**FTK Imager:**

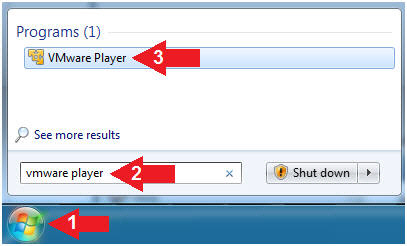
**Create Virtual Hard Drive, Delete File, Recover File**

**Section 0. Background Information**

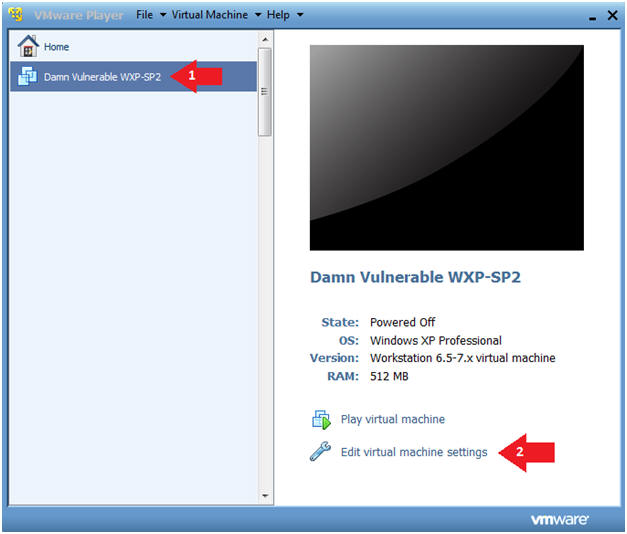
1. **What is FTK Imager?**
   * The FTK toolkit includes a standalone disk imaging program called FTK Imager. The FTK Imager has the ability to save an image of a hard disk in one file or in segments that may be later reconstructed.
   * It calculates MD5 hash values and confirms the integrity of the 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**
   * FTK Imager: Lesson 1: Install FTK Imager
3. **Lab Notes**
   * In this lab we will do the following:
     1. Create a Virtual Hard Drive.
     2. Download a Picture
     3. Delete the Picture from the Recycle Bin
     4. Export Picture with FTK Imager
     5. View Exported Picture

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

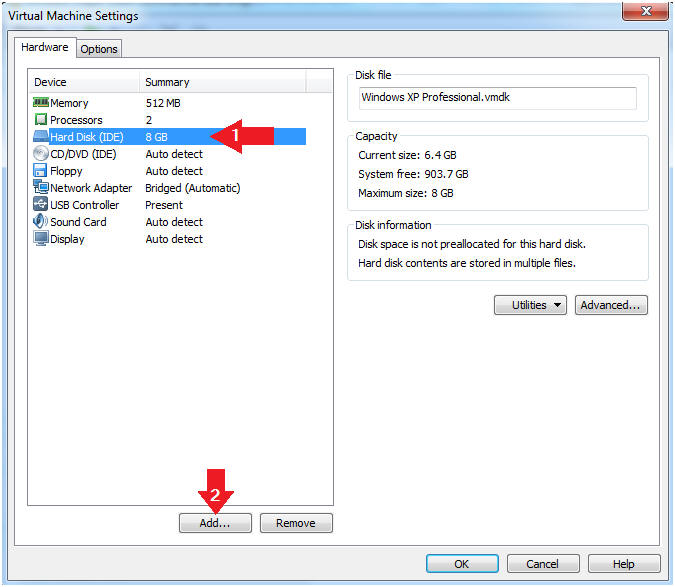
1. Start VMware Player
   * **Instructions**
     1. For Windows 7
        1. Click Start Button
        2. Search for "vmware player"
        3. Click VMware Player
     2. For Windows XP
        1. Starts --> Programs --> VMware Player



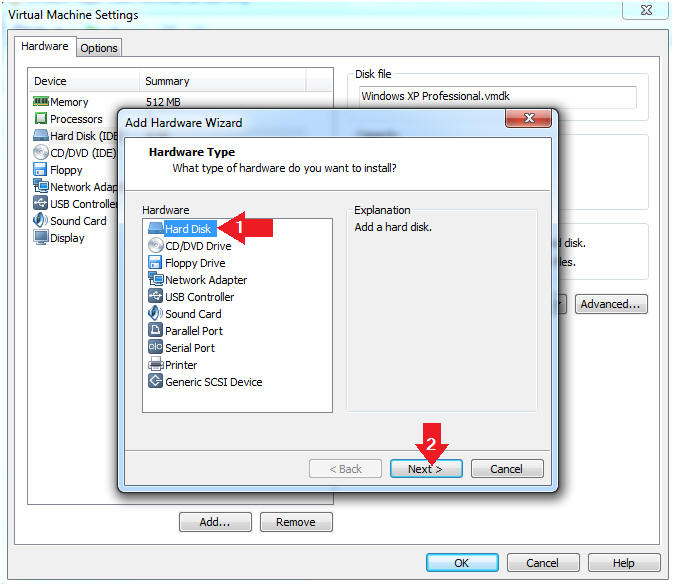
1. Start Up WXP-SP2.
   * **Instructions:**
     1. Click on WXP-SP2
     2. Click on Edit virtual machine Settings
   * **Note(FYI)**:
     1. For those of you not part of my class, this is a Windows XP machine running SP2.



1. Add Device
   * **Instructions:**
     1. Click on the Hard Disk
     2. Click on the Add Button



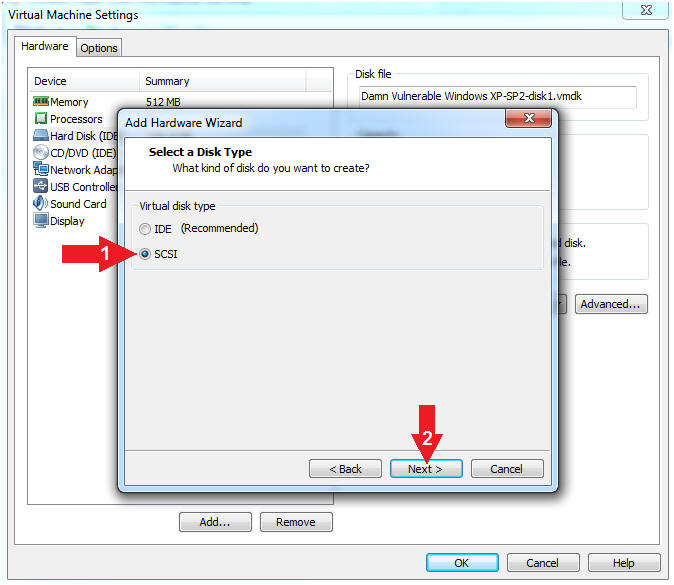
1. Add Hard Disk
   * **Instructions:**
     1. Click on the Hard Disk
     2. Click on the Next Button



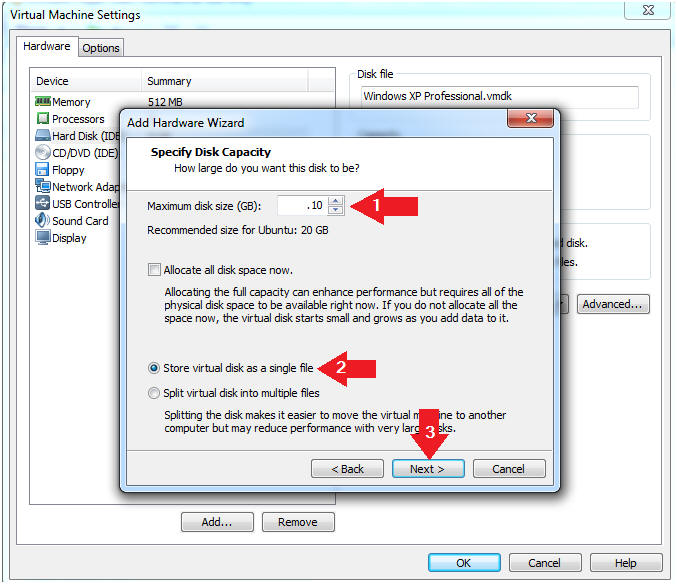
1. Select a Disk
   * **Instructions:**
     1. Click on "Create a new virtual disk"
     2. Click on the Next Button



