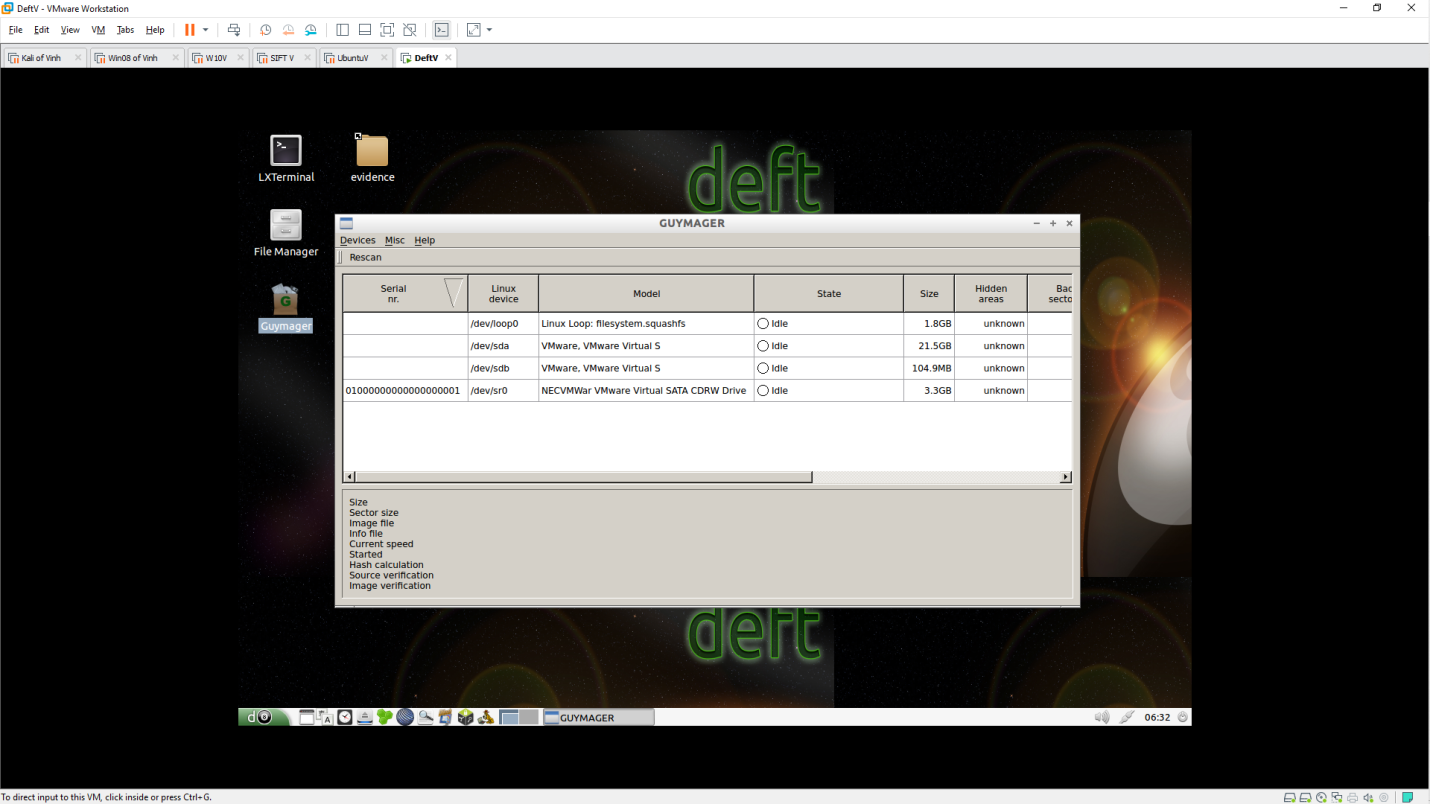
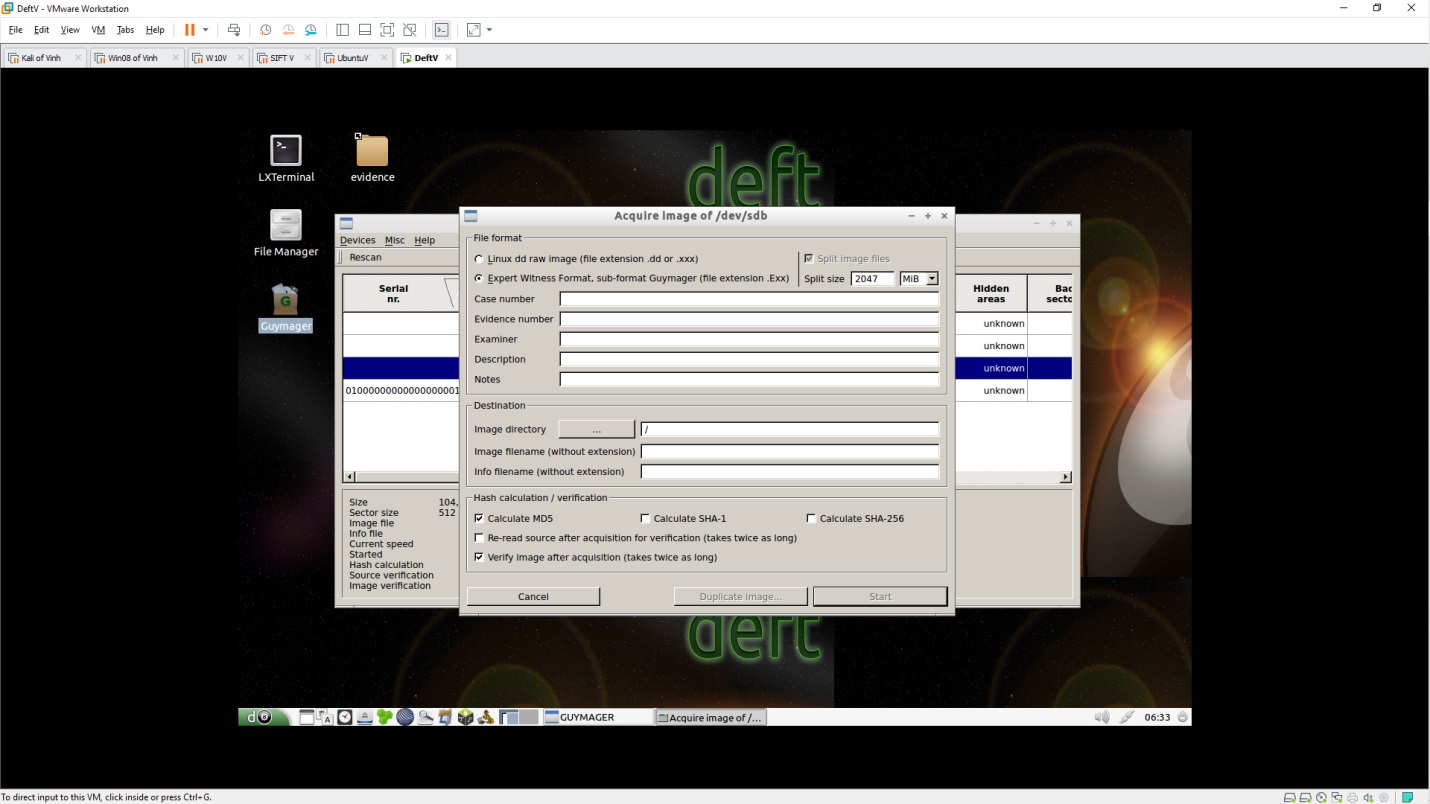
