DIGITAL FORENSICS LAB SERIES

Lab 15: Memory Analysis

Objective - Digital Forensics Fundamentals

Document Version: 2014-02-07 (Beta)

(DF613, DF268)

Organization: Moraine Valley Community College
Authors: Jesse Varsalone and Kevin Vaccaro

The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

Contents

Introduction

This lab is part of a series of lab exercises intended to support courseware for Forensics training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, students will utilize various methods to determine if an attacker attempted a breach or successfully compromised a system. Some information about the attacker, such as his IP address, may be lost if the machine is shutdown. For this reason, an investigator collects volatile data before shutting down a system.

This lab includes the following tasks:

1. Obtaining a Dump of Physical Memory Using DumpIt
2. Using Volatility to Analyze Processes
3. Attacking the Victim System with Armitage
4. Using Volatility to Determine Remote Connections

Objective: Extract Physical Memory and Analyze its Contents

Memory analysis is a new and growing field in forensics. RAM captures much of the data that the hard drive does not capture. The proper tool can extract passwords and hidden processes from a live running machine. This information can aid the investigator or incident response person during an investigation into computer crimes and malware infections.

DumpIt – generates a copy of the system's physical memory and saves it as a file.

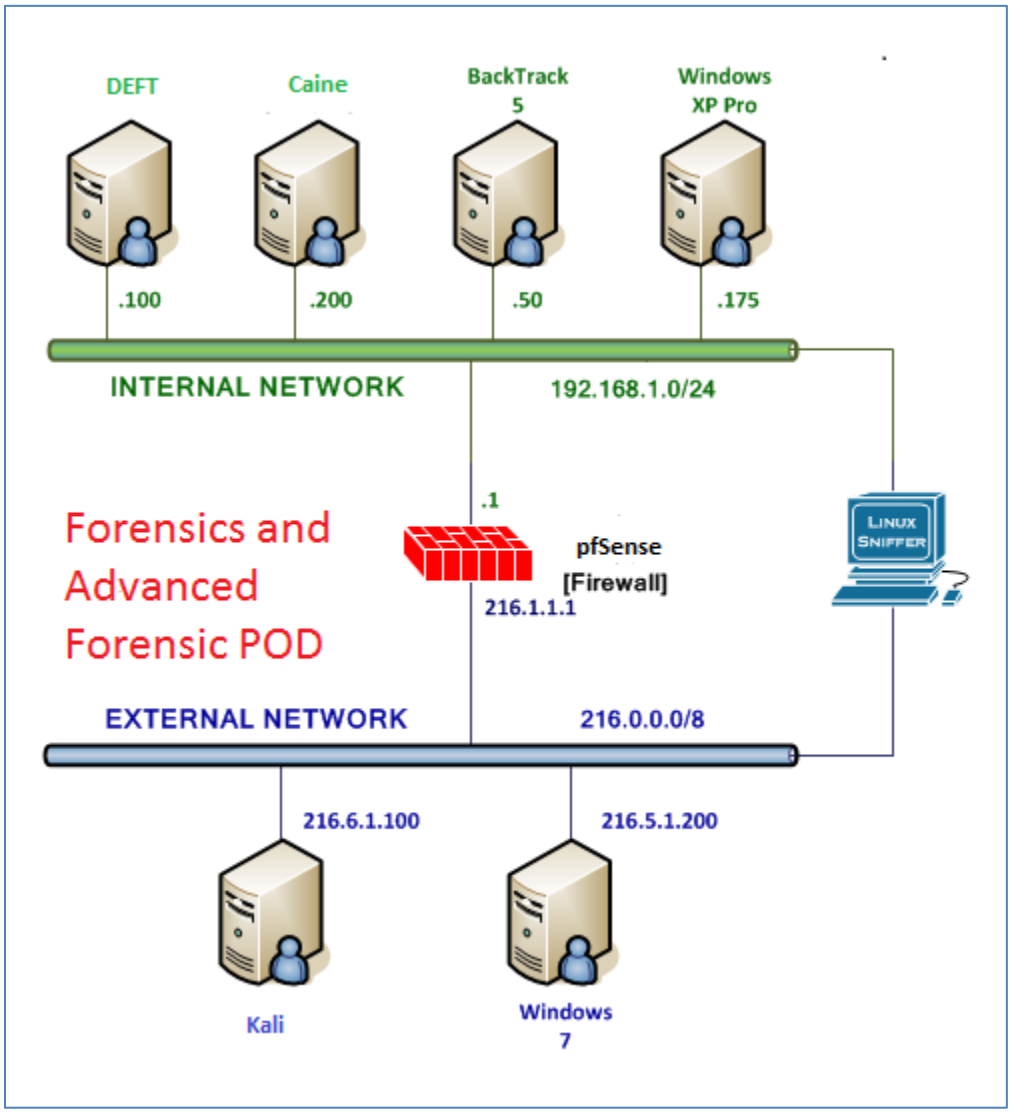
Volatility – an open source analysis tool used for incident response and analysis.

Pslist – will determine the running processes in RAM along with their corresponding PIDs

connscan – will determine the network connections (including IPs and ports) in RAM

Armitage – Armitage is a GUI frontend for Metasploit that has many powerful capabilities. Metasploit is a very powerful exploitation framework but it requires that the user be comfortable using the command line. An attacker can use Armitage to identify and exploit victim machines within an easy to use graphical environment.

Lab Topology



Lab Settings

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
BackTrack 5 R3 Internal Machine	192.168.1.50	root	toor
Windows XP Pro Internal Machine	192.168.1.175		
Kali Linux External Machine	216.6.1.100	root	toor

1 Use Dumpit to Extract Running Physical Memory

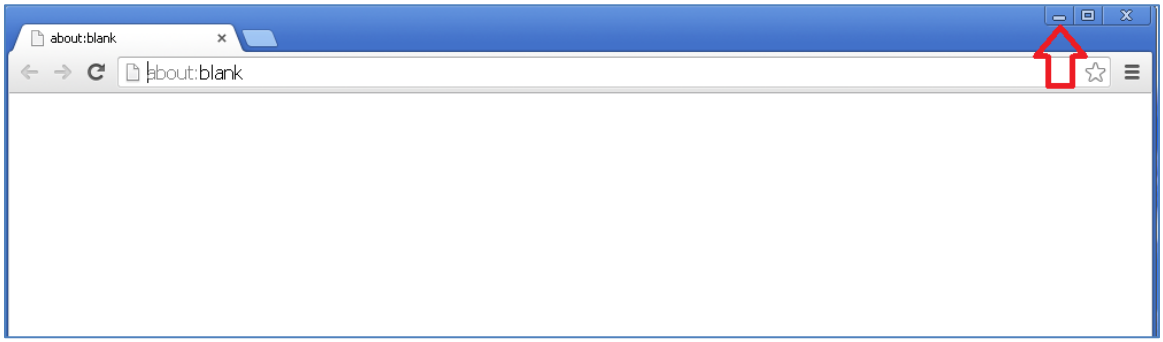
Dumpit is an executable file that runs on either a 32 or 64-bit version of Windows. This tool generates a copy of the system's physical memory and saves it as a file in the same directory that you used to run the command. Dumpit can also be run from a USB drive.

1.1 Extracting Running Physical Memory

Perform the following steps on the machine running Windows XP Professional.

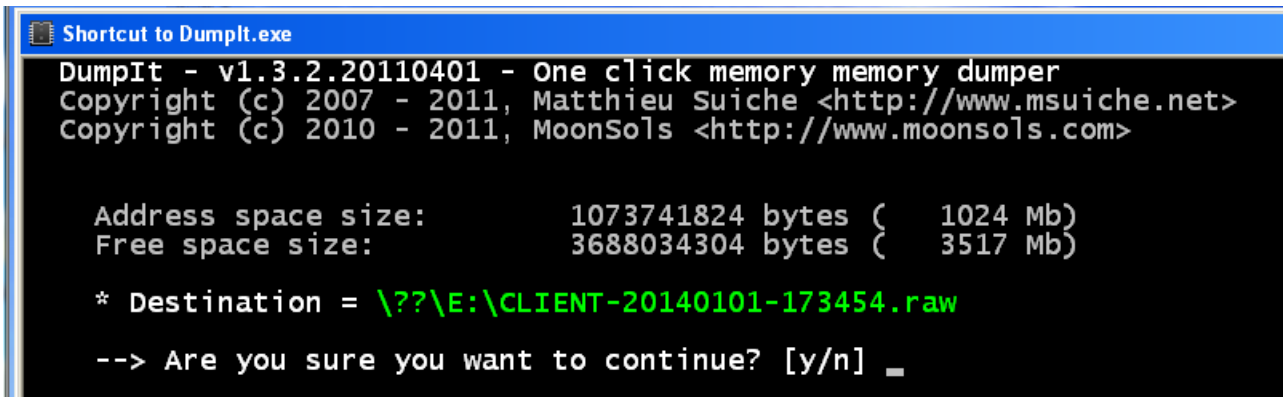
1. On the Windows XP Pro Internal Machine, open Chrome by double=clicking on the shortcut on the desktop.

