**FTK Imager:**

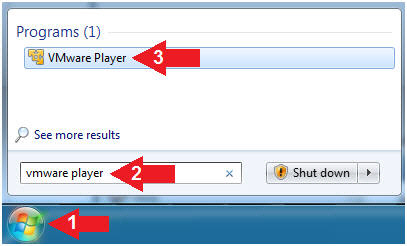
**Mount Image File, Recover Deleted File**

**Section 0. Background Information**

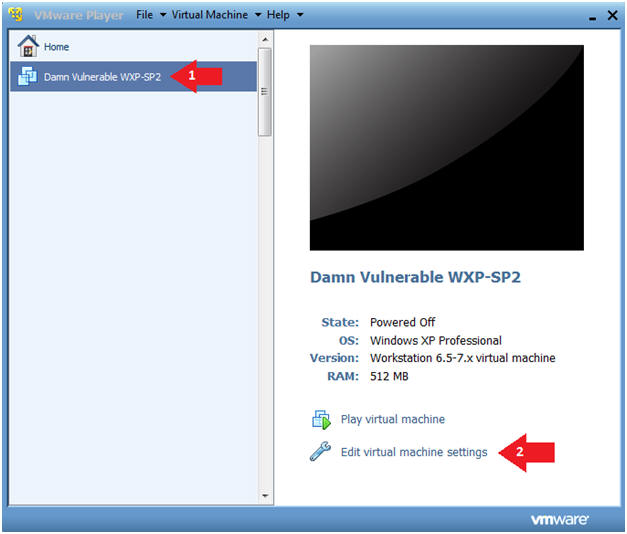
1. **What is FTK Imager?**
   * The FTK toolkit includes a standalone disk imaging program called FTK Imager. The FTK Imager has the ability to save an image of a hard disk in one file or in segments that may be later reconstructed.
   * It calculates MD5 hash values and confirms the integrity of the 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**
   * 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.
   * Create Disk Image after Deleting a Picture
     + **Note**: This lab is necessary, because you will need to create an image after deleting a file.
3. **Lab Notes**
   * In this lab we will do the following:
     + Mount the Image File.
     + View the deleted file.
     + Recover the deleted file.
     + Compare the MD5 sum of the image after work has been completed to its' original MD5 sum.

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

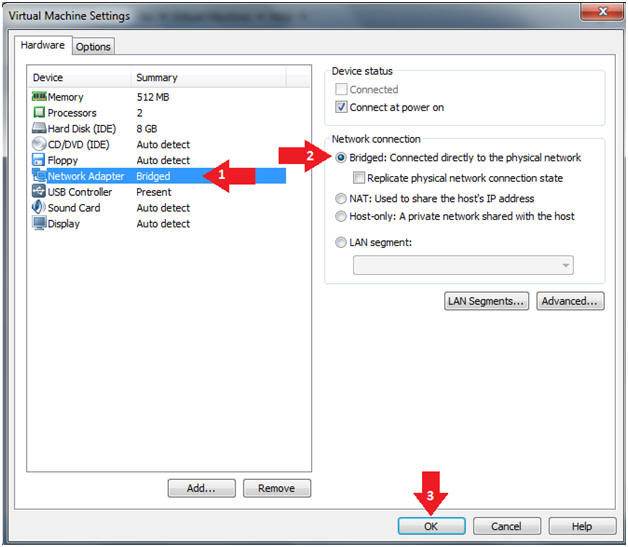
1. Start VMware Player
   * **Instructions**
     1. For Windows 7
        1. Click Start Button
        2. Search for "vmware player"
        3. Click VMware Player
     2. For Windows XP
        1. Starts --> Programs --> VMware Player