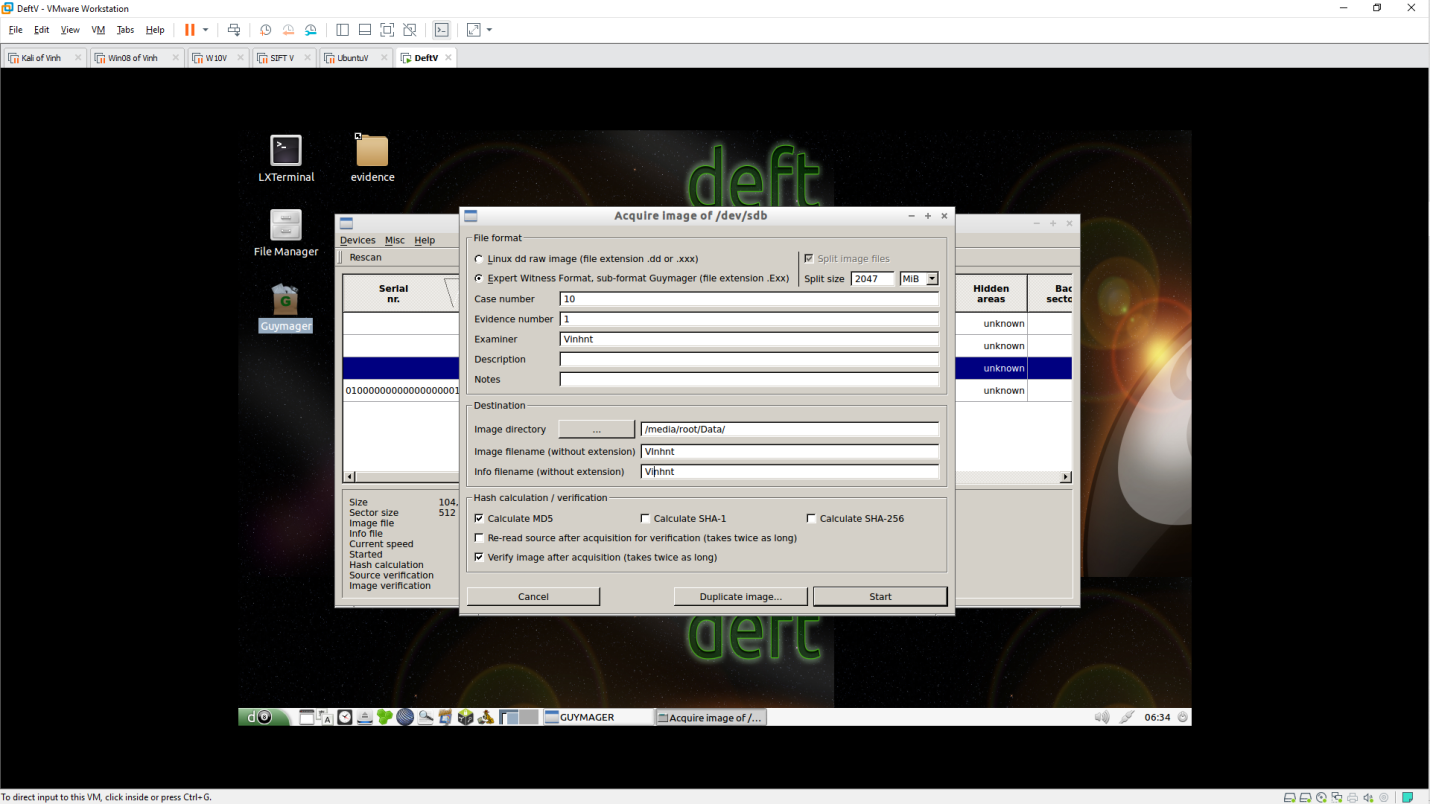
