**Progress test 1**

**FTK Imager:**

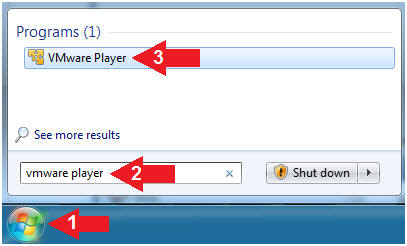
**Install FTK Imager**

**Section 0. Background Information**

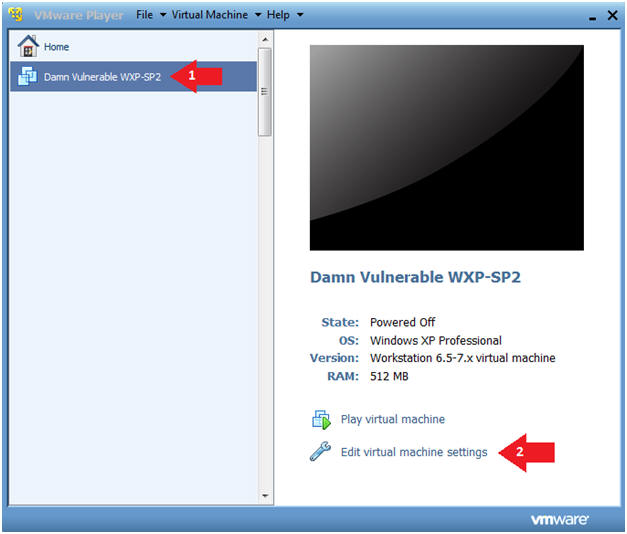
1. **What is FTK Imager?**
   * The FTK toolkit includes a standalone disk imaging program called FTK Imager. The FTK Imager has the ability to save an image of a hard disk in one file or in segments that may be later reconstructed.
   * It calculates MD5 hash values and confirms the integrity of the data before closing the files.
   * In addition to the FTK Imager tool can mount devices (e.g., drives) and recover deleted files.
2. **Lab Notes**
   * In this lab we will do the following:
     1. Download FTK Imager.
     2. Install FTK Imager.

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

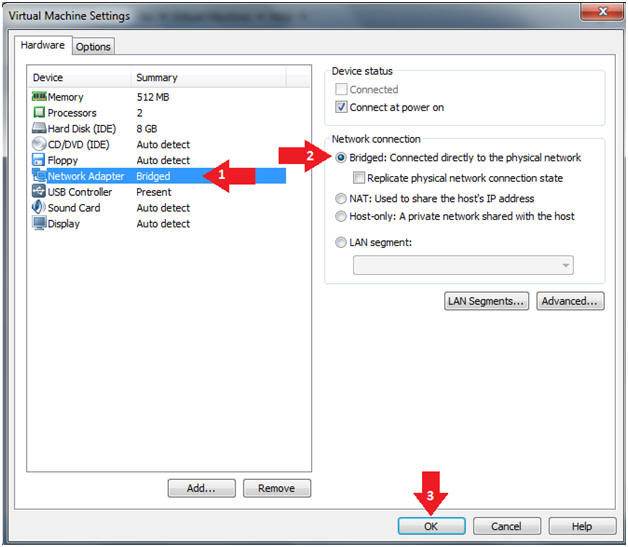
1. Start VMware Player
   * **Instructions**
     1. For Windows 7
        1. Click Start Button
        2. Search for "vmware player"
        3. Click VMware Player
     2. For Windows XP
        1. Starts --> Programs --> VMware Player