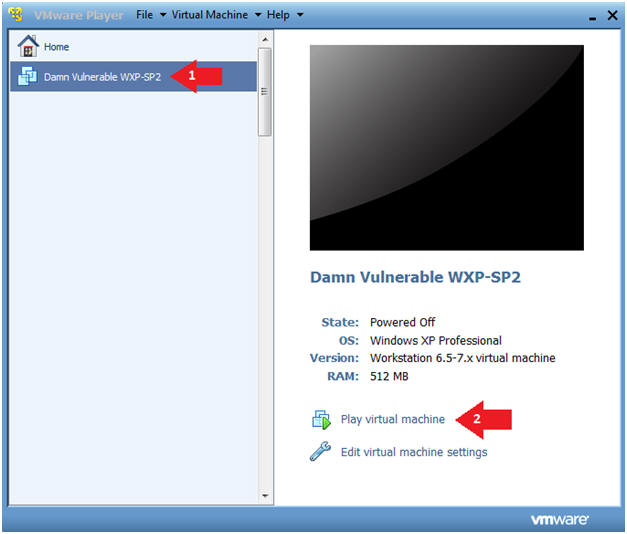
1. Start Up WXP-SP2.
   * **Instructions:**
     1. Click on WXP-SP2
     2. Click on Edit virtual machine Settings
   * **Note(FYI)**:
     1. For those of you not part of my class, this is a Windows XP machine running SP2.



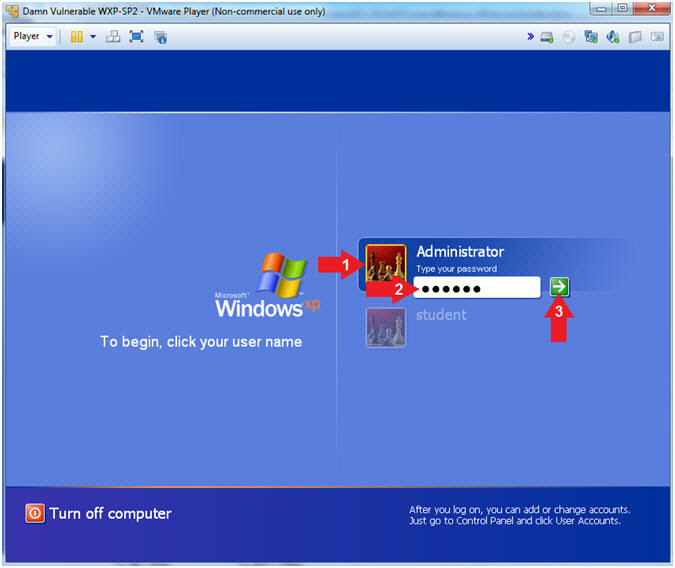
1. Edit Virtual Machine Settings
   * **Instructions:**
     1. Click on Network Adapter
     2. Click on the Bridged Radio button
     3. Click on the OK Button



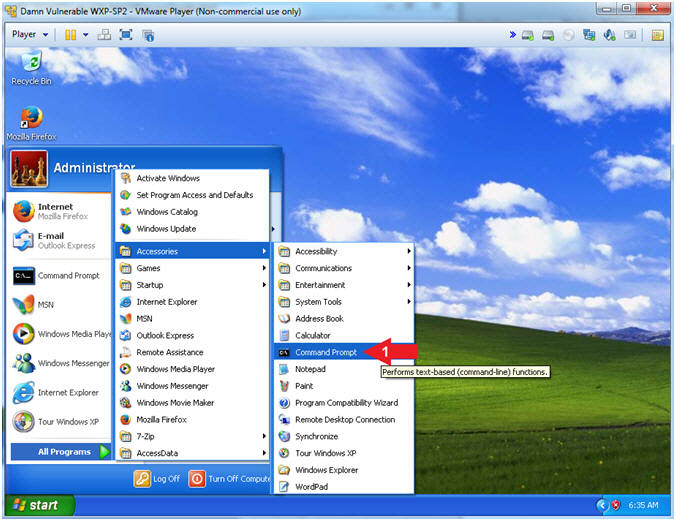
1. Play Virtual Machine
   * **Instructions:**
     1. Click on WXP-SP2
     2. Click on Play virtual machine