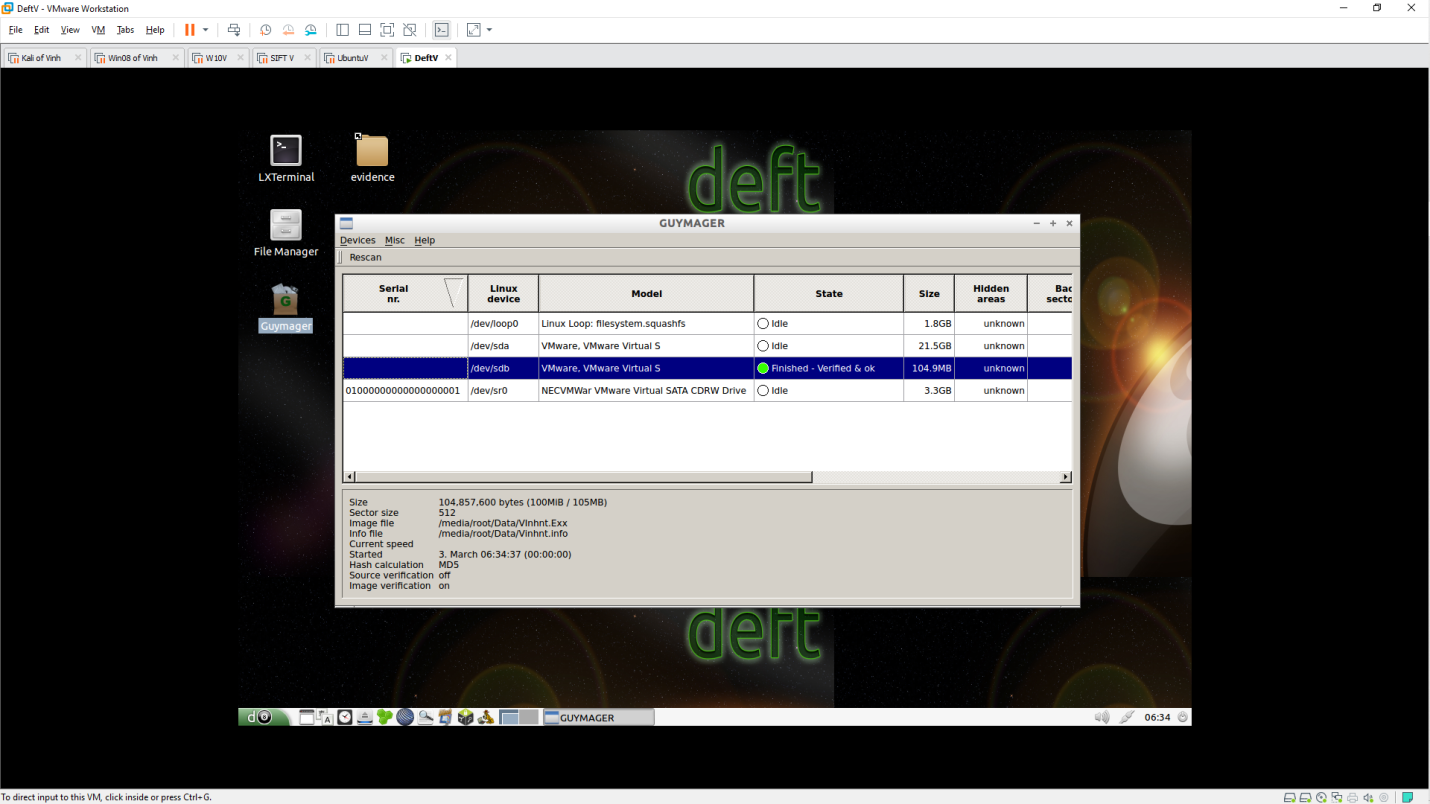
**Connecting the Evidence Drive**