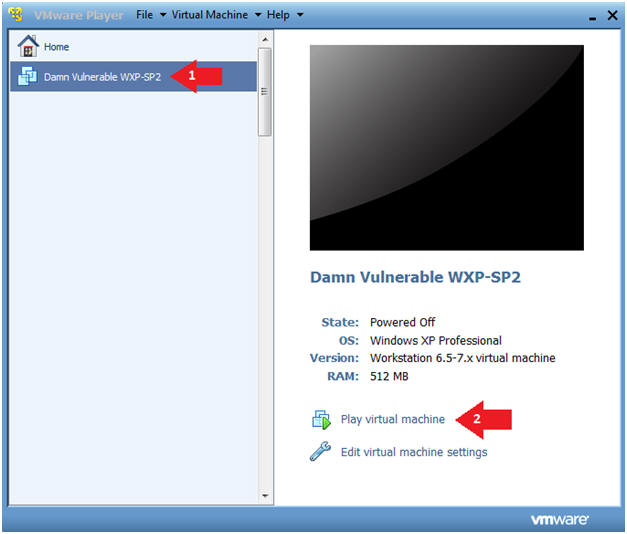
1. Start Up WXP-SP2.
   * **Instructions:**
     1. Click on WXP-SP2
     2. Click on Edit virtual machine Settings
   * **Note(FYI)**:
     1. For those of you not part of my class, this is a Windows XP machine running SP2.



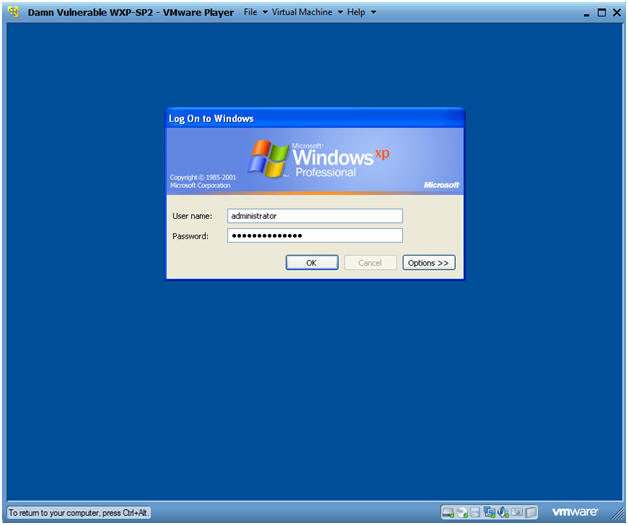
1. Edit Virtual Machine Settings
   * **Instructions:**
     1. Click on Network Adapter
     2. Click on the Bridged Radio button
     3. Click on the OK Button



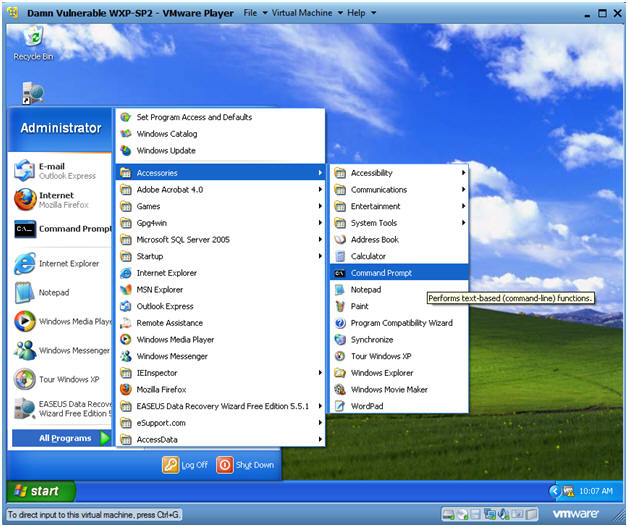
1. Play Virtual Machine
   * **Instructions:**
     1. Click on WXP-SP2
     2. Click on Play virtual machine



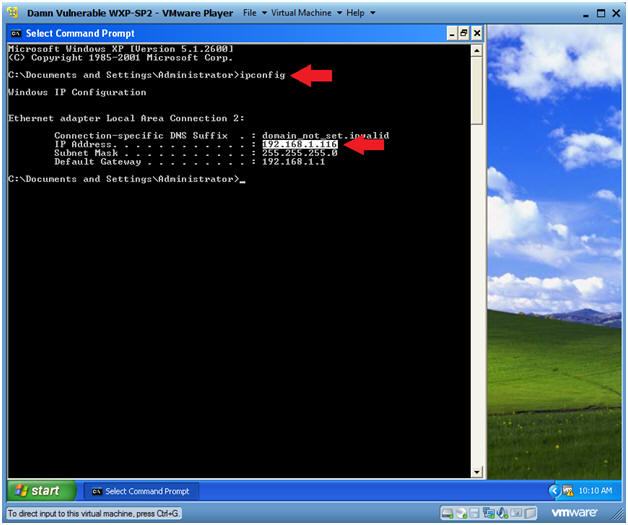
1. Logging into WXP-SP2.
   * **Instructions:**
     1. Username: administrator
     2. Password: Use the Class Password or whatever you set it.