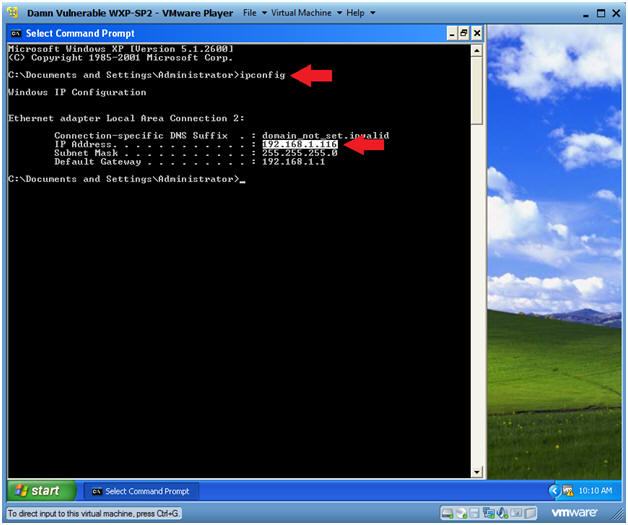
1. Logging into WXP-SP2.
   * **Instructions:**
     1. Click on **Administrator**
     2. Password: Supply Password
     3. Press <Enter> or Click the Arrow



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

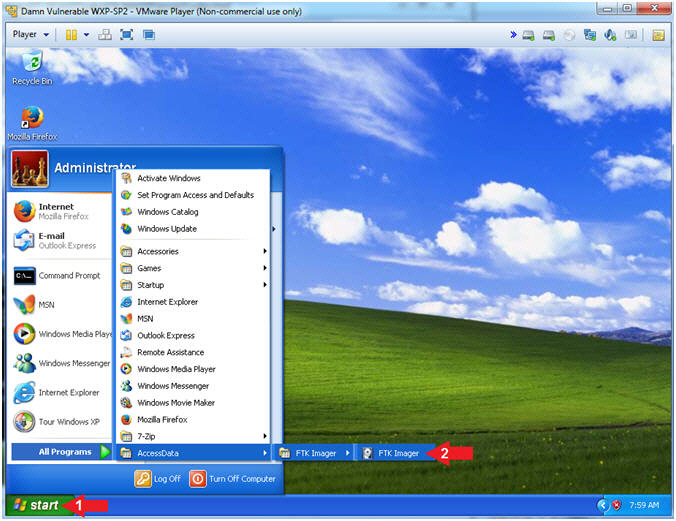


1. Obtain WXP-SP2's IP Address
   * **Instructions:**
     1. ipconfig
   * **Note(FYI)**:
     1. In my case, WXP-SP2's IP Address 192.168.1.116.
     2. This is the IP Address of the Victim Machine that will be attacked by Metasploit.
     3. Record your WXP-SP2's IP Address.

.

