**Helix**

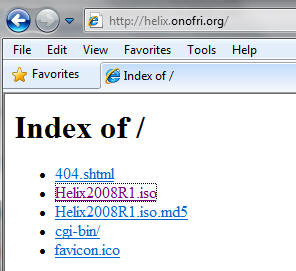
**Install Helix Linux Image to Hard drive**

**Section 0. Background Information**

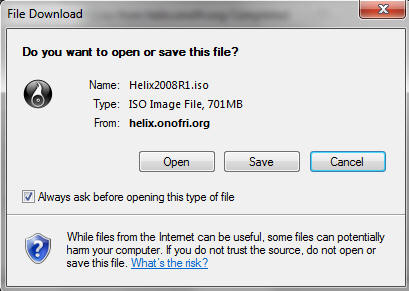
* Helix3 is a Live CD built on top of Ubuntu. It focuses on incident response and computer forensics. According to Helix3 Support Forum, e-fense is no longer planning on updating the free version of Helix.
* See <http://www.e-fense.com/products.php>

**Section 1. Downloading Helix**

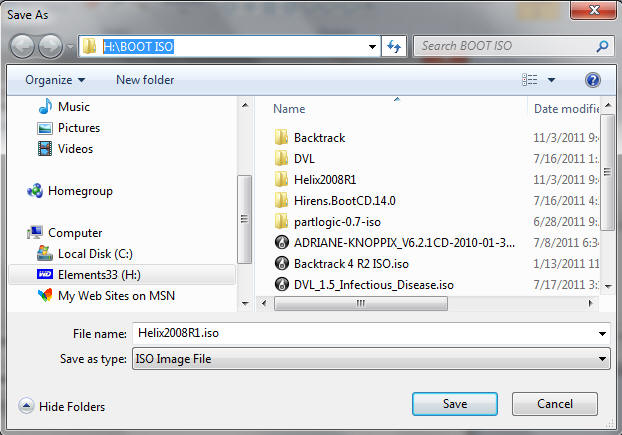
1. On any machine connected to the Internet, bring up a Web Browser.
   * In my case, I am using a Windows Machine that has a USB hard drive attached to it.
2. Go To <http://helix.onofri.org/Helix2008R1.iso>



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

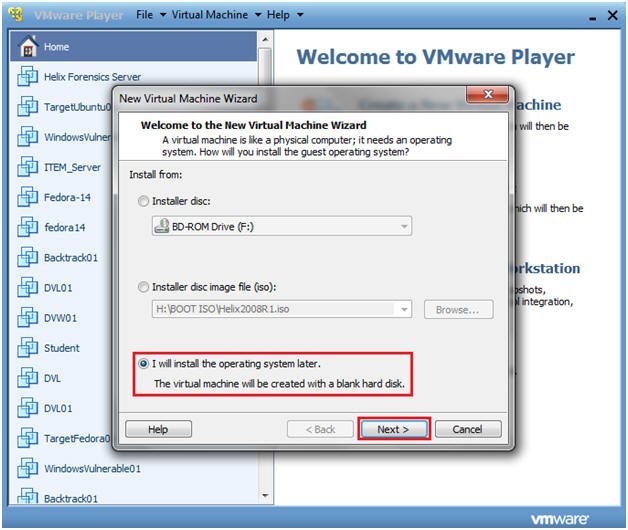


**Section 2. Create a New Virtual Machine**

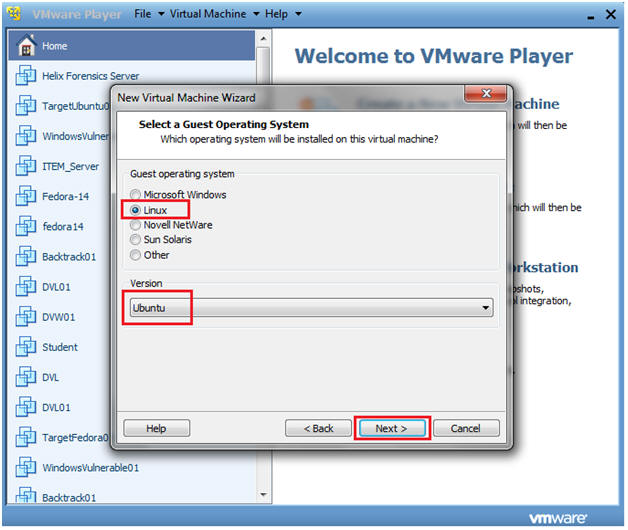
1. Create a New Virtual Machine
   * **Command**: Click on "Create a New Virtual Machine"