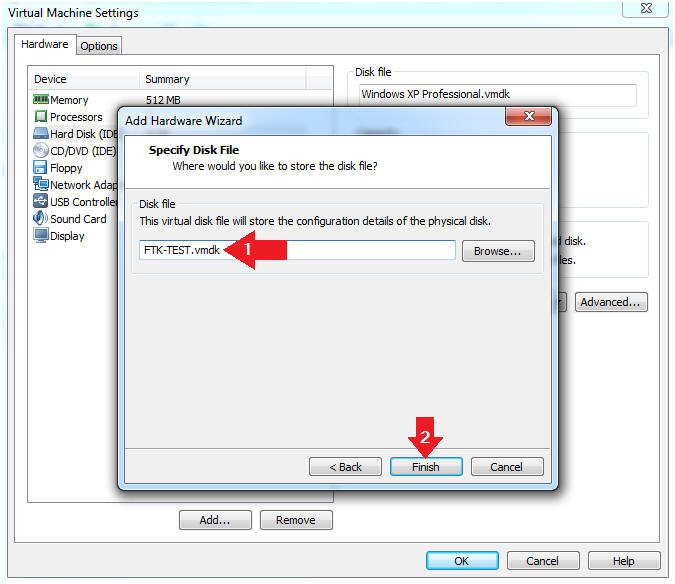
1. Select a Disk Type
   * **Instructions:**
     1. Click on **SCSI**
     2. Click on the Next Button



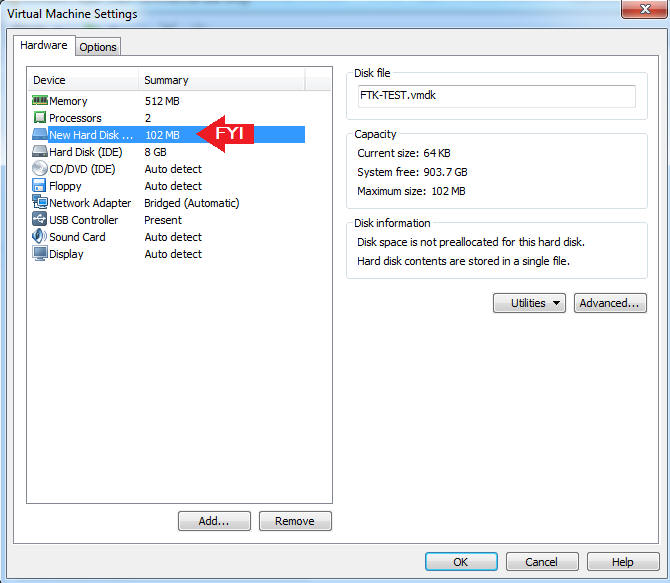
1. Select Disk Capacity
   * **Instructions:**
     1. Maximum disk size (GB): **.10**
     2. Click on "Store virtual disk as a single file"
     3. Click on the Next Button



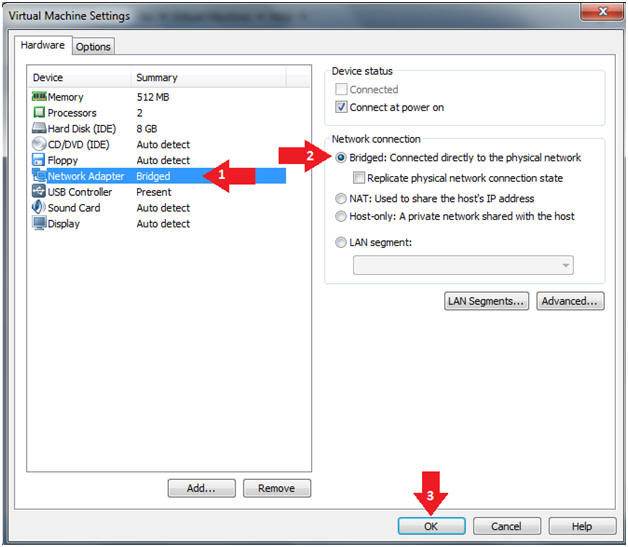
1. Specify Disk File
   * **Instructions:**
     1. Disk File Name: **FTK-TEST.vmdk**
     2. Click on the Finish Button



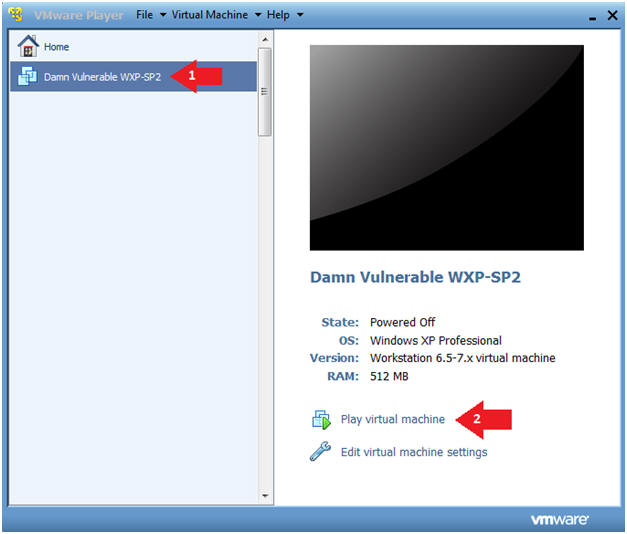
1. View Results
   * **Note(FYI):**
     1. Notice there is a New Hard Disk Entry with the size of a 102 MB.
     2. Continue to next step



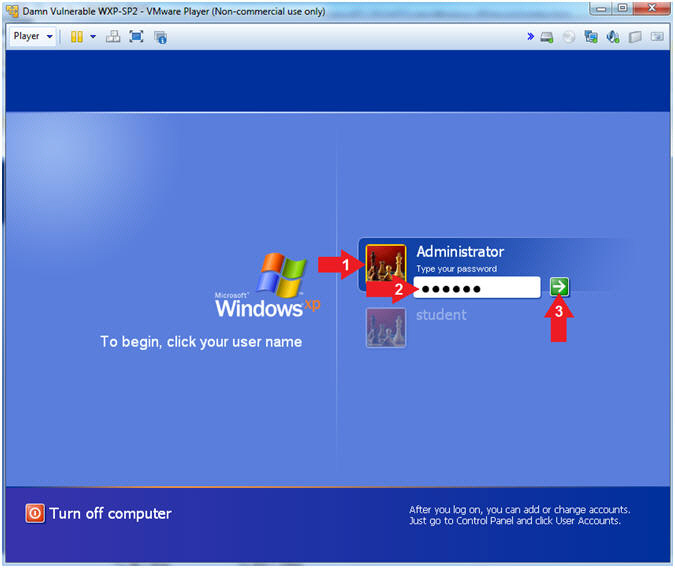
1. Edit Virtual Machine Settings
   * **Instructions:**
     1. Click on Network Adapter
     2. Click on the Bridged Radio button
     3. Click on the OK Button



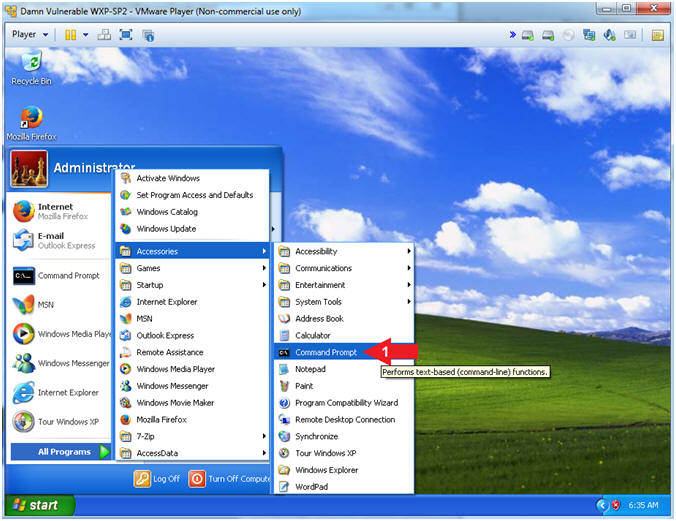
1. Play Virtual Machine
   * **Instructions:**
     1. Click on WXP-SP2
     2. Click on Play virtual machine



