**FTK Imager:**

**Create Disk Image after Deleting a Picture**

**Course Name**: FRS301-Digital Forensics

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

**Instructor Name**: Lê Tiến Dũng

**Lab Due Date**: 7/2/2023

**Section 0. Background Information**

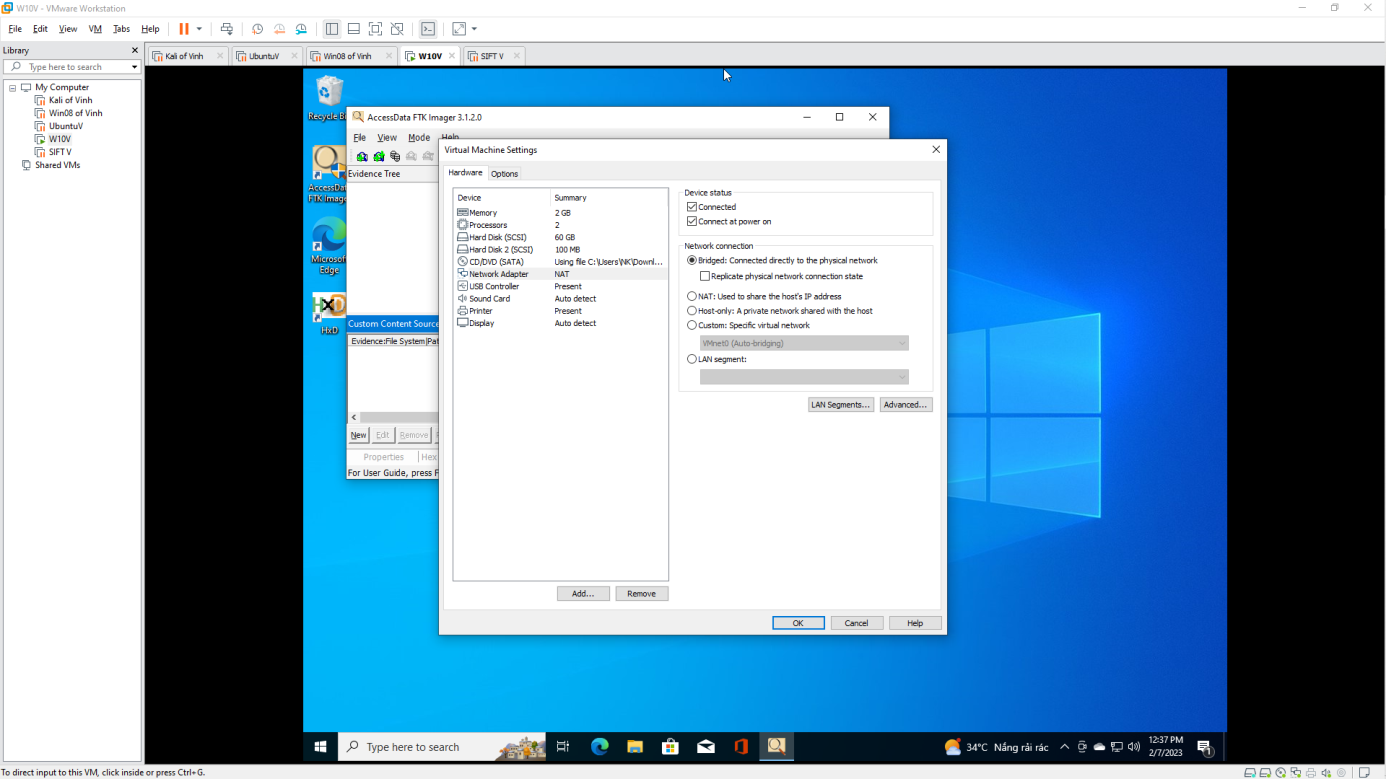
1. **What is FTK Imager?**
   * The FTK toolkit includes a standalone disk imaging program called FTK Imager. The FTK Imager has the ability to save an image of a hard disk in one file or in segments that may be later reconstructed.
   * It calculates MD5 hash values and confirms the integrity of the data before closing the files.
   * In addition to the FTK Imager tool can mount devices (e.g., drives) and recover deleted files.
2. **Pre-Requisite**
   * Install FTK Imager
   * Create Virtual Hard Drive, Delete File, Recover File
     + **Note**: This lab is necessary, because you will need to create a Virtual Hard Drive.
3. **Lab Notes**
   * In this lab we will do the following:
     + Download a Picture to the Virtual Hard Drive
     + Delete a Picture from the Virtual Hard Drive
     + Delete the Picture from the Recycle Bin
     + Create an image of the Virtual Hard Drive with FTK Imager

**Section 1: Log into WXP-SP2**

1. Start VMware Player
   * **Instructions**
     1. For Windows 7
        1. Click Start Button
        2. Search for "vmware player"
        3. Click VMware Player
     2. For Windows XP
        1. Starts --> Programs --> VMware Player

1. Start Up WXP-SP2.
   * **Instructions:**
     1. Click on WXP-SP2
     2. Click on Edit virtual machine Settings
   * **Note(FYI)**:
     1. For those of you not part of my class, this is a Windows XP machine running SP2.

1. Edit Virtual Machine Settings
   * **Instructions:**
     1. Click on Network Adapter
     2. Click on the Bridged Radio button
     3. Click on the OK Button

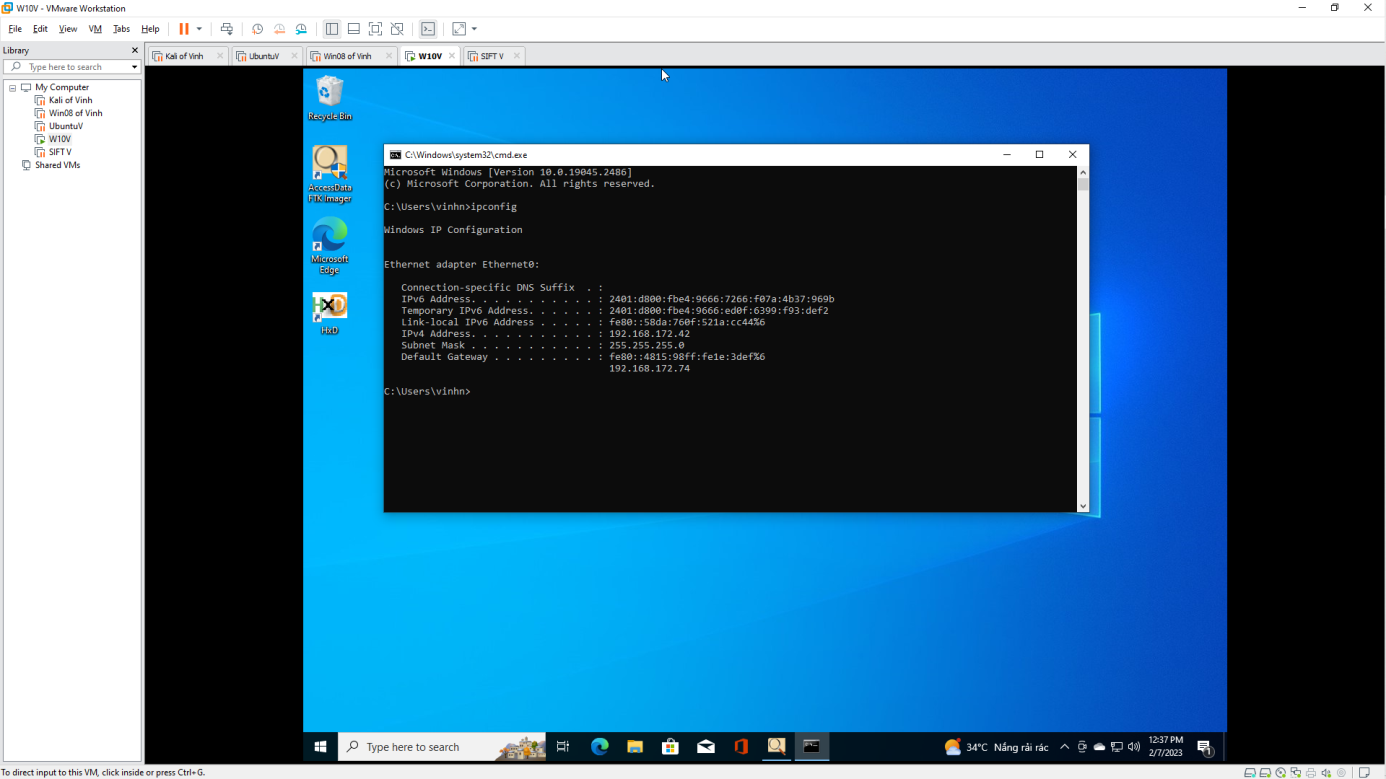


1. Play Virtual Machine
   * **Instructions:**
     1. Click on WXP-SP2
     2. Click on Play virtual machine

1. Logging into WXP-SP2.
   * **Instructions:**
     1. Click on **Administrator**
     2. Password: Supply Password
     3. Press <Enter> or Click the Arrow