****

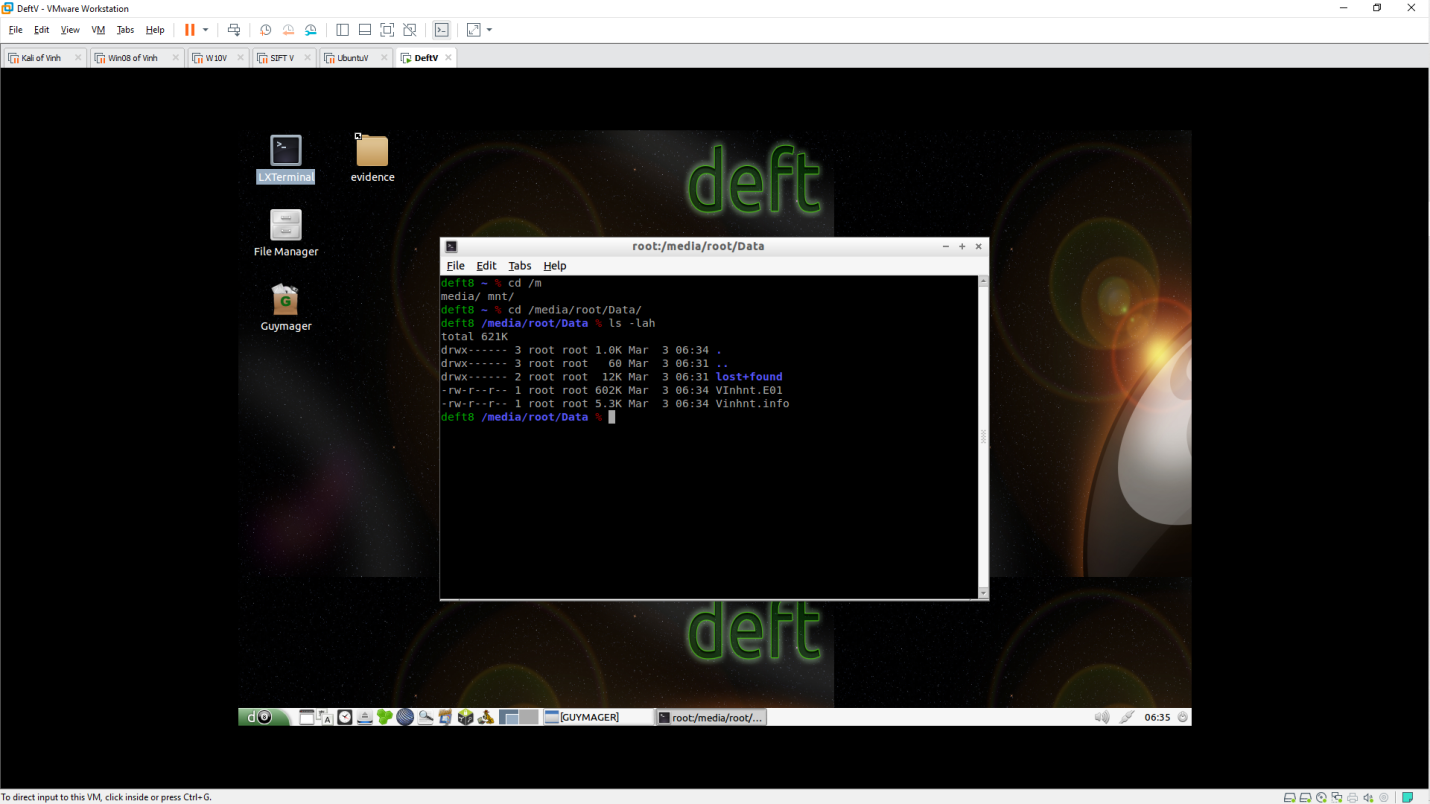
**Preparing a Partition to Acquire Data**