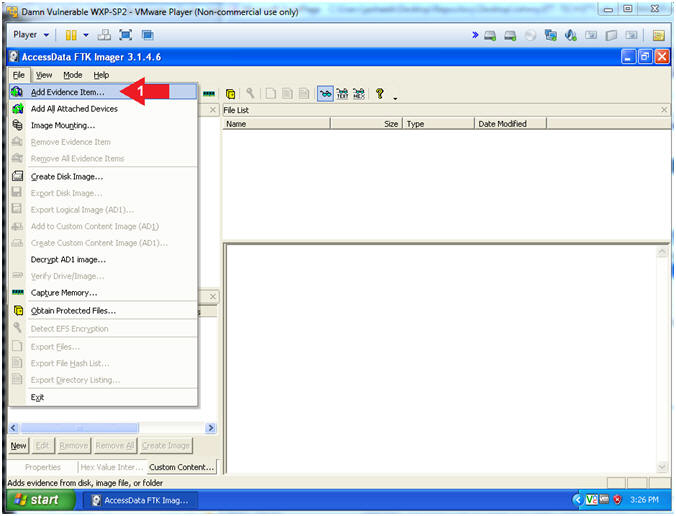
**Section 2: Start FTK Imager**

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

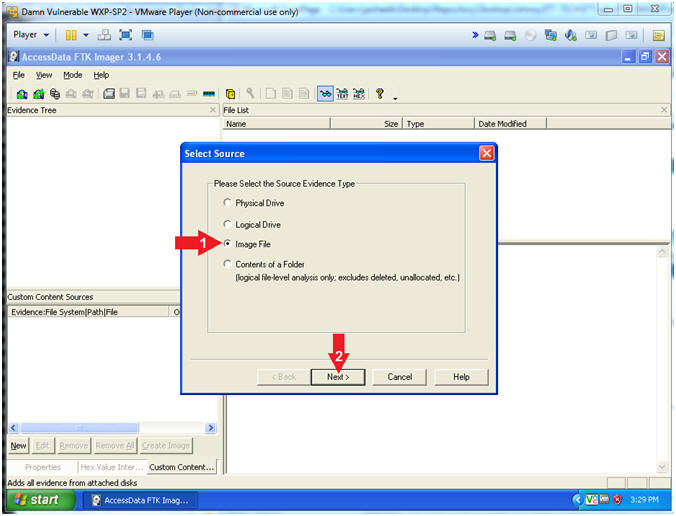


**Section 3: Mount Image**

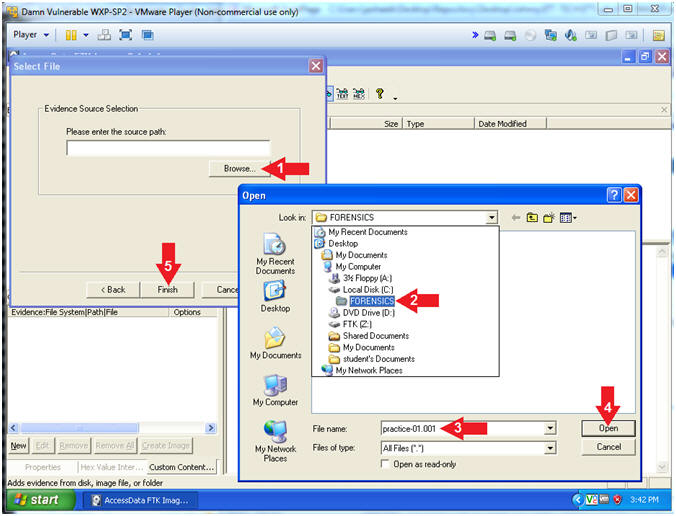
1. Add Evidence
   * **Instructions**:
     1. File --> Add Evidence Item...



1. Select Source
   * **Instructions**:
     1. Click on the Image File radio button
     2. Click the Next Button

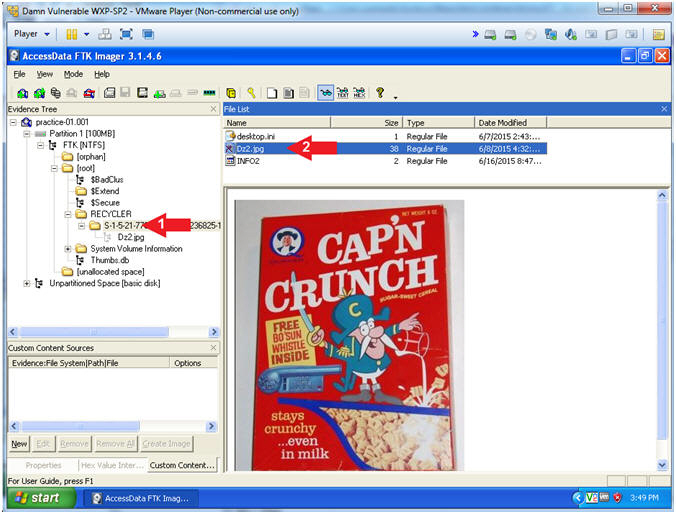


1. Select File
   * **Instructions**:
     1. Click the Browse Button
     2. Navigate to C:\FORENSICS
     3. Select practice-01.001
     4. Click the Open Button
     5. Click the Finish Button