2. Minimize Chrome. This gives us a process we can identify running in memory.

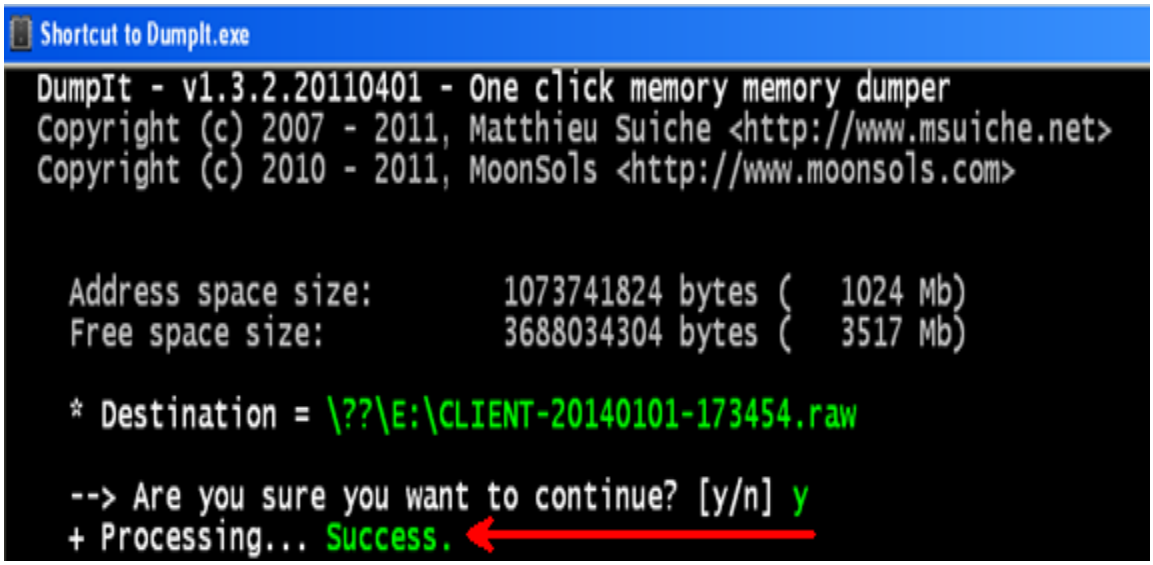


3. Click on the **Shortcut to DumpIt** on the desktop.

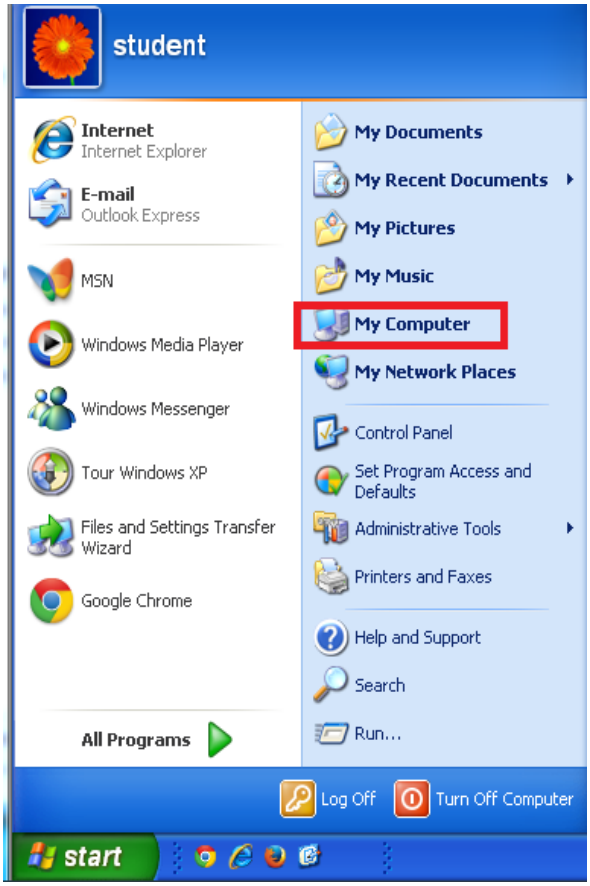
4. A command prompt window will appear asking, *Are you sure you want to continue?* Respond with **y.**



5. The ram will be dumped. DumpIt will create a file with the .raw extension and place the file in the root of E: After a short amount of time, you will receive the message, *Processing... Success*.

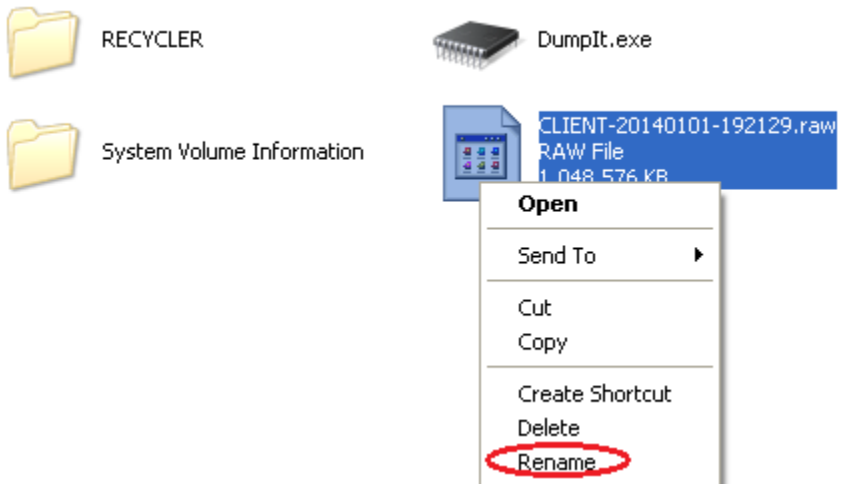


6. Press Enter to close the Dumpit memory capture utility.
7. Click on the start button and select the **My Computer** link from the Start Menu.



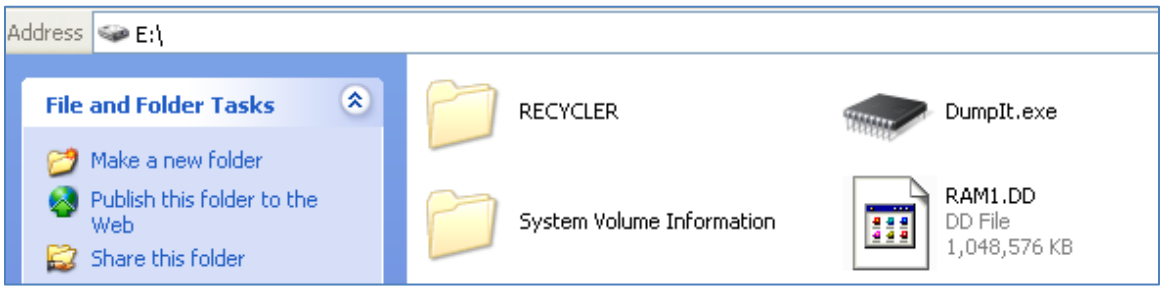
8. Double-click on New Volume (E:).

9. Right-click on the name of the RAM dump and select **Rename.**



10. Name the file **RAM1.DD**.

Please use all capital letters for the name and extension.



1.1 Conclusion

Dumpit is a program that will allow you to capture RAM from a system. When a machine is turned off, the information in RAM will not be retained. If a tool like Dumpit is used, the volatile data within the captured RAM image can be analyzed with a tool such as Volatility, which we will explore in the next task.

1.2 Discussion Questions

1. Where does Dumpit place the image of RAM?
2. Why is it important to capture the information within RAM?
3. When a computer is turned off, what happens to the information in RAM?
4. Can the Dumpit program be used on a USB drive?

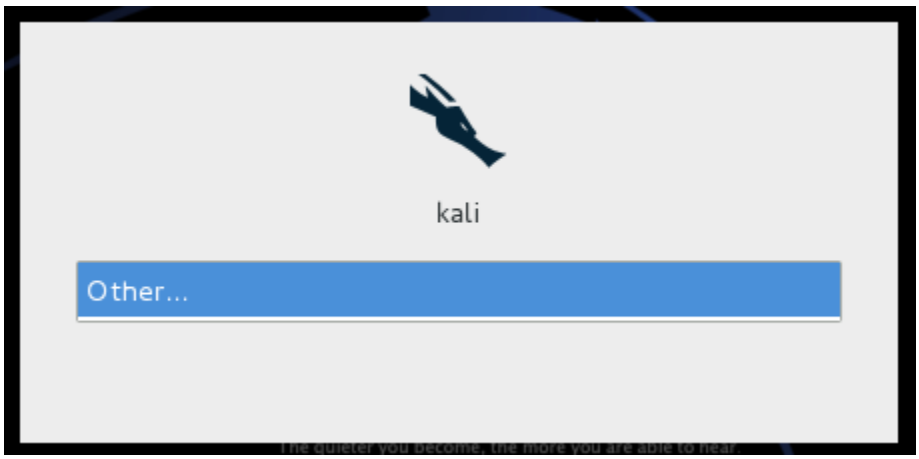
2 Using Volatility to Analyze Processes

Volatility is an open source analysis tool used for incident response and analysis. Several tools make up Volatility and it uses the Python language. We will use some of the tools to extract information from the memory image we created on the Kali Linux system.