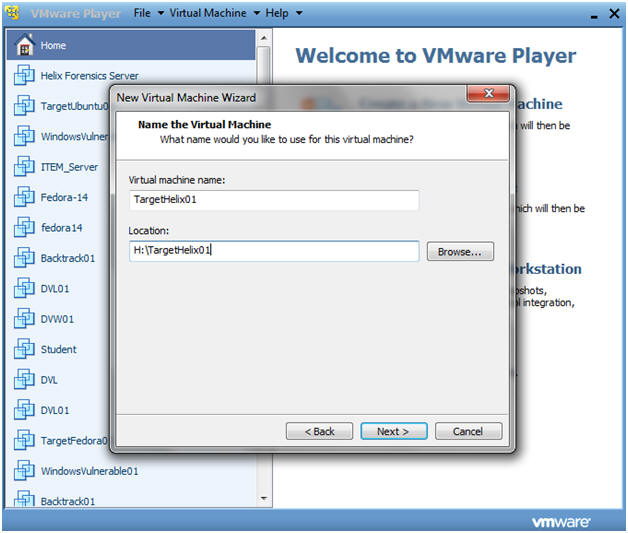
1. New Virtual Machine Wizard
   * **Instructions**:
     1. Click on the "I will install the operating system later" radio button.
     2. Click Next.



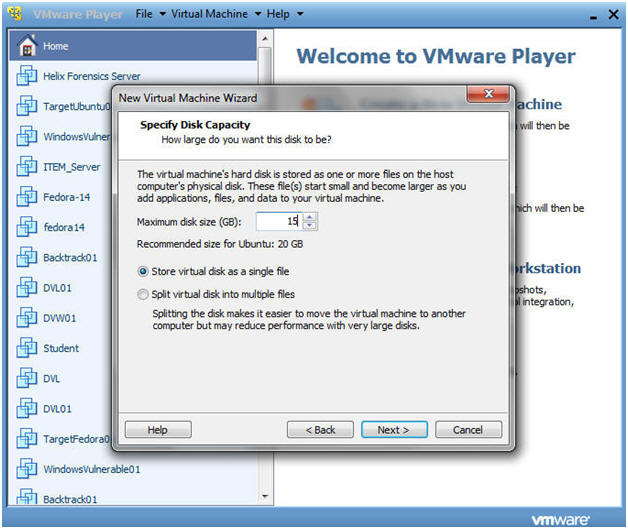
1. Customer Operating System and Version
   * **Instructions**:
     1. Guest operating system: Linux
     2. Version: Ubuntu
     3. Click Next.



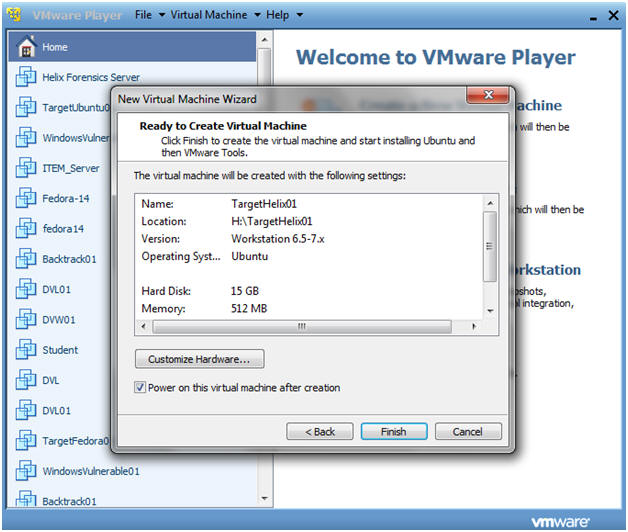
1. Personalize Linux
   * **Instructions**:
     1. Virtual machine name: TargetHelix01
        + Note: Name it whatever you like.
     2. Location: H:\TargetHelix01
        + Note: If you can, save this image to a USB Hard drive.
     3. Click Next.



1. Personalize Linux
   * **Instructions**:
     1. Maximum disk size (GB): 15
        + Note: You can make this a little as 3.5 GB.  It really depends if you instead on analyzing images with Autopsy.
     2. Click on the "Store virtual disk as a single file"
     3. Click Next.



