**Progress test 2-2**

**Helix**

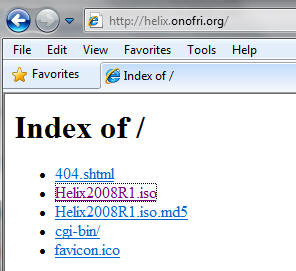
**Getting Started**

**Section 0. Background Information**

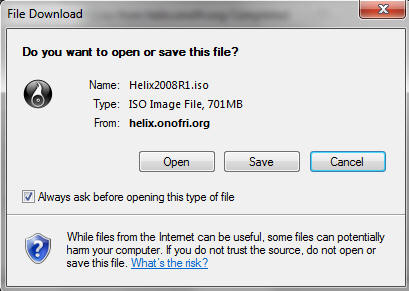
* Helix3 is a Live CD built on top of Ubuntu. It focuses on incident response and computer forensics. According to Helix3 Support Forum, e-fense is no longer planning on updating the free version of Helix.
* See <http://www.e-fense.com/products.php>

**Section 1. Downloading Helix**

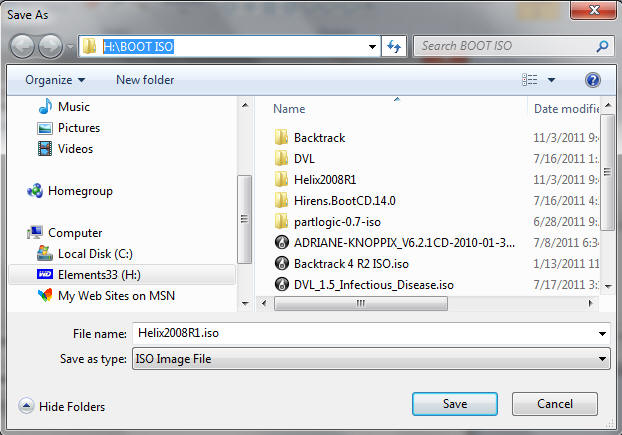
1. On any machine connected to the Internet, bring up a Web Browser.
   * In my case, I am using a Windows Machine that has a USB hard drive attached to it.
2. Go To <http://helix.onofri.org/Helix2008R1.iso>



1. Saving the ISO
   * **Command**:  Click Save

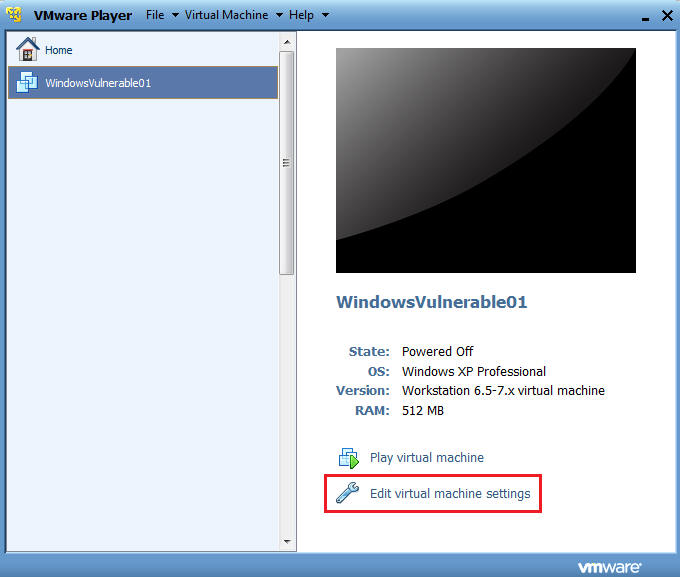


1. Saving ISO to a location
   * **Instruction**: It's up to you where you want to save the file.  In my case, I will save the ISO to H:\BOOT ISO