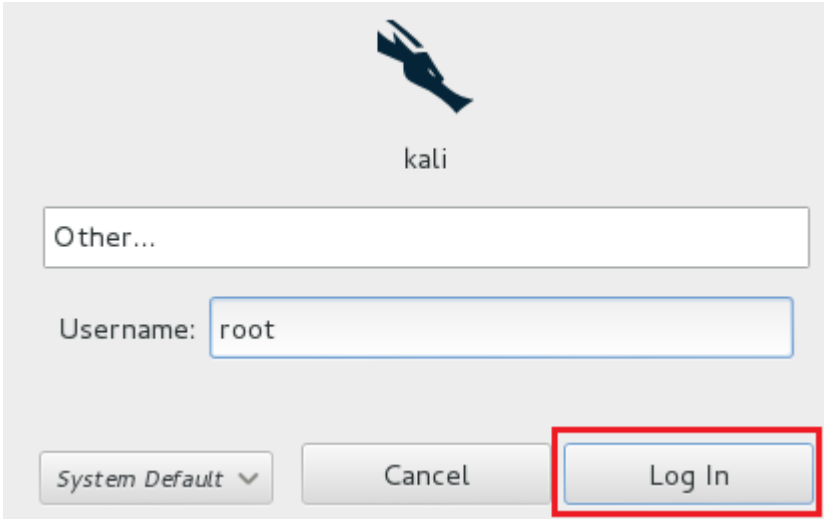
Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

2.1 Memory Analysis

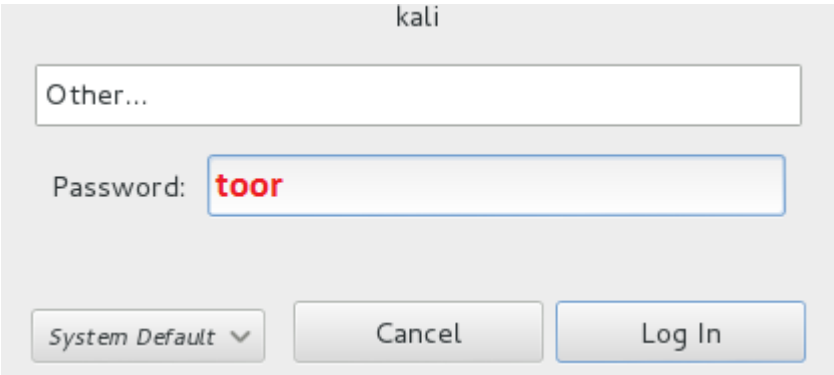
1. On the Kali Linux External Machine, click the **Other** link.



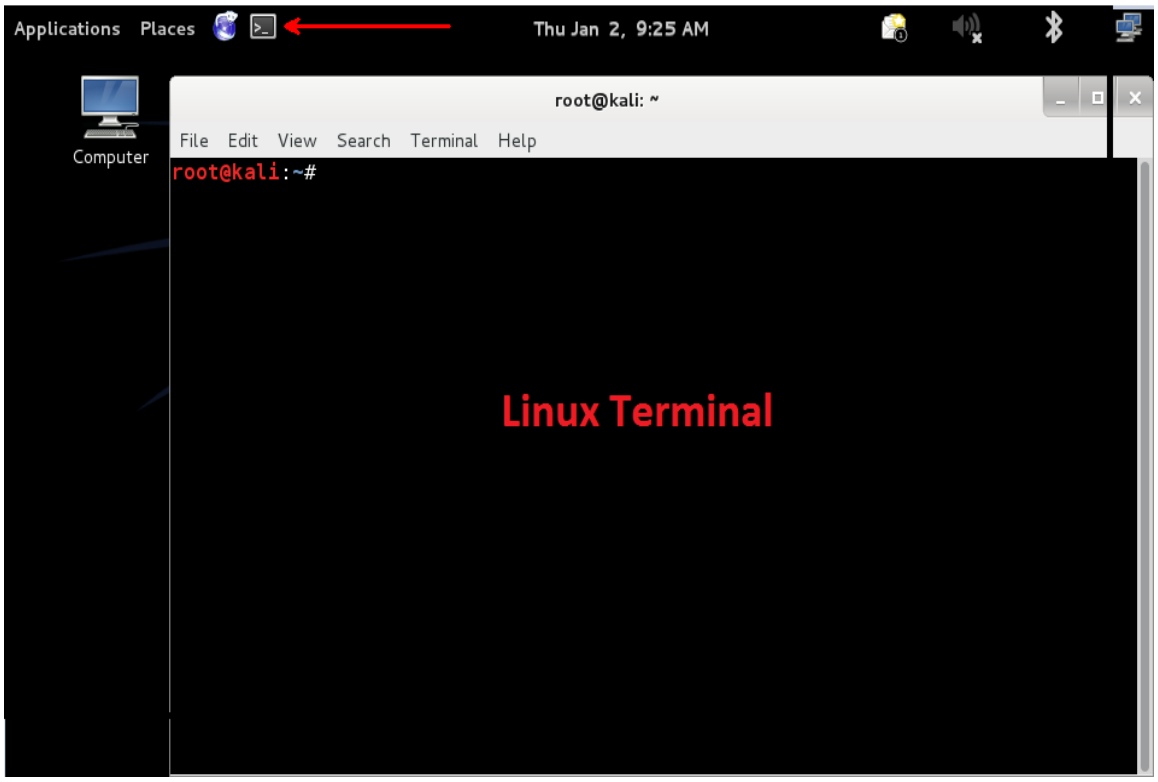
2. For the username on the Kali system, type **root** and click the **Log In** button.



3. For the password, type **toor** and click the **Log In** button.



4. Open a terminal by clicking on the black icon to the right of the world icon.



5. To generate the keys that will be needed for an SSH connection, type the following command and press Enter three times when prompted for input:
root@kali:~# **ssh-keygen**

```
root@kali:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
41:cd:73:1a:73:60:d2:5a:18:a0:f6:01:41:6c:97:95 root@kali
The key's randomart image is:
+--[ RSA 2048]----+
|   o+..+=Bo.     |
|    ooo.Eo0 o    |
|   .o.. .o B     |
|   . . ....      |
|      . S        |
|                 |
|                 |
|                 |
|                 |
+-----------------+
```

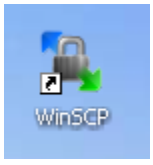
6. To start the SSH server, type:
root@kali:~# **/etc/init.d/ssh start**

```
root@kali:~# /etc/init.d/ssh start
[ ok ] Starting OpenBSD Secure Shell server: sshd.
```

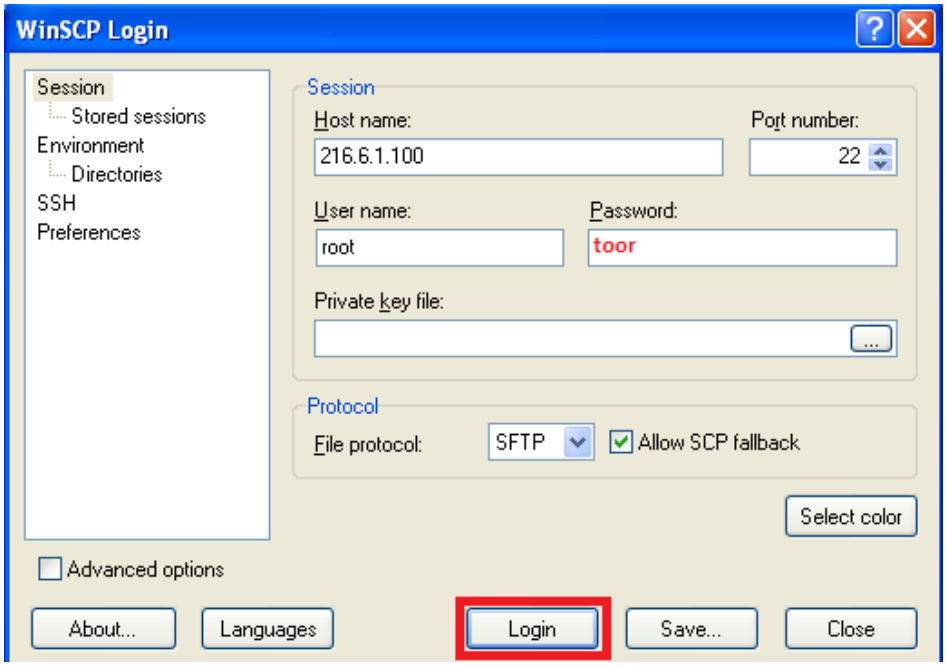
7. To verify that the SSH server service is running on the machine, type:
root@kali:~# **netstat -tan**

```
root@kali:~# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
```

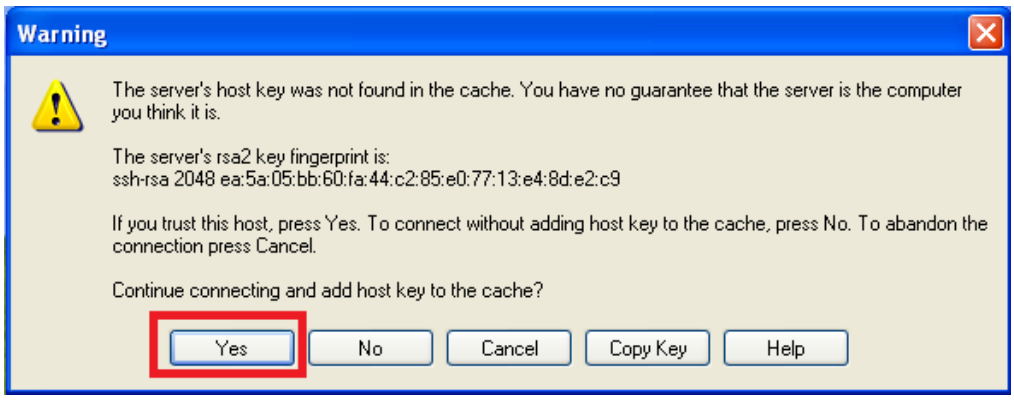
8. On the Windows XP Pro Internal Machine , open WinSCP by double-clicking on the shortcut to the desktop.