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

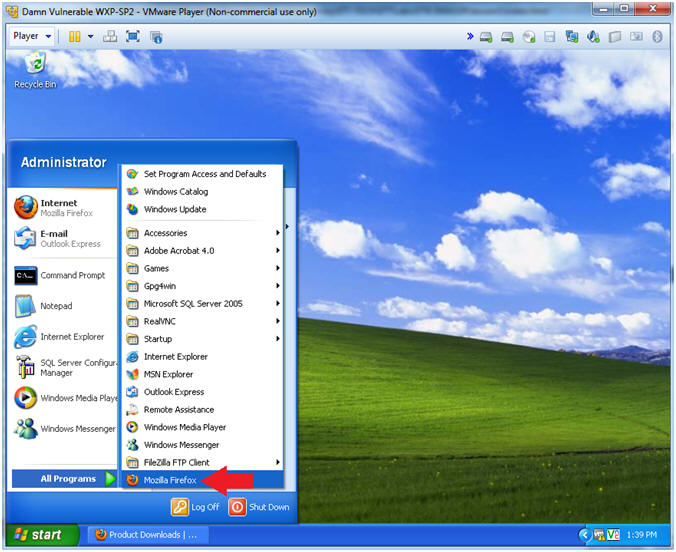


1. Obtain WXP-SP2's IP Address
   * **Instructions:**
     1. ipconfig
   * **Note(FYI)**:
     1. In my case, WXP-SP2's IP Address 192.168.1.116.
     2. This is the IP Address of the Victim Machine that will be attacked by Metasploit.
     3. Record your WXP-SP2's IP Address.

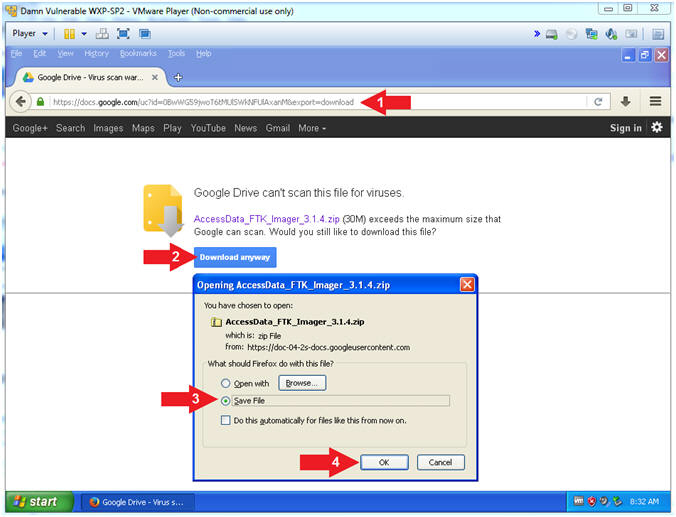
.

**Section 2: Download FTKImager**

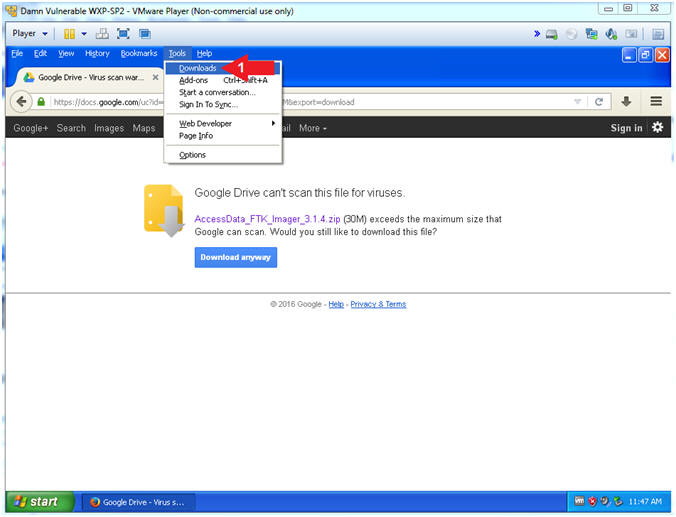
1. Open Firefox
   * **Instructions**:
     1. Start --> All Programs --> Firefox