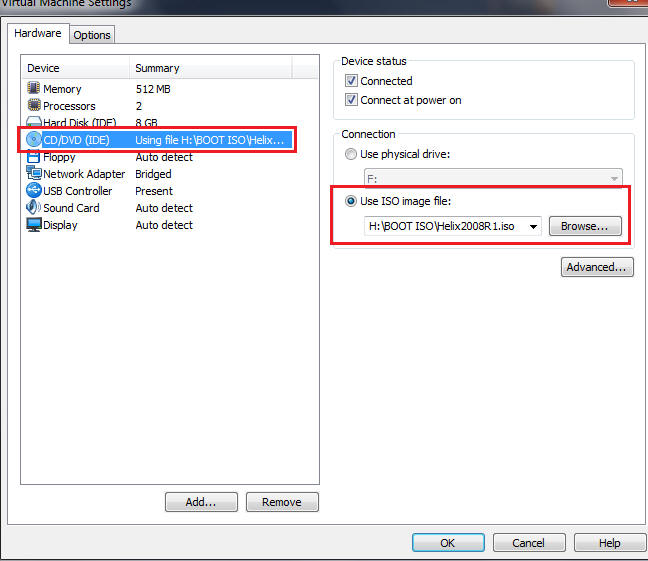


**Section 2. Configure the Windows Virtual Machine to boot up Helix**

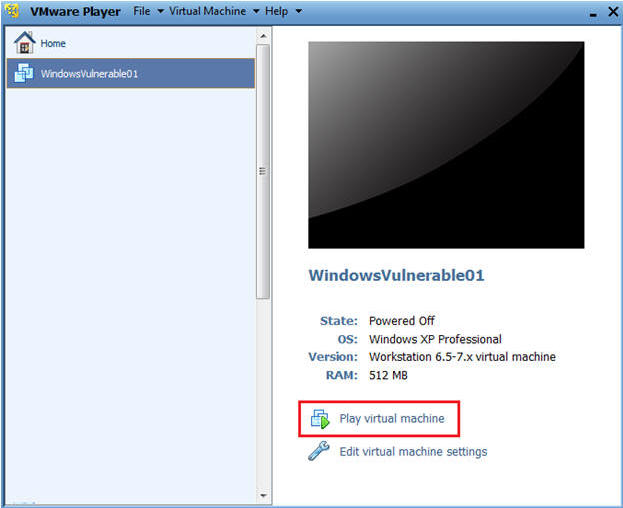
1. Edit the WindowsVulnerable01 virtual machine. (See Below)
   * **Note**: For those of you that don't have access to class material, this can be Windows XP, 2000, 2003 and 7.



1. Configure Windows to boot off of Helix
   * **Instructions**:
     1. Select CD/DVD (IDE)
     2. Select the Use ISO image file
     3. Browse to where you saved the Helix iso.
     4. Note:  In my case, I save it in the following location:
     5. H:\BOOT ISO\Helix2008R1.iso



1. Play the Virtual Machine
   * Select Play Virtual Machine

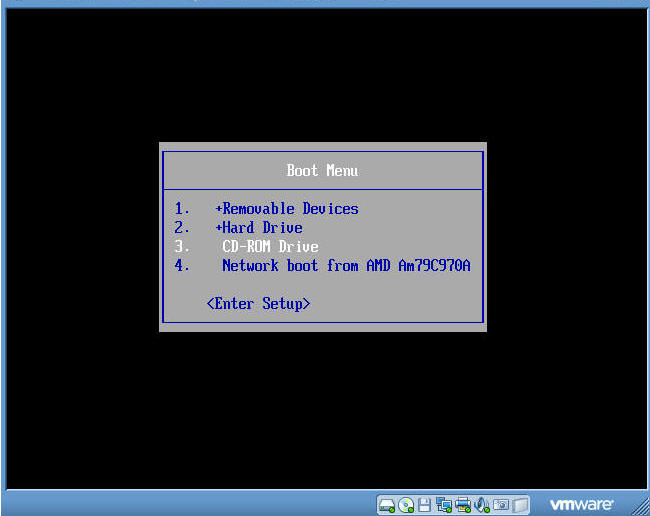


**Section 3. Start Up Helix**

1. Booting from the ISO
   * At the same time, Click the right mouse key and the press the ESC button, when the screen starts to change to the VMware screen below.
   * **Note**: This might take you a few times so be patient!!!



