



Information Assurance Security+ Lab Series

Lab 1: Network Devices and Technologies - Capturing Network Traffic

Security+ Domain 1

**Objective 1.1: Explain the security function and purpose of
network devices and technologies**

Document Version: 2012-07-02 (Beta)

Lab Author: Jesse Varsalone
Organization: Assistant Professor
Cyber Security
Community College of Baltimore County

Copyright © 2003-2012 Center for Systems Security and Information Assurance (CSSIA)

The development of this document is funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) is an entity of Moraine Valley Community College. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation. A copy of this license can be found at <http://www.gnu.org/licenses/fdl.html>.

Contents

1	Introduction.....	3
2	Objective: Explain the security function and purpose of network devices and technologies.....	3
3	Pod Topology.....	4
4	Lab Settings	5
Task 1	Using tcpdump to Capture Network Traffic	6
Task 1.1	Using tcpdump.....	6
Task 1.2	Conclusion	16
Task 1.3	Discussion Questions.....	16
Task 2	Capturing and Analyzing Traffic with Wireshark.....	17
Task 2.1	Using Wireshark.....	17
Task 2.2	Conclusion	25
Task 2.3	Discussion Questions.....	25
Task 3	Capturing and Analyzing Traffic with Network Miner	26
Task 3.1	Using Network Miner	26
Task 3.2	Conclusion	30
Task 3.3	Discussion Questions.....	30
5	References	31

1 Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This series of lab exercises is intended to support courseware for Security+ certification.

By performing this lab, students will learn the process of capturing network traffic using three different methods, the `tcpdump` command, Wireshark, and Network Miner. The `tcpdump` command has no Graphical User Interface (GUI) and is only utilized within a Linux terminal. Wireshark shows you the raw output of network traffic captures and allows you to analyze them. Network Miner will allow you to capture data, and it will also pull out items like clear text messages and pictures.

This lab includes the following tasks:

- [Task 1](#) - Using `tcpdump` to capture Network Traffic
- [Task 2](#) - Capturing and Analyzing Traffic with Wireshark
- [Task 3](#) - Capturing and Analyzing Traffic with Network Miner

2 Objective: Explain the security function and purpose of network devices and technologies

An essential part of network administration is the ability to capture and analyze network traffic. This can be important in order to identify the cause of bottlenecks, determining who is responsible for certain download activity, or analyzing an intrusion.

Wireshark [1] – A protocol analyzer that reads binary capture files. Wireshark will also allow you to capture network traffic and runs on Windows, Linux, and on Mac OS X.

Network Miner [2] – Network Miner allows you to capture and analyze network traffic. It is an NFAT, or Network Forensics Tool, that runs on the Windows operating system.

tcpdump [3] – A Linux/UNIX program that allows you to capture network traffic.

Sniffer – A sniffer is used to capture network traffic on a Network. Software programs like `tcpdump`, Wireshark, and Network Miner can be used to sniff traffic.

PCAP File – Programs that can sniff network traffic such as `tcpdump`, Wireshark, and Network Miner allow you to save the network capture to a PCAP file format. In order to read the PCAP format, you need a tool like Wireshark or Network Miner.

3 Pod Topology

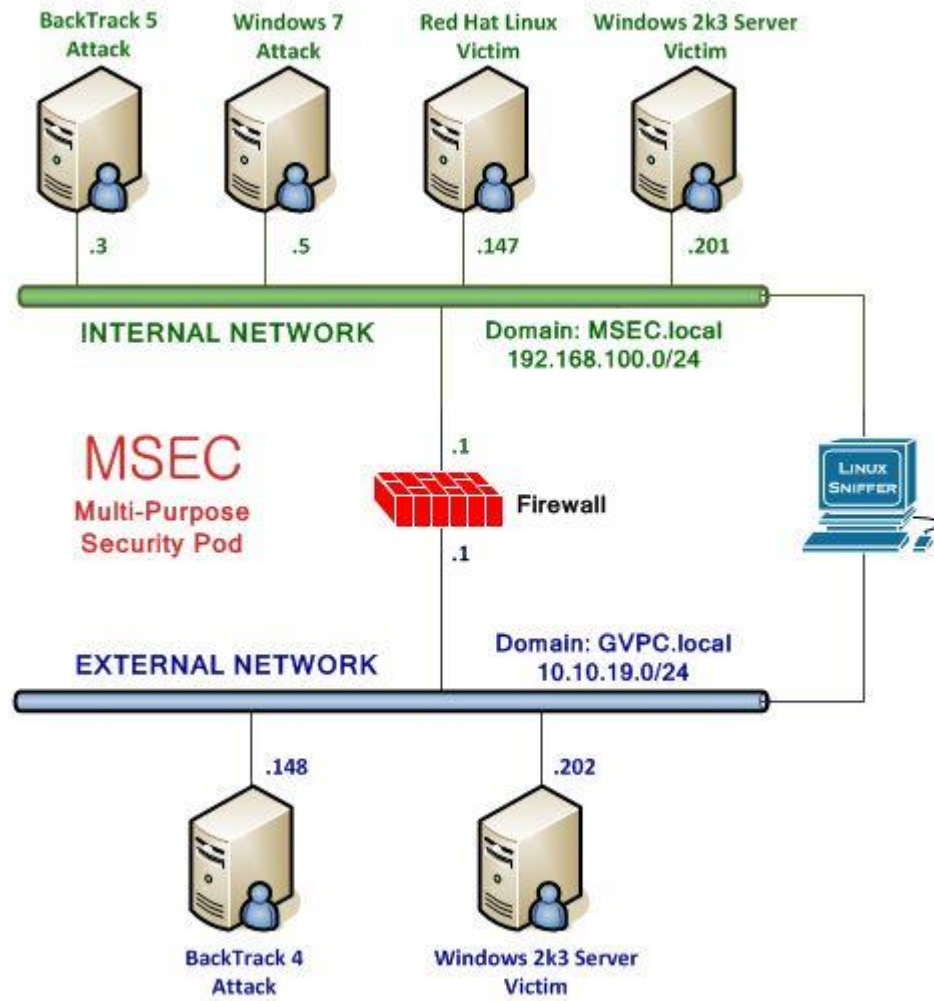


Figure 1: MSEC Network Topology

4 Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

This lab requires the use of the Windows Internal Attack Machine running Windows 7, the Sniffer, the Linux External Attack Machine, Windows 2003 External server, and the Windows 2003 Internal server.

Windows 7 Internal Attack Machine	192.168.100.5
Windows student password	password
Linux Sniffer	No IP Addresses
Linux Sniffer root password	toor
Linux Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password
Windows Internal Victim Machine	192.168.100.201
Windows Server administrator password	password
Linux External Attack Machine	10.10.19.148
Linux External root password	password
Windows External Victim	10.10.19.202
Windows administrator password	password

Task 1 Using tcpdump to Capture Network Traffic

Part of a network administrator's job can be to capture and analyze network traffic. This is done for a variety of reasons, including the identification of the cause of bottlenecks, determining who is responsible for certain download activity, or analyzing an intrusion.

There are many tools that can be utilized to capture network traffic, including tcpdump.

Task 1.1 Using tcpdump

The Linux distribution BackTrack is installed on the sniffer machine. BackTrack is a distribution used by security professionals for penetration testing and forensics.

Log on to the sniffer.

1. Log into the Linux Sniffer with the username of root with the password of toor.

For security purposes, the password will not be displayed.

Type the following command to initialize the GUI, Graphical User Environment:
`root@bt:~#startx`

```

bt login: root
Password:
Last login: Sun Feb  8 18:33:44 EST 2009 on tty1
Linux bt 2.6.28.1 #2 SMP Wed Feb  4 21:50:02 EST 2009 i686
++ WELCOME TO THE BACKTRACK LIVE CD ++

[*] To start Networking - "/etc/init.d/networking start"
[*] To start KDE - "startx"
[*] To start FVWM - "bt4-crystal"

[*] http://www.remote-exploit.org/
root@bt:~# startx
    
```

Figure 2: Logging on to the Sniffer

2. Open a terminal on the Linux system by clicking on the image to the left of Firefox in the task bar, in the bottom of the screen in BackTrack.