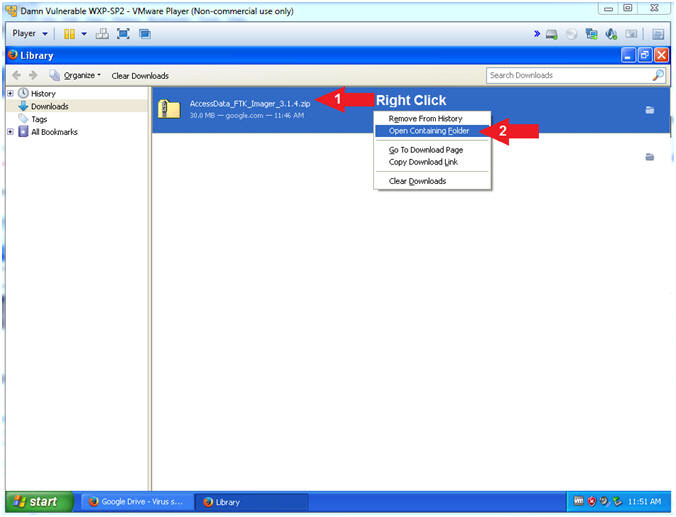
1. Download FTK Imager 3.1.4
   * **Instructions**:
     1. Place the following URL into the address textbox (See Picture)
        + https://docs.google.com/uc?id=0BwWG59jwoT6tMUlSWkNFUlAxanM&export=download
     2. Click **Download anyway**
     3. Select the **Save File** radio button
     4. Click on the **OK** Button
   * **Note(FYI)**:
     1. This lesson is based on FTK Imager 3.1.x.  FTK Imager 3.1.x is no longer downloadable from Access Data.
     2. In order to complete this lesson, FTK Imager 3.1.x has been made available on Google Drive. Accordingly, you**must** comply with Access Data's [License Agreements](http://accessdata.com/company/enduserlicenseagreement).
     3. The latest version of FTK Imager can be found below.
        + <http://accessdata.com/product-download>



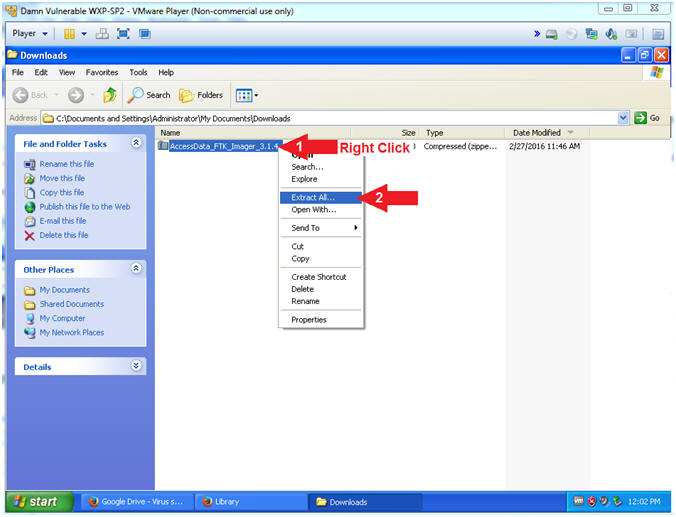
1. Go To Downloads
   * **Instructions**: (On Firefox)
     1. Tools --> Downloads