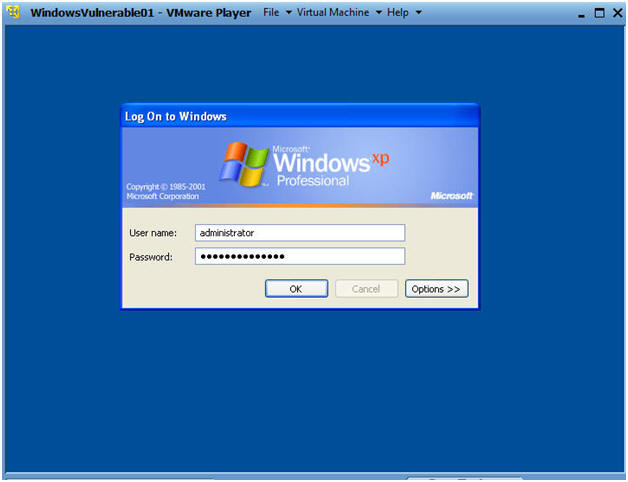
1. Boot Menu Selection
   * **Command**:
     1. Select CD-ROW Drive
     2. Press Enter



1. Booting from Helix Options
   * **Instructions**:
     1. Boot into the Helix Live CD
        + This will take you into a knoppix/linux operating systems.
        + Unfortunately, VMware seems to not allow mouse clicks.
        + In the future, I will experiment with VirtualBox to see if the same issue is present.
     2. Boot from first hard disk
        + Select this option.
        + This will allow you to run the Helix CD from Windows.



1. Log into your Windows Machine
   * **Instructions**:
     1. Its probably a good idea to long in with an administrator account to ensure you can run the Helix CD.

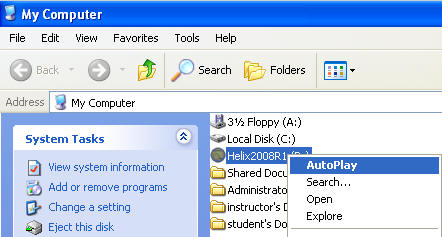
.