1. Open a Command Prompt
   * **Instructions:**
     1. Start --> All Programs --> Accessories --> Command Prompt

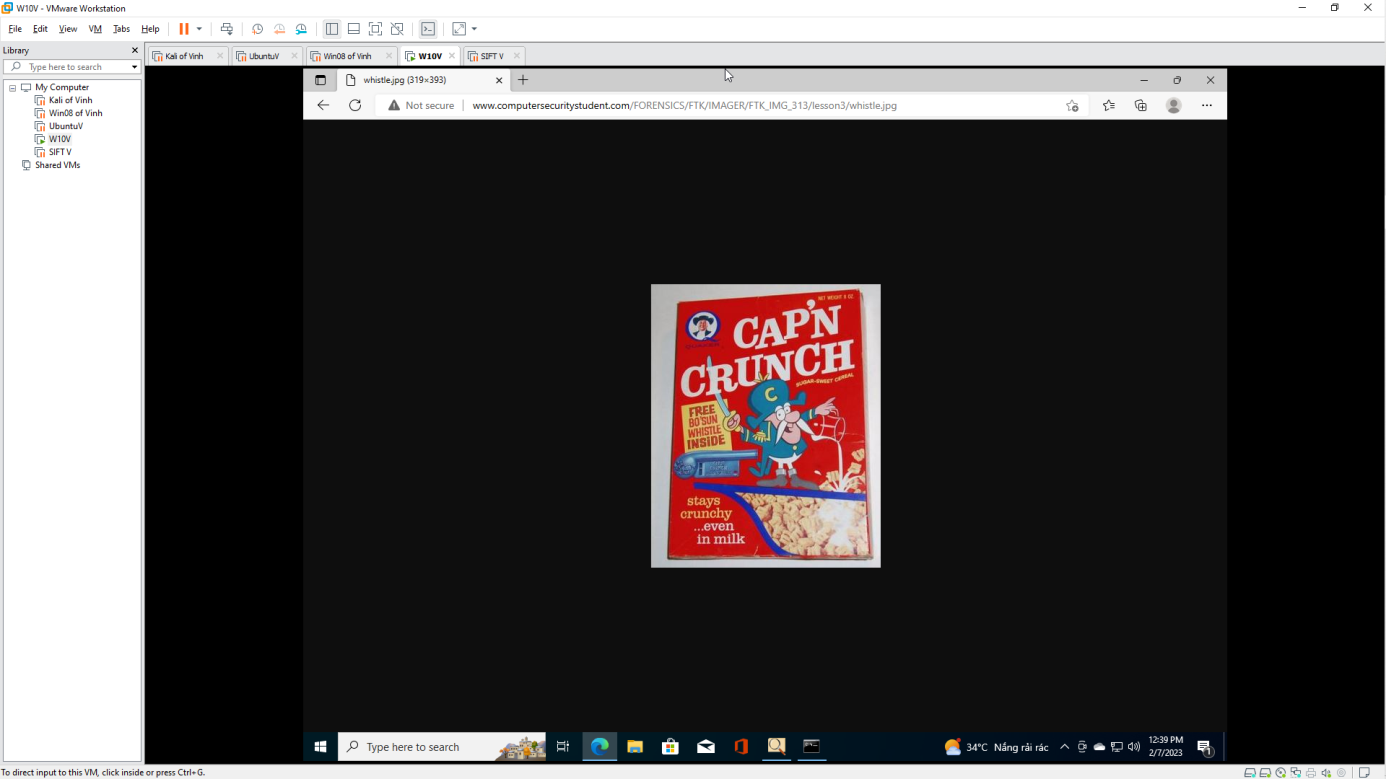
1. Obtain WXP-SP2's IP Address
   * **Instructions:**
     1. ipconfig
   * **Note(FYI)**:
     1. In my case, WXP-SP2's IP Address 192.168.1.116.
     2. This is the IP Address of the Victim Machine that will be attacked by Metasploit.
     3. Record your WXP-SP2's IP Address.

.

**Section 2: Download Test Picture**

1. Start Firefox
   * **Instructions**:
     1. Click the Start Button
     2. All Programs --> Mozilla Firefox

1. Start Test Picture Download
   * **Instructions**:
     1. Place the following URL in the Firefox Address Textbox
        + http://www.computersecuritystudent.com/FORENSICS/FTK/IMAGER/FTK\_IMG\_313/lesson3/whistle.jpg
     2. Right Click on the image
     3. Click on "Save Image As..."

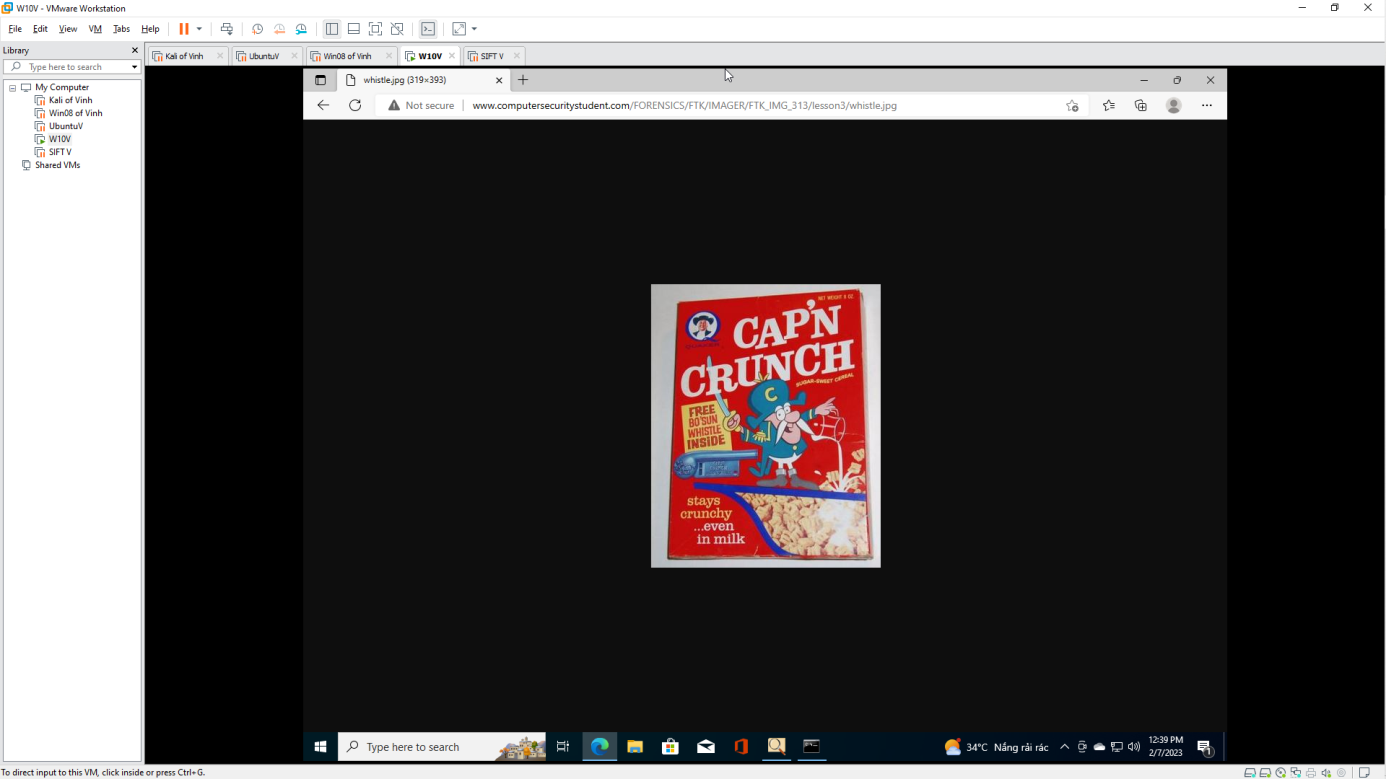


1. Save Test Picture Download
   * **Instructions**:
     1. Save in: Select the FTK (Z:) Drive
     2. Filename: whistle
     3. Save as type: JPEG Image
     4. Click the Save Button