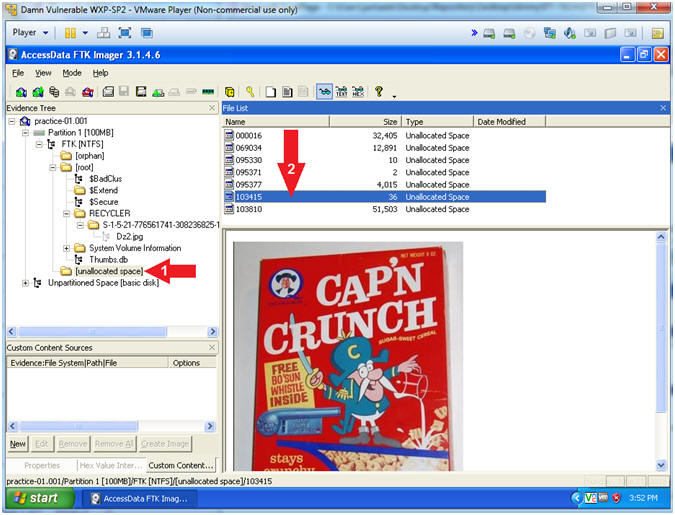


**Section 4: View Deleted Image**

1. View Deleted File(s) in the Recycler
   * **Instructions**:
     1. Navigate to practice-01-001 --> Partition 1 --> FTK[NTFS] --> [root] --> RECYCLER --> RECYCLER SUBDIR
        + The RECYCLER SUBDIR Directory name varies
     2. Click on the jpg file if it exists.
        + The naming convention of existing jpg's also varies.

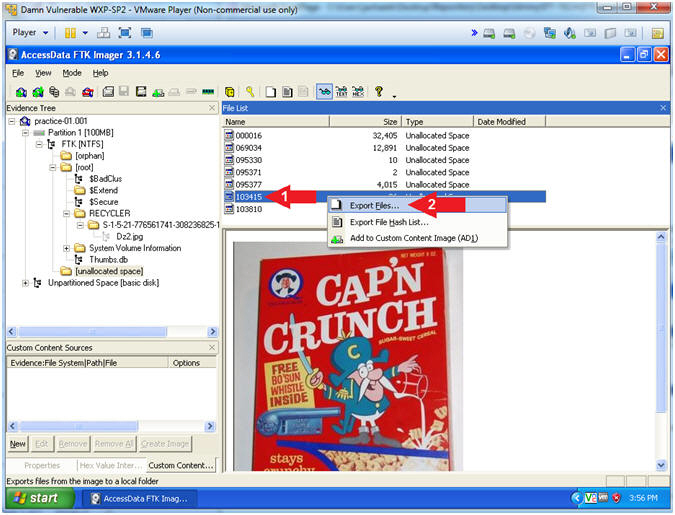


1. View Deleted File(s) in [unallocated space]
   * **Instructions**:
     1. Navigate to practice-01-001 --> Partition 1 --> FTK [NTFS] --> [root] --> [unallocated space]
     2. Scroll through all the files until you see the Captain Crunch Picture