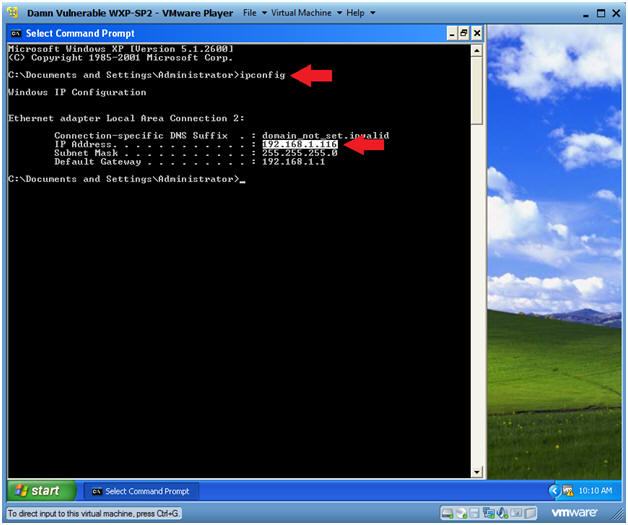
1. Logging into WXP-SP2.
   * **Instructions:**
     1. Click on **Administrator**
     2. Password: Supply Password
     3. Press <Enter> or Click the Arrow



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

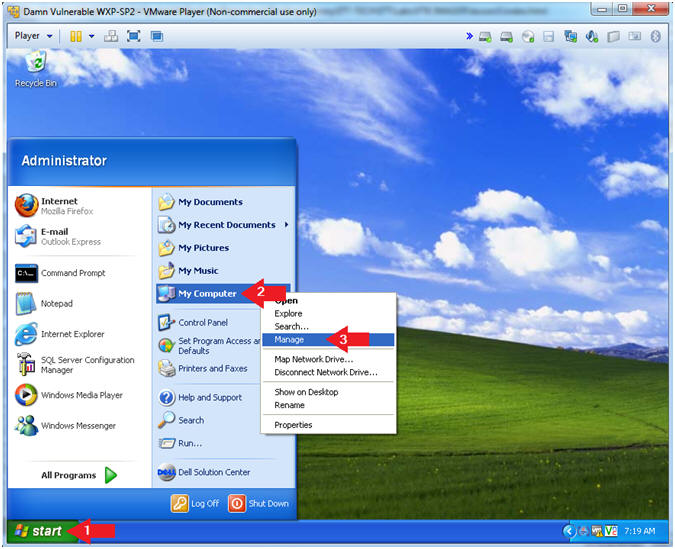


1. Obtain WXP-SP2's IP Address
   * **Instructions:**
     1. ipconfig
   * **Note(FYI)**:
     1. In my case, WXP-SP2's IP Address 192.168.1.116.
     2. This is the IP Address of the Victim Machine that will be attacked by Metasploit.
     3. Record your WXP-SP2's IP Address.

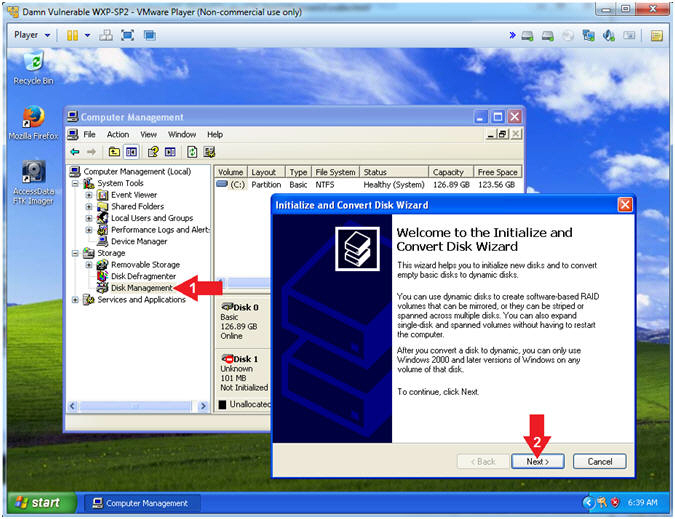
.

**Section 2: Format New Hard Disk**

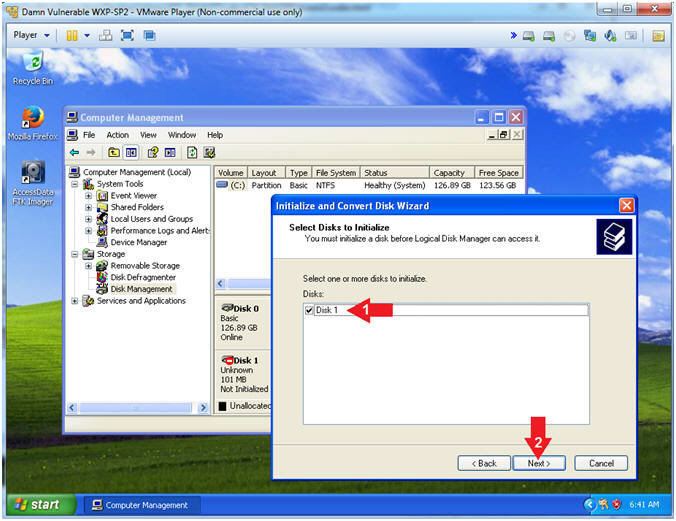
1. Open Computer Management
   * **Instructions:**
     1. Click the Windows Start Button
     2. Right Click on My Computer
     3. Click on Manage



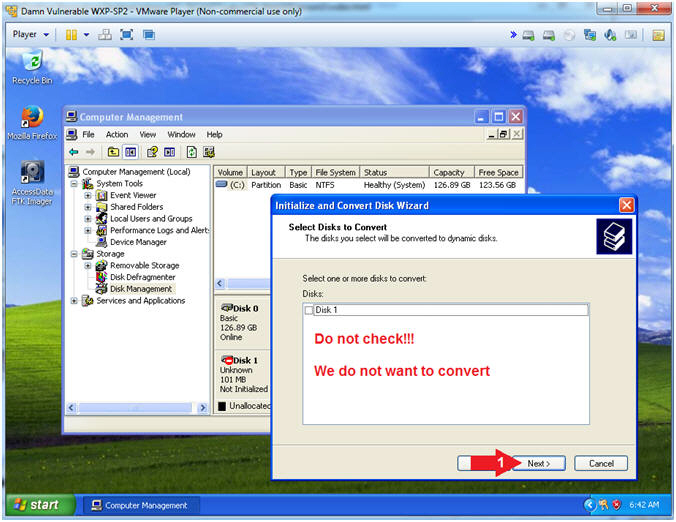
1. Disk Management
   * **Instructions:**
     1. Click on Disk Management
     2. Click on the Next Button



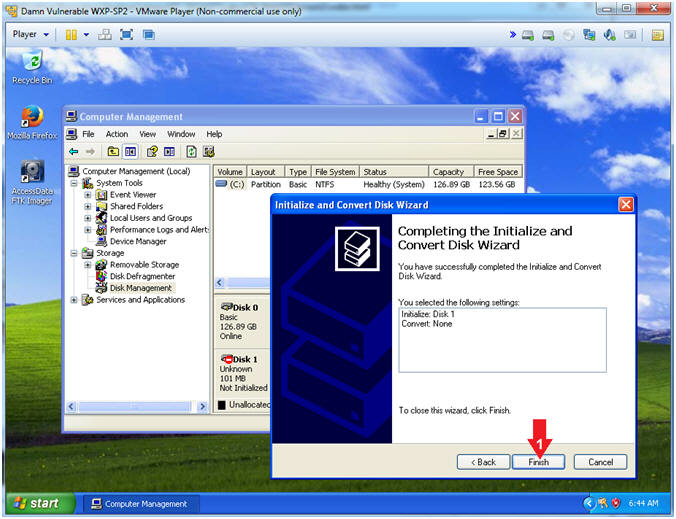
1. Select Disks to Initialize
   * **Instructions:**
     1. Check on Disk 1
     2. Click on the Next Button