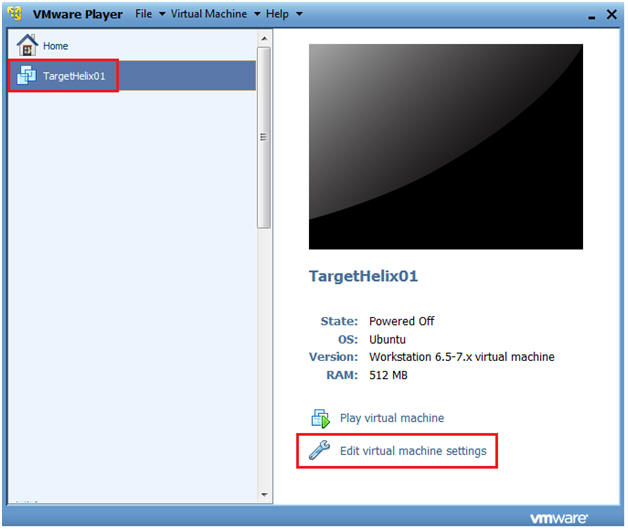
1. Personalize Linux
   * **Instructions**:
     1. Click Finished
   * **Note**:
     1. Helix will now boot off of the Helix2008R1.iso.



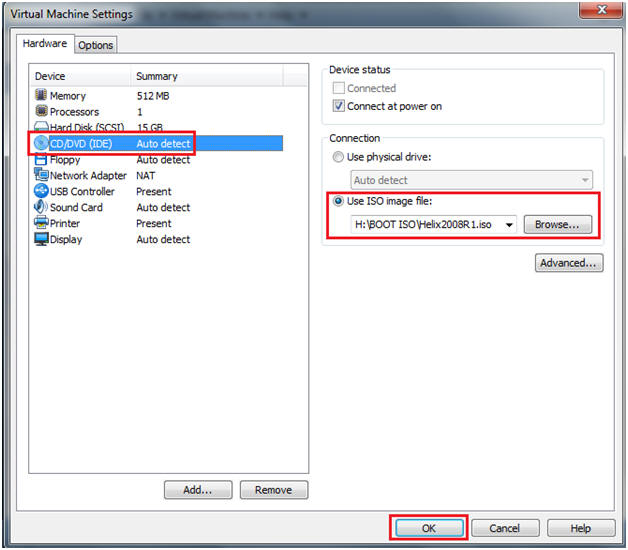
**Section 3. Install Helix to the Hard drive (Part 1)**

* **Warning**:  Step 10 will fail.  Unfortunately, you will have to go through the install steps twice, due to an os-prober issue that has trouble seeing the logical volumes.  So, don't get frustrated and just follow along step by step.

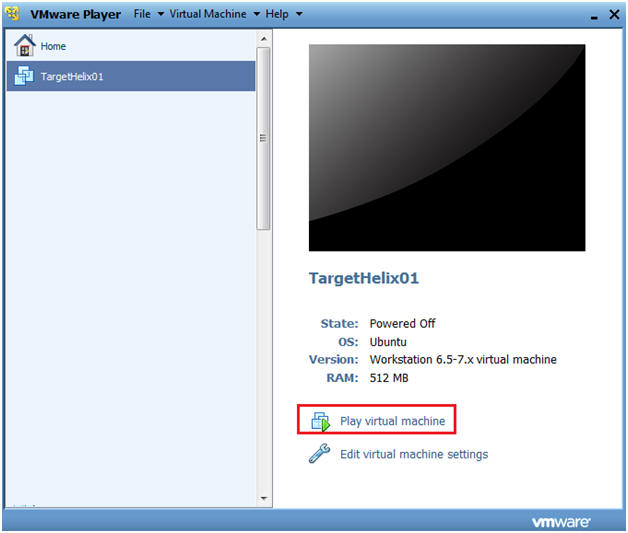
1. Edit TargetHelix01 Virtual Machine
   * **Command**: Click Edit virtual machine settings



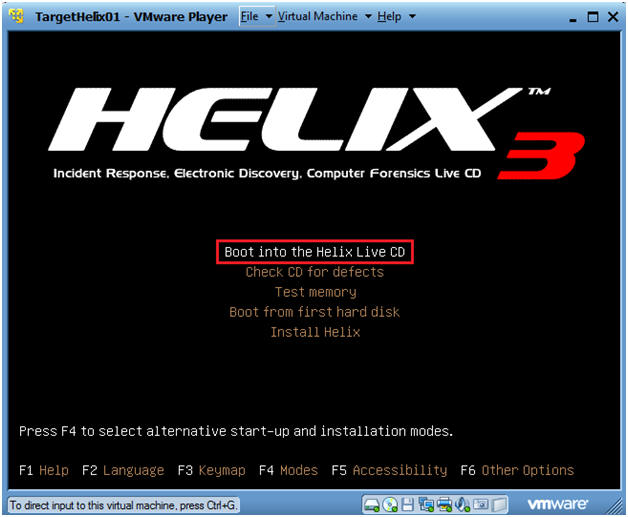
1. Virtual Machine Settings
   * **Command**:
     1. Select CD/DVD (IDE)
     2. Select the "Use ISO image file:" radio button.
     3. Browse to where you saved the Helix2008R1.iso
     4. Select OK.