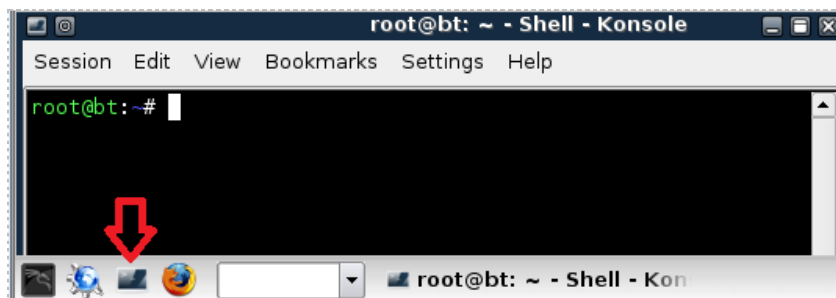
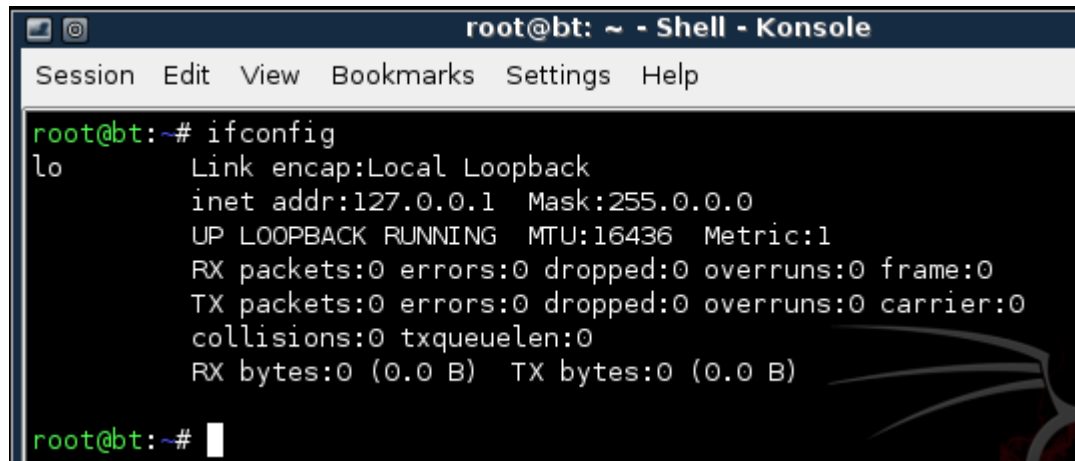


Figure 3: The Terminal Windows within BackTrack

One of the nice features of some versions of BackTrack is that they are not automatically assigned IP Addresses though the use of DHCP, or Dynamic Host Configuration Protocol. The idea is to come on the network quietly, without being detected.

- Only the loopback address, 127.0.0.1, is displayed when you type:
root@bt:~#ifconfig



```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# ifconfig
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bt:~#

```

Figure 4: No IP Address, other than the Loopback Address of 127.0.0.1, is Displayed

- Type the following command to view all available interfaces on the system:
root@bt:~#ifconfig -a



```

root@bt:~# ifconfig -a
eth0    Link encap:Ethernet  HWaddr 00:0c:29:31:4f:f2
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
        Interrupt:19 Base address:0x2000

eth1    Link encap:Ethernet  HWaddr 00:0c:29:31:4f:fc
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
        Interrupt:19 Base address:0x2080

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

```

Figure 5: All Available Interfaces on the System

Neither of the interfaces, eth0 or eth1, are assigned IP Addresses on their respective networks. The reason the sniffer has two interfaces is that it is located on two networks.

Note: The pfSense Firewall also has 2 interfaces and is also connected to both networks.

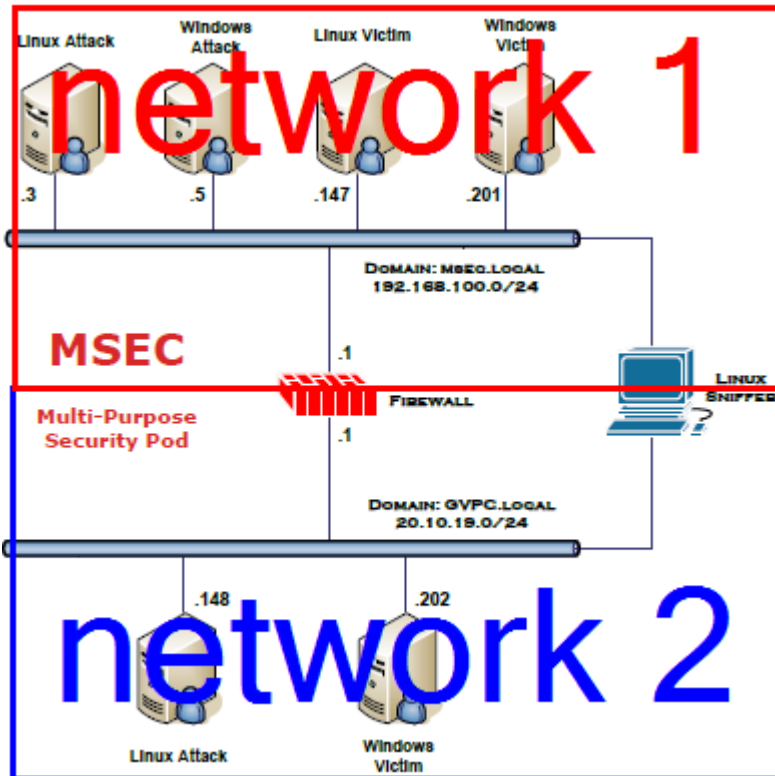


Figure 6: The Sniffer is Connected to Two Networks

A sniffer should be operating in promiscuous mode so it can see all network traffic.

Two ways to ensure that a sniffer will capture all traffic on a network segment are:

- Connect the Sniffer and other devices on the Network to a Hub
 - Connect the Sniffer to a switch's SPAN port, Switched Analyzed Network Port
5. To activate the first interface, type the following command:
- ```
root@bt:~#ifconfig eth0 up
```

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# ifconfig eth0 up
root@bt:~#
```

Figure 7: Activating the First Interface



- To verify the first interface, type the following command:

```
root@bt:~#ifconfig eth0
```

```
root@bt:~# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:0c:29:31:4f:f2
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
 Interrupt:19 Base address:0x2000

root@bt:~#
```

Figure 8: The Interface is activated without an IP Address

- To activate the second interface, type the following command:

```
root@bt:~#ifconfig eth1 up
```

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# ifconfig eth1 up
```

Figure 9: Activating the Second Interface

- To verify the second interface, type the following command:

```
root@bt:~#ifconfig eth1
```

```
root@bt:~# ifconfig eth1
eth1 Link encap:Ethernet HWaddr 00:0c:29:31:4f:fc
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
 Interrupt:19 Base address:0x2080

root@bt:~#
```

Figure 10: The Interface is activated without an IP Address

The Linux/UNIX utility tcpdump is commonly used by network administrators to capture network traffic on a sniffer. Many sniffer machines do not have GUI, or Graphical User Interfaces, so running GUI based tools like Wireshark or Network Miner is not possible. Another benefit to using tcpdump is that it handles very large capture files with no problem.

9. Type the following command to view several available switches for tcpdump:

```
root@bt:~#tcpdump --help
```

```
root@bt:~# tcpdump --help
tcpdump version 3.9.8
libpcap version 0.9.8
Usage: tcpdump [-aAdDeflLnNOpqRStuUvxx] [-c count] [-C file_size]
[-E algo:secret] [-F file] [-i interface] [-M secret]
[-r file] [-s snaplen] [-T type] [-w file]
[-W filecount] [-y datalinktype] [-Z user]
[expression]
```

Figure 11: The Available Options for tcpdump

10. To run tcpdump on the network segment interface eth0 is connected to, type:

```
root@bt:~#tcpdump -i eth0
```

Wait until at least one packet is displayed before stopping the capture.

```
root@bt:~# tcpdump -i eth0
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
18:10:47.797078 IP 192.168.100.5.netbios-dgm > 192.168.100.255.netbios-dgm: NBT UDP PACKET(138)
```

Figure 12: The output of tcpdump on the network segment interface eth0 is connected

After a packet or more is displayed, hit Control + C to stop the network capture.  
If the network 192.168.100.0/24 is displayed, eth0 is located on the first network.  
If the network 10.10.19.0/24 is displayed, eth0 is located on the second network.  
Also, notice that the default for tcpdump is to only capture the first 96 bytes.

11. To run tcpdump on the network segment interface eth1 is connected to, type:

```
root@bt:~#tcpdump -i eth1
```

Wait until at least one packet is displayed before stopping the capture.

```
root@bt:~# tcpdump -i eth1
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
18:33:25.983374 IP 10.10.19.202.netbios-dgm > 10.10.19.255.netbios-dgm: NBT UDP PACKET(138)
```

Figure 13: The output of tcpdump on the network segment interface eth1 is connected

After one packet or more is displayed, hit **CTRL-C** to stop the network capture.  
If the network 192.168.100.0/24 is displayed, eth1 is located on the first network.  
If the network 10.10.19.0/24 is displayed, eth1 is located on the second network.