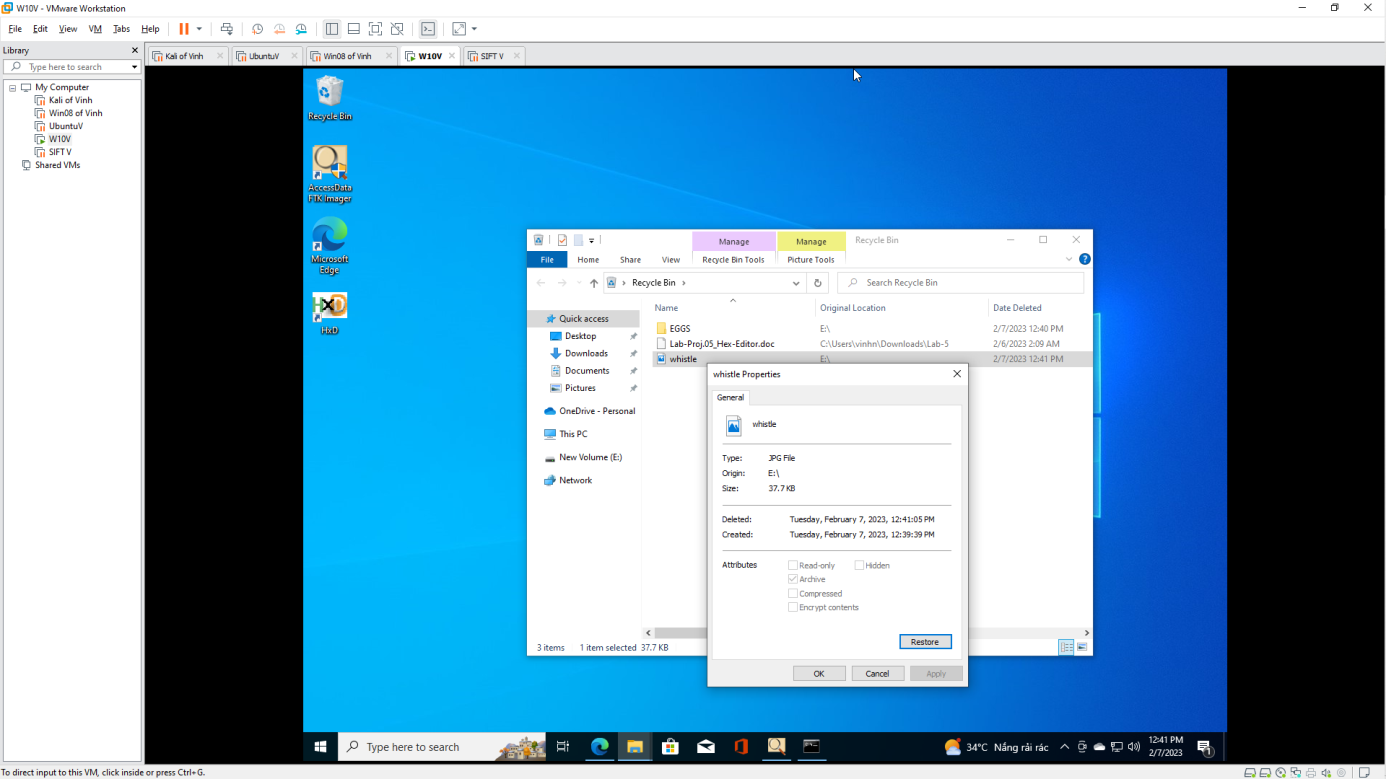
1. Open My Computer
   * **Instructions**:
     1. Click the Start Button
     2. All Programs --> My Computer

1. Open your FTK(Z:) Drive
   * **Instructions**:
     1. Navigate to your FTK(Z:) Drive

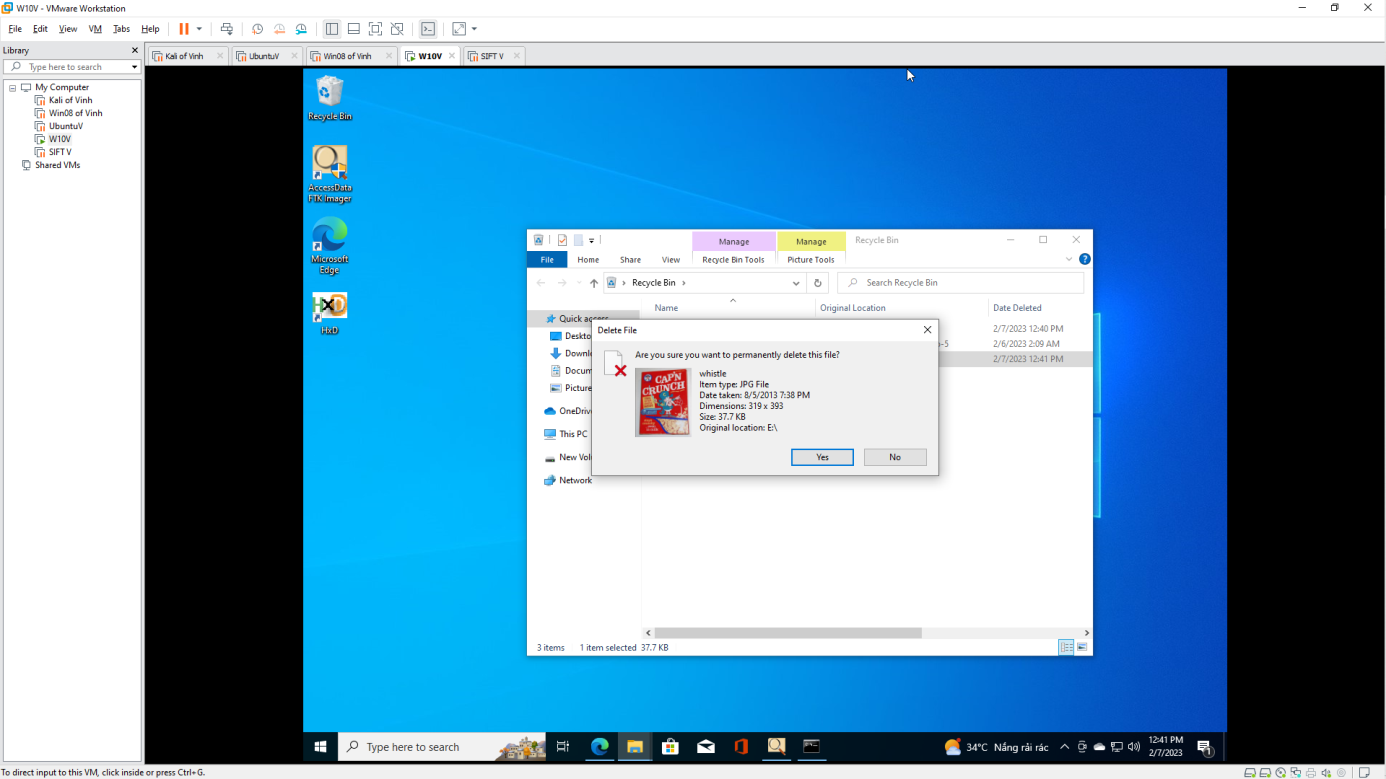
1. Delete the Test Image
   * **Instructions**:
     1. Right Click on whistle.jpg
     2. Click Delete
     3. Click the OK Button in the "Confirm Deletion" warning window.