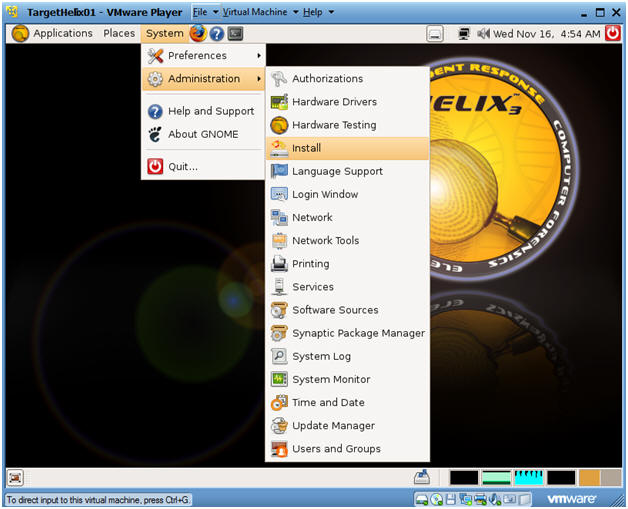
1. Booting from Helix Options
   * **Instructions**:
     1. Select TargetHelix01
     2. Play Virtual Machine



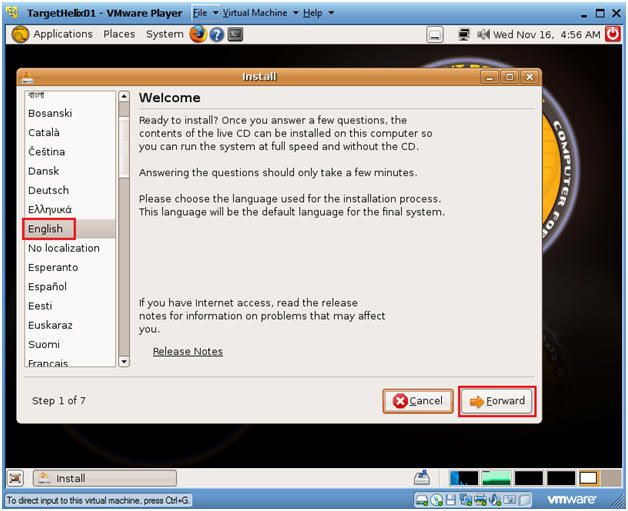
1. Boot into the Helix Live CD
   * **Command**:
     1. Arrow Down to "Boot into the Helix Live CD"
     2. Press Enter



1. Install to Hard drive (Part 1)
   * **Instructions**:
     1. System --> Administration --> Install



1. Language Selection
   * **Instructions**:
     1. English
     2. Forward



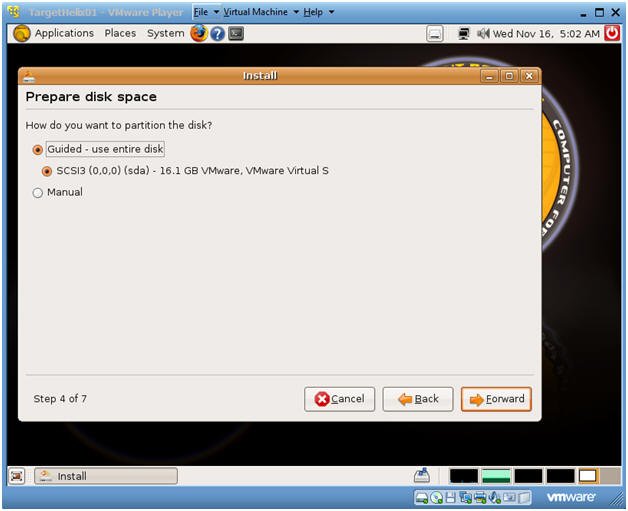
1. Timezone Selection
   * **Instructions**:
     1. Select City: Chicago
     2. Forward



