**Progress test 2-1**

**Volatility: Lesson 1**

**Installing Volatility on BackTrack 5 R1**

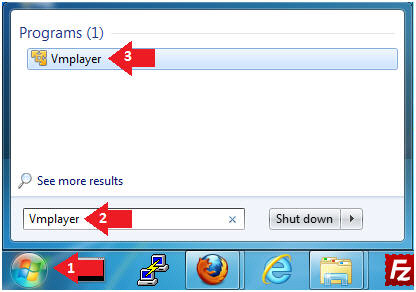
**Section 0. Background Information**

1. **Volatility Overview**
   * <https://www.volatilesystems.com/>
   * The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offer unprecedented visibility into the runtime state of the system. The framework is intended to introduce people to the techniques and complexities associated with extracting digital artifacts from volatile memory samples and provide a platform for further work into this exciting area of research.
2. **Pre-Requisite Lesson**
   * Installing BackTrack 5 R1

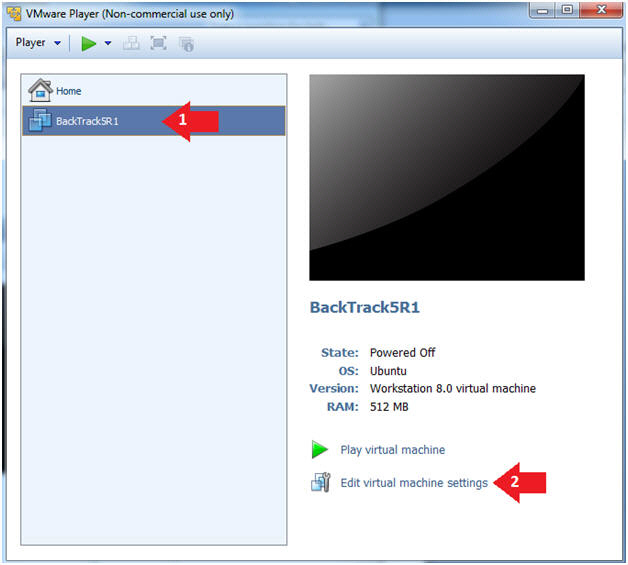
1. **Lab Notes**
   * In this lab we will do the following:
     1. Download Volatility 2.0
     2. Un-Tar Volatility 2.0
     3. Test Volatility 2.0
2. **Next Lesson**
   * [Helix: Lesson 4: Dump Window's Physical Memory Using NetCat to BackTrack](http://www.computersecuritystudent.com/FORENSICS/HELIX/lesson4/index.html)
3. **Capabilities**
   * The Volatility Framework currently provides the following extraction capabilities for memory samples
     1. Image date and time
     2. Running processes
     3. Open network sockets
     4. Open network connections
     5. DLLs loaded for each process
     6. Open files for each process
     7. Open registry handles for each process
     8. A process' addressable memory
     9. OS kernel modules
     10. Mapping physical offsets to virtual addresses (strings to process)
     11. Virtual Address Descriptor information
     12. Scanning examples: processes, threads, sockets, connections, modules
     13. Extract executables from memory samples
     14. Transparently supports a variety of sample formats (ie, Crash dump, Hibernation, DD)
     15. Automated conversion between formats

**Section 1: Login to BackTrack**

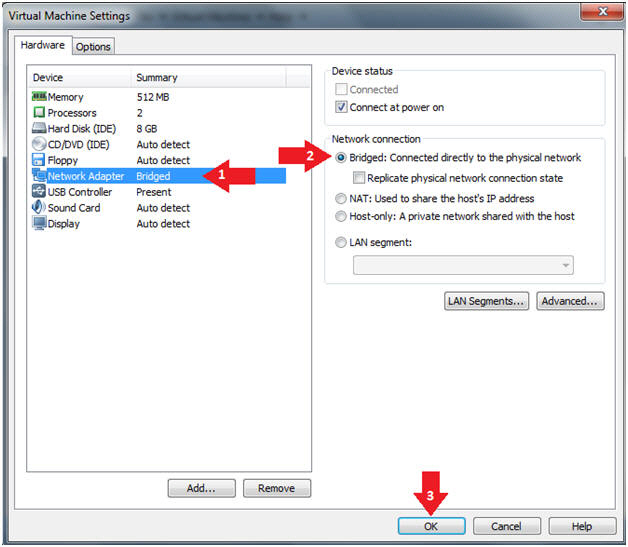
1. Start Up VMWare Player
   * **Instructions:**
     1. Click the Start Button
     2. Type Vmplayer in the search box
     3. Click on Vmplayer