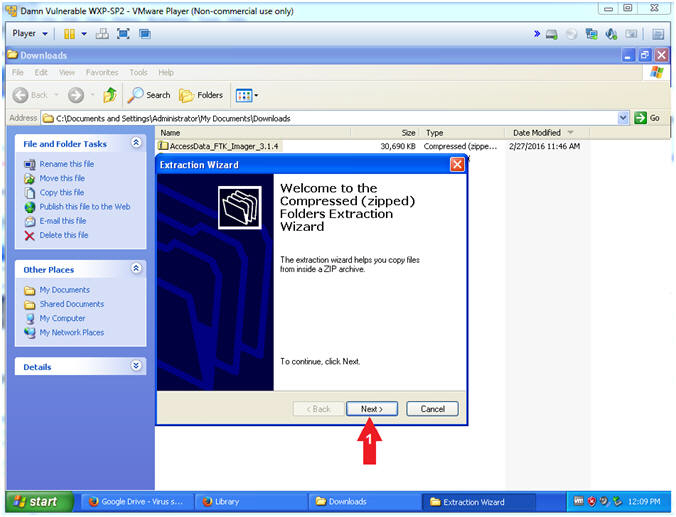
1. Open Containing Folder
   * **Instructions**:
     1. Right Click on the AccessData\_FTK\_Imager\_3.1.4.zip
     2. Select **Open Containing Folder**



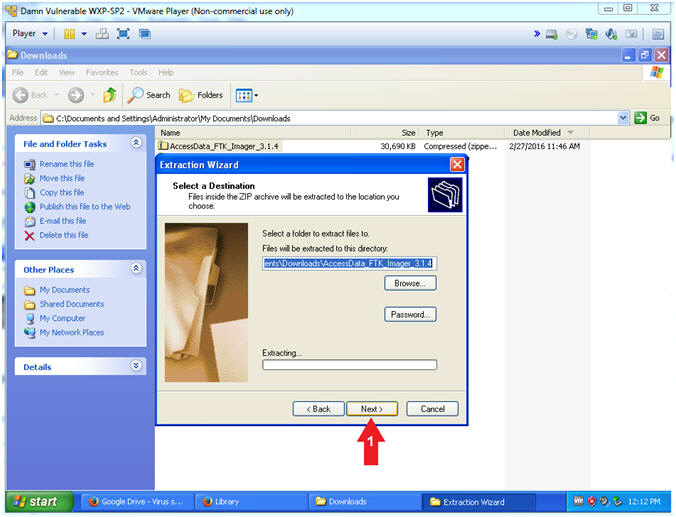
1. Extract Executable
   * **Instructions**:
     1. Right Click on **AccessData\_FTK\_Imager\_3.1.4.zip**
     2. Select **Extract All...**



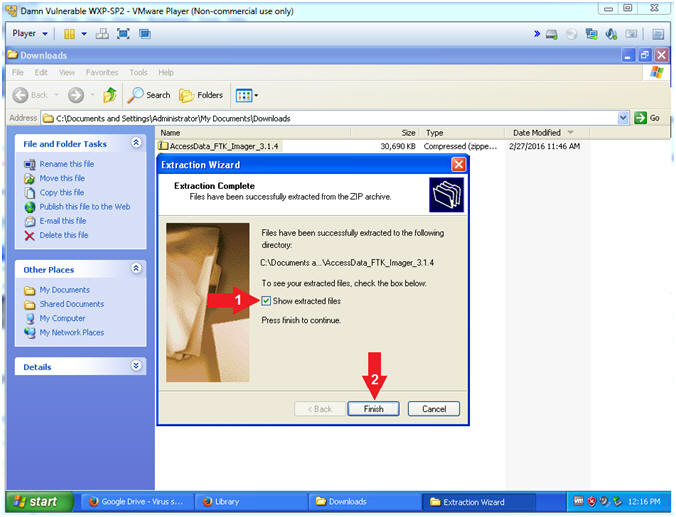
1. Extraction Wizard
   * **Instructions**:
     1. Click **Next**