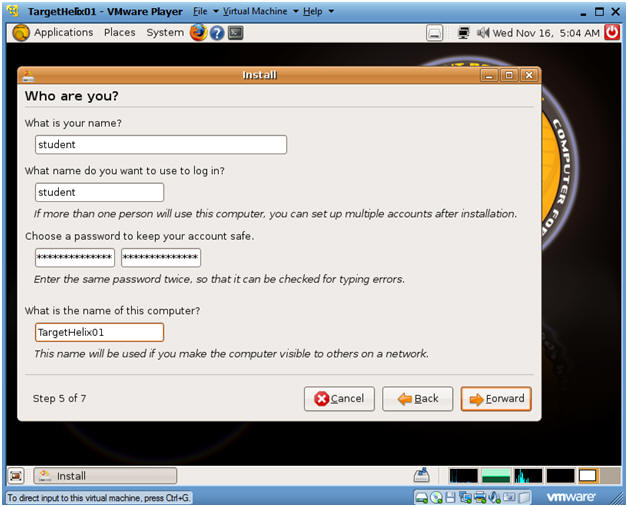
1. Keyboard layout
   * **Instructions**:
     1. Which layout is most similar to your keyboard? USA
     2. USA
     3. Forward



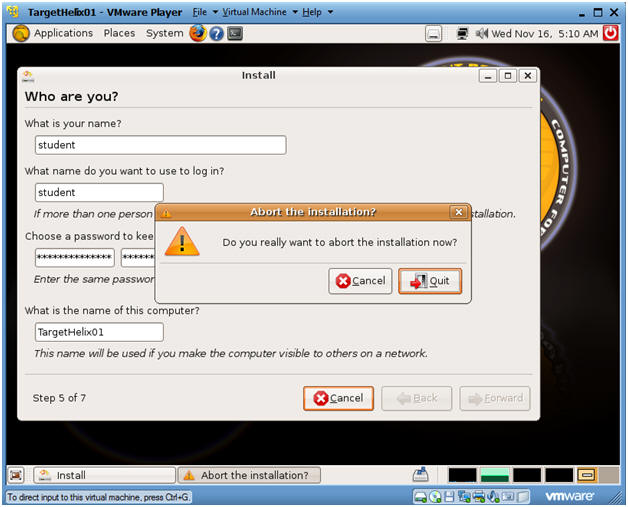
1. Prepare disk space
   * **Instructions**:
     1. Make sure Guided - use entire disk is selected.
     2. Forward



1. Who are you?
   * **Instructions**:
     1. What is your name? student
     2. What name do you want to use to log in? student
     3. Choose a password
     4. What is the name of this computer? TargetHelix01
     5. Forward
   * **Warning Instructions**:
     1. After pressing forward the os-prober will fail because it cannot the volume groups.
     2. Click Cancel
        + I realize you are saying what the hell, but please continue to follow along to get Helix to install to disk.

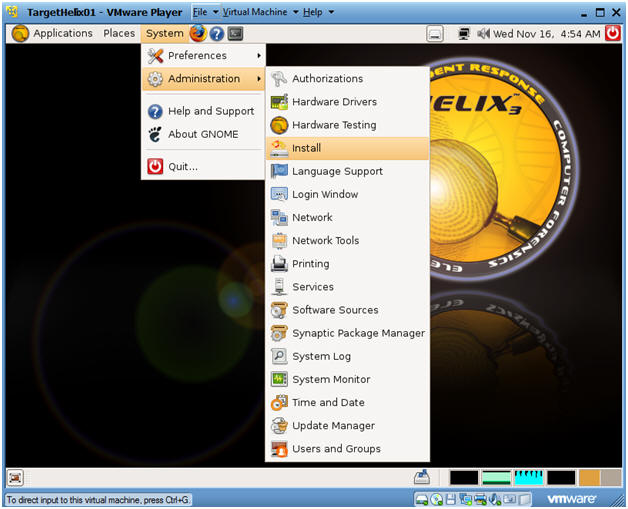


1. Abort the installation?
   * **Instructions**:
     1. Click on Quit
   * **Notes**: I know this sounds crazy, but continue to Section 4.