1. Open the Recycle Bin
   * **Instructions**:
     1. Double Click on the Recycle Bin



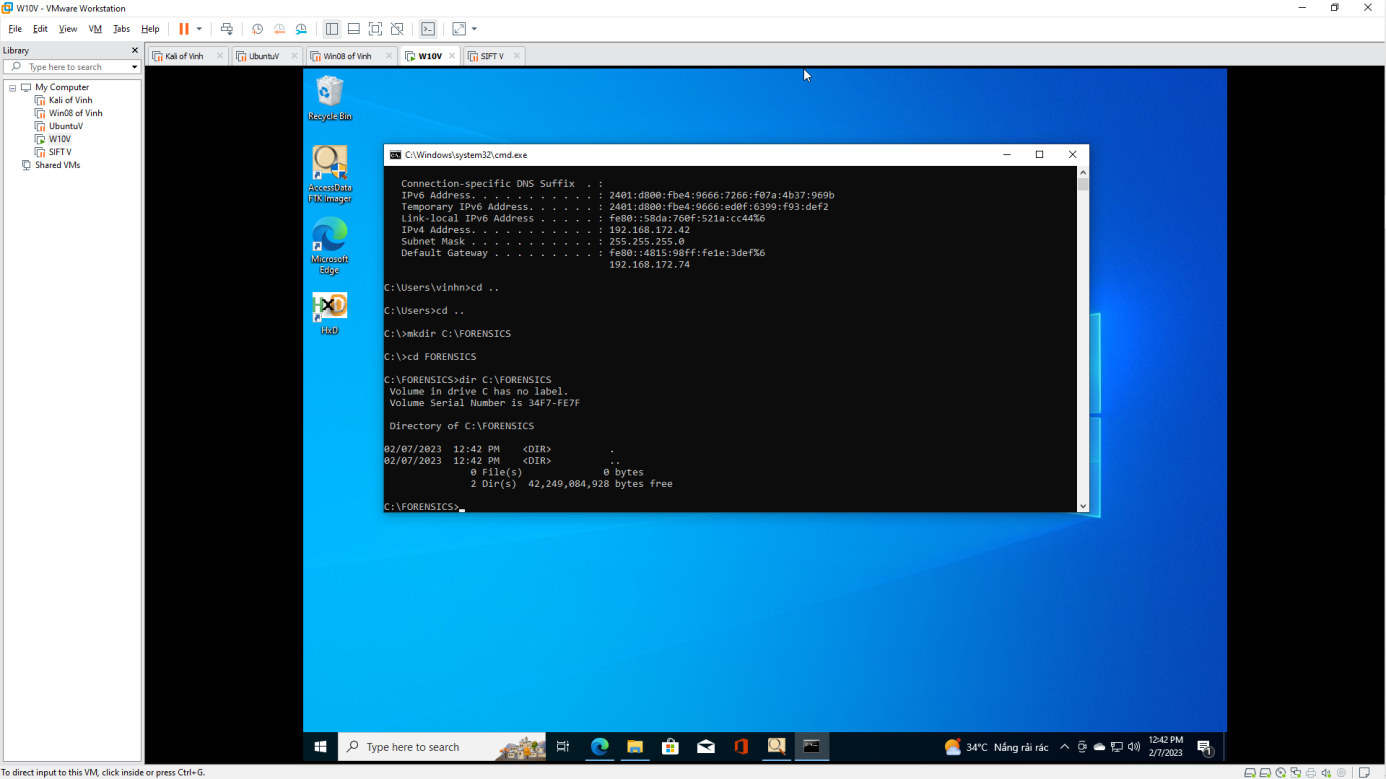
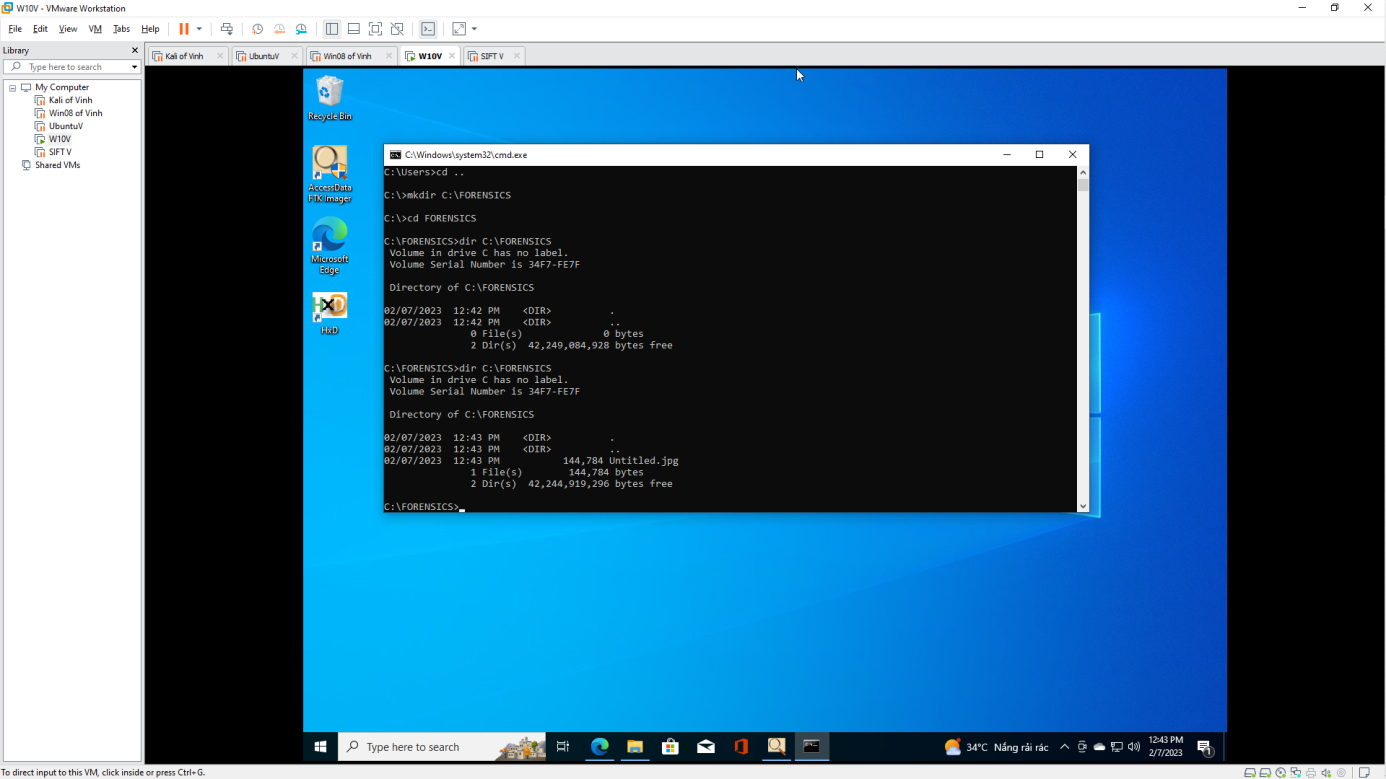
1. Delete Test Picture From the Recycle Bin
   * **Instructions**:
     1. Right Click on whistle.jpg
     2. Click Delete
     3. Confirm File Delete Windows: Click the Yes Button.