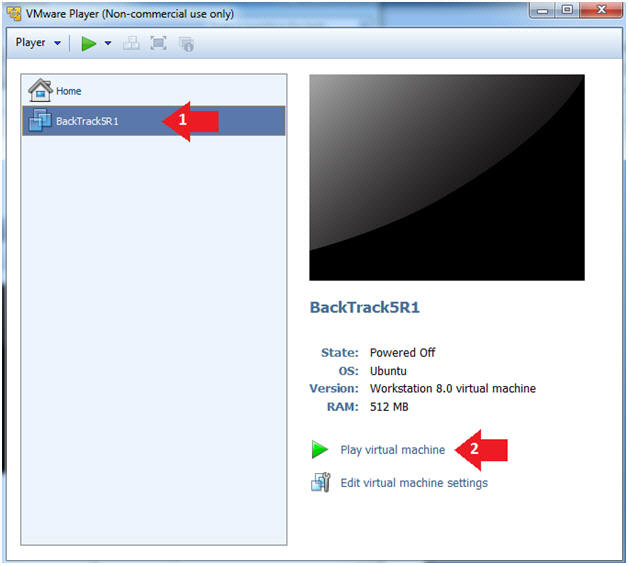
1. Edit the BackTrack5R1 VM
   * **Instructions:**
     1. Select BackTrack5R1 VM
     2. Click Edit virtual machine settings



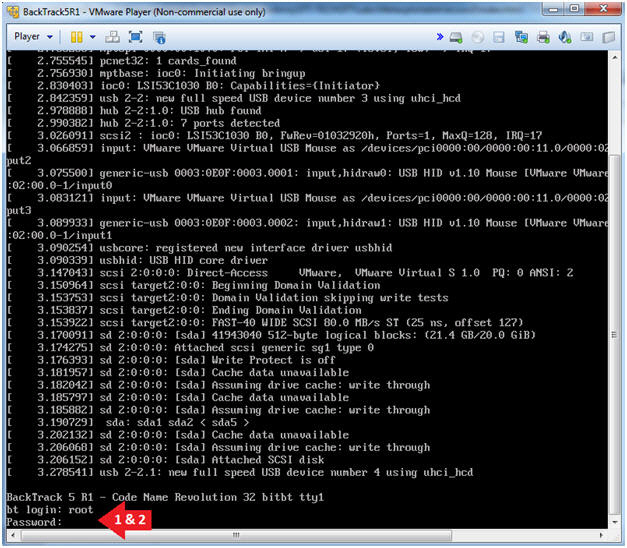
1. Edit Virtual Machine Settings
   * **Instructions:**
     1. Click on Network Adapter
     2. Click on the Bridged Radio button
     3. Click on the OK Button



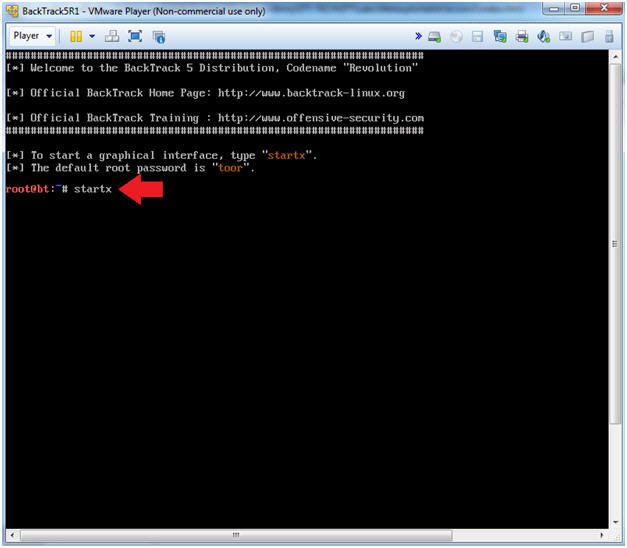
1. Play the BackTrack5R1 VM
   * **Instructions:**
     1. Click on the BackTrack5R1 VM
     2. Click on Play virtual machine