12. To capture traffic on the 192.168.100.0/24 network and send it to a file, type:  
**root@bt:~#tcpdump -i eth0 -nntttt -s 0 -w capnet1.pcap -C 100**

```
root@bt:~# tcpdump -i eth0 -nntttt -s 0 -w capnet1.pcap -C 100
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```

Figure 14: tcpdump syntax

The following table lists details of the switches used with the tcpdump command:

|         |                                                              |
|---------|--------------------------------------------------------------|
| -i eth0 | Use interface zero                                           |
| -nntttt | Disable DNS resolution, date and time format                 |
| -s 0    | Disables default packet size of 96 bytes, full packet size   |
| -w      | Write to a capture file, instead of displaying to the screen |
| -C      | Split the captures into files of this size                   |

The diagram shows the command `tcpdump -i eth0 -nntttt -s 0 -w capnet1.pcap -C 100` with red arrows pointing to each option. Below the arrows are labels: 'Interface' under `-i eth0`, 'format' under `-nntttt`, 'size' under `-s 0`, 'file name' under `-w capnet1.pcap`, and 'PCAP size' under `-C 100`.

Figure 15: Detailed tcpdump Syntax Explained

Wait about 5 minutes so that your capture file will have some generated traffic. Press **CTRL-C** to stop tcpdump from running and discontinue the network capture.

13. To view the capture file, type the following command at the BackTrack terminal:  
**root@bt:~#wireshark capnet1.pcap**

The screenshot shows a terminal window titled 'root@bt: ~ - Shell'. The menu bar includes 'Session', 'Edit', 'View', 'Bookmarks', 'Settings', and 'Help'. The terminal prompt shows the command `root@bt:~# wireshark capnet1.pcap` being entered.

Figure 16: Opening the tcpdump capture with Wireshark

14. Check the **Don't show the message again** box and click the **OK** button.



Figure 17: Opening the tcpdump capture with Wireshark

Wireshark will open and the capture file will appear, similar to the one seen below:  
Notice that the traffic listed takes place on the 192.168.100.0/24 network.

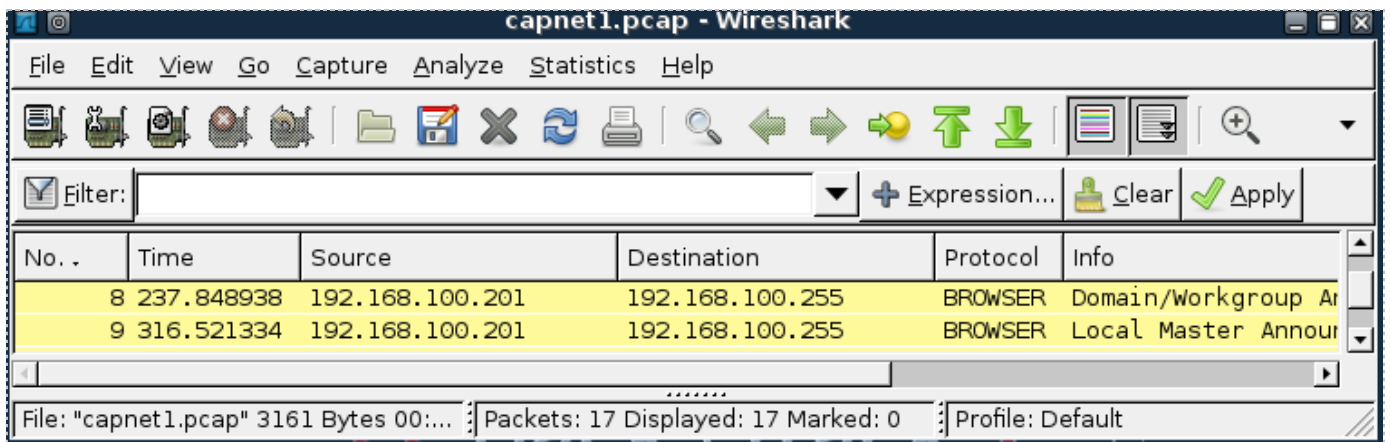


Figure 18: The tcpdump Capture is Displayed within Wreshark

15. To capture traffic on the 10.10.19.0/24 network and send it to a file, type:  
`root@bt:~#tcpdump -i eth1 -nntttt -s 0 -w capnet2.pcap -C 100`

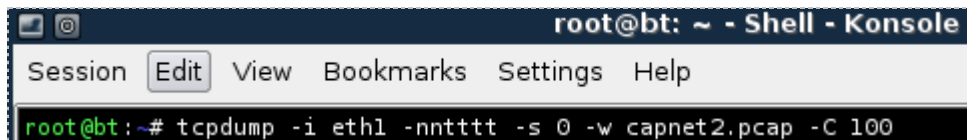


Figure 19: tcpdump syntax

Wait about 5 minutes so that your capture file will have some generated traffic.  
Press **CTRL-C** to stop tcpdump from running and discontinue the network capture.

16. To view the capture file, type the following command at the BackTrack terminal:  
**root@bt:~#wireshark capnet2.pcap**

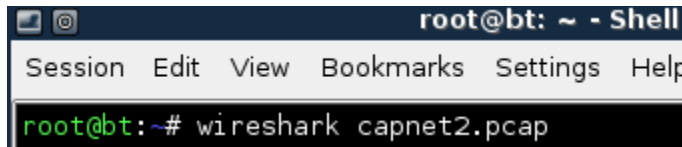


Figure 20: Opening the tcpdump capture with Wireshark

Wireshark will open and the capture file will appear similar to the one seen below:  
 Notice that the traffic listed takes place on the 10.10.19.0/24 network.

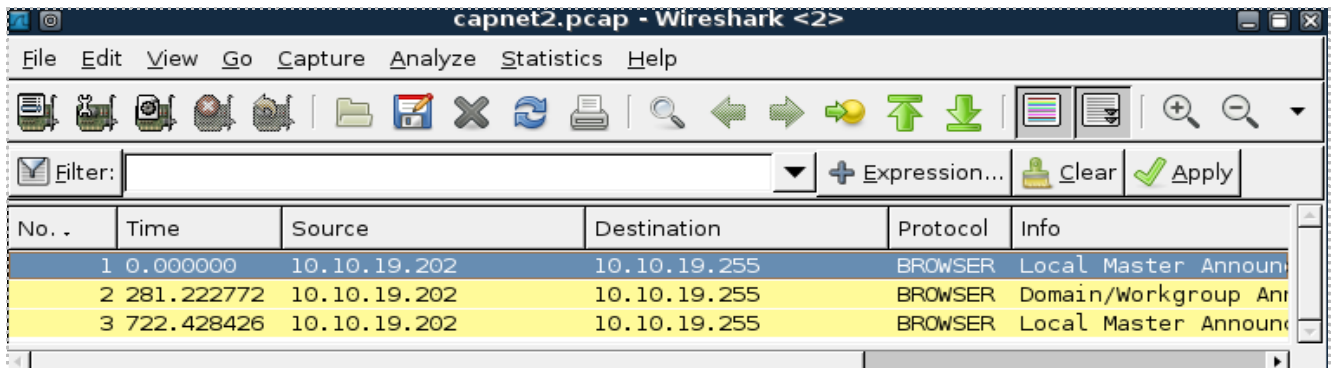


Figure 21: The tcpdump Capture is Displayed within Wireshark

You can also filter which type of traffic you want to see with tcpdump. For example, if you just want to see ICMP traffic, you can filter tcpdump for that type of traffic.

17. Log on to the Windows Internal 2003 Server by clicking the **Send Ctrl-Alt-Del** link in the bottom right hand corner of the browser window. Log on to the 2003 server with the username of **Administrator** and the password of **password**.



Figure 22: Send Ctrl-Alt-Del to the Windows 2003 Server

18. Click the shortcut to the command prompt icon on the Windows 2003 Desktop.

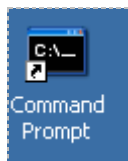


Figure 23: Windows 2003 Command Prompt

19. Type the following command to initiate a continuous ping of the gateway:  
**C:\ping 192.168.100.1 -t**

```

c:\ Command Prompt - ping 192.168.100.1 -t
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>ping 192.168.100.1 -t

Pinging 192.168.100.1 with 32 bytes of data:

Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64

```

Figure 24: Pinging the Gateway

20. On the Sniffer Machine, type the following to capture ICMP traffic on Network 1:  
**root@bt:~#tcpdump -i eth0 icmp**

```

root@bt:~# tcpdump -i eth0 icmp
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
19:36:43.440828 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 512, seq 56576, length 40
19:36:43.443998 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 512, seq 56576, length 40
19:36:44.440599 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 512, seq 56832, length 40
19:36:44.440617 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 512, seq 56832, length 40
19:36:45.440482 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 512, seq 57088, length 40
19:36:45.440743 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 512, seq 57088, length 40
19:36:46.440444 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 512, seq 57344, length 40
19:36:46.440709 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 512, seq 57344, length 40

```

Figure 25: Capturing ICMP Traffic with tcpdump

Press **CTRL-C** to stop tcpdump from running and discontinue the network capture.

21. Log on to the Windows External 2003 Server by clicking the **Send Ctrl-Alt-Del** link in the bottom right hand corner of the browser window. Log on to the 2003 server with the username of **Administrator** and the password of **password**.



Figure 26: Send Ctrl-Alt-Del to the Windows 2003 Server

22. Click the shortcut to the command prompt icon on the Windows 2003 Desktop.



Figure 27: Windows 2003 Command Prompt

23. Type the following command to continuously ping the External BackTrack VM:  
**C:\>ping 10.10.19.148 -t**

```
C:\> Command Prompt - ping 10.10.19.148 -t
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>ping 10.10.19.148 -t

Pinging 10.10.19.148 with 32 bytes of data:

Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
```

Figure 28: Pinging the External BackTrack Machine

24. On the Sniffer Machine, type the following to capture ICMP traffic on Network 2:

```
root@bt:~#tcpdump -i eth1 icmp
```

```
root@bt:~# tcpdump -i eth1 icmp
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
19:53:43.231657 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 512, seq 38144, length 40
19:53:43.233400 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 512, seq 38144, length 40
19:53:44.231331 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 512, seq 38400, length 40
19:53:44.231593 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 512, seq 38400, length 40
19:53:45.231149 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 512, seq 38656, length 40
19:53:45.231413 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 512, seq 38656, length 40
19:53:46.231294 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 512, seq 38912, length 40
19:53:46.231575 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 512, seq 38912, length 40
19:53:47.231192 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 512, seq 39168, length 40
```

Figure 29: Capturing ICMP Traffic with tcpdump

Press **CTRL-C** to stop tcpdump from running and discontinue the network capture.

## Task 1.2 Conclusion

The tcpdump command is built into the Linux and Unix operating systems. It can be used to capture network traffic. The benefits of using tcpdump include the fact that many sniffer machines do not have GUI, or Graphical User Interfaces, so running GUI based tools like Wireshark is not possible. Another benefit to using tcpdump is that it handles very large capture files with no problem, and it allows you to filter for specific traffic.

## Task 1.3 Discussion Questions

1. Does a network interface on a sniffer machine require an IP Address?
2. In what mode does a sniffer's network interface operate?
3. How do you determine available switches for tcpdump?
4. How can you display all of the network interfaces in Linux?



## Task 2 Capturing and Analyzing Traffic with Wireshark

Wireshark is a GUI, or Graphical User Interface, tool that will allow you to capture and analyze network traffic. Wireshark runs on Windows, Linux, and on Mac OS X.

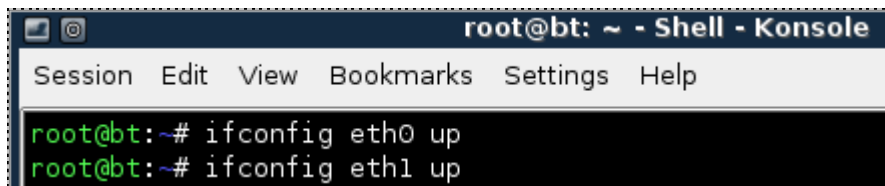
Wireshark can be downloaded from the following link:

<http://www.wireshark.org/download.html>.

### Task 2.1 Using Wireshark

Before using Wireshark, it is important to bring the sniffer interfaces up. Even though this was done in [Task 1](#), it is a good idea to start over to practice all of the required steps.

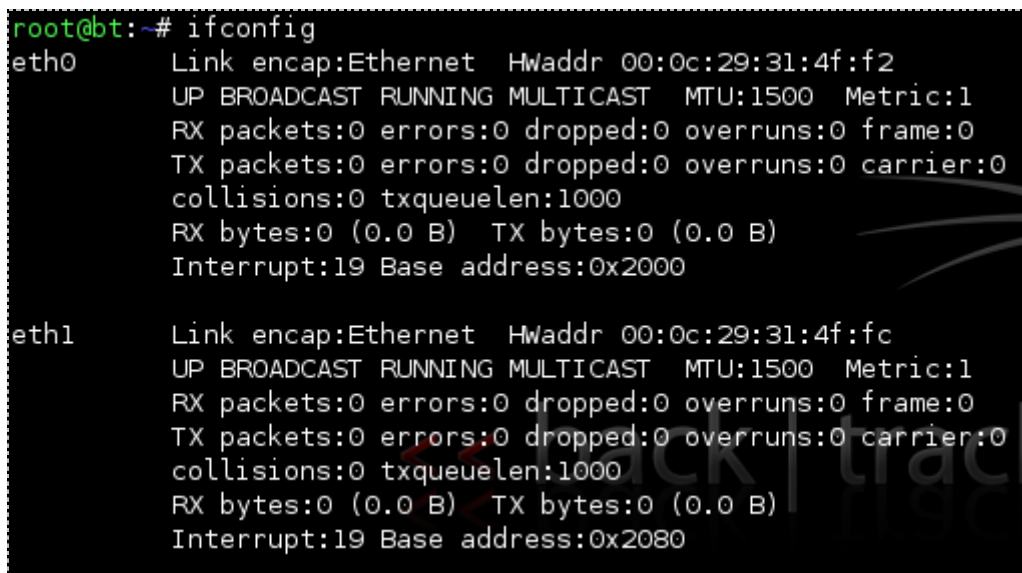
1. Bring both of the sniffer interfaces up by typing the following two commands:
  - a. `root@bt:~#ifconfig eth0 up`
  - b. `root@bt:~#ifconfig eth1 up`



```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# ifconfig eth0 up
root@bt:~# ifconfig eth1 up
```

Figure 30: Turning both Sniffer Interfaces on

2. Type the following to verify that no IP Address has been set for either interface:  
`root@bt:~#ifconfig`



```
root@bt:~# ifconfig
eth0 Link encap:Ethernet Hwaddr 00:0c:29:31:4f:f2
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
 Interrupt:19 Base address:0x2000

eth1 Link encap:Ethernet Hwaddr 00:0c:29:31:4f:fc
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
 Interrupt:19 Base address:0x2080
```

Figure 31: Verifying that the Sniffer Interfaces do not have IP Addresses

3. In the BackTrack terminal, type the following command to start Wireshark:  
root@bt:~#wireshark

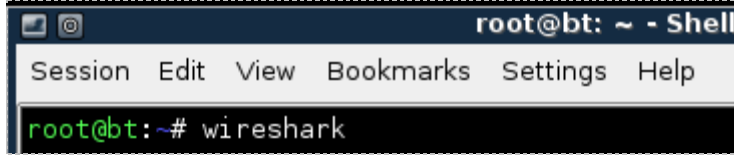


Figure 32: Opening Wireshark

4. To view the available interfaces, select **Capture** then go down to **Interfaces**.

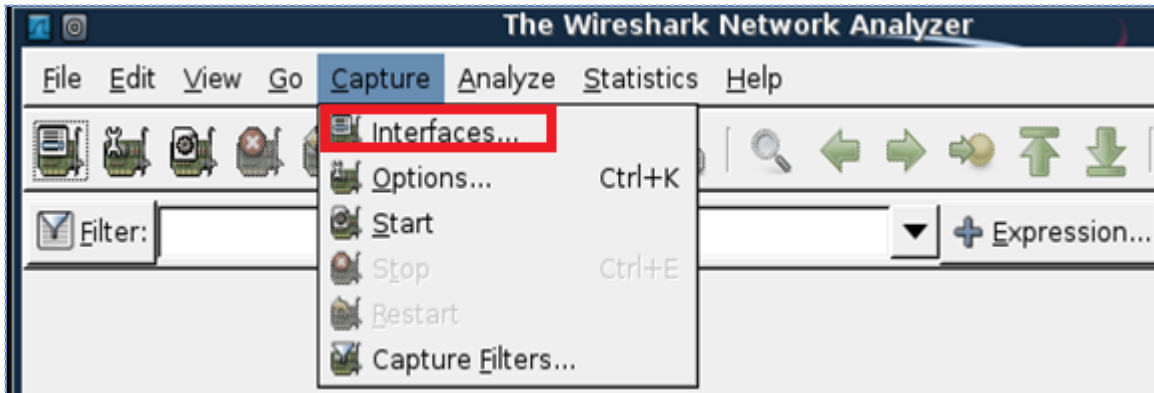


Figure 33: Selecting Interfaces from the Capture Menu

The **Wireshark: Capture Interfaces** pop-up box will be displayed on the sniffer.

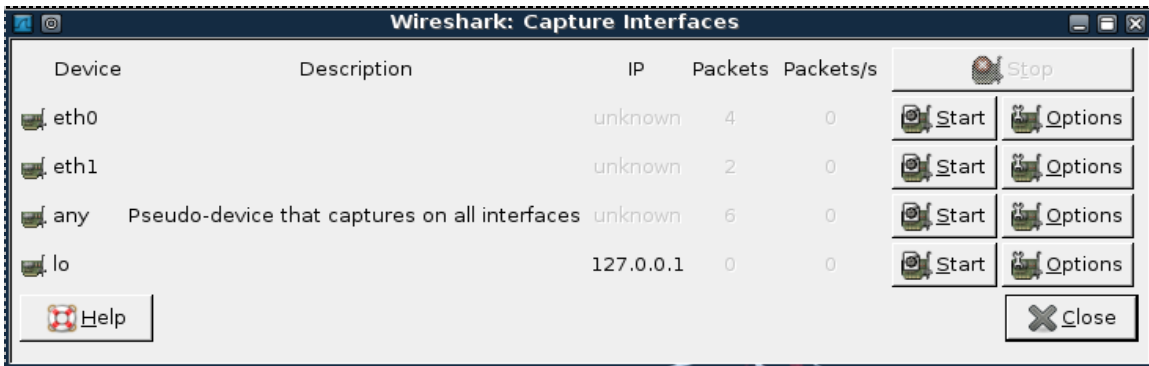


Figure 34: The Devices eth0 and eth1 do not have IP Addresses listed

Notice that eth0 and eth1 do not have IP Addresses listed under the IP column.

5. Within the **Capture Interfaces** menu, click **Start** for the eth0 network device.

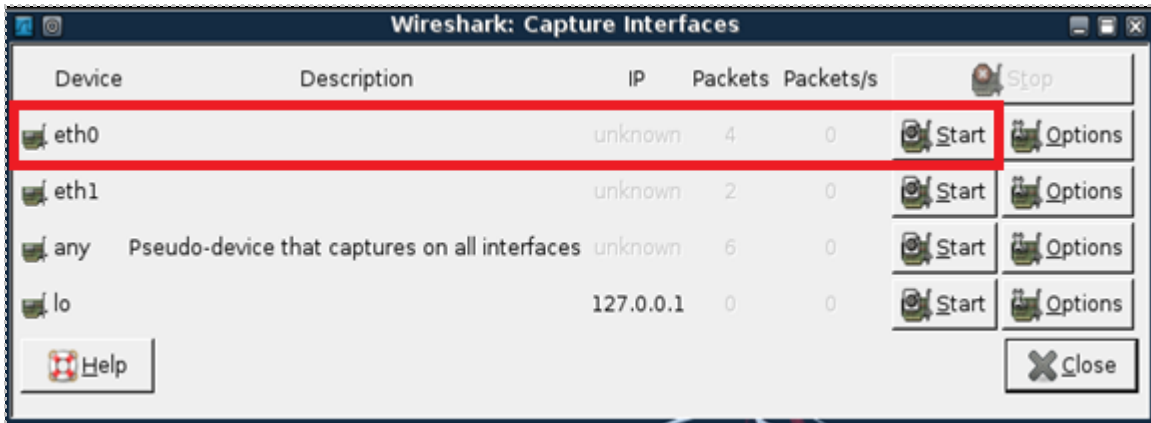


Figure 35: Starting a Capture on the Network using Interface eth0

During this exercise, we will be capturing plain text FTP, or File Transfer Protocol, traffic from the Windows 7 Internal Machine to the Windows 2003 Internal machine.

6. Open a command prompt on the Windows 7 machine by double clicking on the **cmd-Shortcut** on the desktop.

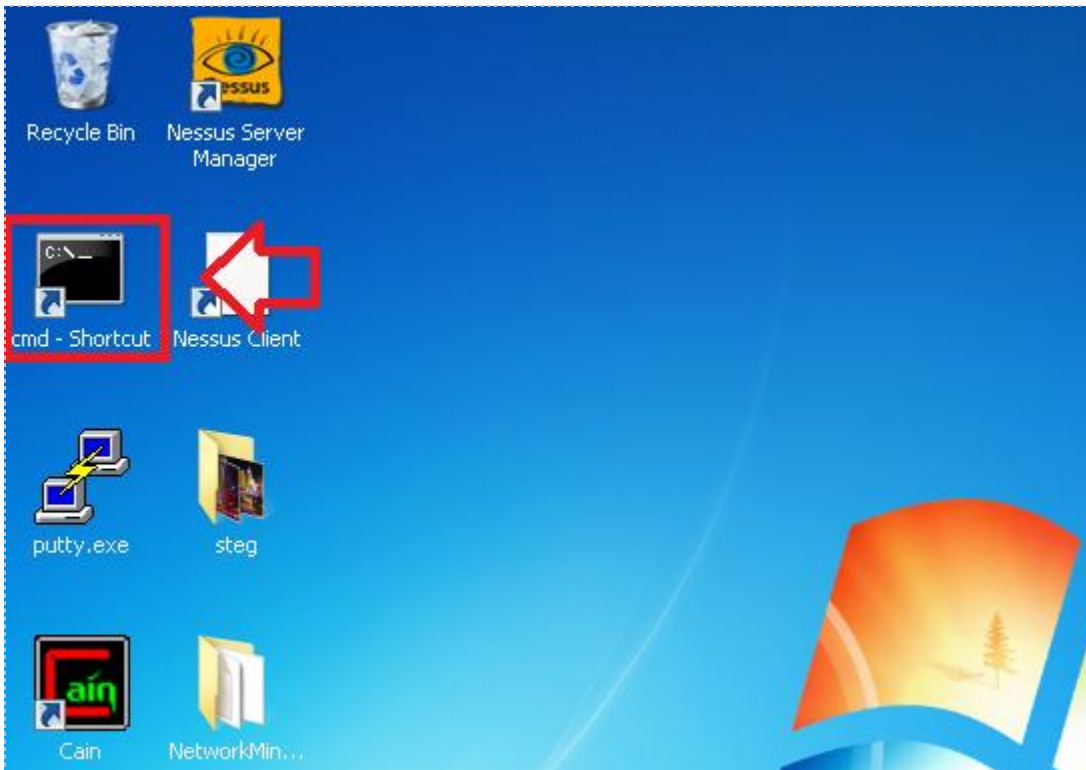


Figure 36: Opening a Command Prompt on Windows 7

7. Type the following command to connect to the Windows 2003 FTP Server:  
**C:\ftp 192.168.100.201**