**Section 4. Start Up Terminal Window**

1. Open Up My Computer
   * **Command**:  Start --> My Computer



1. Starting Up Helix
   * **Command**:
     + Right Click on Helix2008R1
     + Click on AutoPlay

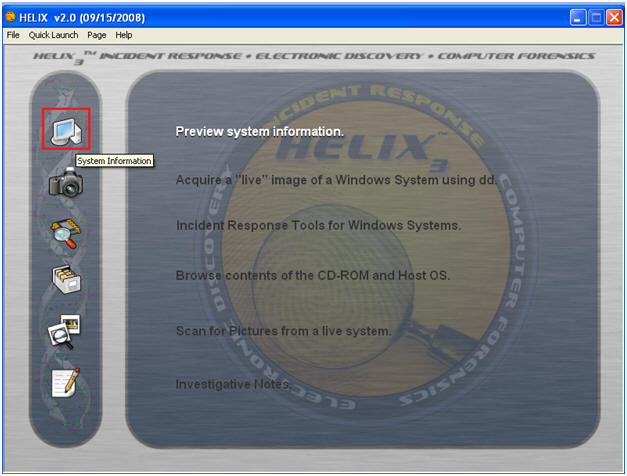


1. Select Language
   * **Command**:
     + Select English
     + Click Accept

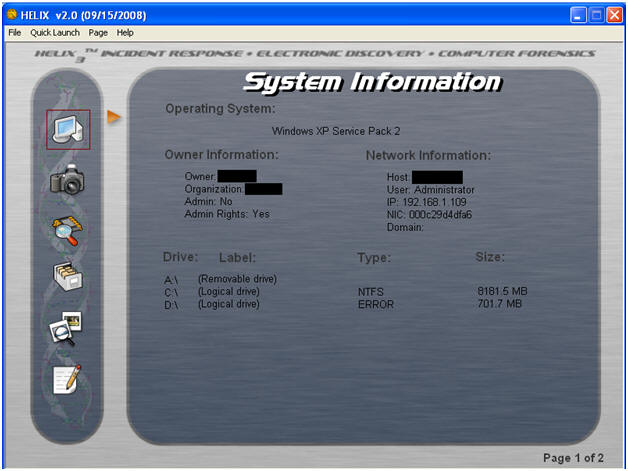


**Section 5. Preview system information**

1. Preview system information
   * **Command**: Select System Information

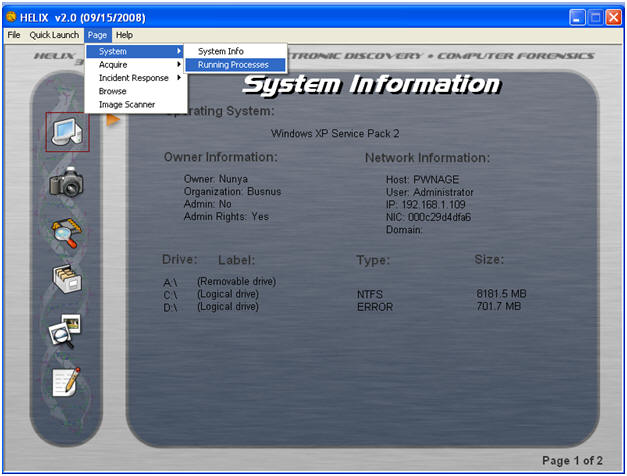


1. Review System Information
   * **Note**: The basic system information is included here like hostname, owner, organization, IP address, NIC, and drives.

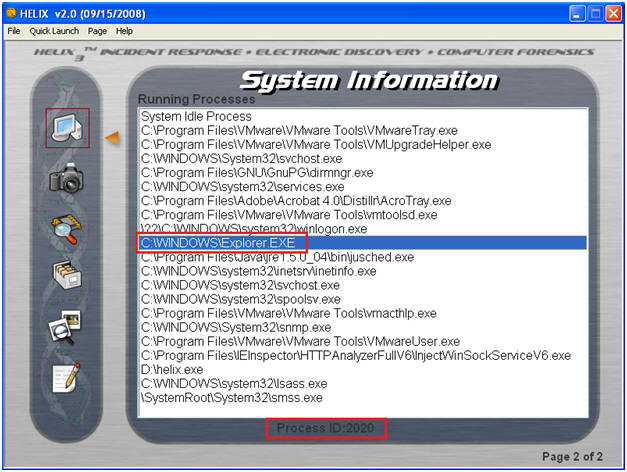


**Section 6. Preview Running Processes**

1. Preview Running Processes
   * **Command**: Select: Page --> System --> Running Processes

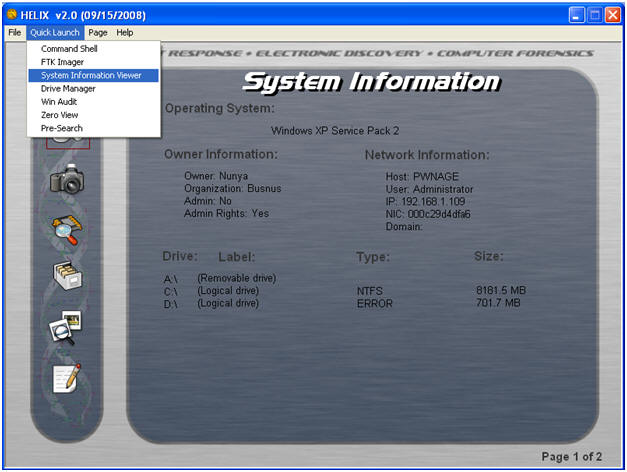


1. View a Process ID (PID)
   * **Command**: Select any process.
   * **Note**: The Process ID number is displayed down low.