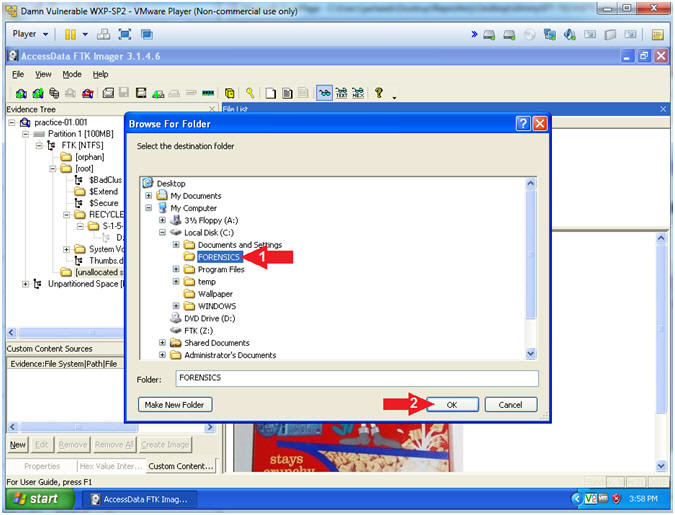


**Section 5: Recover Deleted Image**

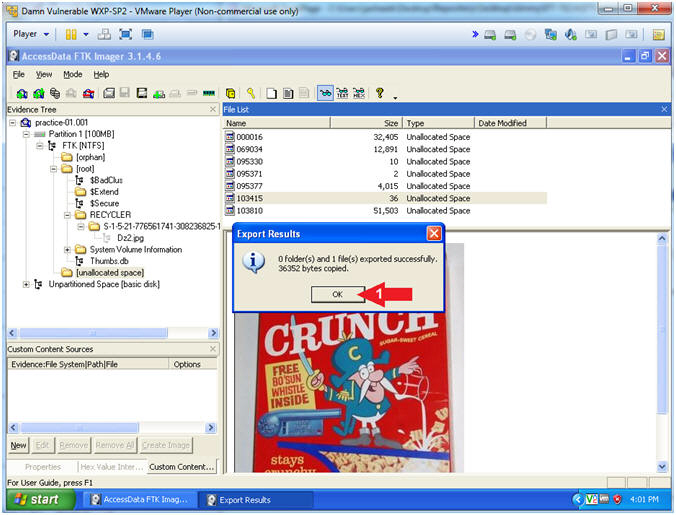
1. Export File
   * **Instructions**:
     1. Right Click on the file that contains the picture
     2. Select Export Files...