**Section 3: Forensics Directory**

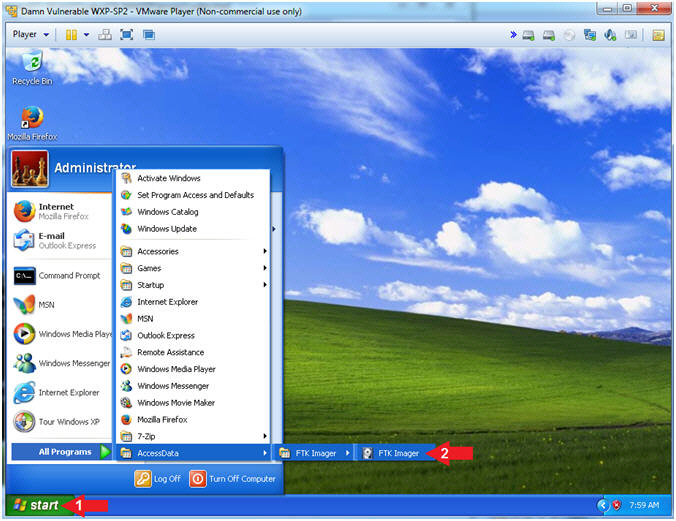
1. Open a Command Prompt
   * **Instructions**:
     1. Start --> All Programs --> Accessories --> Command Prompt

1. Create a Forensics Directory
   * **Instructions**:
     1. mkdir C:\FORENSICS
     2. dir C:\FORENSICS
   * **Note(FYI)**:
     1. If you completed the previously lab you will receive an error that states "A subdirectory or file C:\FORENSICS already exists."
     2. In Addition, the directory listing might list remnant files (eg., horse.jpg) from the previous lab.

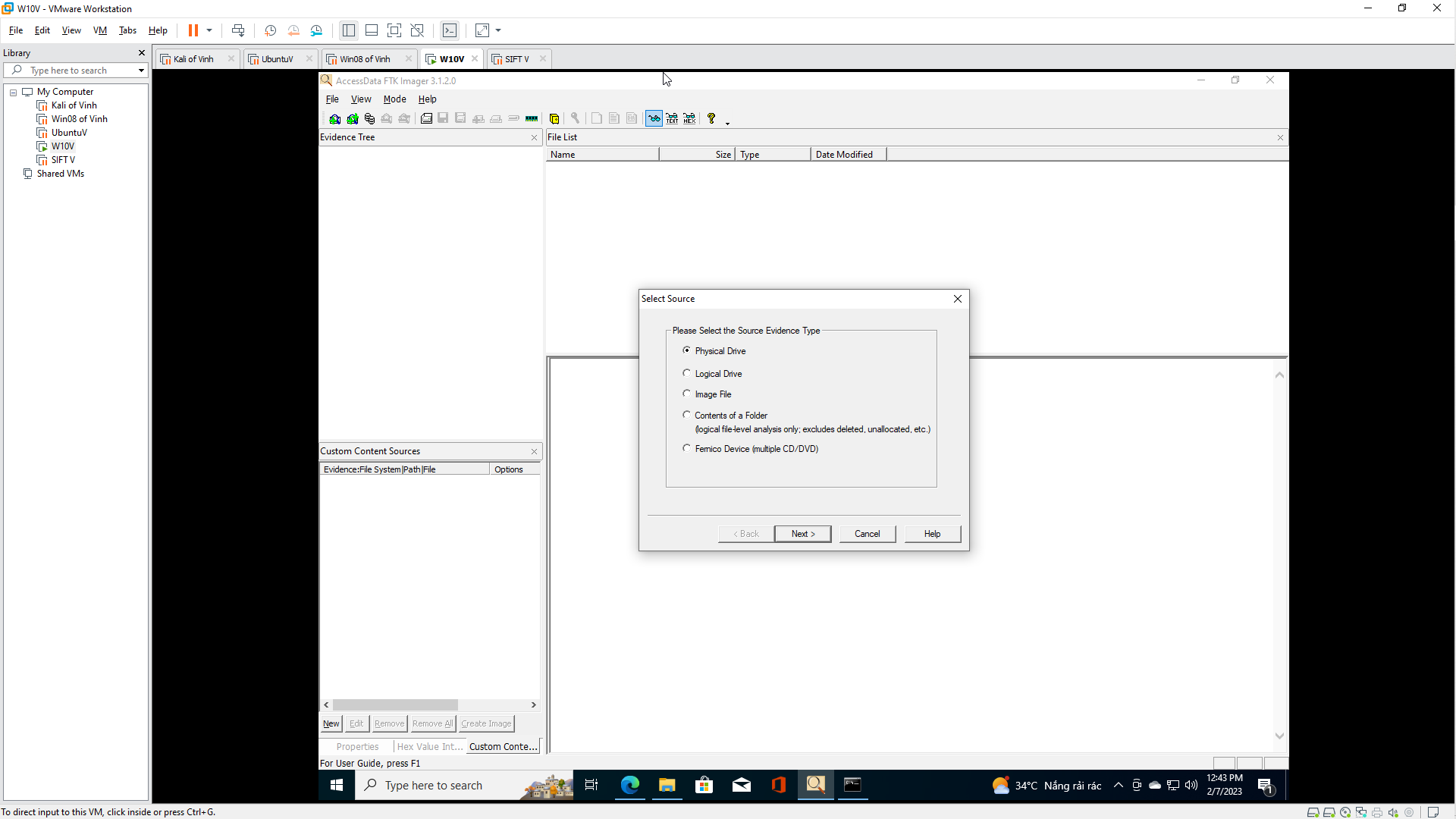
**Section 4: Start FTK Imager**

1. Start FTK Imager
   * **Instructions**:
     1. Click on the Start Button
     2. All Programs --> AccessData --> FTK Imager --> FTK Imager