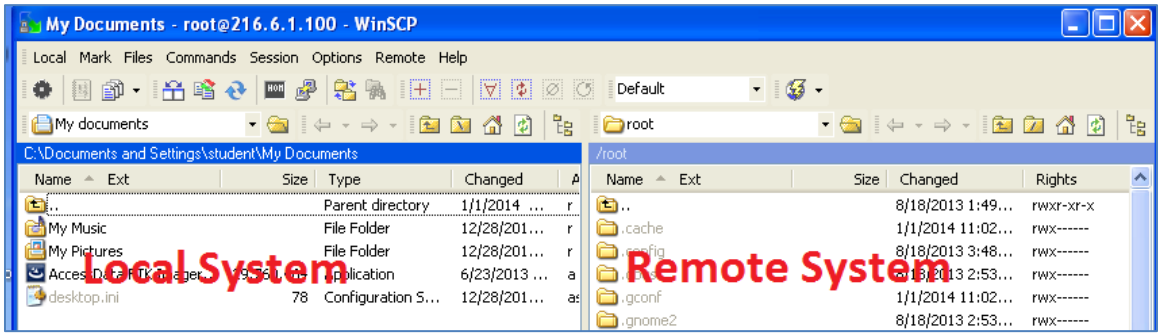
9. Type **216.6.1.100** for the host name, **root** for the user name, and **toor** for password. Click the **Login** button to connect to the remote Kali system.



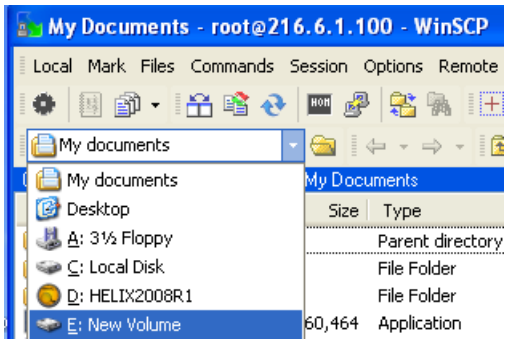
10. Click **Yes** when asked if you want to continue connecting and add the key.



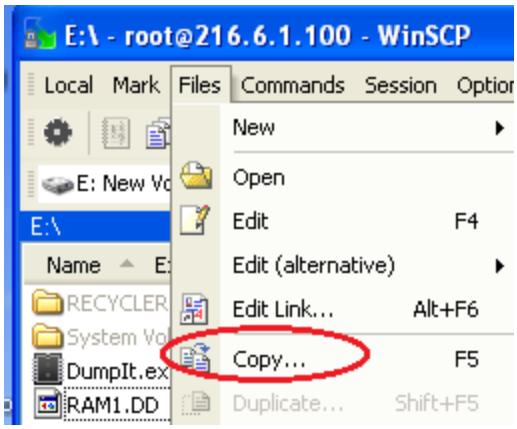
11. You will be logged in to the remote system and see the local and remote drives.



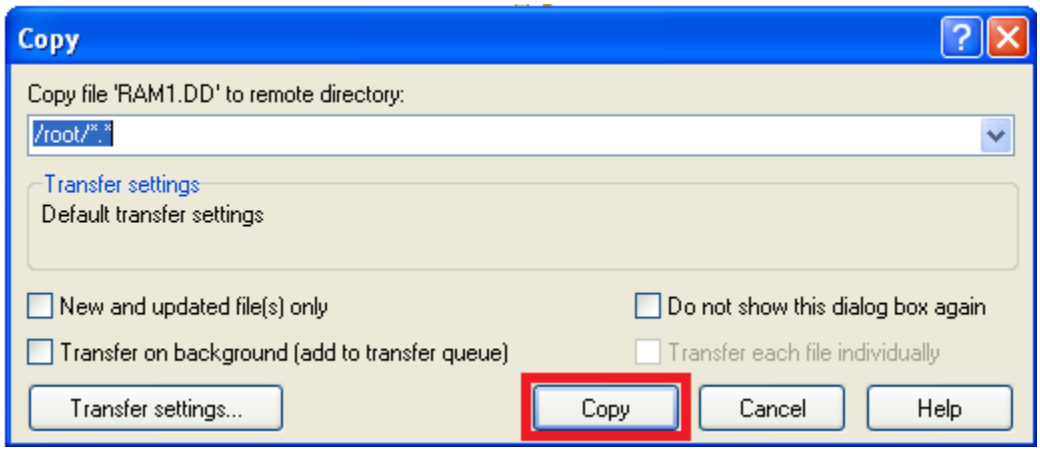
12. Change the location on the local system from My Documents to **E: New Volume**.



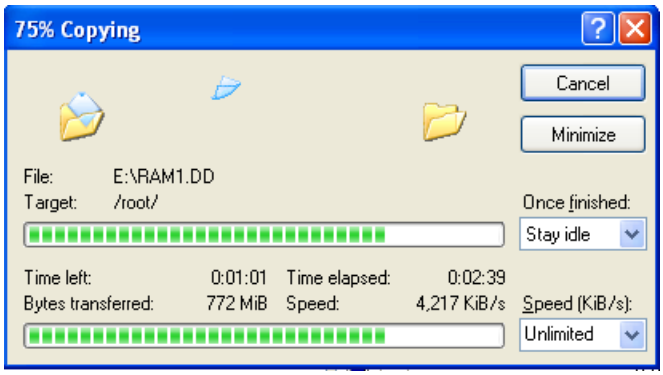
13. Highlight RAM1.DD. From the menu, choose Files and then select **Copy**.



14. Verify that you are copying RAM1.DD to the root directory. Click **Copy**.



15. Wait for the file copy process to finish (progress is indicated).



16. Close the WinSCP program by clicking the red X when the file finishes copying.

17. On the Kali Linux External Machine, type the following command to verify that the file has been transferred:
root@kali:~# **ls**

```
root@kali:~# ls
Desktop  forensics  RAM1.DD  vmware-tools-distrib
```

18. Type the following command to see all the available options for volatility:
root@kali:~# **vol -h**

```
root@kali:~# vol -h
Volatile Systems Volatility Framework 2.2
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/root/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/root/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the timezone for displaying timestamps
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
                        Name of the profile to load
  -l LOCATION, --location=LOCATION
                        A URN location from which to load an address space
  -w, --write           Enable write support
  --dtb=DTB             DTB Address
  --cache-dtb           Cache virtual to physical mappings
```


19. Type the following command to parse information from the image of RAM:
root@kali:~# **vol -f /root/RAM1.DD imageinfo**

```
root@kali:~# vol -f /root/RAM1.DD imageinfo
Volatile Systems Volatility Framework 2.2
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : JKIA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/RAM1.DD)
                      PAE type : PAE
                           DTB : 0x334000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2014-01-02 02:21:05 UTC+0000
     Image local date and time : 2014-01-01 21:21:05 -0500
```

20. Type the following command to parse the processes running in RAM:
root@kali:~# **vol -f /root/RAM1.DD pslist**

```
root@kali:~# vol -f /root/RAM1.DD pslist
Volatile Systems Volatility Framework 2.2
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
 Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ -------------------
 -------------------
0x865c6830 System                    4      0     56      367 ------      0

0x85fc5b40 smss.exe                592      4      3       21 ------      0 2014-01-02 01:41:44

0x86269020 csrss.exe               640    592     12      392      0      0 2014-01-02 01:41:46

0x86278020 winlogon.exe            664    592     17      491      0      0 2014-01-02 01:41:46
```

21. Type the following command to parse the chrome processes running in RAM:
root@kali:~# **vol -f /root/RAM1.DD pslist | grep chrome**

```
root@kali:~# vol -f /root/RAM1.DD pslist | grep chrome
Volatile Systems Volatility Framework 2.2
0x85f24558 chrome.exe             1796   1444     30      426      0      0 2014-01-02 02:20:47

0x85f78228 chrome.exe              820   1796      7      119      0      0 2014-01-02 02:20:53

0x862e6c10 chrome.exe              544   1796      8      114      0      0 2014-01-02 02:20:55
```


2.2 Conclusion

Dumpit is a program that will allow you to capture RAM from a system. When a machine is turned off, the information in RAM will not be retained. If a tool like Dumpit is used, the volatile data within the captured RAM image can be analyzed with a tool such as volatility.

2.3 Discussion Questions

1. What were the different process IDs for Chrome? (Answers will vary)
2. Based on image info, was the operating system a 32-bit or 64-bit system?
3. What is the date that the image was created?
4. Based on image info, what was the operating system installed?

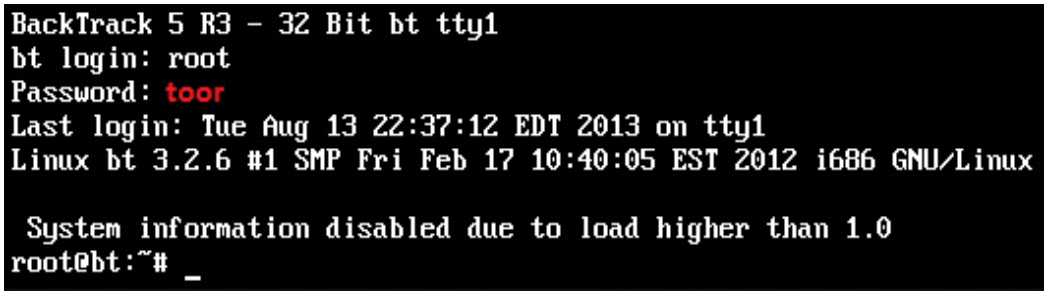
3 Attacking a Remote System Utilizing Armitage

In this section, you will be introduced to Armitage, a Graphical User Interface, or GUI, front end for Metasploit. The website for Armitage, which was developed by Raphael Mudge, is fastandeasyhacking.com. Armitage provides the user with a visual interface which illustrates what is happening in the background of Metasploit.