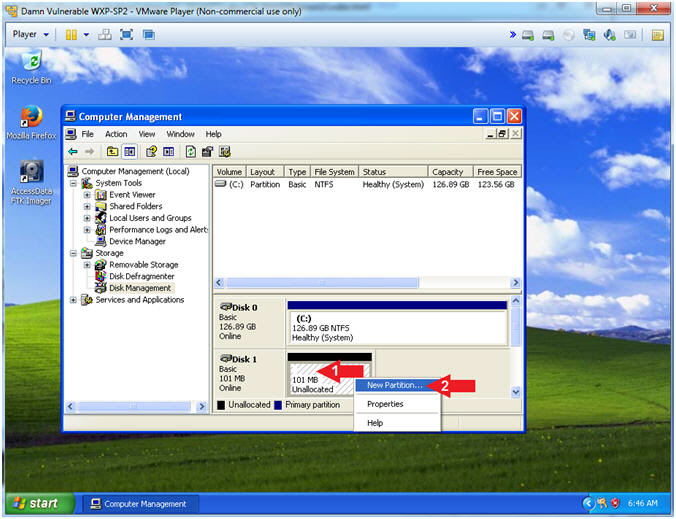
1. Select Disks to Convert
   * **Note(FYI):**
     1. Do not check any disks to convert!!!
   * **Instructions:**
     1. Click the Next Button



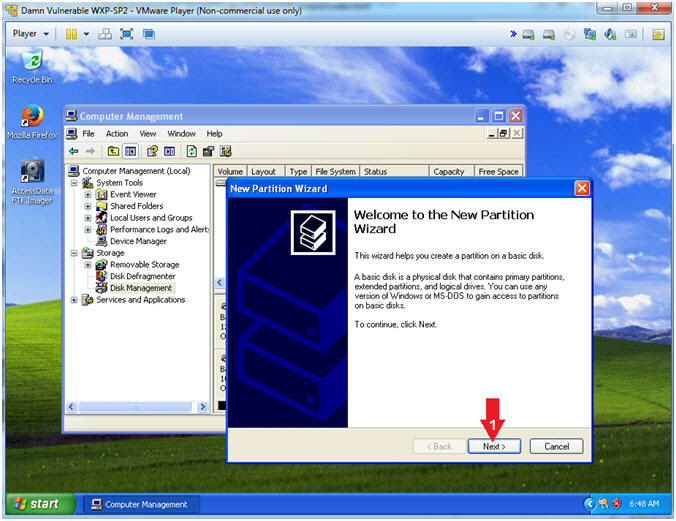
1. Complete Disk Wizard
   * **Instructions**:
     1. Click the Finish Button



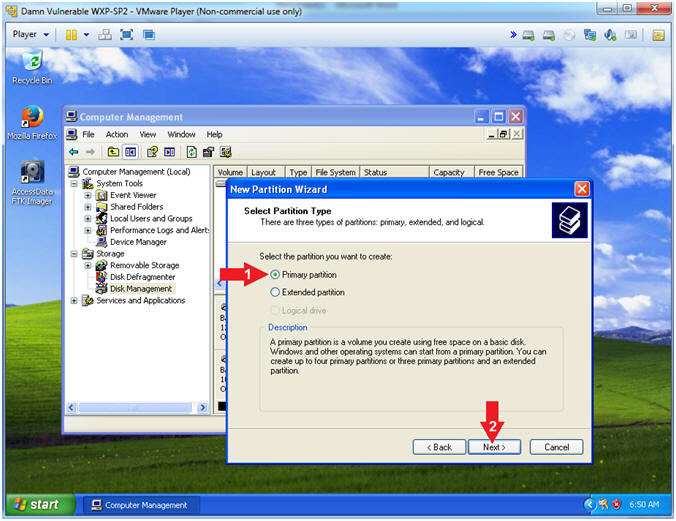
1. Create New Partition
   * **Instructions**:
     1. Right click in Disk 1's Unallocated Rectangle (See Picture)
     2. Click New Partition



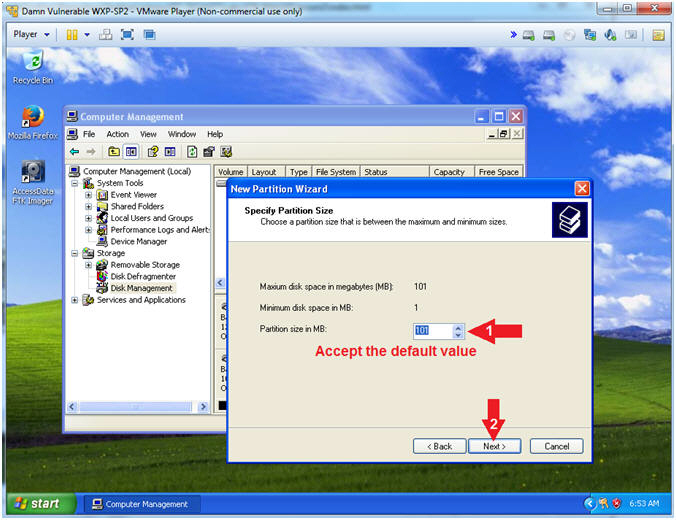
1. New Partition Wizard
   * **Instructions**:
     1. Click the Next Button



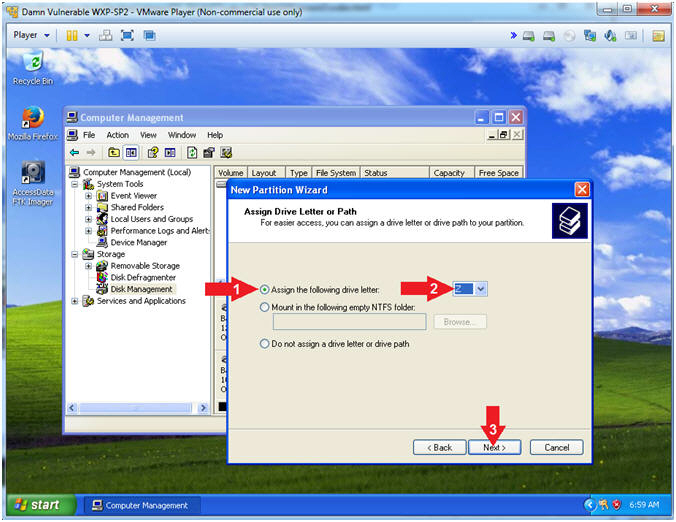
1. Select Partition Type
   * **Instructions**:
     1. Click on the "Primary partition" radio button
     2. Click the Next Button



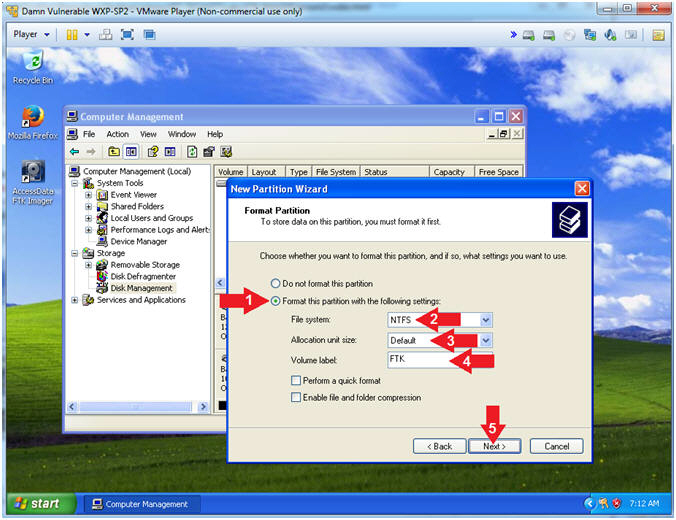
1. Specify Partition Size
   * **Instructions**:
     1. Partition size in MB: Accept the default number, which should be the maximum size.
     2. Click the Next Button