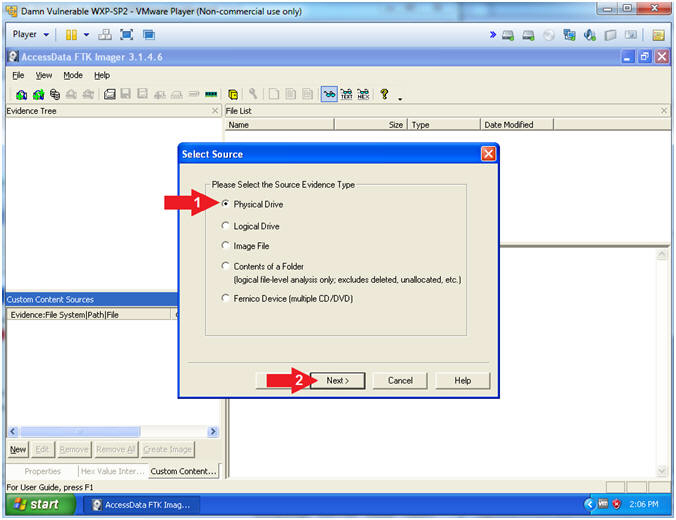


**Section 5: FTK Imager: Create Disk Image…**

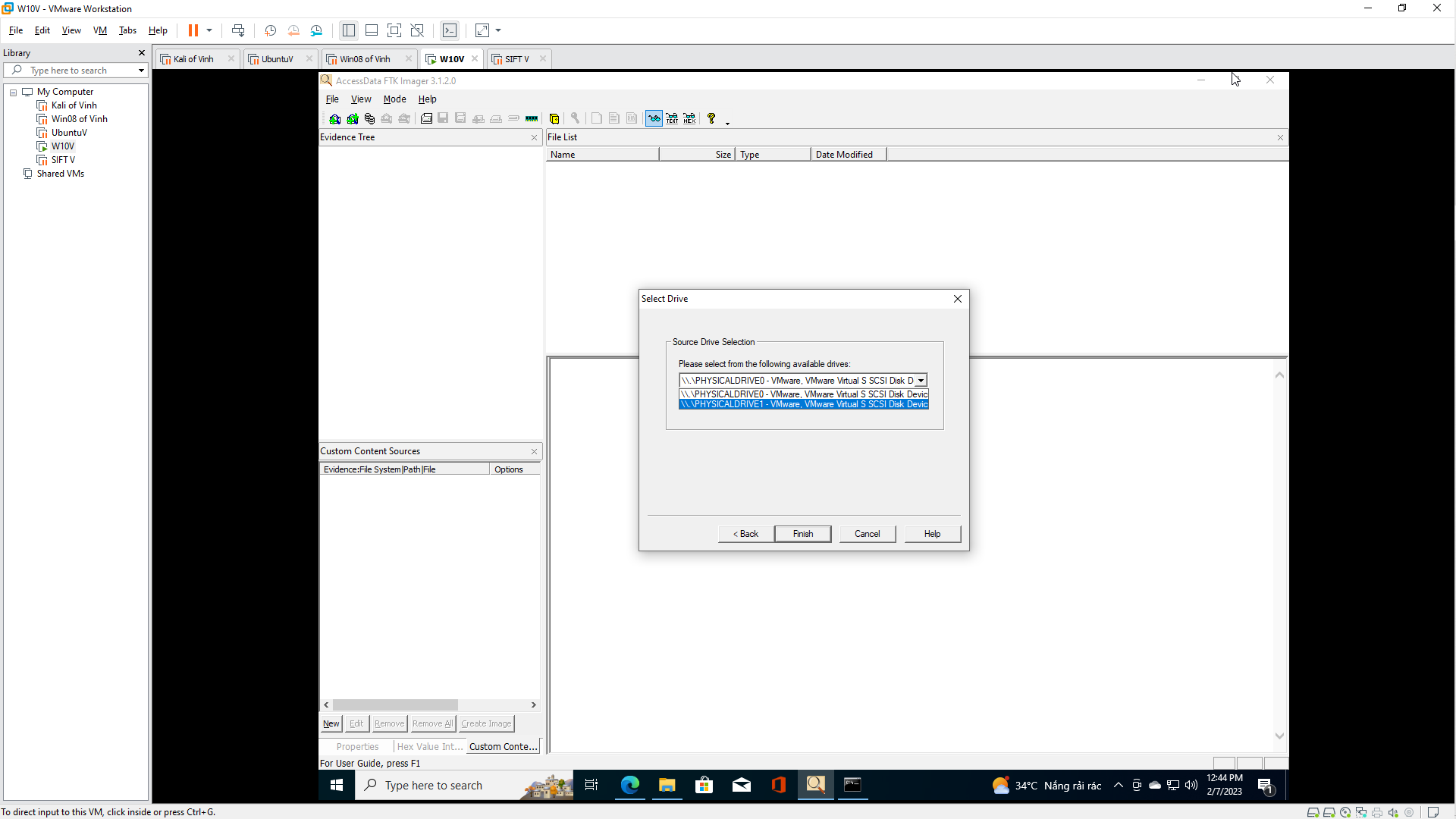
1. Add Evidence
   * **Instructions**:
     1. File --> Create Desk Image...



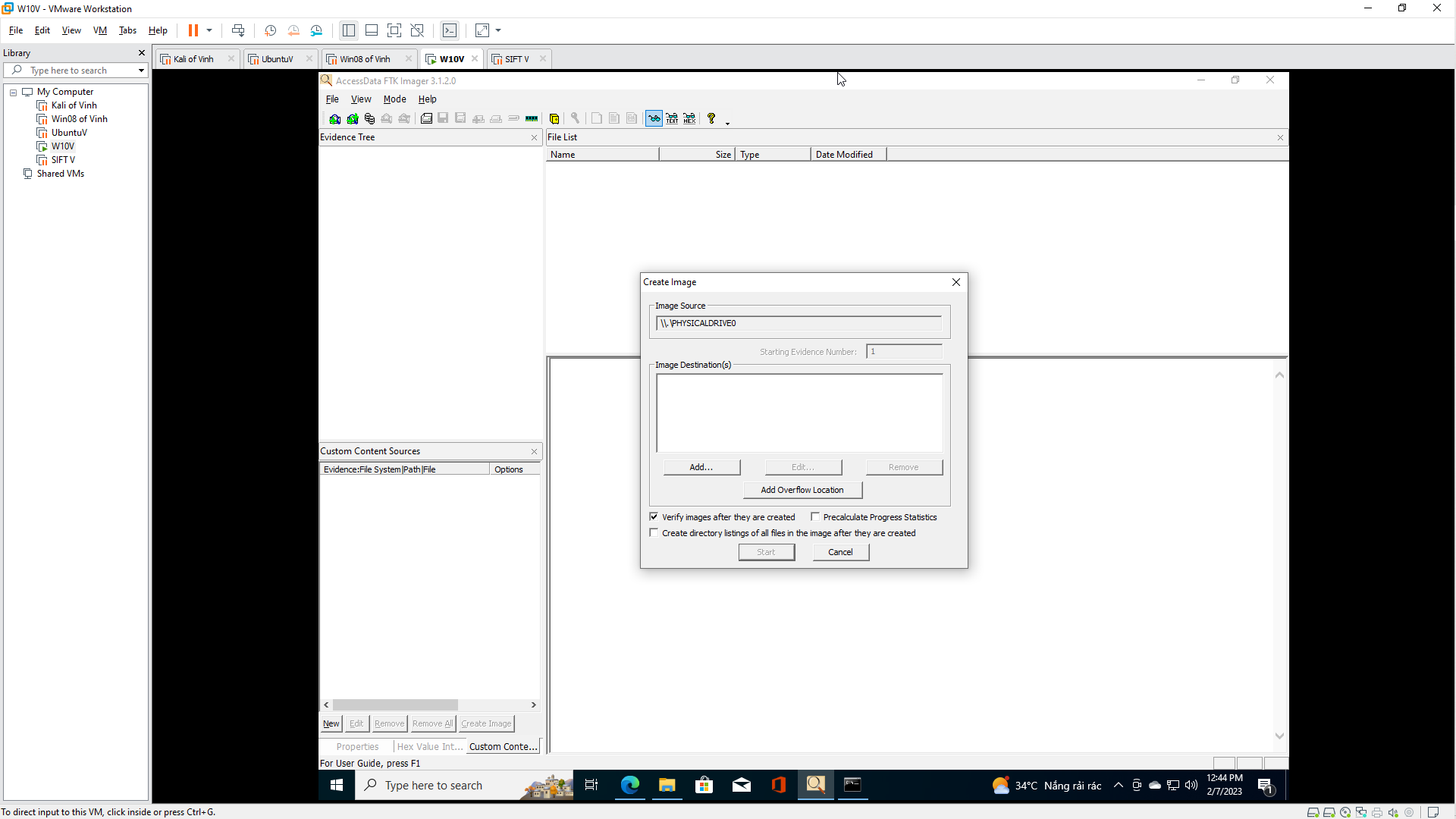
1. Select Source
   * **Instructions**:
     1. Select the "Physical Drive" Radio Button
     2. Click the Next Button