1. Login to BackTrack
   * **Instructions:**
     1. Login: root
     2. Password: toor or <whatever you changed it to>.

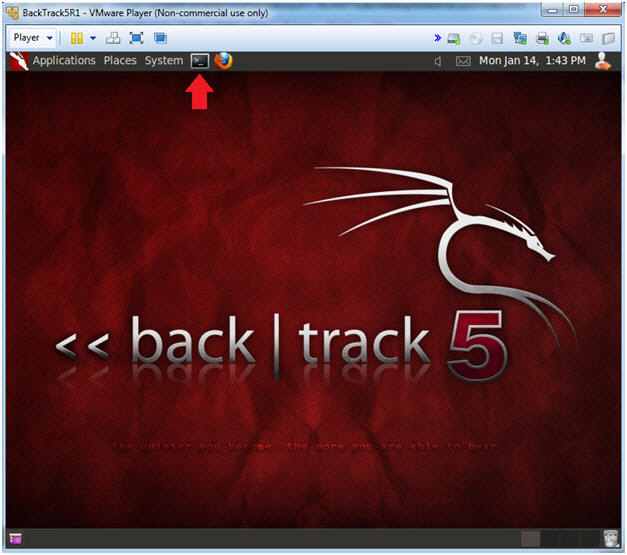


1. Bring up the GNOME
   * **Instructions**:
     1. Type startx

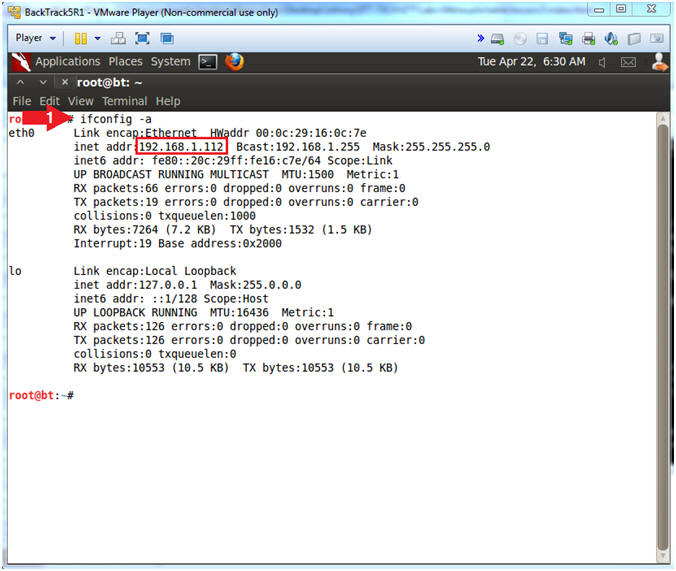


**Section 2: Bring up a console terminal**

1. Start up a terminal window
   * **Instructions**:
     1. Click on the Terminal Window

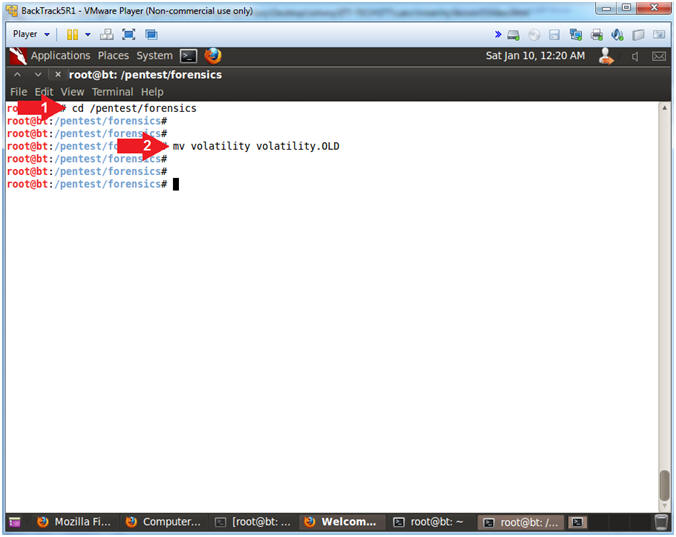


1. Obtain the IP Address
   * **Instructions**:
     1. ifconfig -a
   * **Note(FYI)**:
     1. My IP address **192.168.1.112**.
     2. In your case, it will probably be different.