1. Select the destination folder
   * **Instructions**:
     1. Navigate to C:\FORENSICS
     2. Click the OK Button

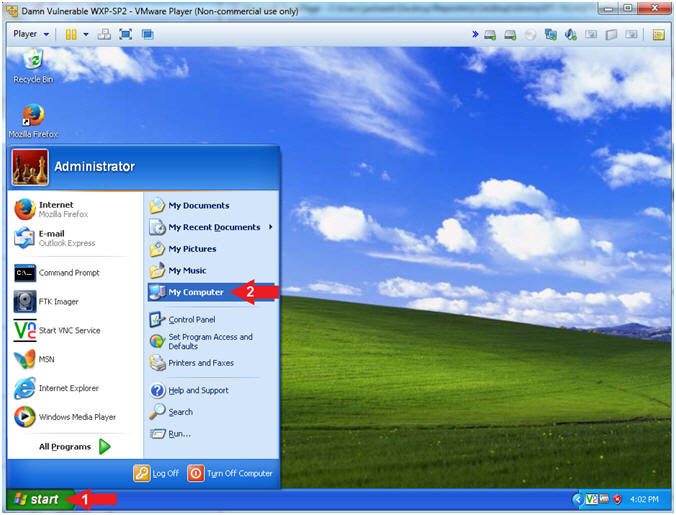


1. Export Results
   * **Instructions**:
     1. Click the OK Button

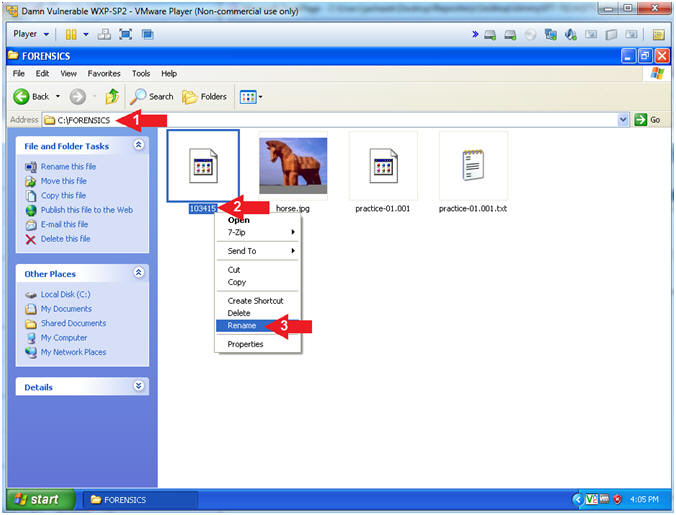


**Section 6: View Recoverd Picture**

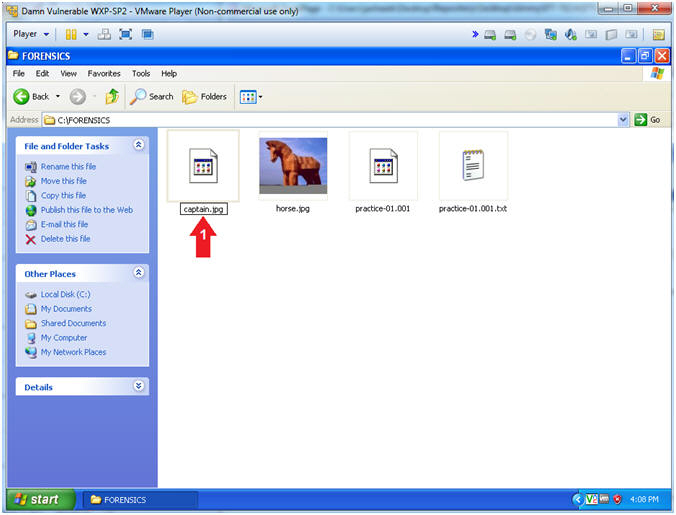
1. Open My Computer
   * **Instructions**:
     1. Click the Start Button
     2. Click on My Computer



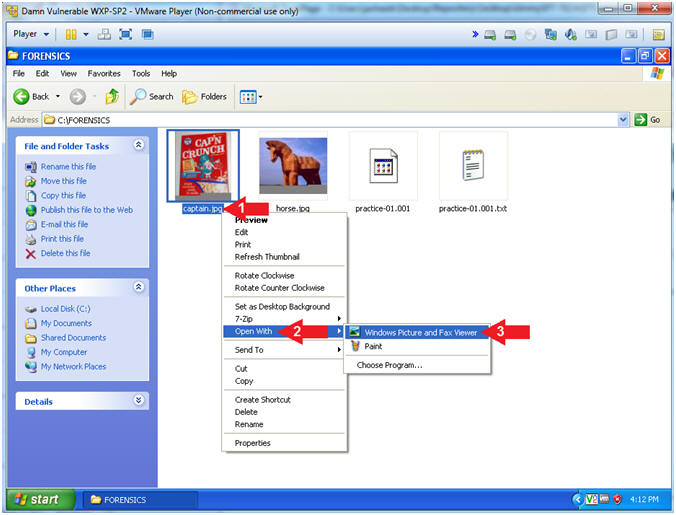
1. Rename File
   * **Instructions**:
     1. Navigate to C:\FORENSICS
     2. Right Click on the filename that contain all numbers
        + In my case the filename is 103415.  In your case, it will probably be named differently.
     3. Click Rename



1. Name File
   * **Instructions**:
     1. Rename file to "captain.jpg"



1. Open File
   * **Instructions**:
     1. Right Click "captain.jpg"
     2. Open With --> Windows Picture and Fax Viewer