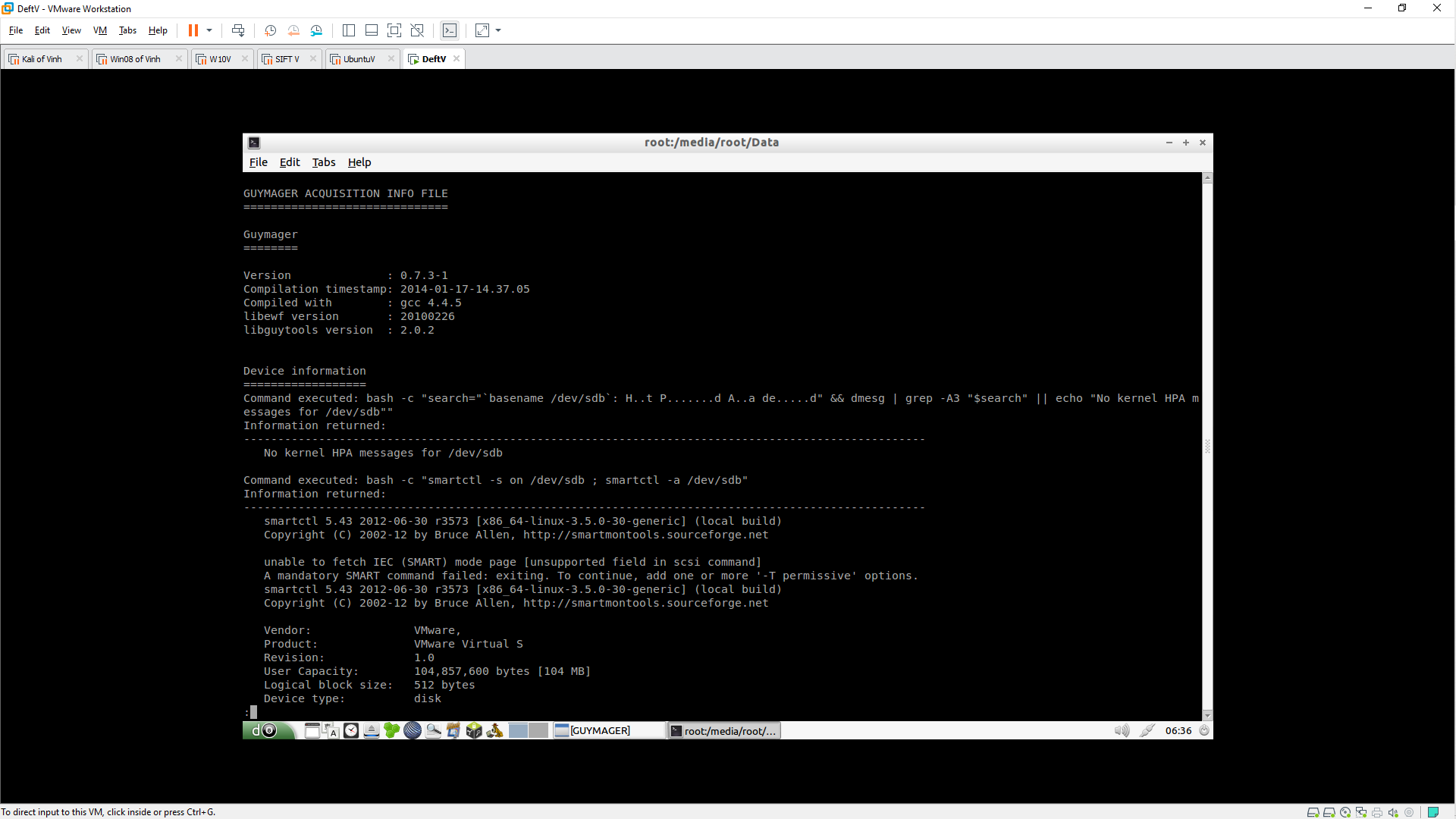
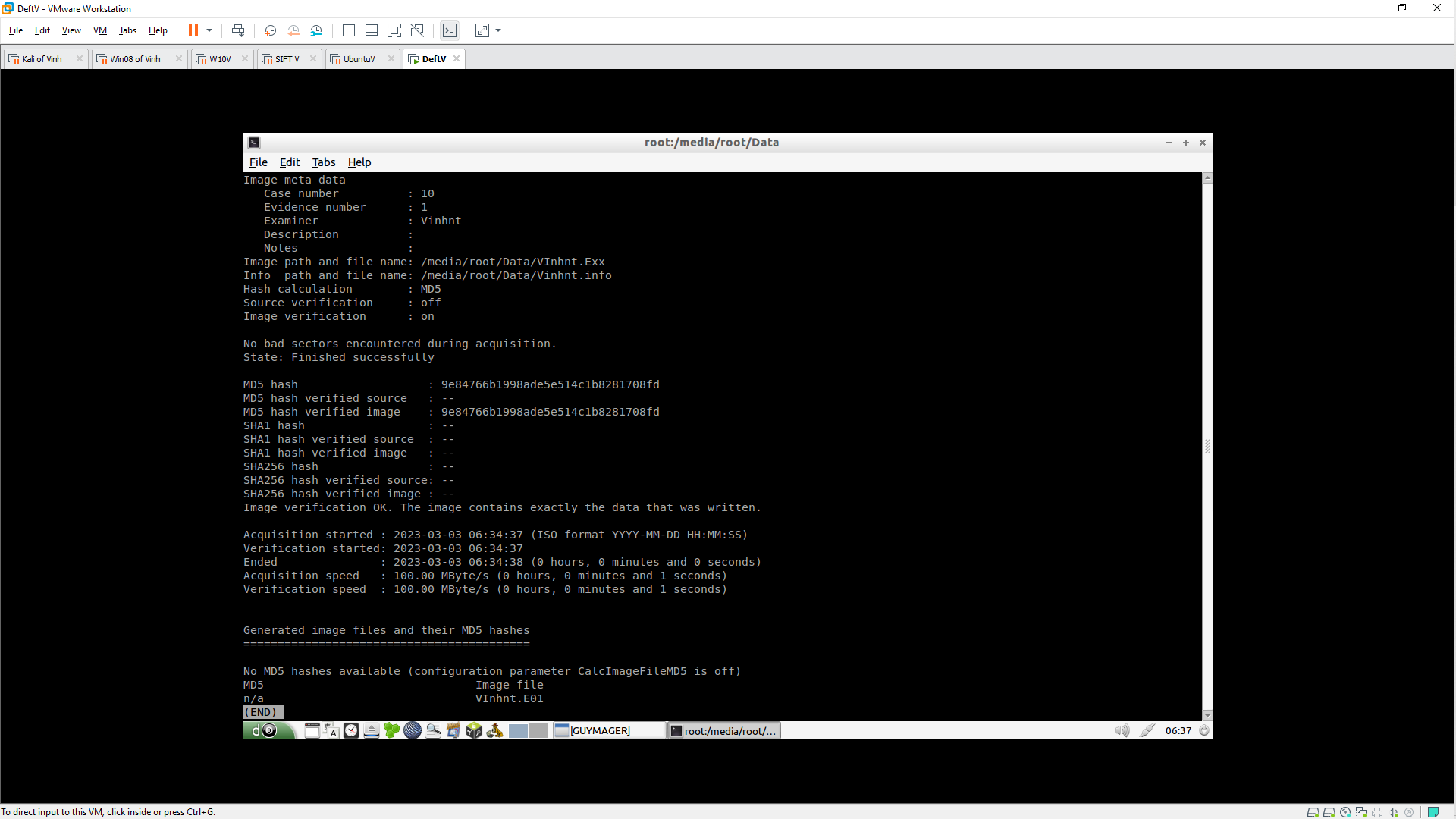
**    **