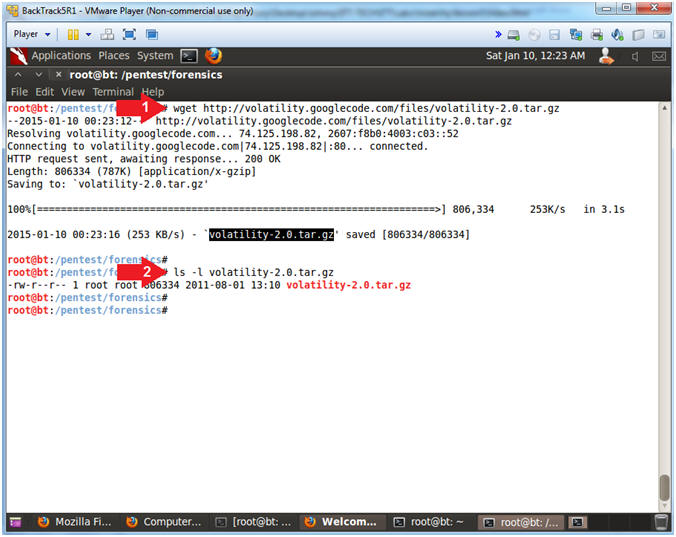


**Section 3: Installing Volatility**

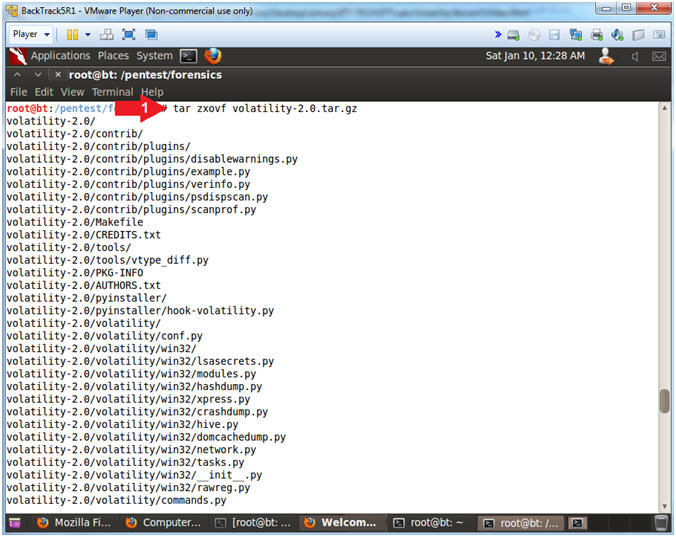
1. Move Old Volatility Instance
   * **Instructions**
     1. cd /pentest/forensics
     2. mv volatility volatility.OLD



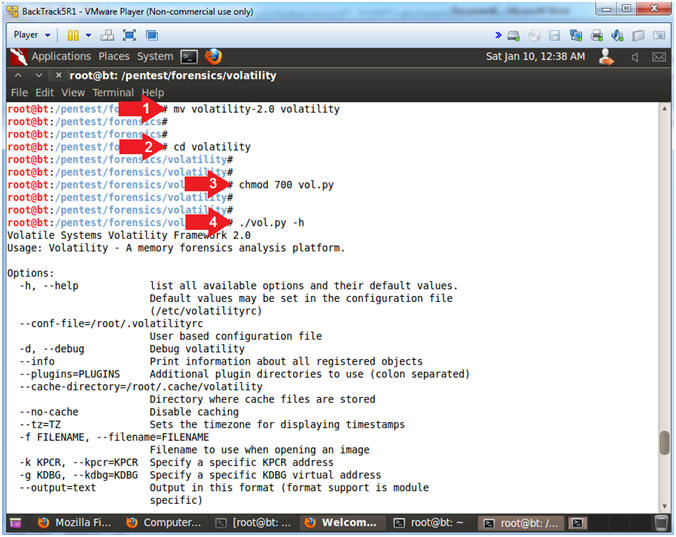
1. Download Volatility 2.0
   * **Instructions**
     1. wget http://volatility.googlecode.com/files/volatility-2.0.tar.gz
        + WGET is a non-interactive downloader.
     2. ls -l volatility-2.0.tar.gz



1. Untar/Uncompress Volatility 2.0
   * **Instructions**
     1. tar zxovf volatility-2.0.tar.gz
   * **Note(FYI)**
     1. tar, stores and extracts files from a tape or disk archive.
        + z(unzip when used with "x"), x(extract), o(keep ownerships), v(verbose), and f(specify archive file)



1. Setup and Test Volatility
   * **Instructions**
     1. mv volatility-2.0 volatility
        + Move volatility 2.0 to the pre-existing volatility Directory
     2. cd volatility
     3. chmod 700 vol.py
        + Give volatility World, Right and Execute User Permissions.
     4. ./vol.py -h
        + Display the volatility help menu



**Section 5: Proof of Lab**

1. Proof of Lab
   * **Instructions**
     1. md5sum vol.py
     2. date
     3. echo "Your Name"
        + Put in your actual name in place of "Your Name"
        + e.g., echo "John Gray"
   * **Proof of Lab Instructions**
     1. Press the <Ctrl> and <Alt> key at the same time.
     2. Press the <PrtScn> key.
     3. Paste into a word document
     4. Upload to Moodle