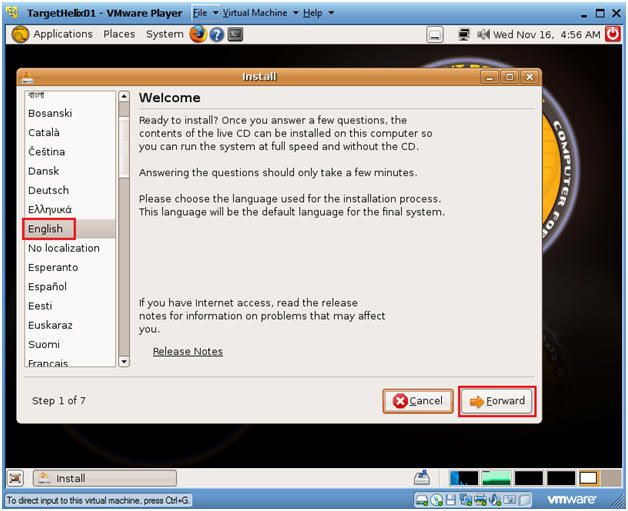


**Section 4. Install Helix to the Hard drive (Part 2)**

1. Install to Hard drive (Part 2)
   * **Instructions**:
     + System --> Administration --> Install



1. Language Selection
   * **Instructions**:
     + English
     + Forward



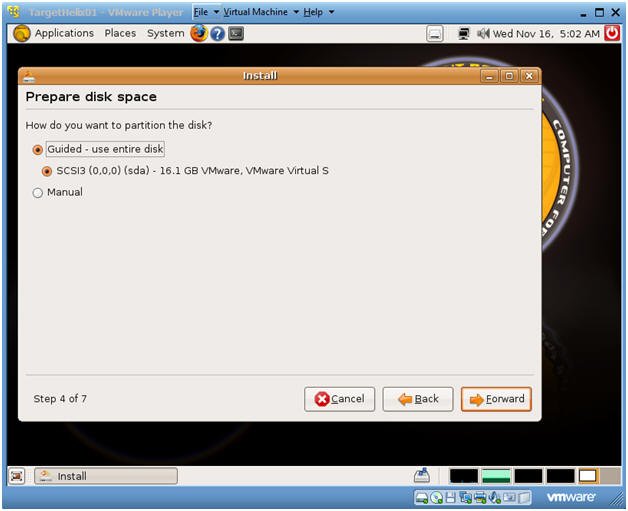
1. Timezone Selection
   * **Instructions**:
     + Select City: Chicago
     + Forward



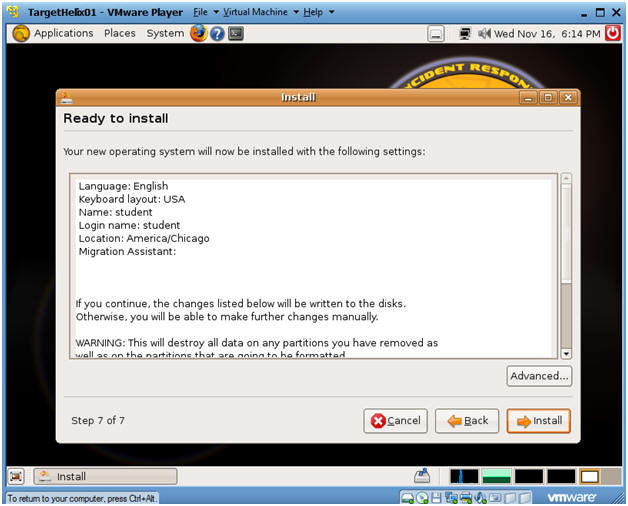
1. Keyboard layout
   * **Instructions**:
     + Which layout is most similar to your keyboard? USA
     + USA
     + Forward



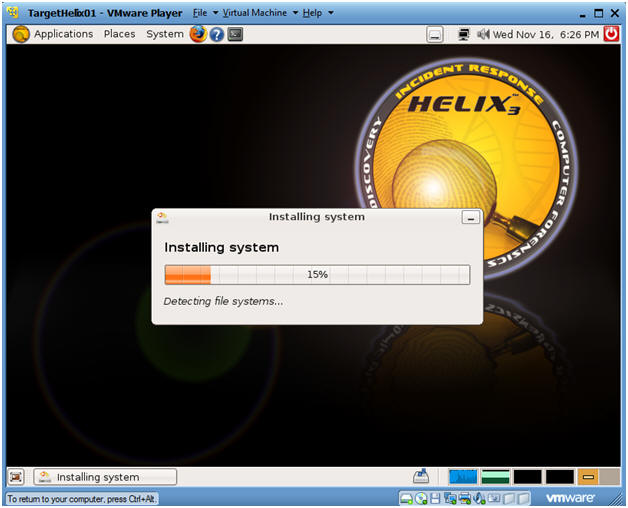
1. Prepare disk space
   * **Instructions**:
     + Make sure Guided - use entire disk is selected.
     + Forward