**Acquiring the Evidence Drive with Guymager**

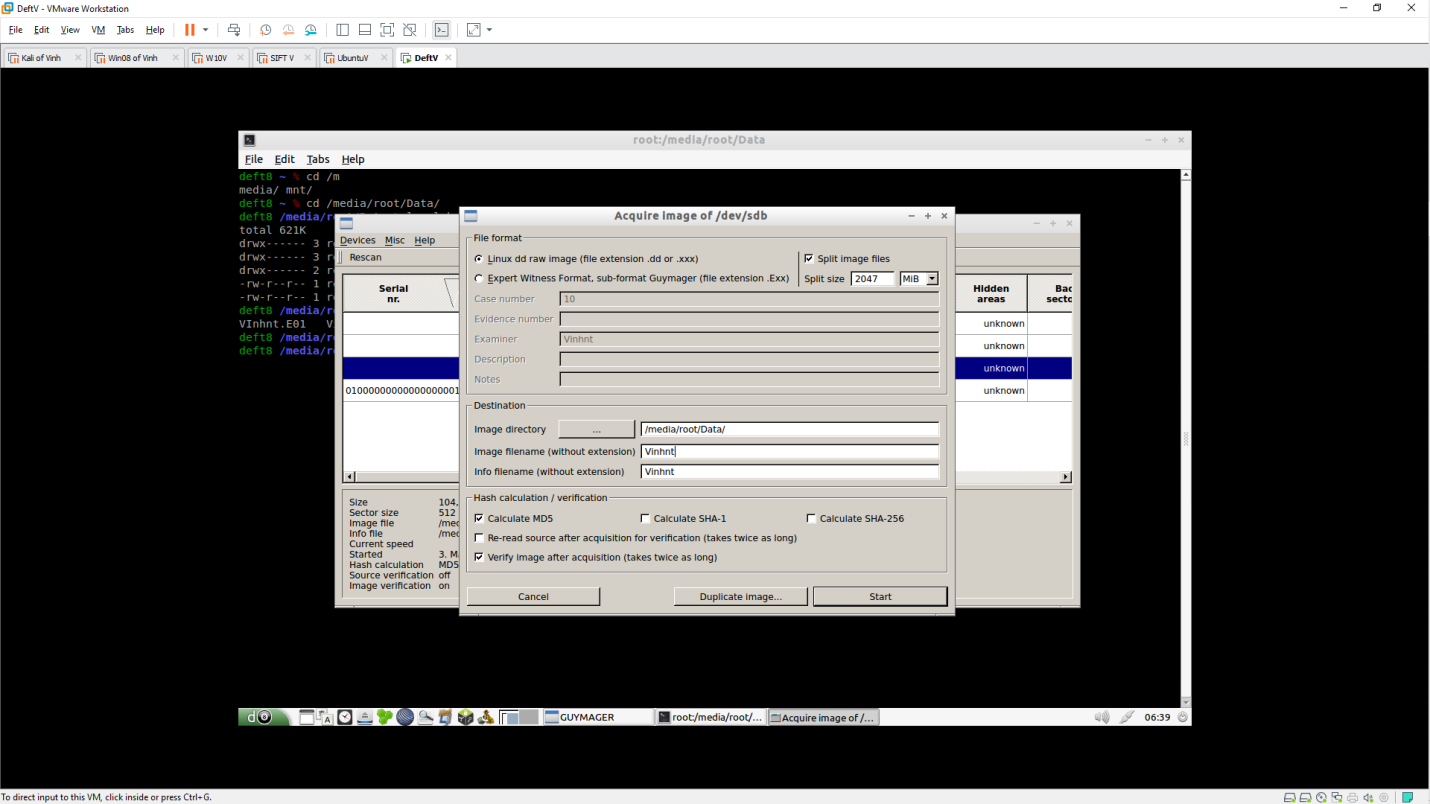
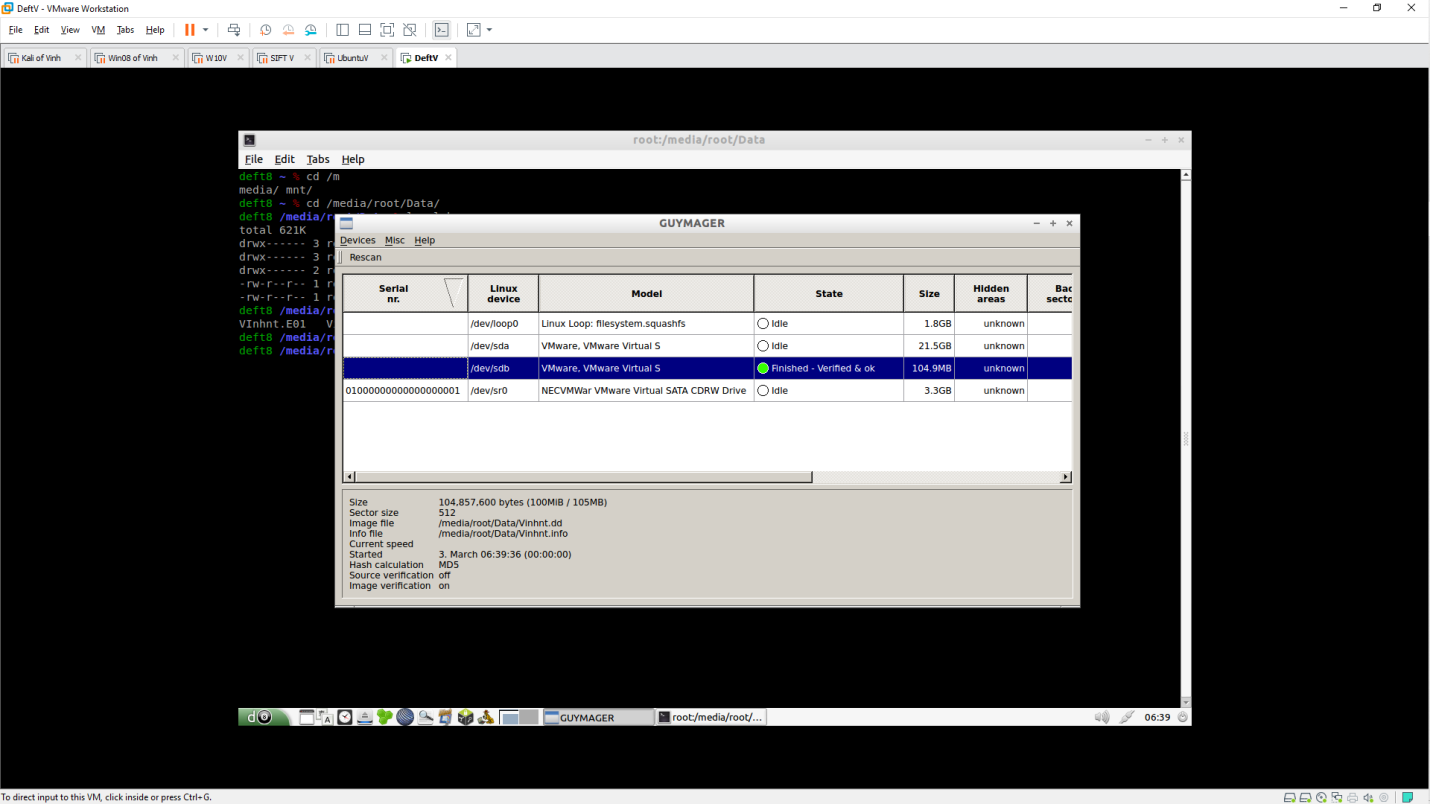
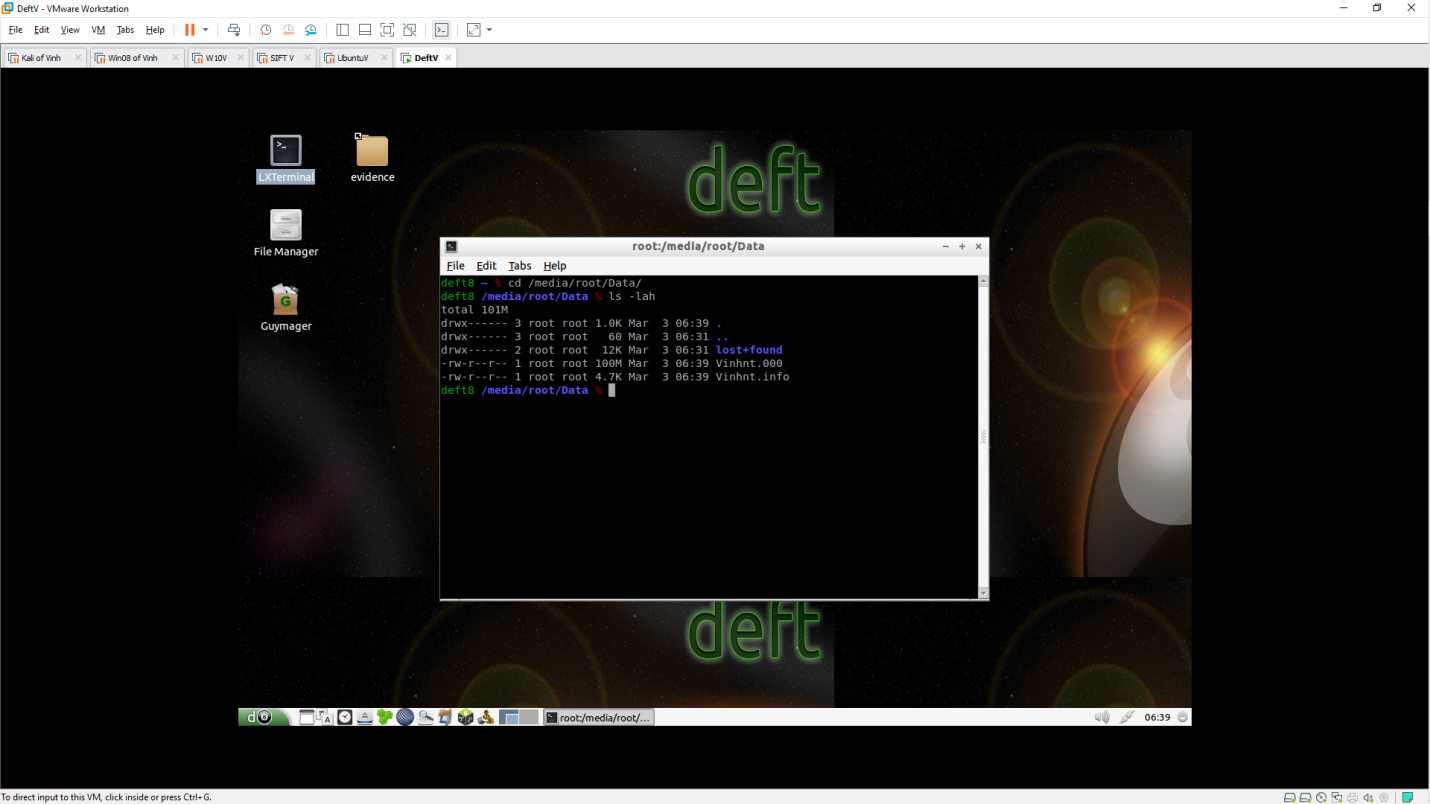
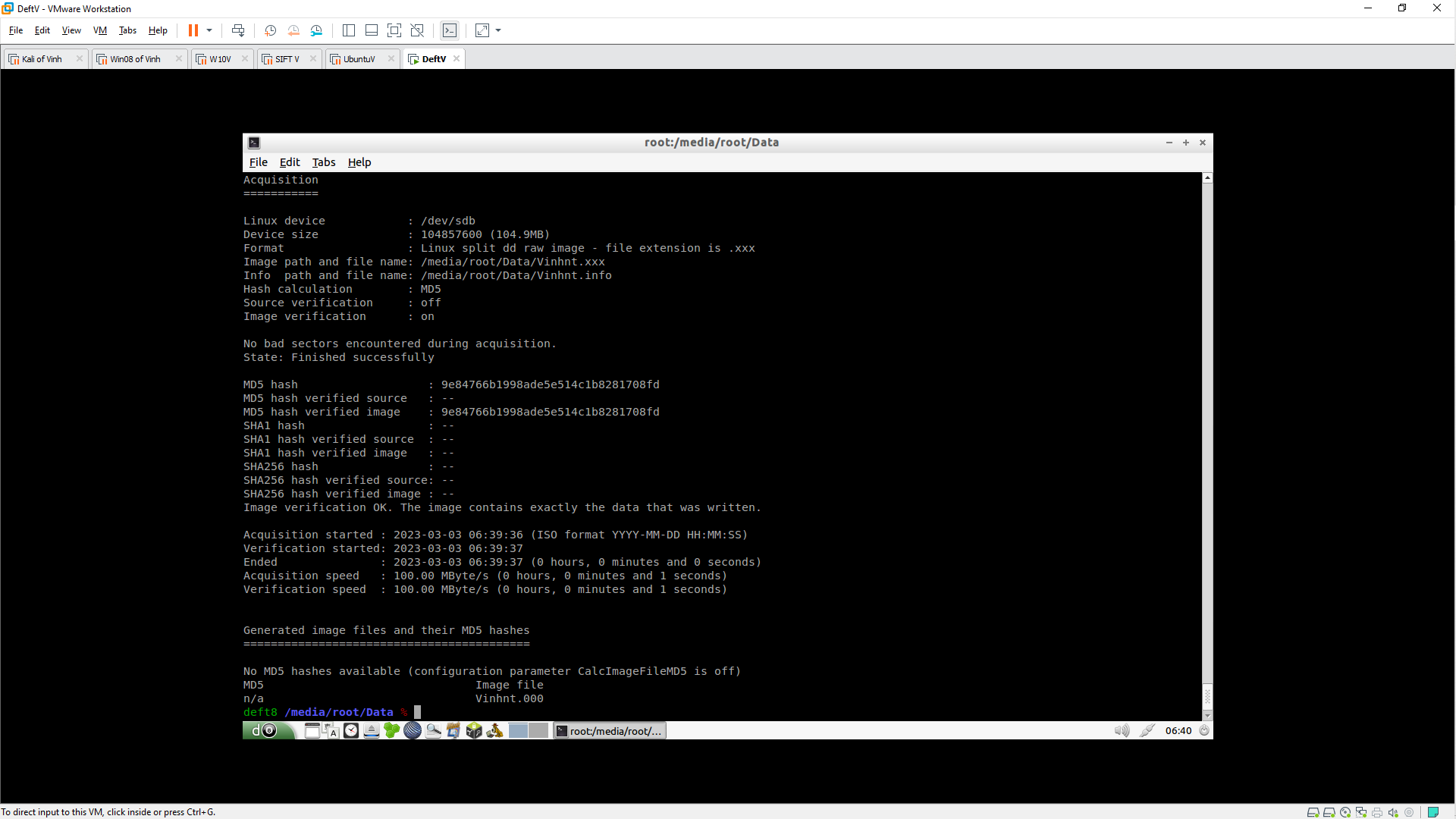
**   **

**Examining the .E01 Acquired Image**

****

** **

**Acquiring a Raw Image**

**    **

1. Why do the .dd and .E01 files have different sizes?

**- Answer:** .dd and .E01 are both forensic image file formats that can be used to store digital evidence. However, they have some differences that may affect their file sizes.

* .dd is a raw image format that stores the exact copy of a disk or partition byte by byte. It does not have any compression or metadata features, so its file size is equal to the size of the original data.
* .E01 is an advanced image format that supports compression and metadata. It can reduce the file size by removing empty space and applying a compression algorithm. It can also store additional information such as notes, hashes, case details, etc.

Depending on the type and amount of data in the original disk or partition, .dd and .E01 files may have different sizes. Generally, .E01 files are smaller than .dd files because of compression, but this may vary depending on how compressible the data is.

2. Which file is the correct evidence image to use in court, or are they both correct?

**- Answer:** Both .dd and .E01 files can be used as evidence images in court, as long as they are verified by hashes and have not been altered or tampered with. However, some courts may have different preferences or requirements for the format of forensic images. Therefore, it is advisable to check with the relevant jurisdiction and legal counsel before submitting any evidence image.