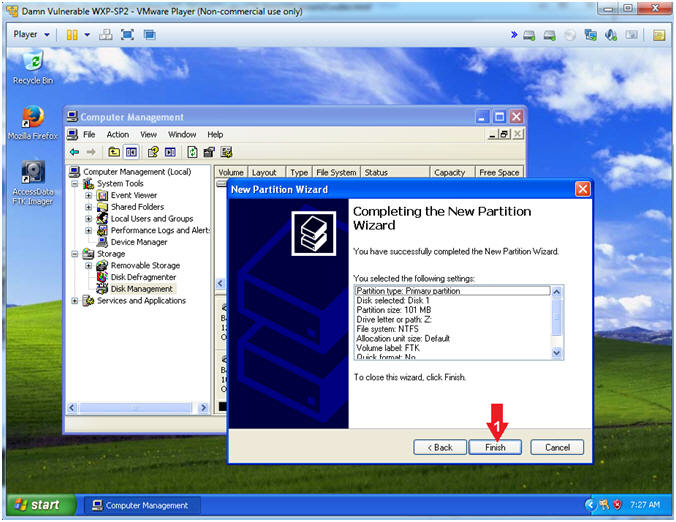
1. Assign Drive Letter or Patch
   * **Instructions**:
     1. Click on the "Assign the following drive letter:" radio button.
     2. Select letter "Z"
     3. Click the Next Button



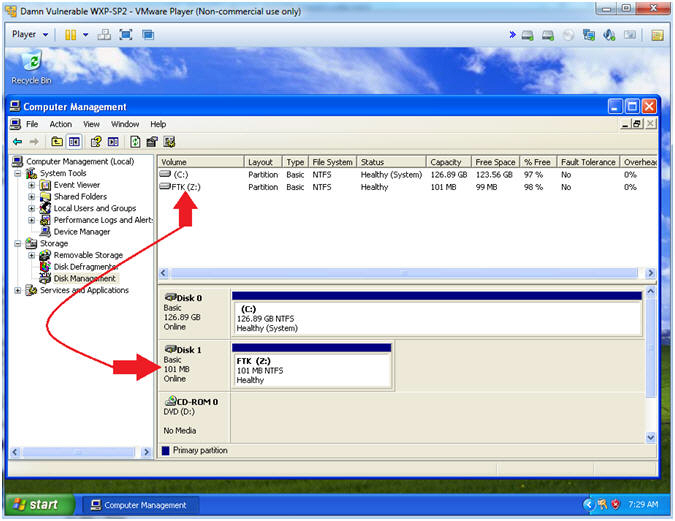
1. Format Partition
   * **Instructions**:
     1. Click on the "Format this partition with the follow settings" radio button.
     2. File system: NTFS
     3. Allocation unit size: Default
     4. Volume label: **FTK**
     5. Click the Next Button



1. Complete the New Partition Wizard
   * **Instructions**:
     1. Click on the Finish Button

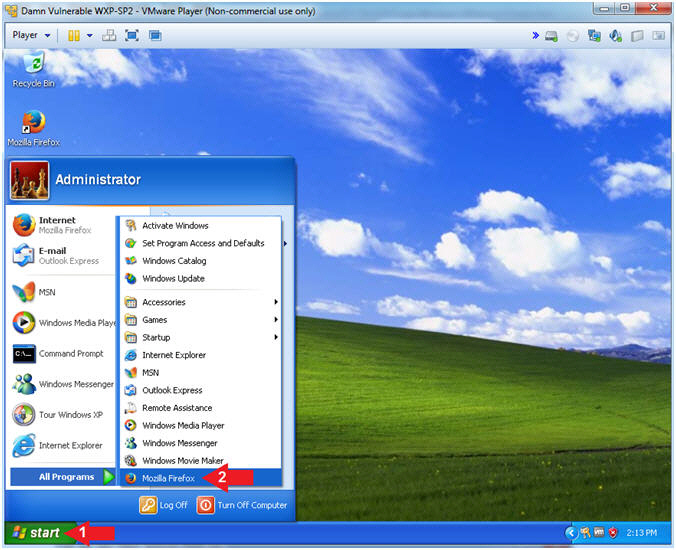


1. Verify Results
   * **Note(FYI)**:
     1. Notice there is a new hard disk with the volumn label "FTK (Z:)".

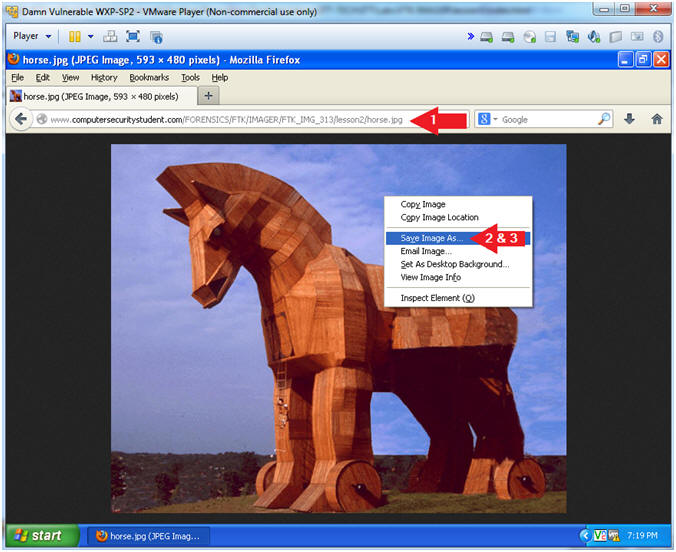


**Section 3: Download Test Picture**

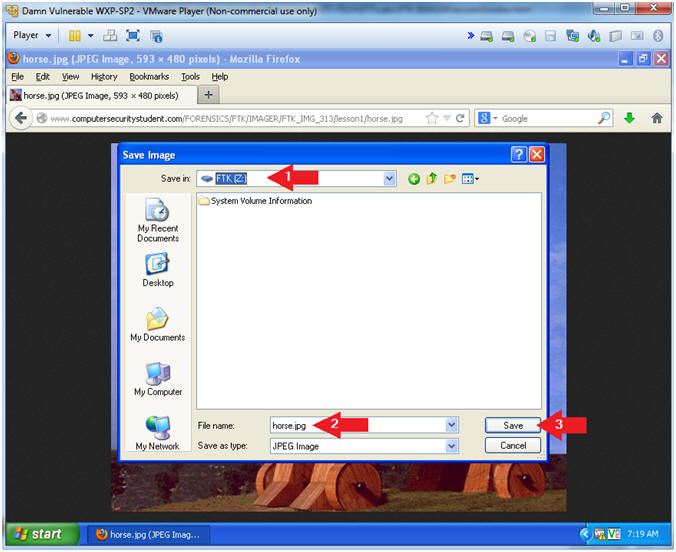
1. Start Firefox
   * **Instructions**:
     1. Click the Start Button
     2. All Programs --> Mozilla Firefox



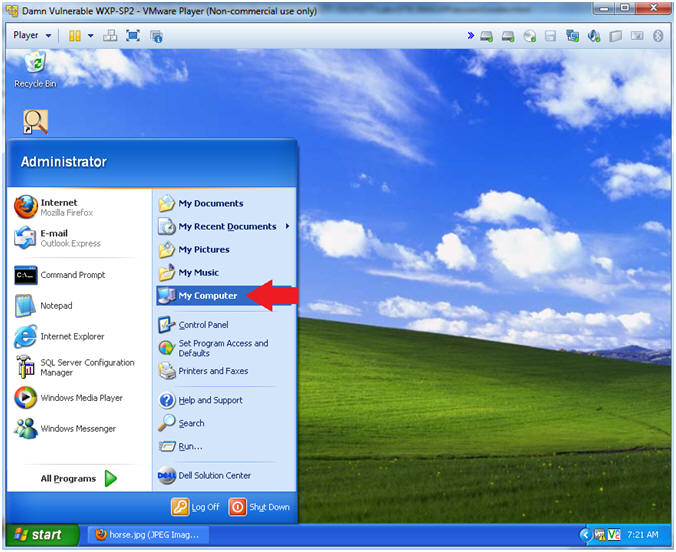
1. Start Test Picture Download
   * **Instructions**:
     1. Place the following URL in the Firefox Address Textbox
        + http://www.computersecuritystudent.com/FORENSICS/FTK/IMAGER/FTK\_IMG\_313/lesson2/horse.jpg
     2. Right Click on the image
     3. Click on "Save Image As..."