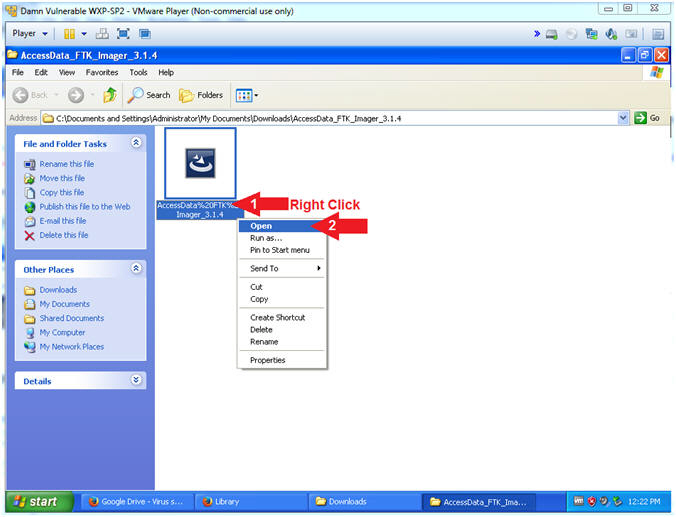
1. Extraction Wizard (Select a Destination)
   * **Instructions**:
     1. Click **Next**



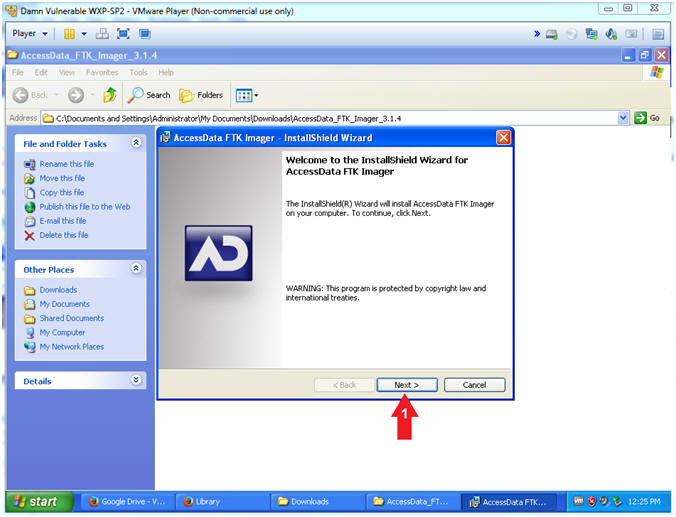
1. Extraction Wizard (Extraction Complete)
   * **Instructions**:
     1. Check **Show extracted files**
     2. Click **Finish**

****

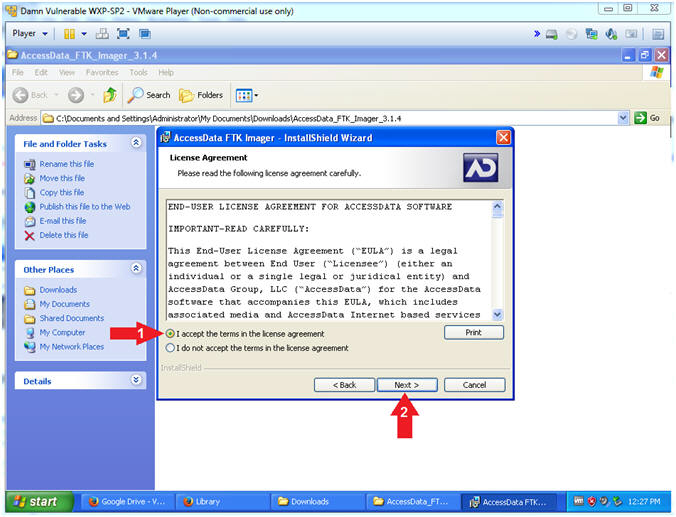
1. Open FTK Imager Executable
   * **Instructions**:
     1. Right Click on the FTK Imager Executable
     2. Select Open