```
c:\>ftp 192.168.100.201
Connected to 192.168.100.201.
220 Microsoft FTP Service
User (192.168.100.201:(none)):
```

Figure 37: Connecting to the FTP Server 192.168.100.201

You should receive the message, *connected to 192.168.100.201*.

8. For the username, type **ftp** and hit enter. For the password, type **mysecurepass**.  
Note: For security purposes, the password will not be displayed when you type it

```
User (192.168.100.201:(none)): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp>
```

Figure 38: Logging in to the FTP Server

You should receive the message, *230 Anonymous user logged in*.

9. On the sniffer machine, click the **stop** button on Wireshark to stop the capture.

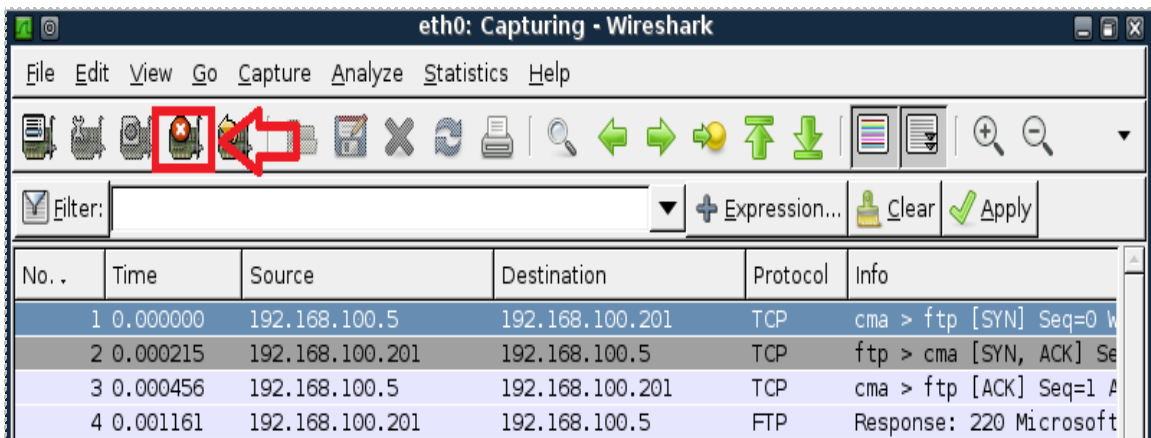


Figure 39: Stopping the Wireshark capture

10. On the sniffer machine, type **ftp** in the filter pane and click apply.

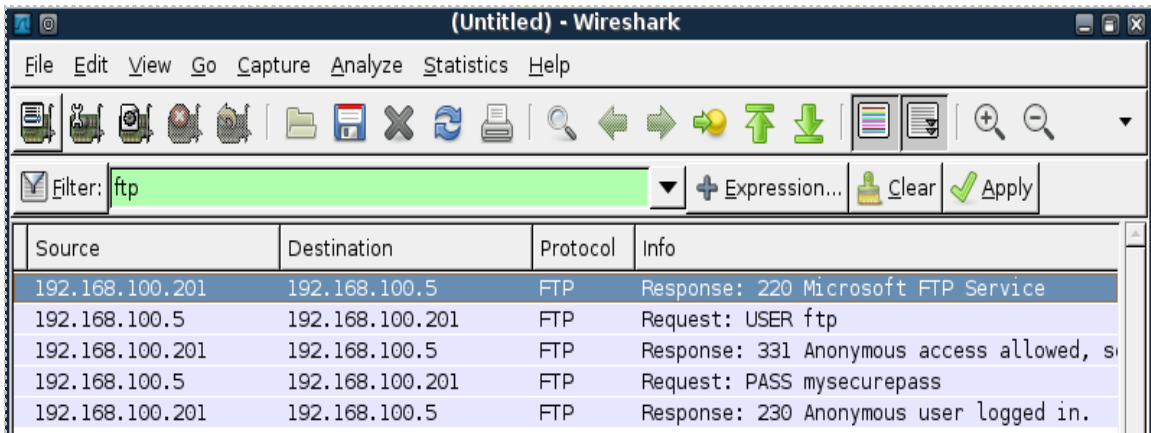


Figure 40: Typing ftp in the Wireshark filter pane

If you scroll over, you can see the username of ftp and the password of **mysecurepass**.

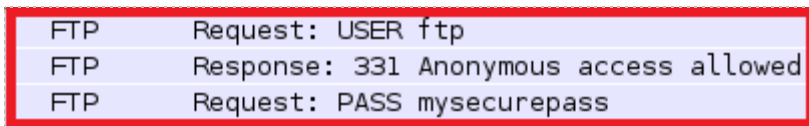


Figure 41: The FTP username and password appear in clear text.

Now, we will capture FTP traffic on the external network using interface eth1.

11. To view the available interfaces, select **Capture** then go down to **Interfaces**.

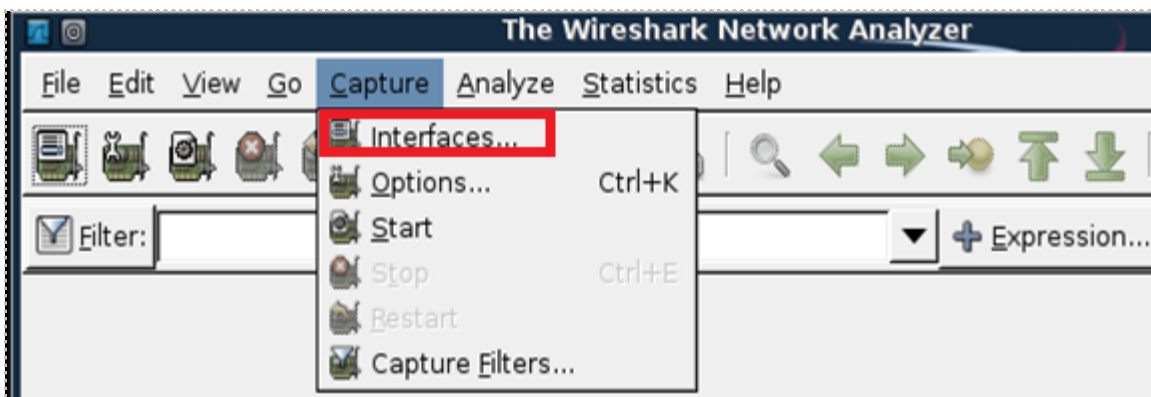


Figure 42: Selecting Interfaces from the Capture Menu

The **Wireshark: Capture Interfaces** pop-up box will be displayed on the sniffer.

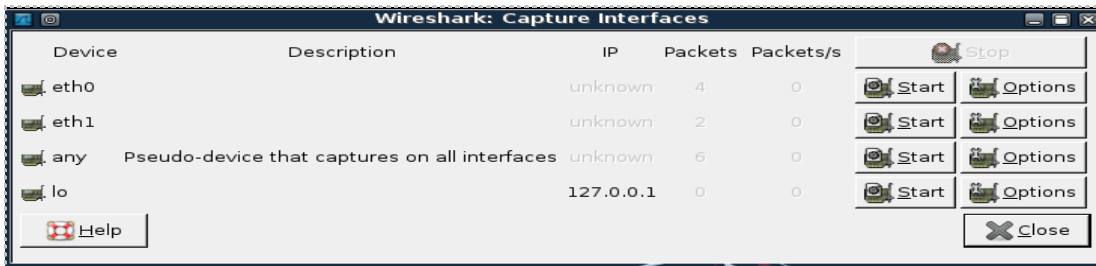


Figure 43: The Devices eth0 and eth1 do not have IP Addresses listed

Notice that eth0 and eth1 do not have IP Addresses listed under the IP column.

12. Within the **Capture Interfaces** menu, click Start for the eth1 network device.



Figure 44: Starting a Capture on the Network using Interface eth1

During this exercise, we will be capturing plain text FTP, or File Transfer Protocol, traffic from the BackTrack External Machine to the Windows 2003 External machine.

13. Click **Continue without Saving** if you receive a warning message.

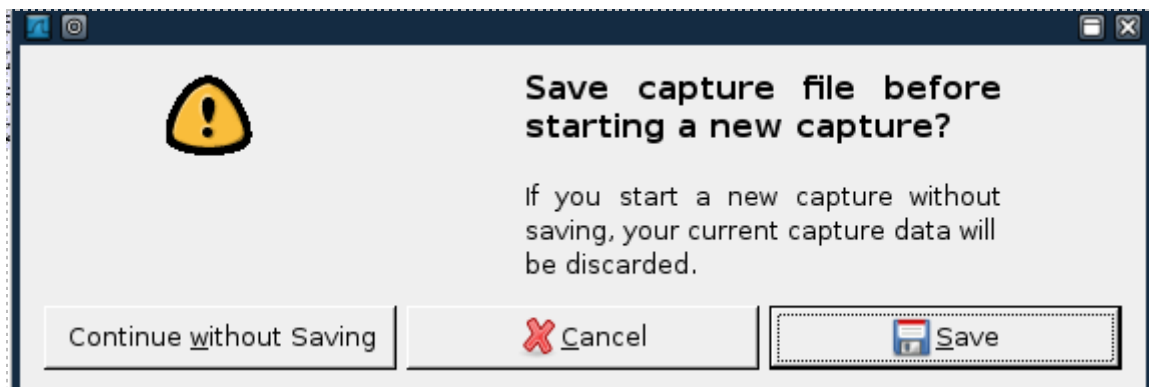


Figure 45: Continue Without Saving

- Log into the External BackTrack Machine with the username of **root** and the password of **password**. For security purposes, the password won't be displayed. Type the following command to initialize the GUI, Graphical User Environment:  
`root@bt:~#startx`