3.1 Using Armitage

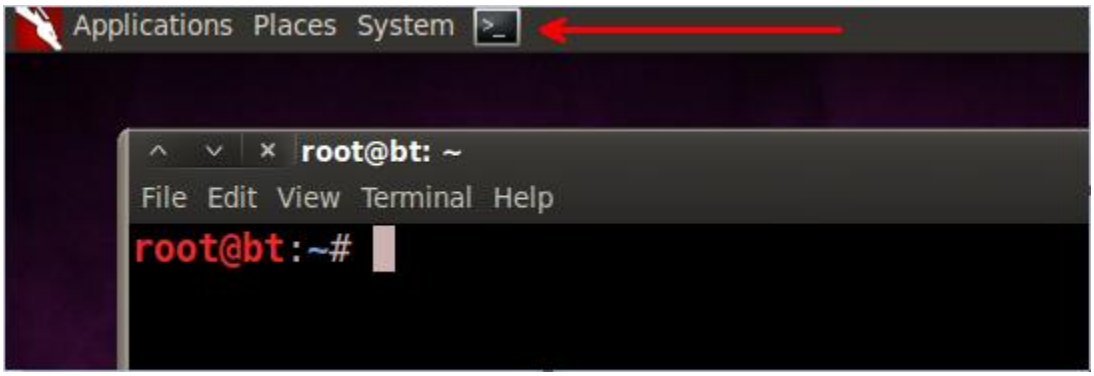
1. Open the **BackTrack 5 R3 Internal Machine**. Type **root** for the login and **toor** *(root spelled backwards)* for the password.

The password will not be displayed when you type it, for security purposes.

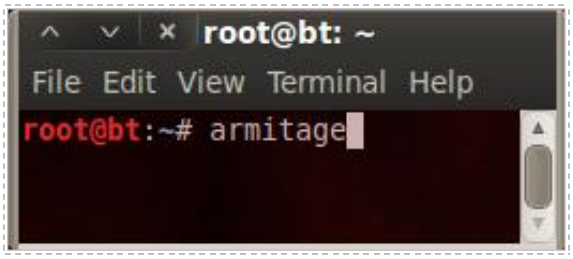


2. Type the following command to start the Graphical User Interface (GUI):
root@bt:~# **startx**

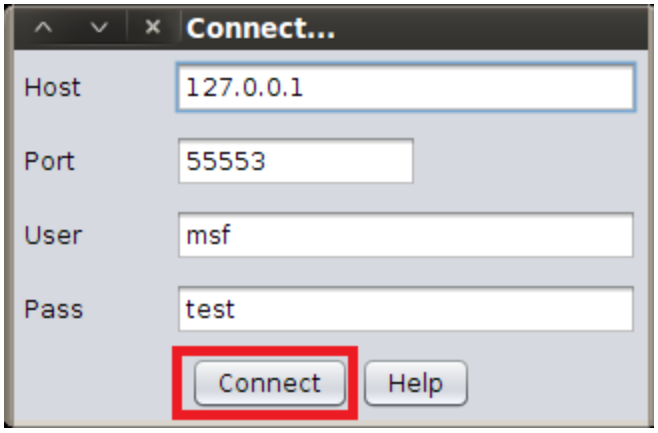
3. Open a terminal by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.



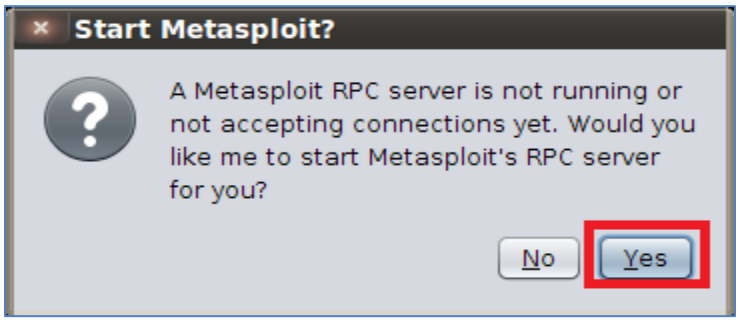
4. Type armitage in the terminal to launch the Armitage program:
root@bt:~# **armitage**



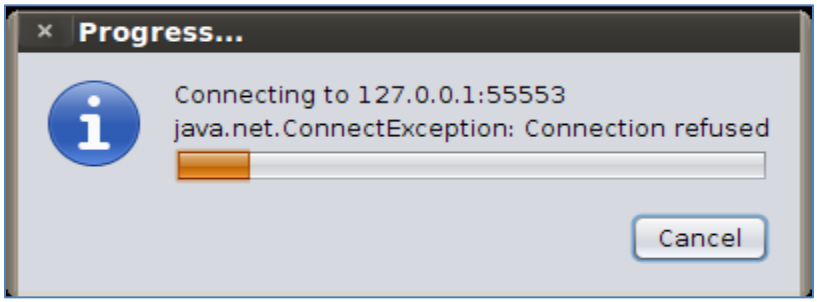
5. A Connect box will appear on your screen. Click **Connect.**



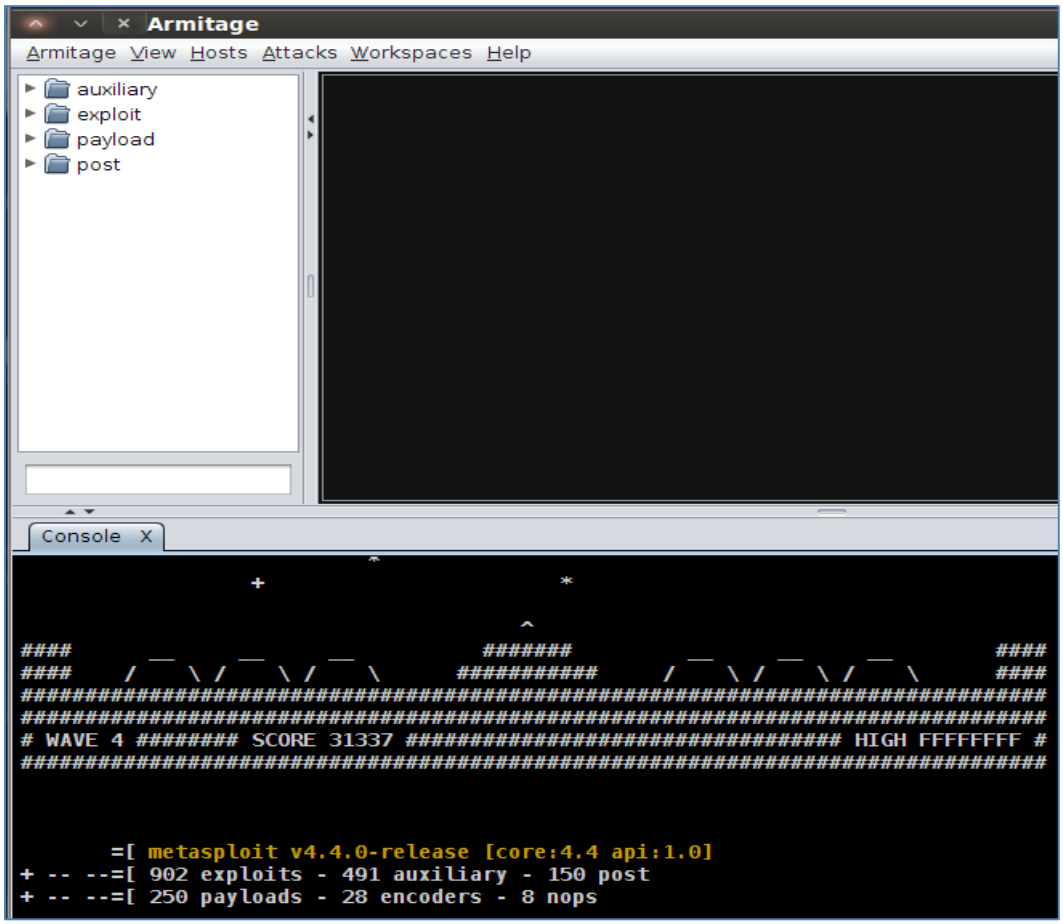
6. Click **Yes** to start Metasploit.



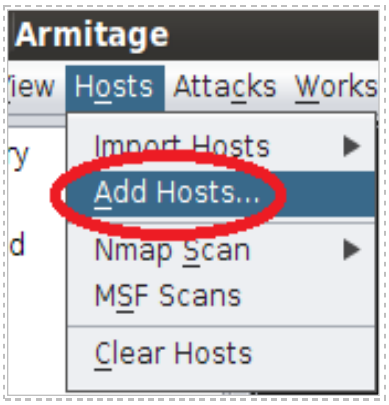
7. You will receive an initial connection refused message. This is normal.



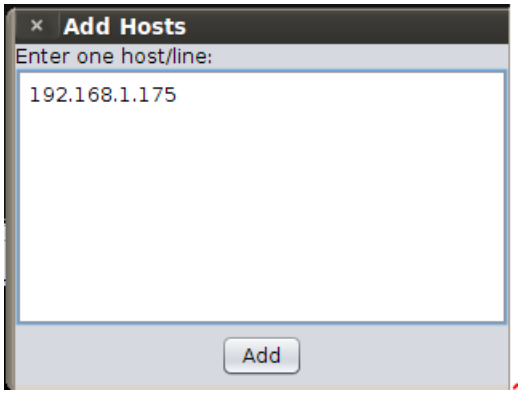
8. Armitage will open. The console pane below lists the number of exploits.



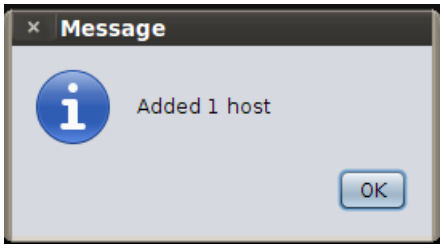
9. From the Armitage menu, click **Hosts**, and select **Add Hosts**.