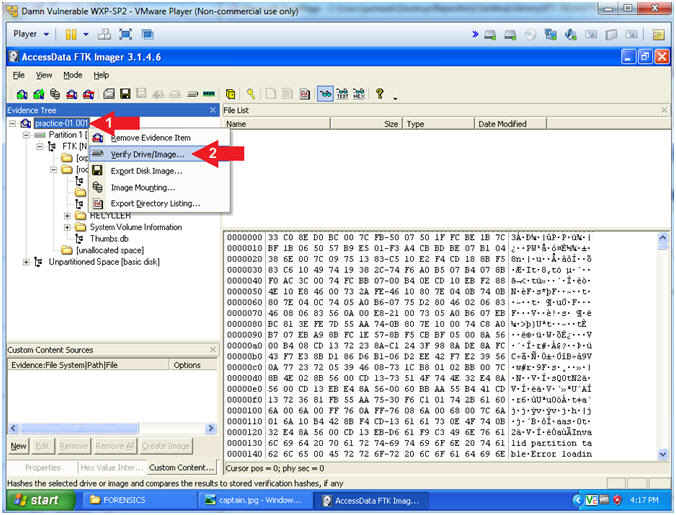


1. View File
   * **Note(FYI)**:
     1. CAP'N Crunch was a h4x0r.... nice whistle.

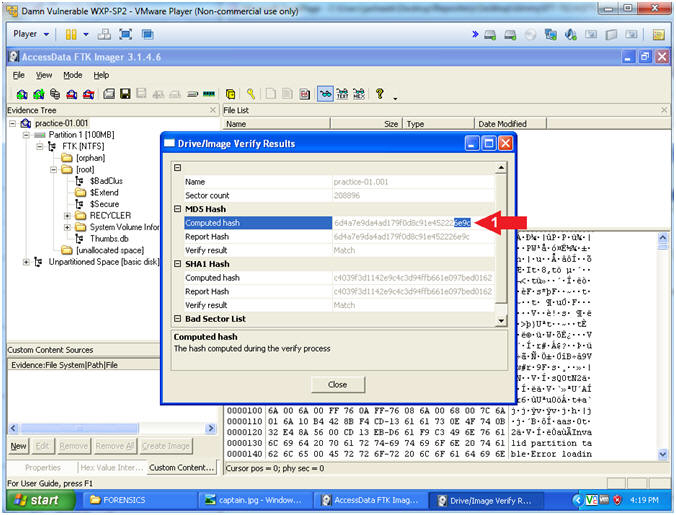


**Section 7: Calculate Post MD5 Hash**

1. Verify Image
   * **Instructions**:
     1. Right Click practice-01-001
     2. Click on Verify Drive/Image

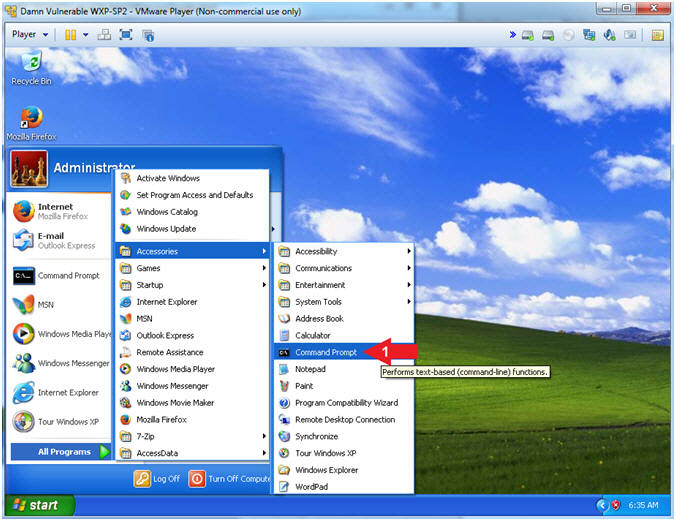


1. Drive/Image Verify Results
   * **Instructions**:
     1. Copy the last 4 characters of your MD5 Hash
        + In my case, it is **6e9c**.
     2. Do **Not** Click the Close Button



**Section 8: Proof of Lab**

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



1. Proof of Lab
   * **Instructions**:
     1. cd C:\FORENSICS
     2. type practice-01.001.txt | findstr "e358c"
        + Replace "e358c" with the string you obtained from (Section 7, Step 2)
        + This step verifies that MD5 Hash did not change since the image was first created.
     3. date /t
     4. 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