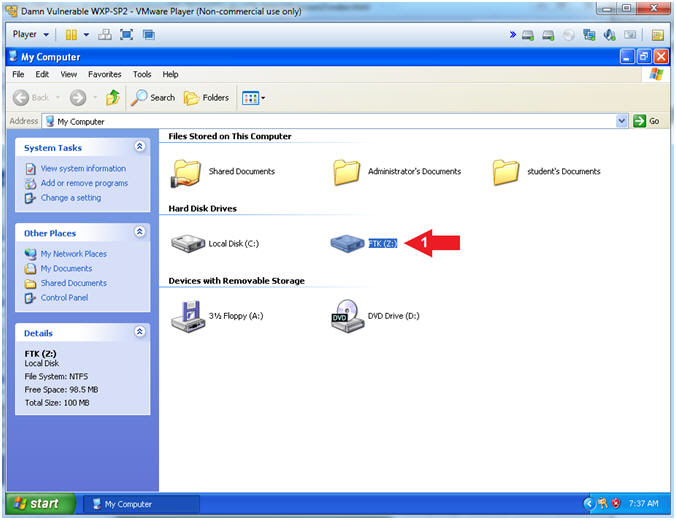
1. Save Test Picture Download
   * **Instructions**:
     1. Save in: Select the FTK (Z:) Drive
     2. Filename: horse.jpg
     3. Click the Save Button



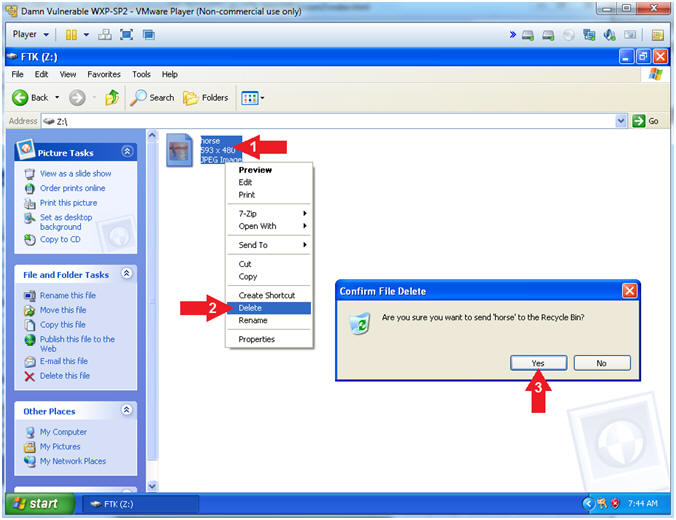
1. Open My Computer
   * **Instructions**:
     1. Start --> My Computer



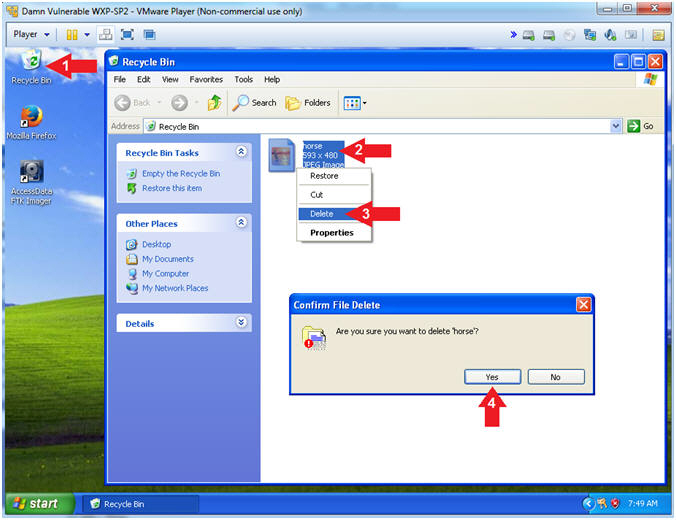
1. Open your FTK(Z:) Drive
   * **Instructions**:
     1. Navigate to your FTK(Z:) Drive



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

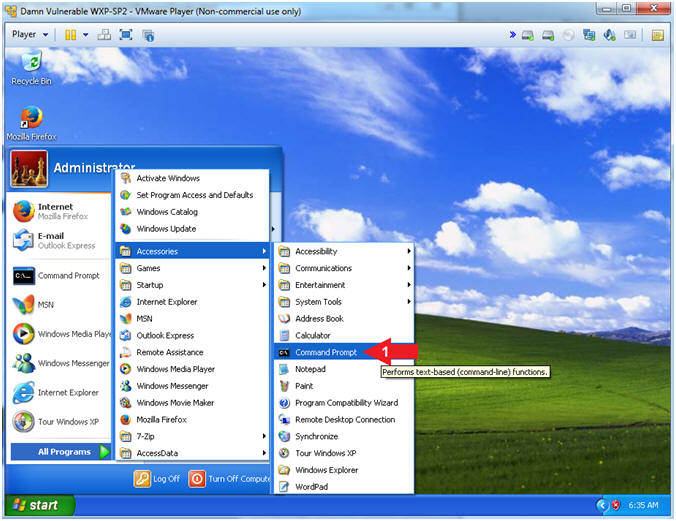


1. Delete Test Picture From the Recycle Bin
   * **Instructions**:
     1. Click on the Recycle Bin Icon located on the Desktop
     2. Right Click on horse.jpg
     3. Click Delete
     4. Confirm File Delete Windows: Click the Yes Button.