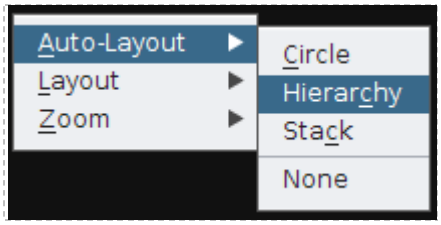
10. Type **192.168.100.175** (the IP address of the Windows XP Pro Internal Machine) then click **Add**.



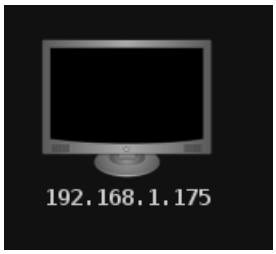
11. You should receive a message that states, *Added 1 host*. Click OK.



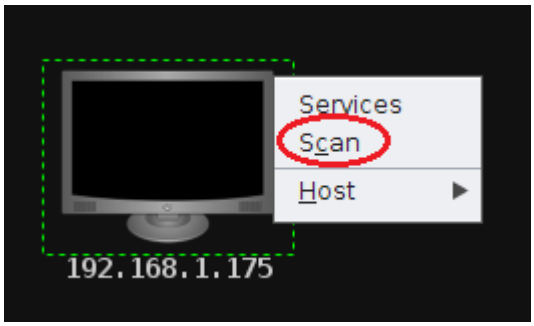
12. In the top-right pane of Armitage, right-click and select **Auto-Layout** > **Hierarchy**.



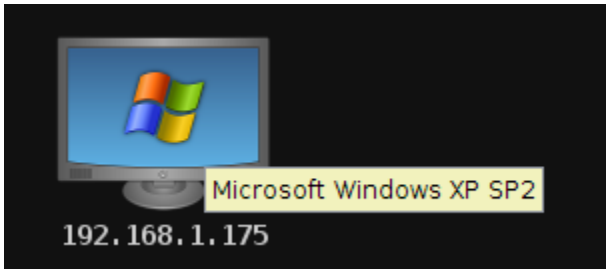
13. Drag the computer icon to the center of the top-right pane of Armitage. At this point, you should be able to view the icon representing the victim machine. Notice that the operating system of the remote machine has yet to be identified.



14. Right-click on the host in the Armitage pane and select **Scan**.

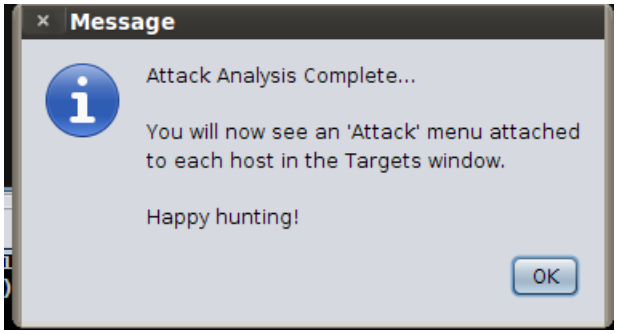


15. You target will now be identified as a Windows machine. If you hover over the icon, the remote machine will be identified as **Microsoft Windows XP SP2**.

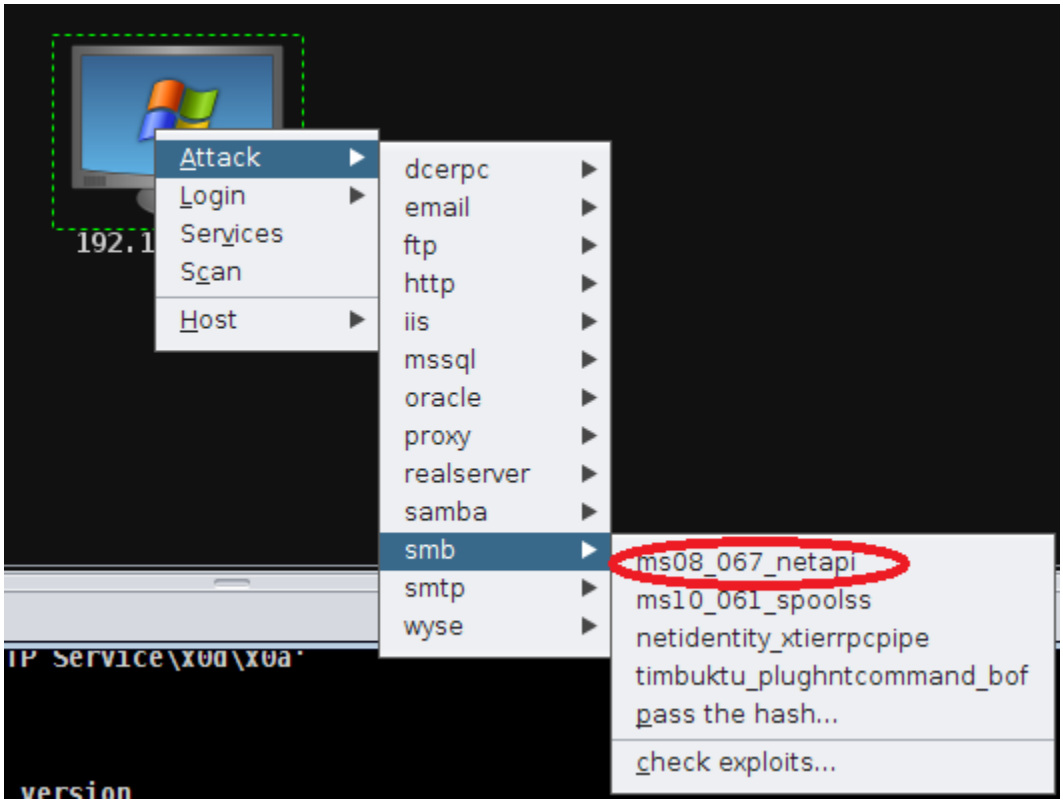


16. From the **Attacks** menu in Armitage, select **Find Attacks.**

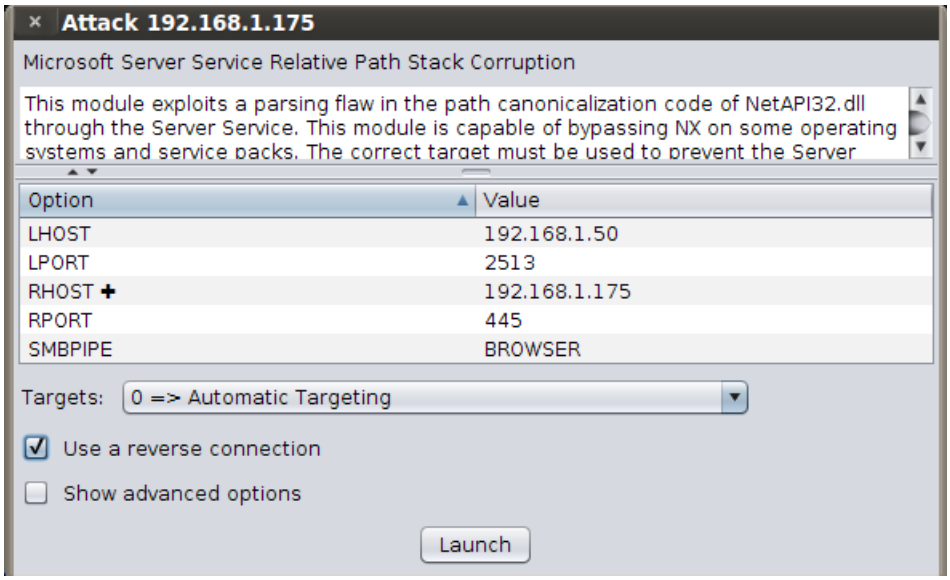
17. Wait until you receive the message, *Happy Hunting*. Click **OK**.



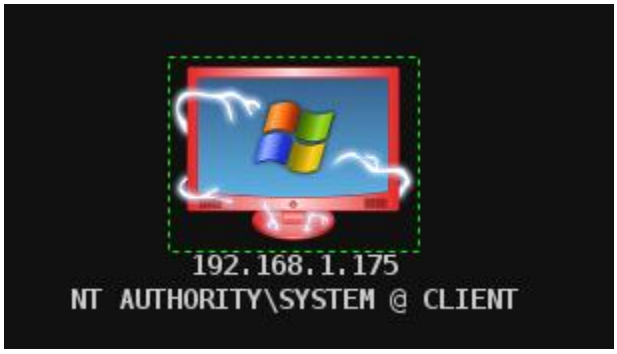
18. Right-click on the icon representing the victim in the Armitage pane and select **Attack** > **smb** > **ms08_067_netapi**. An attack window will pop up.



19. In the attack window, the title should be Attack 192.168.1.175. Notice that a description of the exploit is provided. Also, notice that the remote port of 445 is listed. Check the option to **Use a Reverse Connection**. Click the **Launch Button** to attack.



20. If the attack is successful, the icon of the victim machine will be outlined in **red**. If the attack did not work, you may need to attempt to launch the attack again. If all else fails, reboot the Windows Server. Once the attack is successful, the victim is considered to be in a compromised state.



Notice that the level of access of **NT AUTHORITY\SYSTEM** is displayed at the bottom of the screen. This is actually a higher level of access than the administrator account. The **SYSTEM** account is reserved and users are not permitted to log in as this account.

Do not close the Armitage GUI window. It will be used in the next task.

3.2 Conclusion

Armitage is a GUI frontend for Metasploit that allows attackers to scan, identify, and exploit remote operating systems. After scanning a machine, Armitage will report the operating system and service pack level that the target machine is using. The Armitage tool then allows the attacker to find attacks by open ports. If the attacker is able to successfully connect to a victim machine, the victim will be displayed with a red border.

3.3 Discussion Questions

1. Armitage is a GUI front end for what exploitation tool?
2. What message does Armitage display after you attempt to find attacks by port?
3. Explore the Armitage menu. What are some other features of the tool?
4. At what point is the victim machine considered to be compromised?