```

bt login: root
Password:
Last login: Sun Feb 8 18:33:44 EST 2009 on tty1
Linux bt 2.6.28.1 #2 SMP Wed Feb 4 21:50:02 EST 2009 i686
++ WELCOME TO THE BACKTRACK LIVE CD ++

[*] To start Networking - "/etc/init.d/networking start"
[*] To start KDE - "startx"
[*] To start FVWM - "bt4-crystal"

[*] http://www.remote-exploit.org/
root@bt:~# startx

```

Figure 46: Logging on to the External BackTrack machine

- Open a terminal on the Linux system by clicking on the image to the left of Firefox in the task bar, in the bottom of the screen in BackTrack.

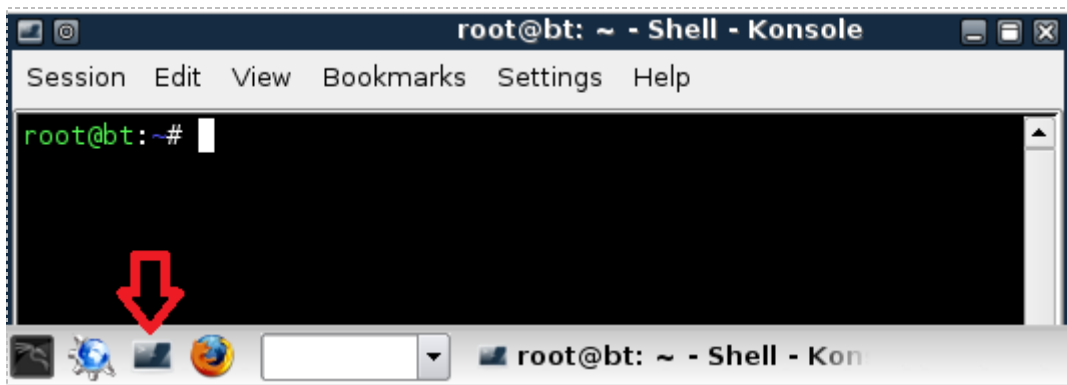


Figure 47: The BackTrack Terminal

- Type the following command to connect to the Windows 2003 FTP Server:  
`root@bt:~#ftp 10.10.19.202`

```

root@bt: ~ - Shell
Session Edit View Bookmarks Settings Help

root@bt:~# ftp 10.10.19.202
Connected to 10.10.19.202.
220 Microsoft FTP Service
Name (10.10.19.202:root):

```

Figure 48: Connecting to the FTP Server 192.168.100.201

You should receive the message, *Connected to 10.10.19.202.*

17. For the username, type **ftp** and hit enter. For the password, type **supersecure**.

For security purposes, the password will not be displayed when you type it.