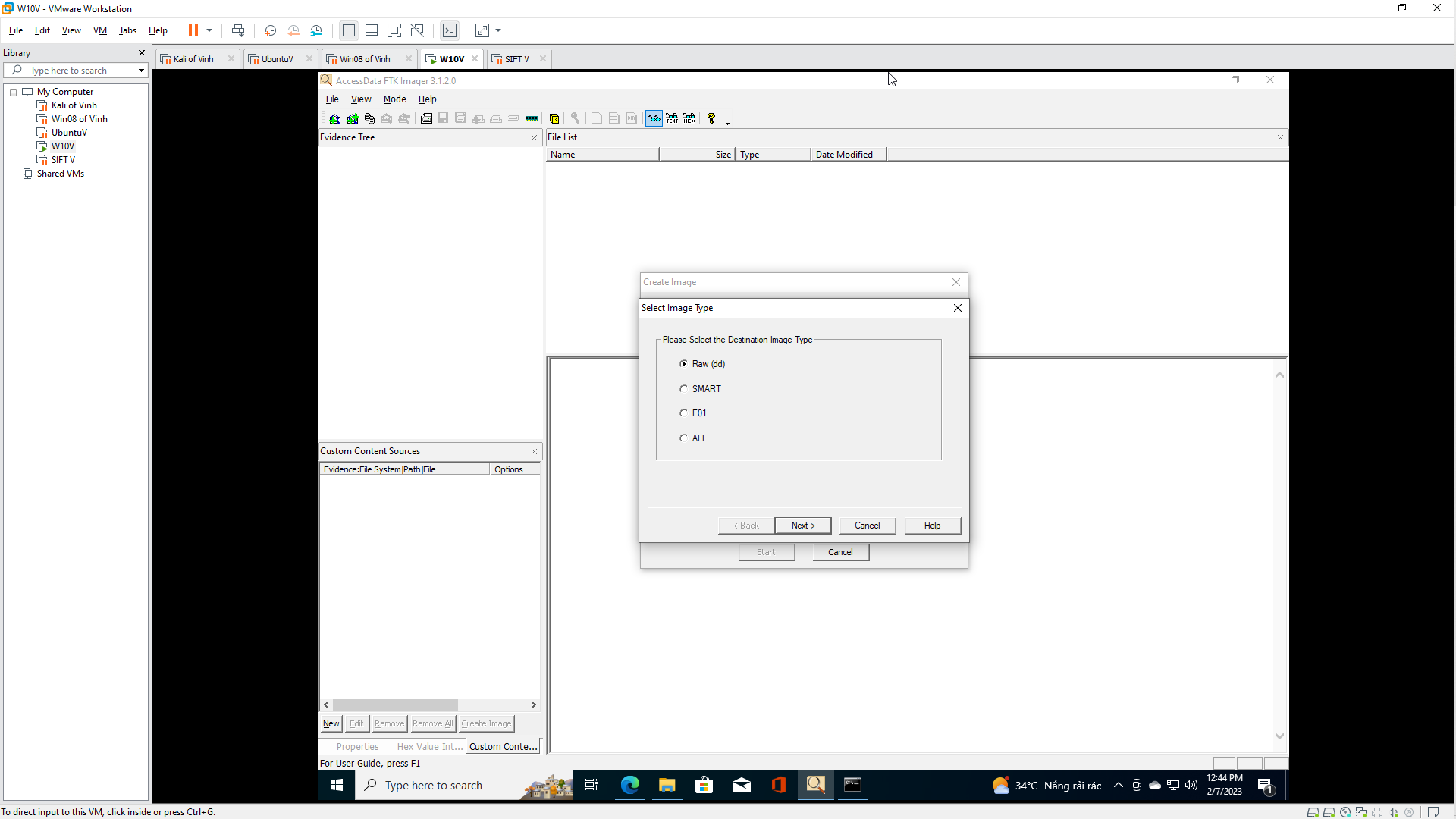
1. Select Drive
   * **Instructions**:
     1. Select \\PHYSICAL DRIVE1 ... (106MB SCSI)
     2. Click the Finish Button



1. Create Image
   * **Instructions**:
     1. Check the "Verify images after they are created" checkbox
     2. Click the Add... Button