**Section 7. System Information Viewer Running Processes**

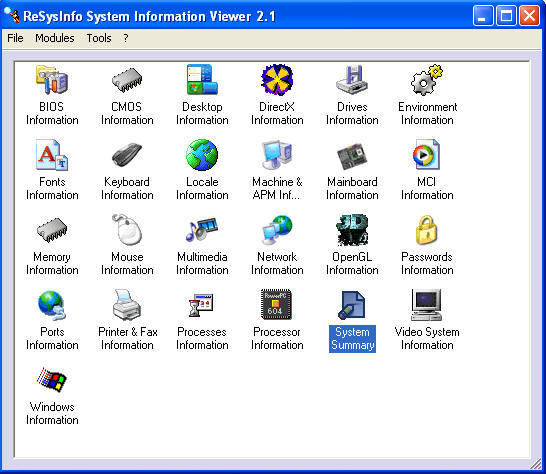
1. Preview Running Processes
   * **Command**: Select: Quick Launch --> System Information Viewer



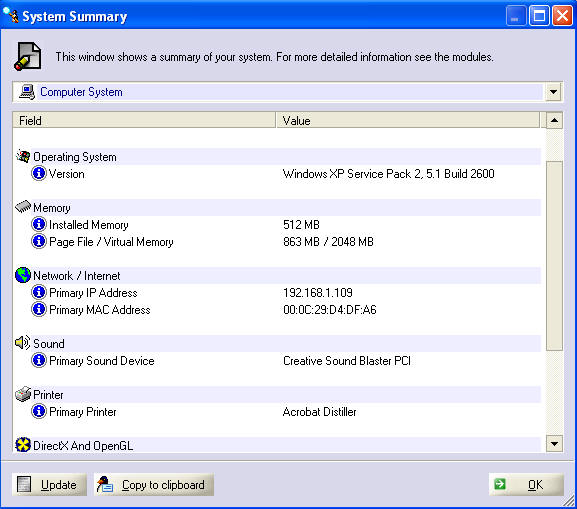
1. Select Yes



1. ReSysInfo System Information Viewer 2.1
   * **Command**: Select System Summary

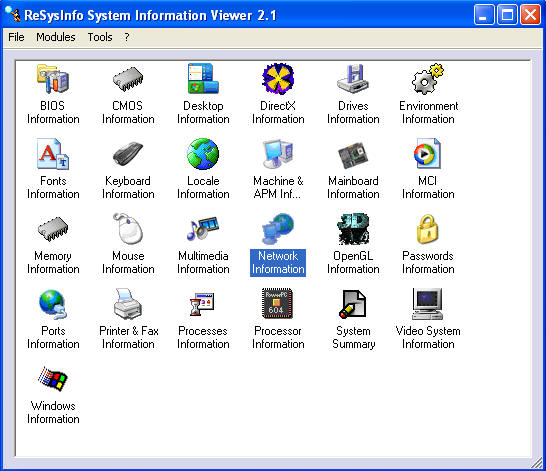


1. System Summary View
   * **Note**: This is another view that show basic system information.  Notice you have the ability to copy to this system information to the clipboard.

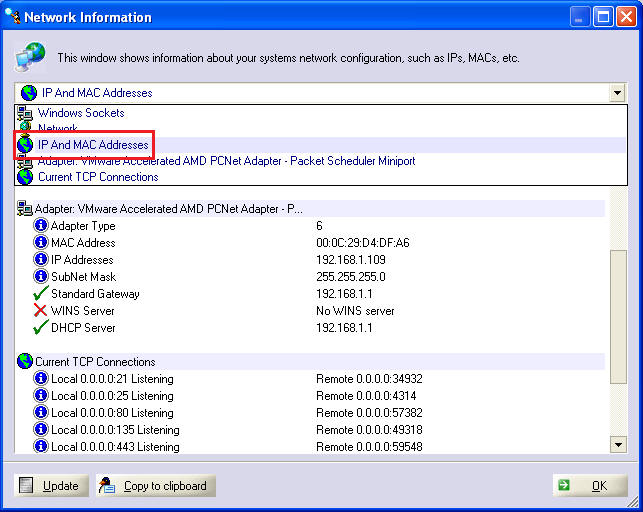


**Section 8. View Network Information**

1. Network Information
   * **Command**: Select Network Information



1. View IP and MAC Information
   * **Command**: Select IP And MAC Address
   * **Proof of Lab**: Cut and Paste a screen shot into a word document and upload to Moodle.



**Section: Proof of Lab**5

1. Cut and Paste a screen shot found in Section 8, Step 2 in a word and upload to Moodle.