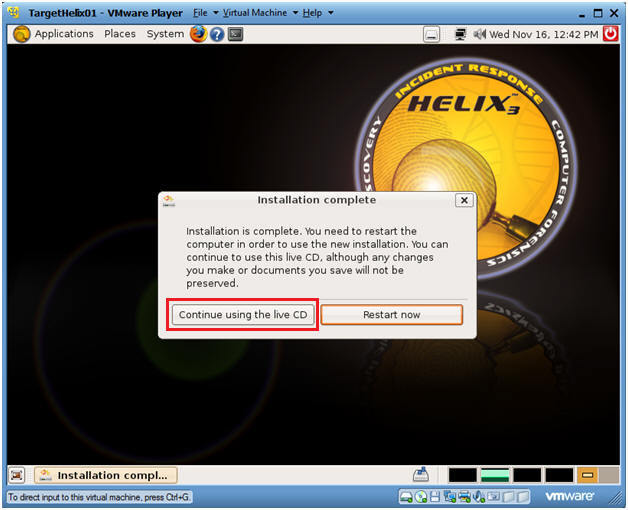
1. Ready to Install
   * **Instructions**:
     + Click Install
   * **Side Note**:
     + See, I am not crazy, it works a second time.  BTW, I discovered this trick by scavenging through many of websites and blogs.



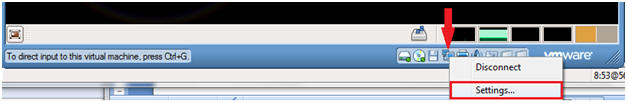
1. Installing system
   * **Side Note**:  This process will take between 10 to 20 minutes.



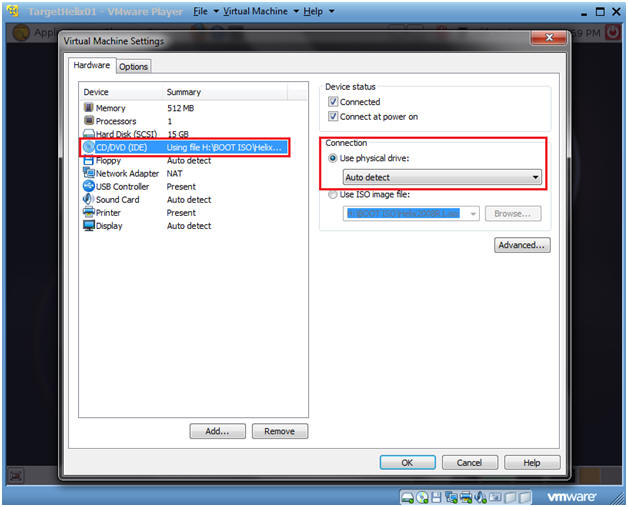
1. Post Installation
   * **Command**:  Click on Continue using the Live CD



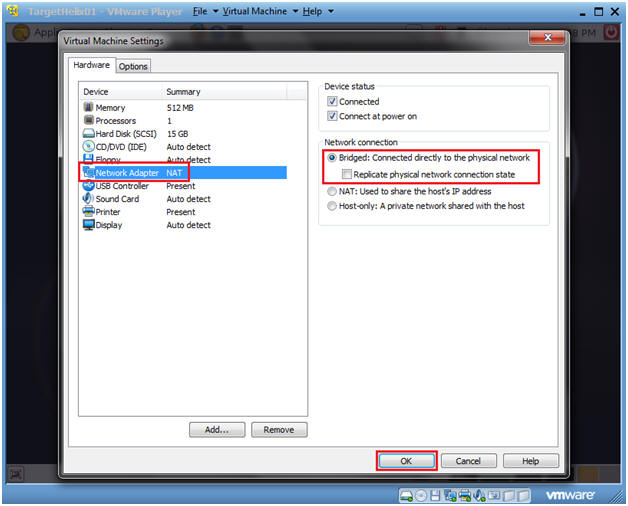
1. Adjust VMware Settings (For VMWare Only, See Below)
   * **Command**:  Click on VMware Settings.



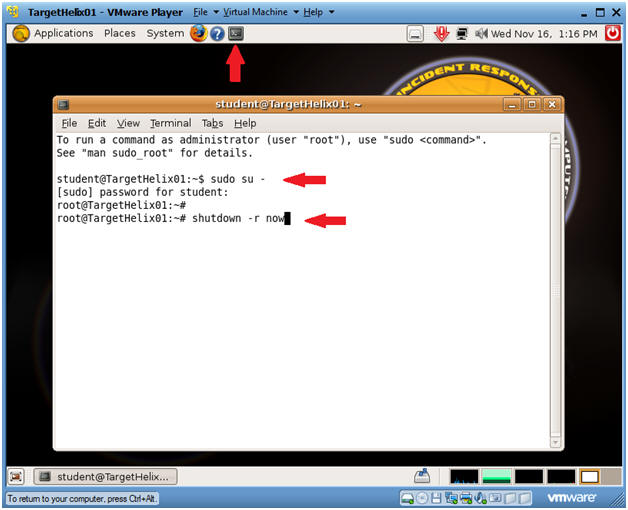
1. Change Physical Drive (For VMWare Only, See Below)
   * **Command**:
     + Select CD/DVD (IDE)
     + Select the "Use physical drive:" Connection radio button.