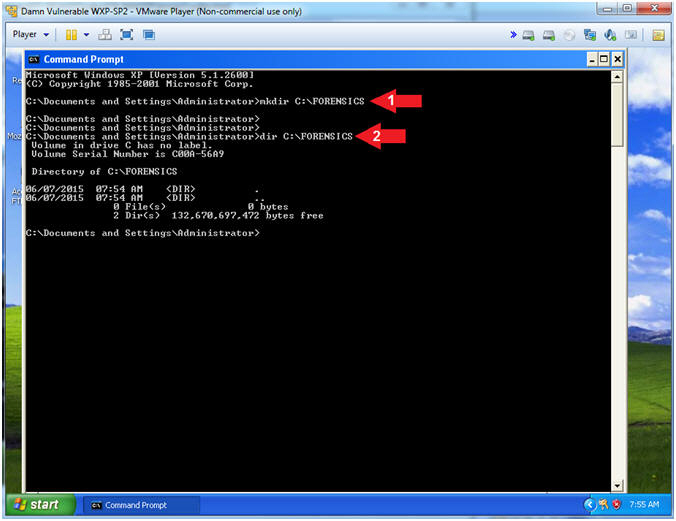


**Section 4: Forensics Directory**

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

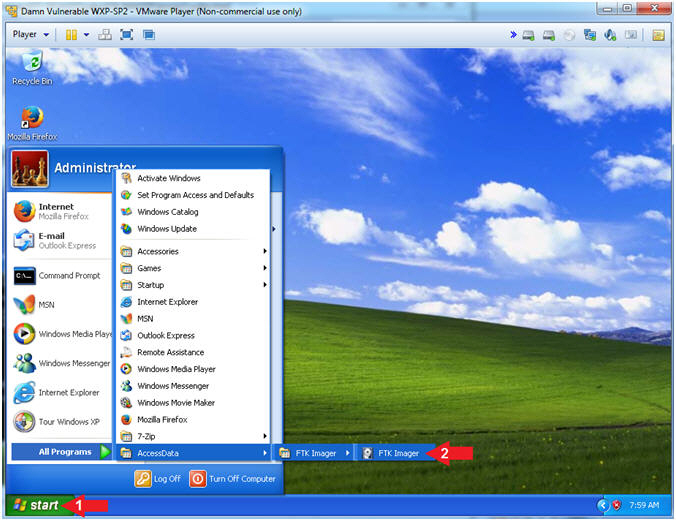


1. Create a Forensics Directory
   * **Instructions**:
     1. mkdir C:\FORENSICS
     2. dir C:\FORENSICS



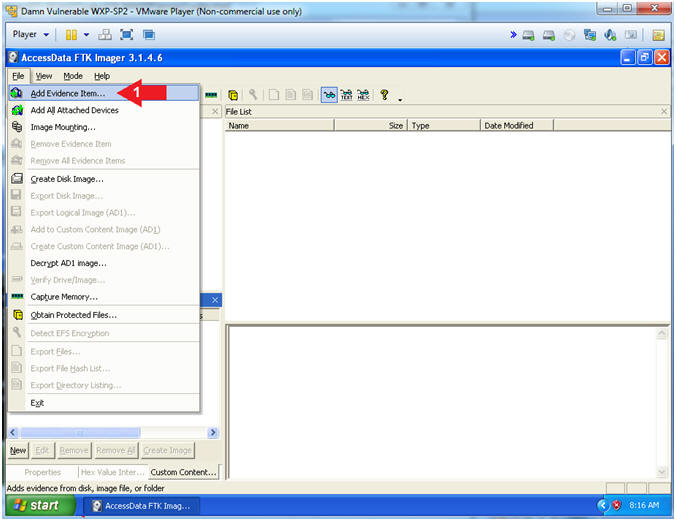
**Section 5: Start FTK Imager**

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

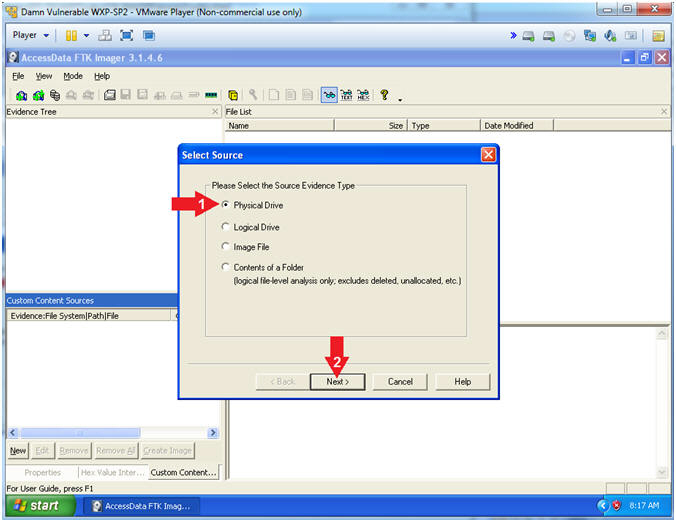


**Section 6: FTK Imager: Add Evidence Item…**

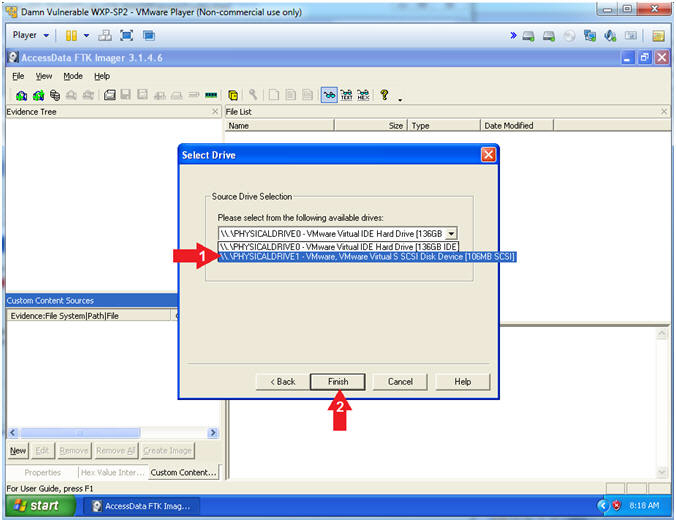
1. Add Evidence
   * **Instructions**:
     1. File --> Add Evidence Item...



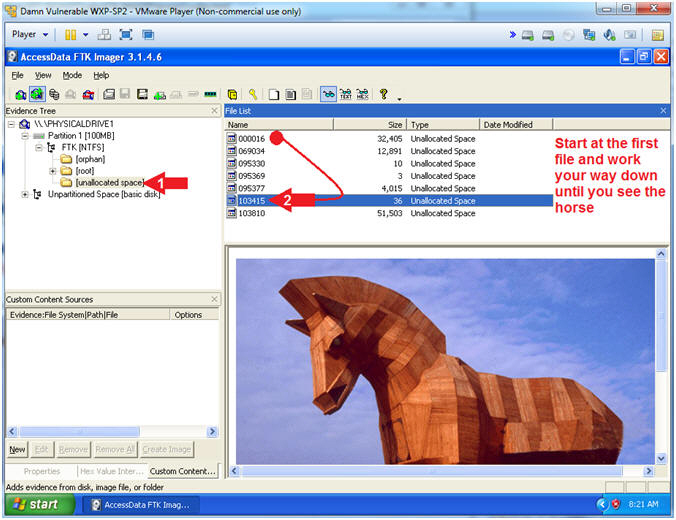
1. Select Source
   * **Instructions**:
     1. Select the "Physical Drive" Radio Button
     2. Click the Next Button



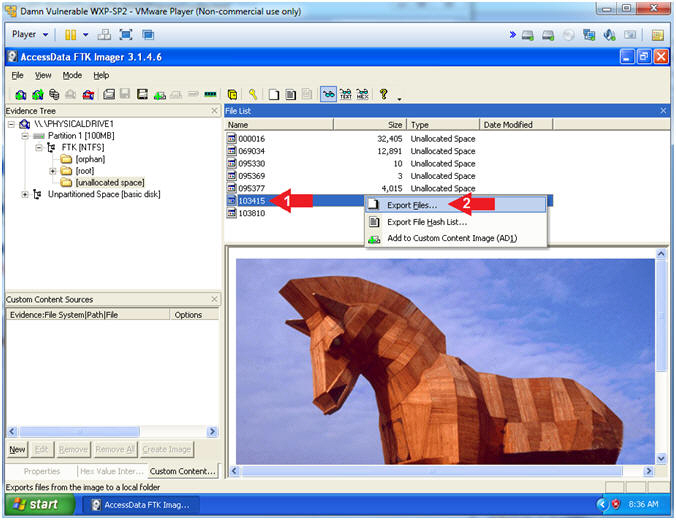
1. Select Drive
   * **Instructions**:
     1. Select \\PHYSICAL DRIVE1 ... (106MB SCSI)
     2. Click the Finish Button



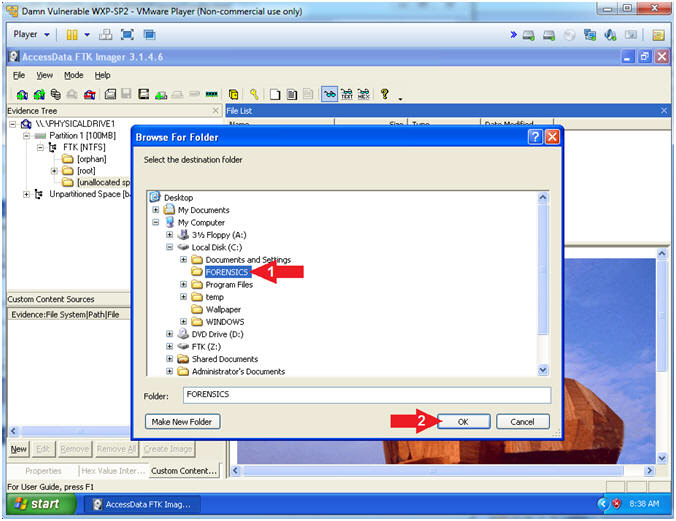
1. View Deleted Picture
   * **Instructions**:
     1. Navigate to the below path
        + \\PHYSICALDRIVE1 --> Partition 1 (100MB) --> FTK(NTFS) --> [unallocated space]
     2. Click on each file in the right window pane until you see the picture.