```
Name (10.10.19.202:root): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
Remote system type is Windows_NT.
ftp> |
```

Figure 49: Logging in to the FTP Server

You should receive the message, 230 Anonymous user logged in.

18. On the sniffer machine, click the stop button on Wireshark to stop the capture.

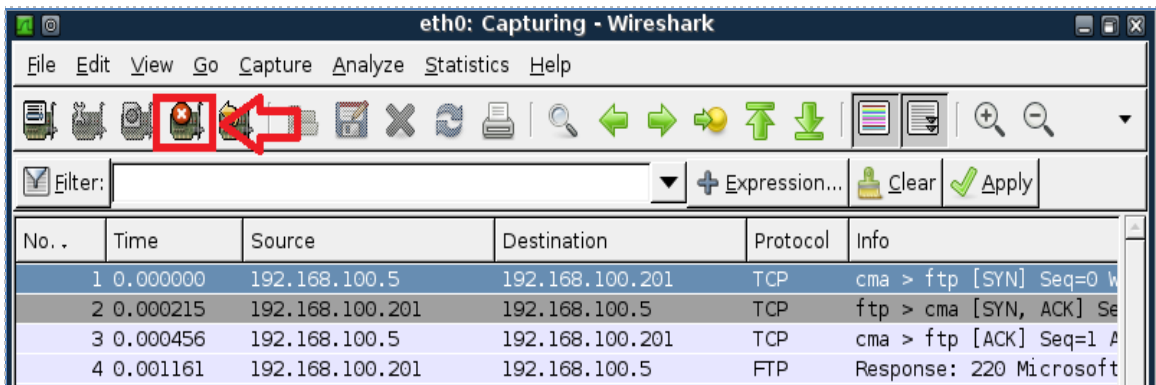


Figure 50: Stopping the Wireshark capture

19. On the sniffer machine, type **ftp** in the filter pane and click apply. (if needed)

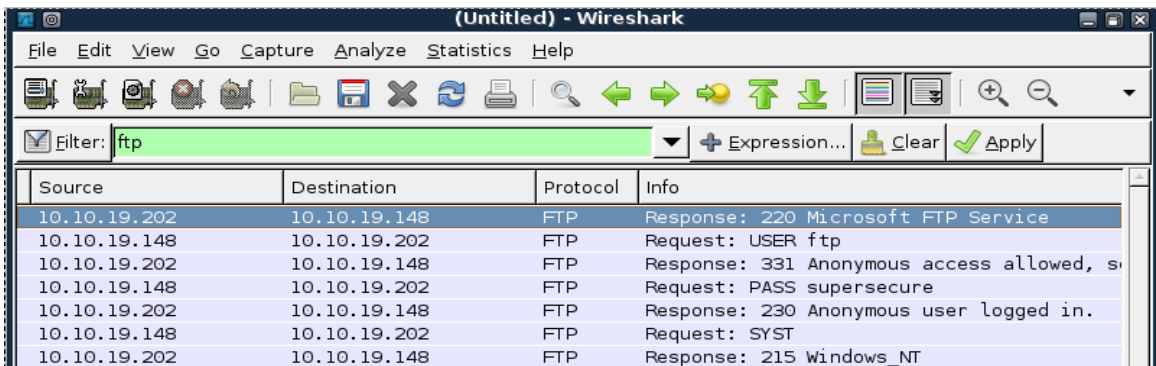
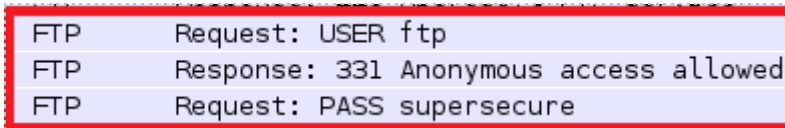


Figure 51: Typing ftp in the Wireshark filter pane



If you scroll over, you can see the username of **ftp** and the password of **supersecure**.



|     |                                        |
|-----|----------------------------------------|
| FTP | Request: USER ftp                      |
| FTP | Response: 331 Anonymous access allowed |
| FTP | Request: PASS supersecure              |

**Figure 52:** The FTP username and password appear in clear text.

## Task 2.2 Conclusion

Wireshark is a GUI, or Graphical User Interface, tool that will allow you to capture and analyze network traffic. Wireshark runs on Windows, Linux, and on Mac OS X. Wireshark can be used to capture network traffic on an interface on the sniffer without an IP Address. The Wireshark filter pane can be used to filter for various types of traffic.

## Task 2.3 Discussion Questions

1. Do FTP usernames and passwords appear in clear text?
2. How do you choose the interface to capture on within Wireshark?
3. How do you filter for a certain protocol within the Wireshark program?
4. How do you open the Wireshark program from the terminal in Linux?

### Task 3 Capturing and Analyzing Traffic with Network Miner

Network Miner is an NFAT, or Network Forensic Analysis Tool, that runs on Windows operating systems. The tcpdump command has no Graphical User Interface and is only utilized within a Linux terminal. Wireshark shows you the raw output of network traffic captures and allows you to analyze them. Network Miner will allow you to capture data, and it will also pull out items like clear text messages and pictures.

#### Task 3.1 Using Network Miner

##### Open Network Miner

1. Open Network Miner on Windows 7 by double clicking on the desktop shortcut.

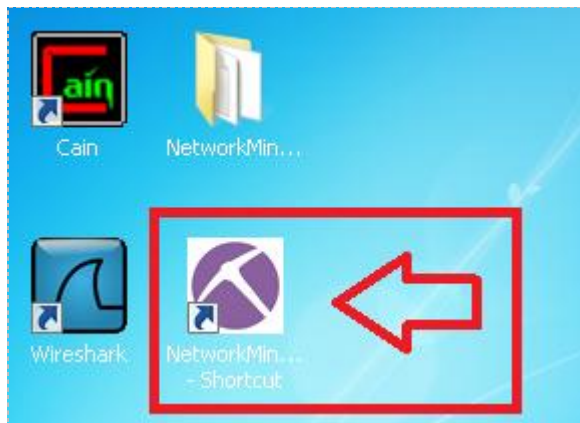


Figure 53: Opening Network Miner

2. Click the arrow to the right of the words **Select a network adapter in the list** and select: **Socket: Intel® PRO/1000MT Network Connection(192.168.100.5)**

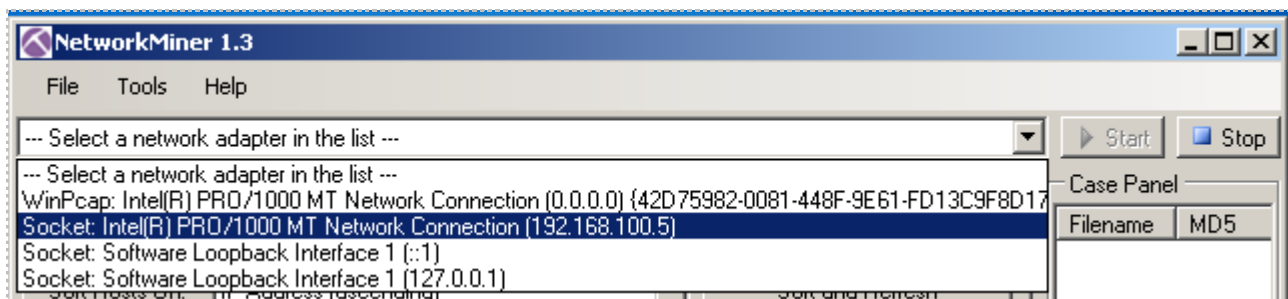


Figure 54: Selecting the Appropriate Interface

Verify that the correct Interface has now been selected within Network Miner.

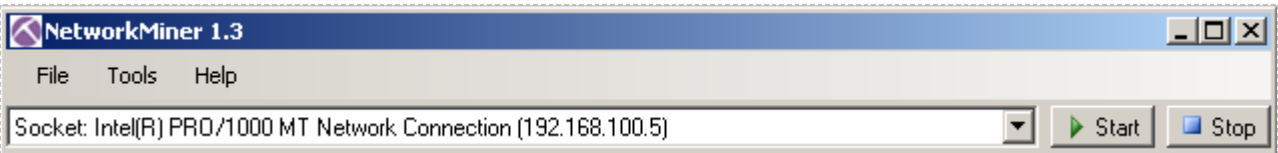