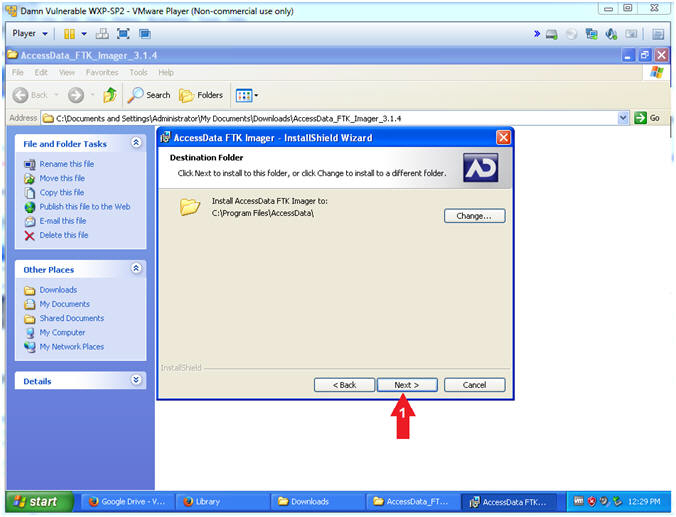
1. AccessData FTK Imager - InstallShield Wizard
   * **Instructions**:
     1. Click the **Next** Button



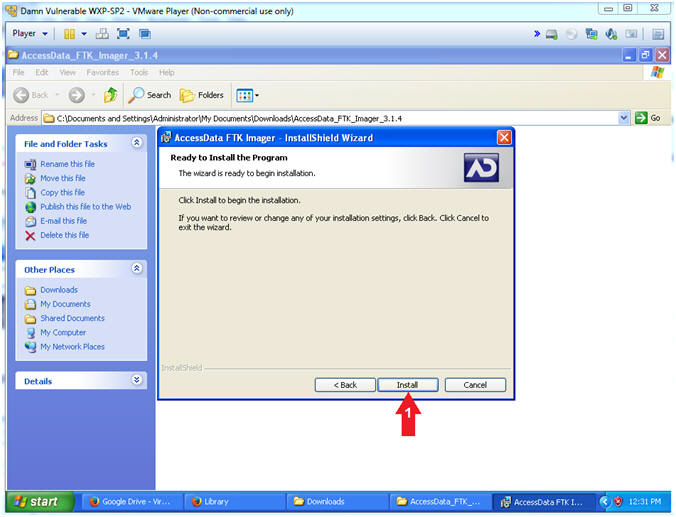
1. AccessData FTK Imager - License Agreement
   * **Instructions**:
     1. Click the "**I accept...**" Radio Button.
     2. Click the **Next** Button



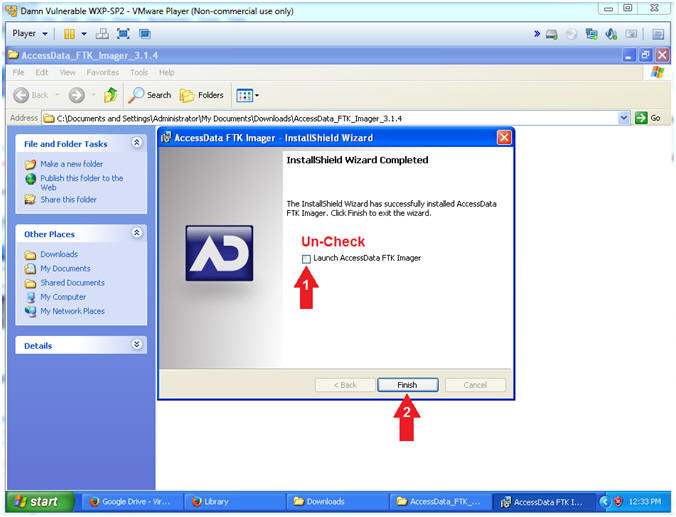
1. AccessData FTK Imager - Destination Folder
   * **Instructions**:
     1. Click the **Next** Button



1. AccessData FTK Imager - Install
   * **Instructions**:
     1. Click the **Install** Button



1. AccessData FTK Imager - Complete
   * **Instructions**:
     1. Un-Check the "Launch AccessData FTK Imager" checkbox.
     2. Click the Finish Button



**Section 3: Proof of Lab**

1. Proof of Lab
   * **Instructions**:
     1. dir "C:\Program Files\AccessData" | findstr "FTK"
     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