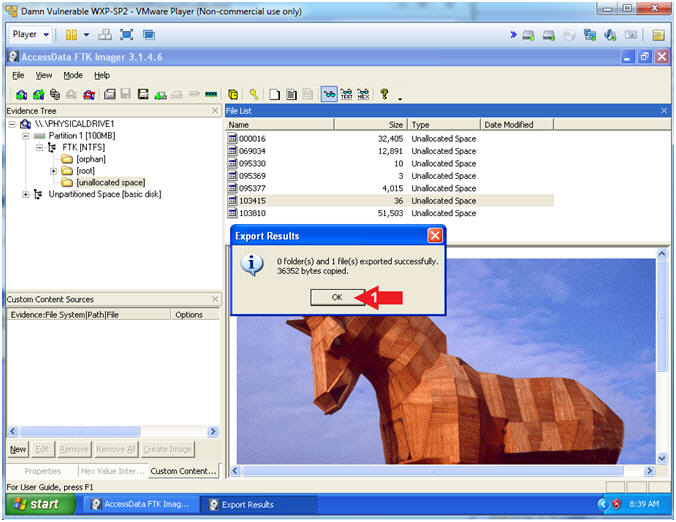
1. Export File
   * **Instructions**:
     1. Right Click on the file that contains the picture
     2. Select Export Files...



1. Browse For Folder
   * **Instructions**:
     1. Navigate to C:\FORENSICS
     2. Click the OK Button

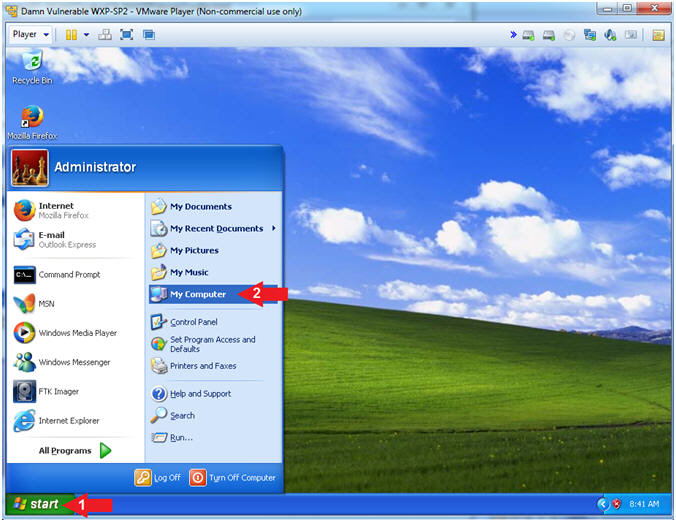


1. Export Results
   * **Instructions**:
     1. Click the OK Button

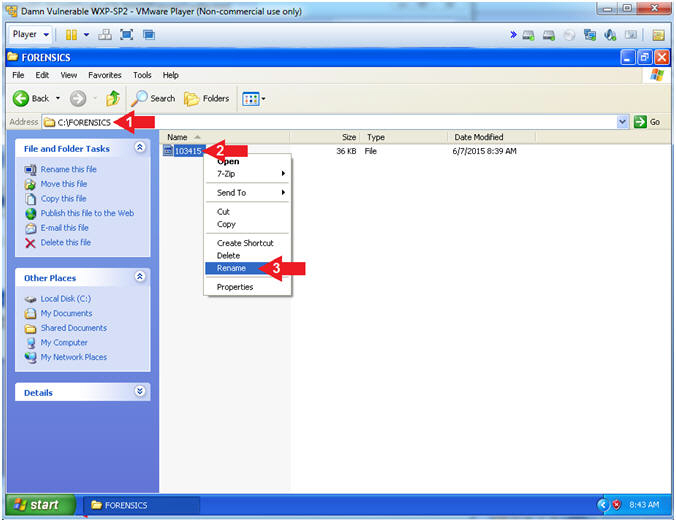


**Section 7: View Recovered Picture**

1. Open My Computer
   * **Instructions**:
     1. Click the Start Button
     2. Select My Computer



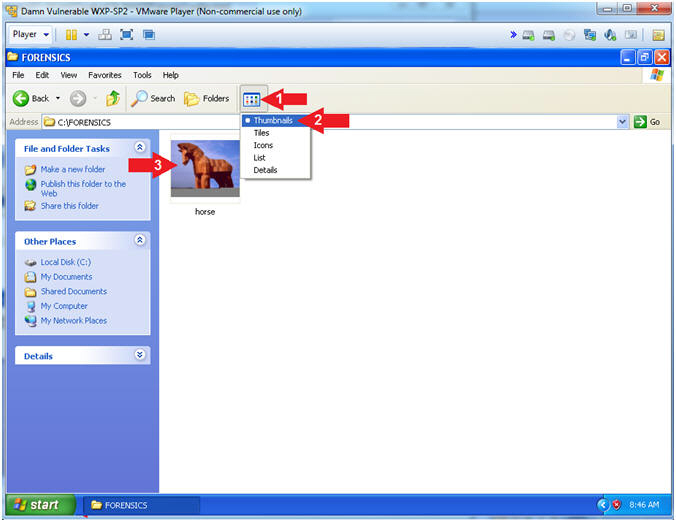
1. Rename File
   * **Instructions**:
     1. Navigate to C:\FORENSICS
     2. Right Click on the file
        + In my case the filename is 103415.  In your case, it will probably be named differently.
     3. Click Rename



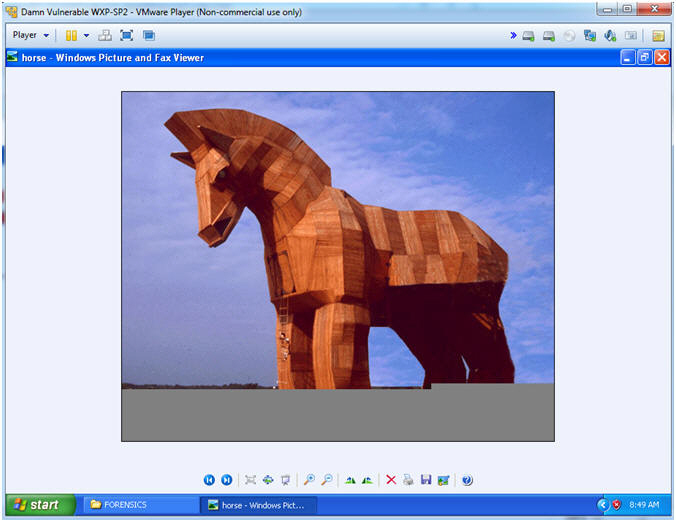
1. Rename File
   * **Instructions**:
     1. Rename file to "horse.jpg"



1. Open My Computer
   * **Instructions**:
     1. Click the View Icon
     2. Select Thumbnails
     3. Double Click on horse.jpg

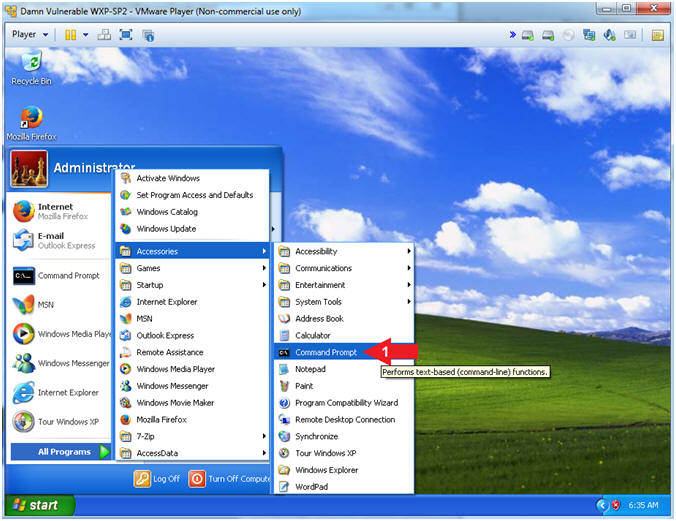


1. View Picture
   * **Note(FYI)**:
     1. Thank you FTK Imager



**Section 8: Proof of Lab**

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



1. Proof of Lab
   * **Instructions**:
     1. dir C:\FORENSICS | findstr "horse"
     2. date /t
     3. 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