1. Change Network Adapter (For VMWare Only, See Below)
   * **Command**:
     + Select Network Adapter NAT
     + Select the "Bridged: Connected directly to the physical network" Network Connection radio button.

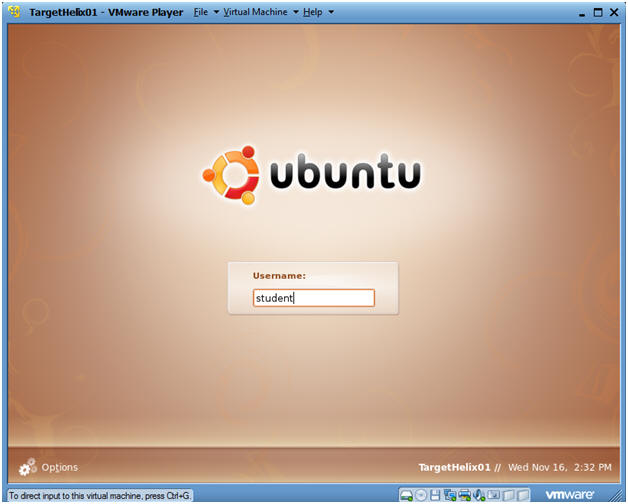


1. Consistency Reboot
   * **Command**:
     + Click on the Terminal Console
     + sudo su -
     + shutdown -r now

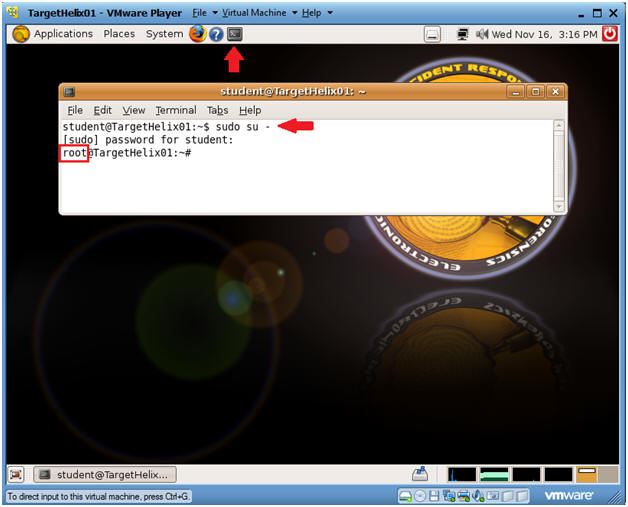


**Section 5. Logging Into TargetHelix01**

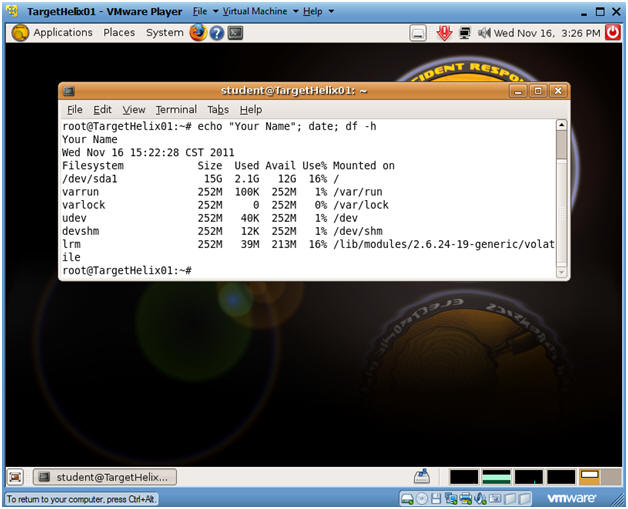
1. Preview system information
   * **Command**:
     1. Login with your the username and password you created earlier.
     2. In my case, I create a username called "student".



1. How to become root
   * **Command**:
     1. sudo su -
     2. Enter your current password for the account your logged in as.



1. Proof of Lab
   * **Command**:
     1. echo "Your Name"; date; df -h
     2. Do an Alt PrtScn (Print Screen)
     3. Cut and Paste into a Word Document
     4. Upload to Moodle.



**Section: Proof of Lab**

1. Cut and Paste a screen shot found in Section 5, Step 3 in a word and upload to Moodle.