Figure 55: The Correct Interface has been selected within Network Miner

3. Click the **Start** button, located on the right, to start a network capture.



Figure 56: Starting the Capture

4. Click on the **Internet Explorer Icon** in the Windows Taskbar.



Figure 57: Opening Internet Explorer

Internet Explorer should open to a Blank Page with **about:blank** in the URL bar.

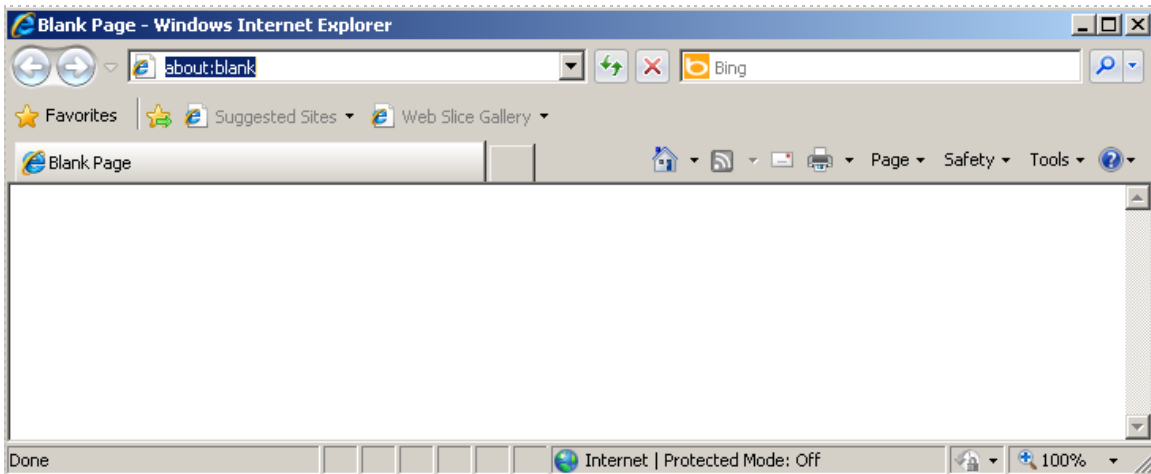


Figure 58: A Blank Page in Internet Explorer

- In the URL bar, type the following to connect to the Windows 2003 Web Page:  
<http://192.168.100.201/>

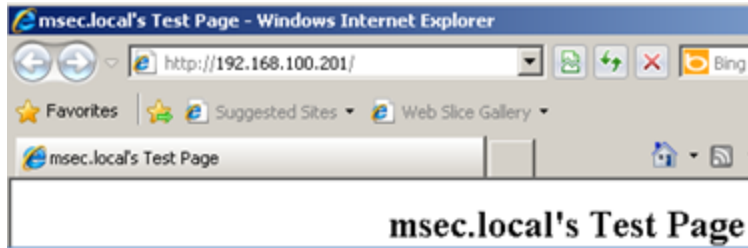


Figure 59: The Windows 2003 Web Page

You should see the msec.local's Test Page when connecting to the Windows 2003 Server.

- In the URL bar, type the following to connect to the RHEL Web Page:  
<http://192.168.100.147/>



Figure 60: The RHEL Web Site

- Click on the **Stop** button to end the Network Miner capture.

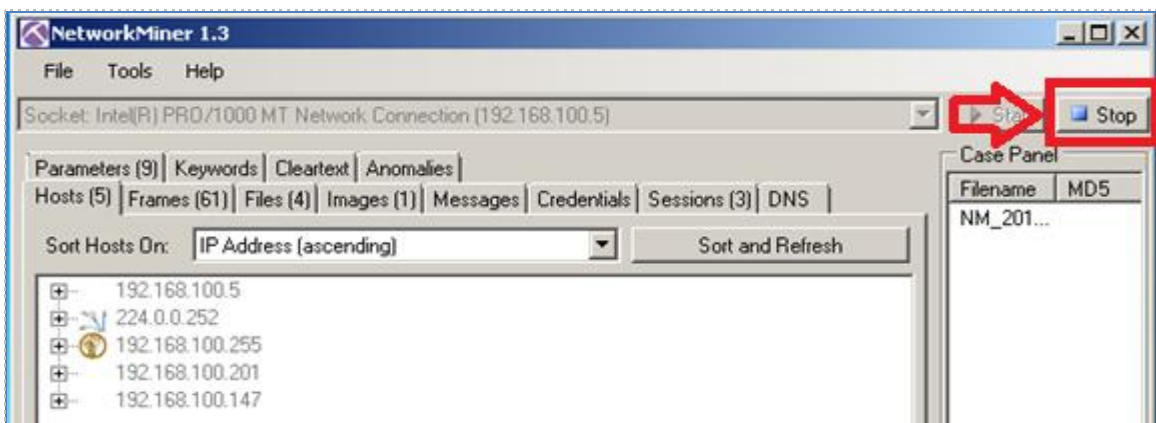


Figure 61: Files within the Network Capture

- Click on the **Files** tab within the Network Miner Program.

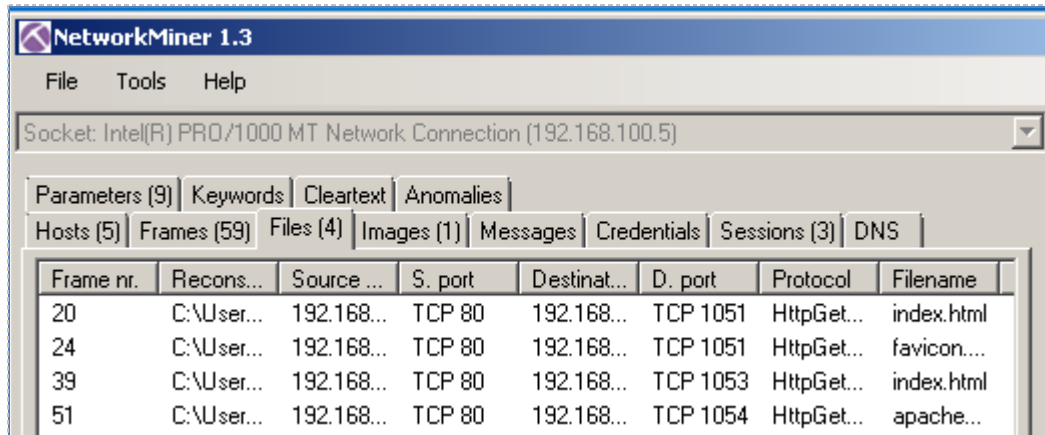


Figure 62: Files within the Network Capture

- Right click on the first **index.html** file and select open file.

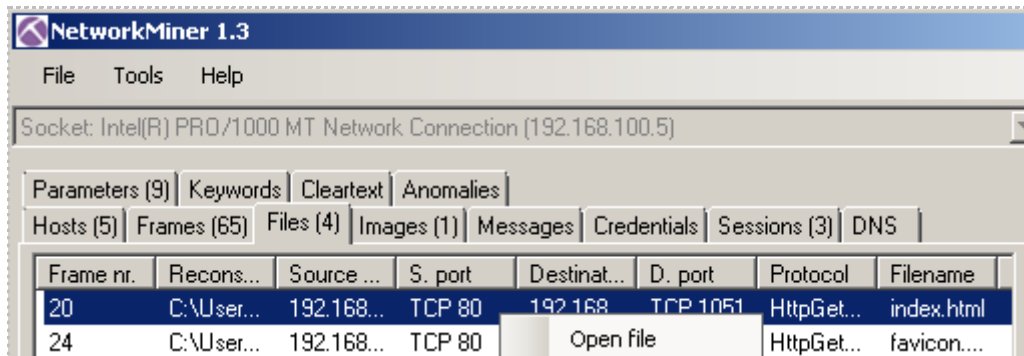


Figure 63: The index.html file saved within the Network Capture

You should see msec.local's test page.

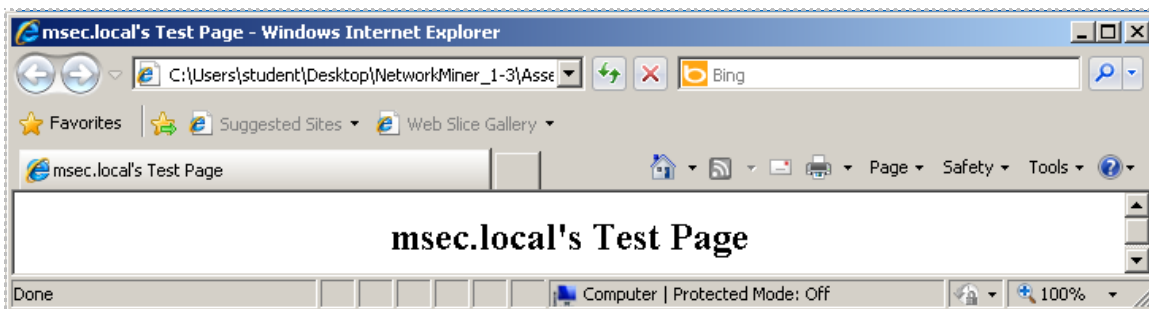


Figure 64: Opening a Local Copy of the Index.html file

10. Right click on the second **index.html** file and select open file.

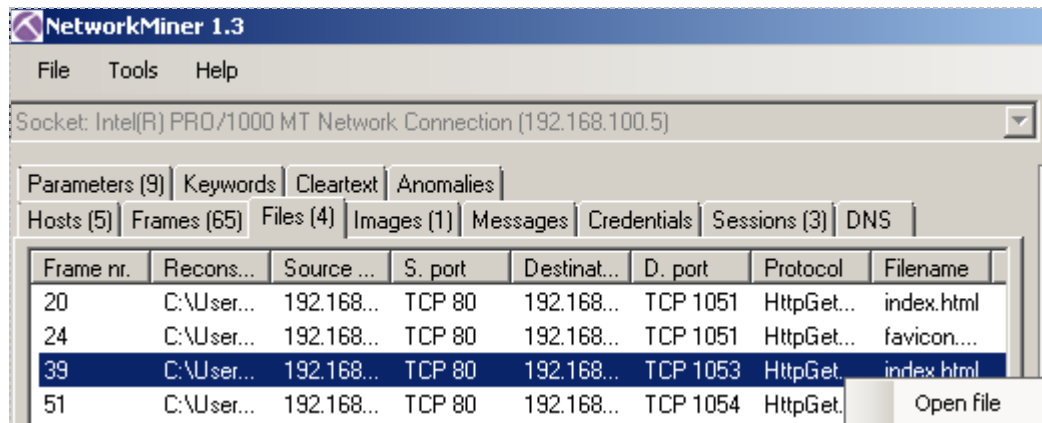


Figure 65: The index.html file saved within the Network Capture

You should see the Red Hat Enterprise Linux Test Page.

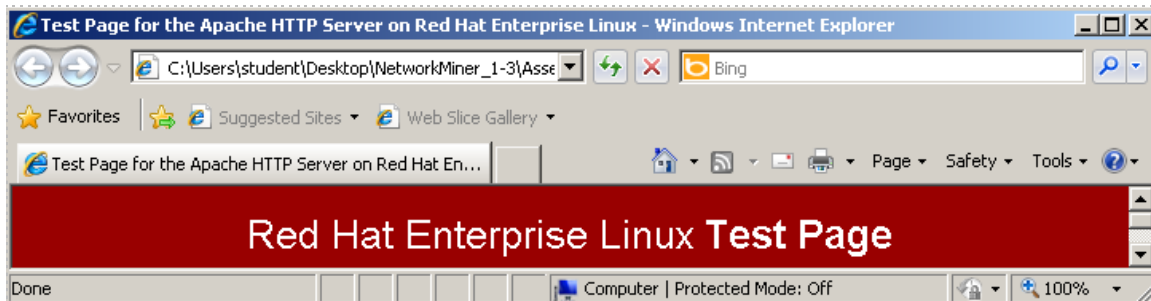


Figure 66: Opening a Local Copy of the Index.html file

### Task 3.2 Conclusion

Network Miner is an NFAT, or Network Forensic Analysis Tool, that runs on Windows operating systems. Network Miner will allow you to capture data and will also pull out items like clear text messages, pictures, and web pages from visited sites.

### Task 3.3 Discussion Questions

1. What kind of tool is Network Miner?
2. On what operating systems will the Network Miner program run?
3. How do you parse out web pages of visited sites in Network Miner?
4. What needs to be configured within Network Miner prior to capturing data?

## 5 References

1. Wireshark:  
<http://www.wireshark.org/>
2. Network Miner:  
<http://www.netresec.com/?page=NetworkMiner>
3. Man Page of tcpdump:  
[http://www.tcpdump.org/tcpdump\\_man.html](http://www.tcpdump.org/tcpdump_man.html)
4. Wireshark Download:  
<http://www.wireshark.org/download.html>
5. Network Miner Download:  
<http://sourceforge.net/projects/networkminer/files/latest/download>