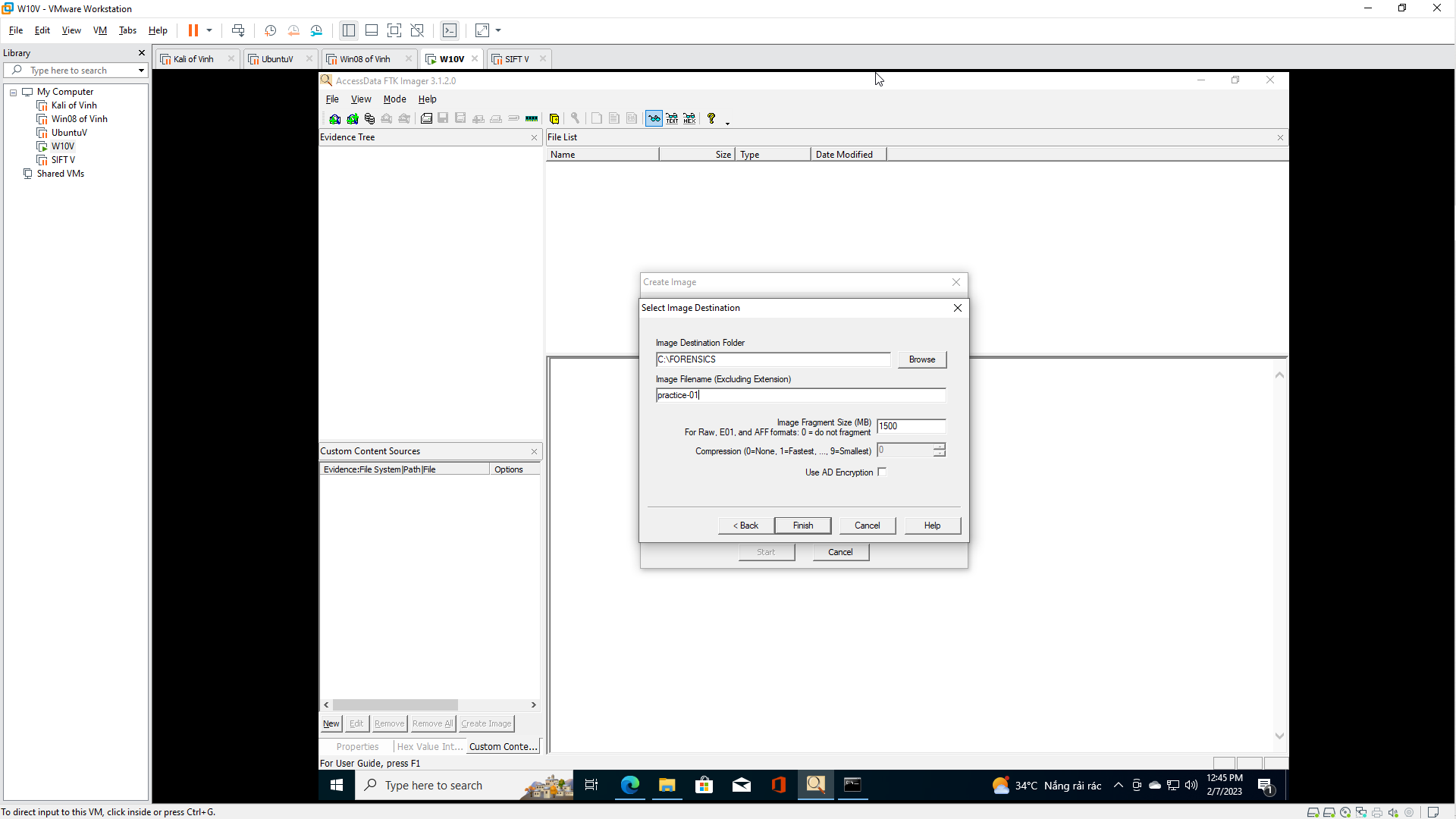


1. Select Image Type
   * **Instructions**:
     1. Select the Raw(dd) Radio Button
     2. Click the Next Button

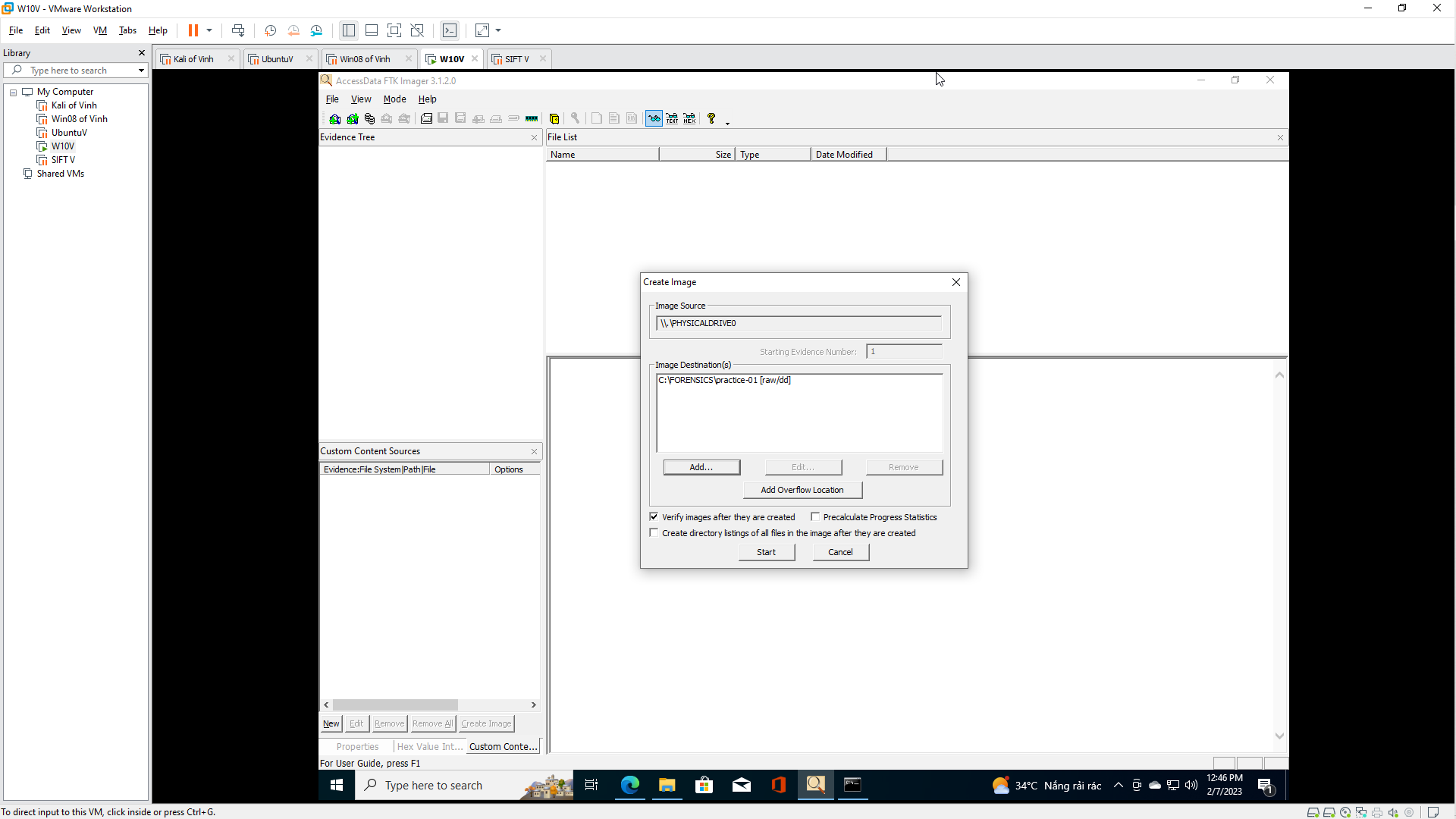


1. Evidence Item Information
   * **Instructions**:
     1. Case Number: 00001
     2. Evidence Number: 001
     3. Unique Description: Practice Image
     4. Examiner: **Your Name**
        + For Proof of Lab purposes, replace the string "Your Name" with your actual name.
     5. Contains a delete Captain Crunch Whistle
     6. Click the Next Button

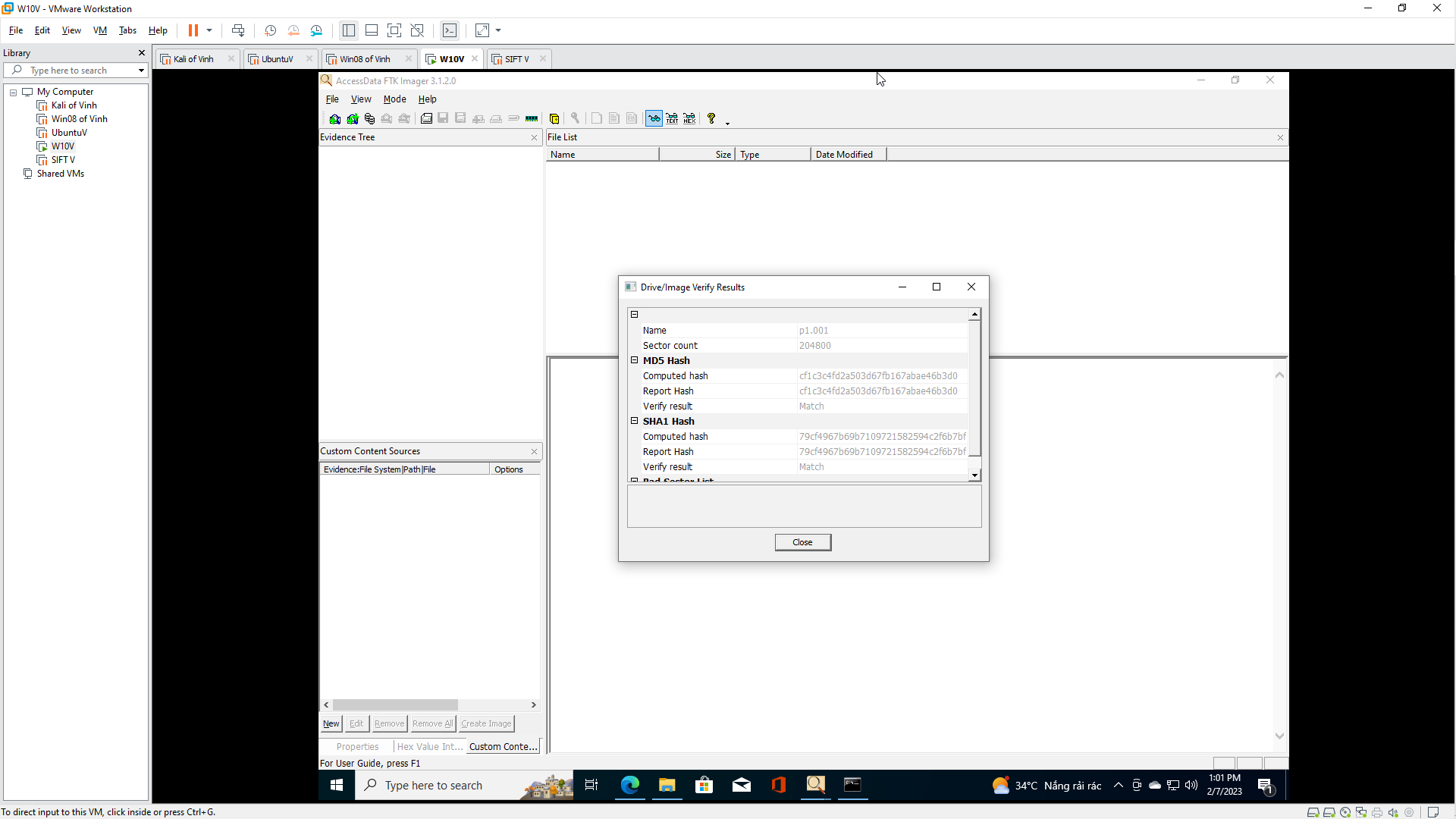
1. Select Image Destination
   * **Instructions**:
     1. Image Destination Folder: C:\FORENSICS
     2. Image Filename (Excluding Extension): practice-01
     3. Image Fragment Size(MB): 1500
     4. Click the Finish Button



1. Create Image
   * **Instructions**:
     1. Check "Verify images after they are created"
     2. Click the Start Button



1. Drive/Image Verify Results
   * **Instructions**:
     1. View MD5 Matching Hashes
     2. View MD5 Matching Hashes
     3. Click the Close Button



1. Image created successfully
   * **Instructions**:
     1. Click the Close Button

**Section 6: Proof of Lab**

1. Proof of Lab
   * **Instructions**:
     1. cd C:\FORENSICS
     2. dir | findstr "practice"
     3. type practice-01.001.txt | findstr "Examiner"
     4. date /t
     5. echo "Your Name"
        + This should be your actual name.
        + e.g., echo "John Gray"
   * **Proof of Lab Instructions**
     1. Press both the <Ctrl> and <Alt> keys at the same time.
     2. Do a <PrtScn>
     3. Paste into a word document
     4. Upload to Moodle