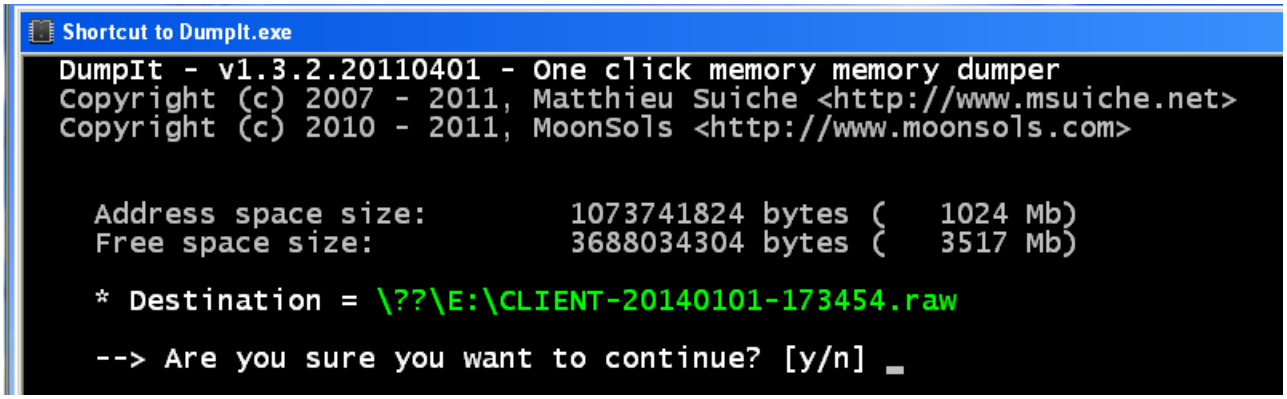
4 Using Volatility to Remote Connections

Volatility is a collection open source analysis tools implemented in Python language, used for incident response and analysis. We will use some of the tools to extract information from the memory image we created on the Kali Linux External Machine.

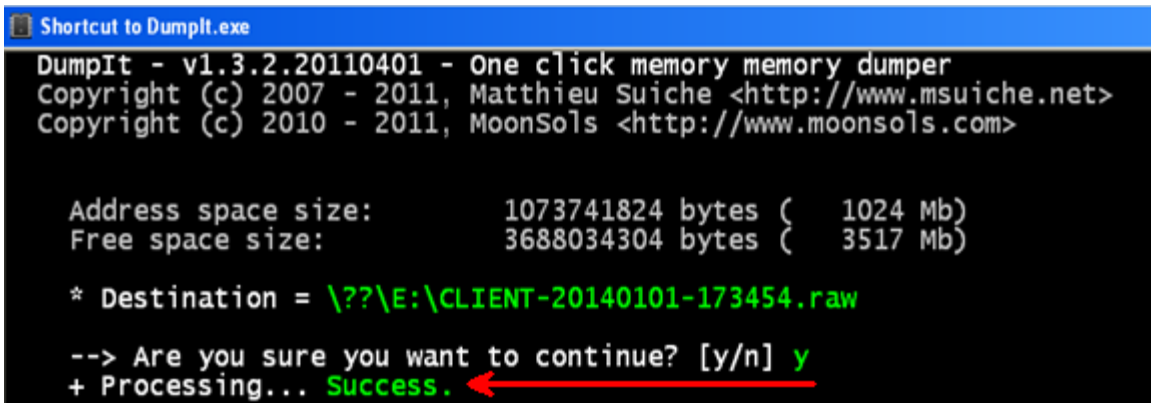
4.1 Memory Analysis

1. Click on the **Shortcut to DumpIt** on the desktop.

2. A command prompt window will appear asking, *Are you sure you want to continue?* Respond with **y.**

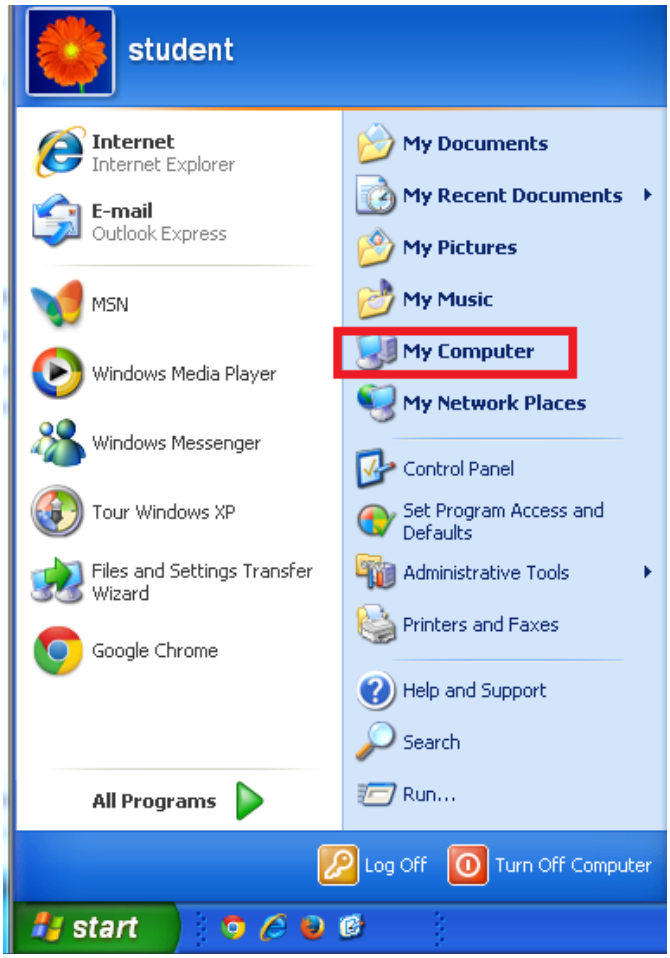


3. The ram will be dumped. DumpIt will create a file with the .raw extension and place the file in the root of E: After a short amount of time, you will receive the message, *Processing... Success*.



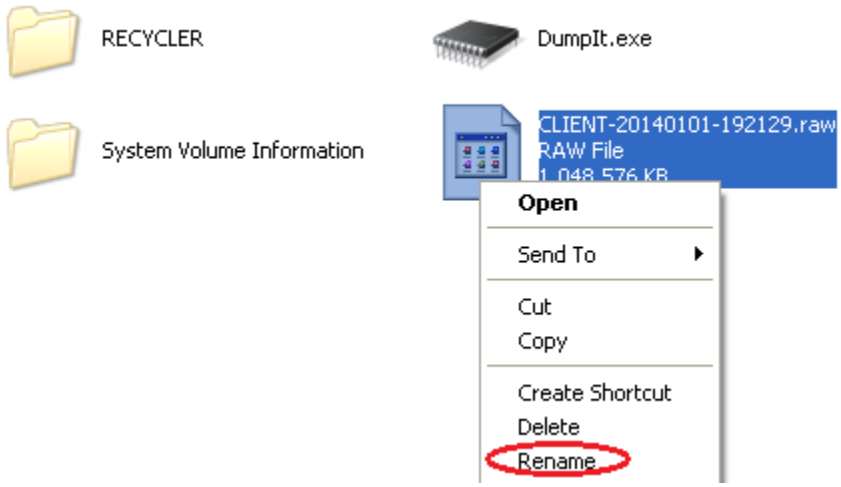
4. Press Enter to close the Dumpit memory capture utility.

5. Click on the Start button and select the **My Computer** link from the Start menu.



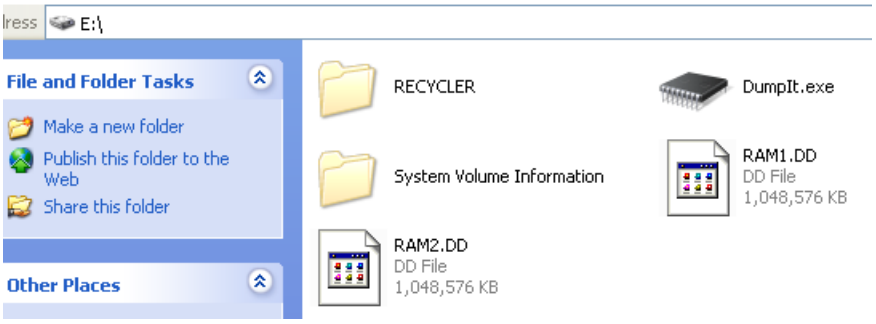
6. Double-click on New Volume (E:).

7. Right-click on the name of the RAM dump and select rename.



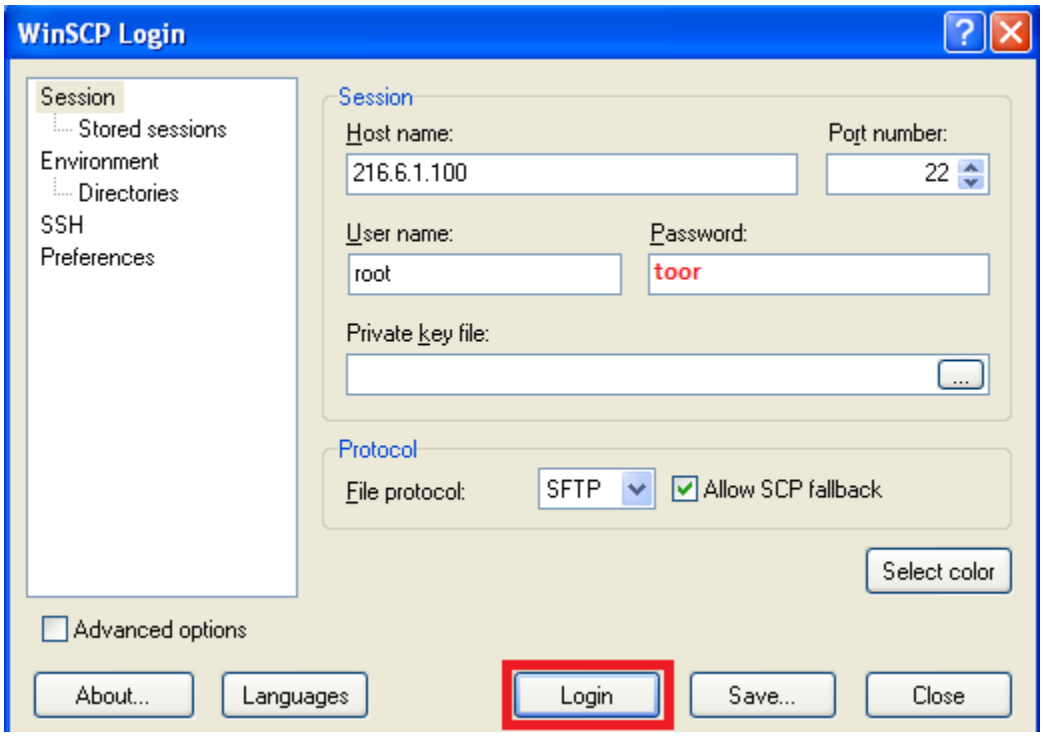
8. Name the file **RAM2.DD**.

Please use all capital letters for the name and extension.

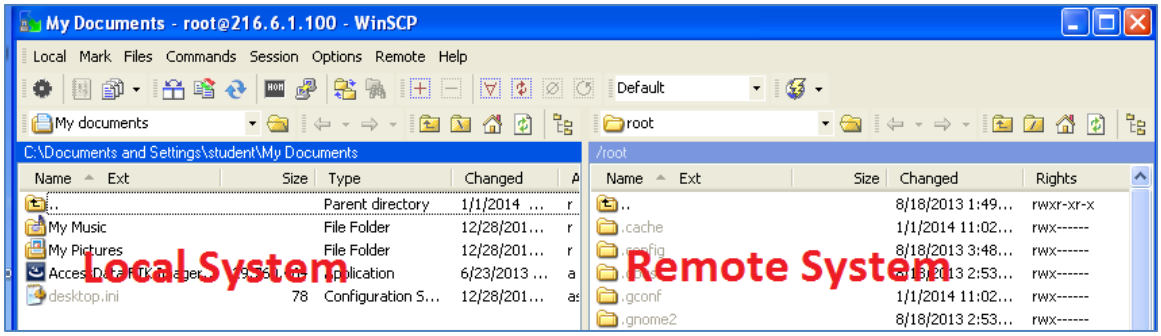


9. On the Windows XP Pro Internal Machine, open WinSCP by double-clicking on the shortcut to the desktop.

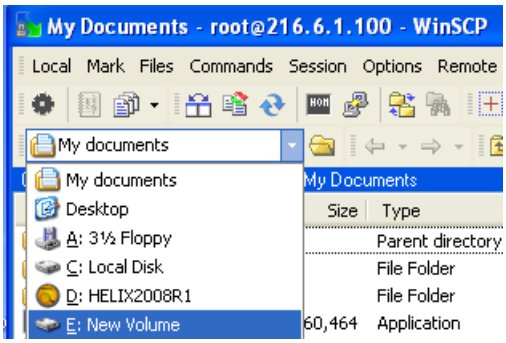
10. Type **216.6.1.100** for the host name (the IP Address of the Kali Linux External Machine), **root** for the user name, and **toor** for password. Click the **Login** button to connect to the Kali Linux External Machine.



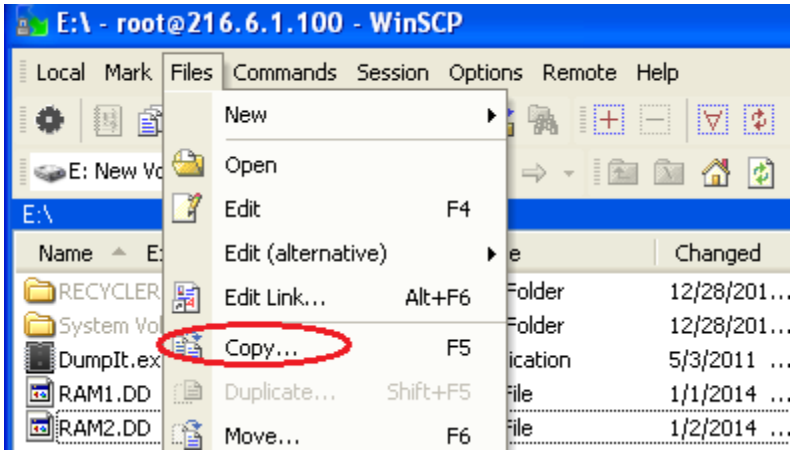
11. You will be logged in to the remote system and see the local and remote drives.



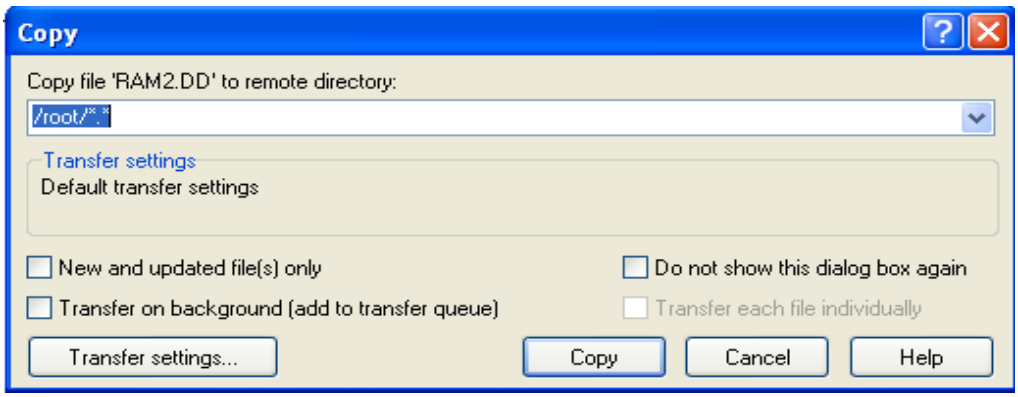
12. Change the location on the local system from My Documents to **E: New Volume**.



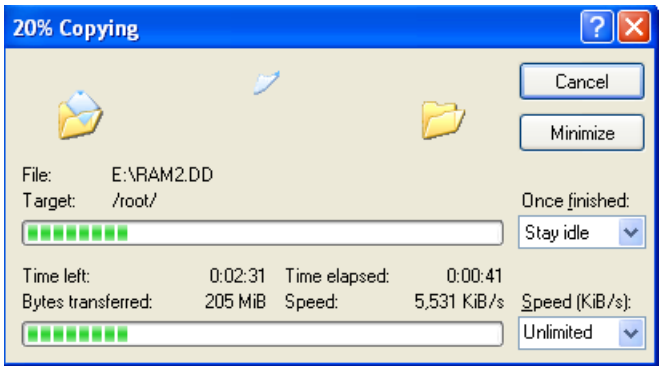
13. Highlight RAM2.DD. From the menu, choose Files and then select **Copy**.



14. Verify that you are copying RAM2.DD to the root directory. Click copy



15. Wait for the file copy process to finish (progress will be indicated).



16. Type the following command on Kali to verify that the file has been transferred:
root@kali:~# **ls**

```
root@kali:~# ls
Desktop  forensics  RAM1.DD  RAM2.DD  vmware-tools-distrib
```

17. Type the following command to parse the active network connections in RAM:
root@kali:~# **vol -f /root/RAM1.DD connscan**

```
root@kali:~# vol -f /root/RAM2.DD connscan
Volatile Systems Volatility Framework 2.2
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x060f9e70 192.168.1.175:21         192.168.1.50:51541        1872
0x064a3628 192.168.1.175:1043       192.168.1.50:31102        1092
0x064b0008 192.168.1.175:1045       216.6.1.100:22            1936
0x064dec88 192.168.1.175:25         192.168.1.50:59671        1872
```

18. Type the following command to parse the network connections to 192.168.1.50:
root@kali:~# **vol -f /root/RAM1.DD connscan | grep 50**

```
root@kali:~# vol -f /root/RAM2.DD connscan | grep 50
Volatile Systems Volatility Framework 2.2
0x060f9e70 192.168.1.175:21         192.168.1.50:51541        1872
0x064a3628 192.168.1.175:1043       192.168.1.50:31102        1092
0x064dec88 192.168.1.175:25         192.168.1.50:59671        1872
```


4.2 Conclusion

Dumpit is a program that will allow you to capture RAM from a system. When a machine is turned off, the information in RAM will not be retained. If a tool like Dumpit is used, the volatile data within the captured RAM image can be analyzed with a tool such as volatility. In the case of a network intrusion, capturing the RAM can be of critical importance, so that you can determine the IP address and port numbers used by the attacking machine.

4.2 Discussion Questions

1. What were the different process IDs for chrome? (Answers will vary)
2. Based on image info, was the operating system a 32-bit or 64-bit system?
3. What is the date that the image was created?
4. Based on image info, what was the operating system installed?

References

1. DumpIt Download:
   http://www.downloadcrew.com/article/23854-dumpit

2. Volatility Download:
   https://code.google.com/p/volatility/

3. Princeton Video on Capturing Memory:
   https://citp.princeton.edu/research/memory/media/

4. Memory Forensics:
   http://en.wikipedia.org/wiki/Memory_forensics

5. Volatility Framework:
   http://www.forensicswiki.org/wiki/Volatility_Framework

