



DIGITAL FORENSICS LAB SERIES

Lab 14: Log Analysis

Objective – Log Analysis

Document Version: **2014-02-07 (Beta)**

Organization: Moraine Valley Community College
Author: Jesse Varsalone

Copyright © National Information Security, Geospatial Technologies Consortium (NISGTC)

The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCT) 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. This work is licensed under the Creative Commons Attribution 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.



The Center for Systems Security and Information Assurance (CSSIA), in partnership with the Network Development Group (NDG) is given a perpetual worldwide waiver to distribute per US Law this lab and future derivatives of these works.

Contents

Introduction	3
Lab Topology	4
Lab Settings	5
1 Examining Windows Event Logs, IIS Logs, and Scheduled Tasks	6
1.1 Windows Event Viewer	6
1.2 Conclusion	16
1.3 Discussion Questions.....	16
2 Examining Windows IIS Logs.....	17
2.1 Connecting to the Windows 7 Website	17
2.2 Conclusion	23
2.3 Discussion Questions.....	23
3 Examining Linux Log Files.....	24
3.1 Examining access_log and auth_log.....	24
3.2 Conclusion	31
3.3 Discussion Questions	31
References	32

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.

This lab includes the following tasks:

1. Examining Windows Event Logs
2. Examining Windows IIS Logs
3. Examining Linux Log Files

Objective - Digital Forensics Fundamentals

Performing this lab will provide the student with a hands-on lab experience meeting the Digital Forensics Fundamentals Objective:

The candidate will demonstrate an understanding of the purpose of the various types of Windows event, service and application logs, and the types of information they can provide

By the end of this lab, students will be parse log files within Linux and Windows for information pertinent to security events on their system. Students will perform administration on Linux and Windows and view the logs from these tasks.

Event Viewer – The Event Viewer keeps track of Windows events. The three main logs within the Windows Event Viewer are the Application, Security, and System Log.

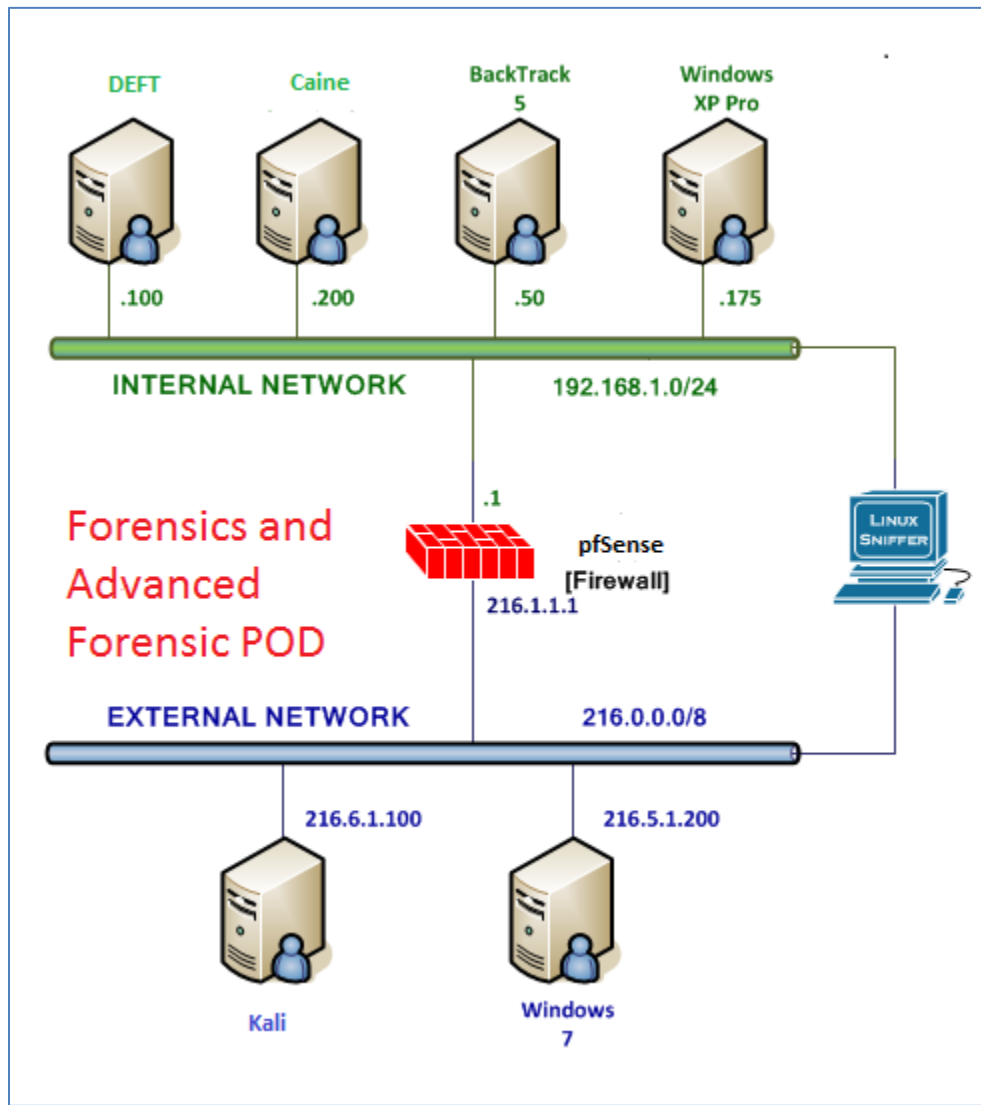
auth_log – This log file tracks SSH, or Secure Shell, connections. It provides information such as IP addresses, and date and time stamps. It also tracks other events related to security, such as the creation of new user accounts and new group accounts.

access_log – This log file tracks HTTP, or Hyper Text Transfer Protocol, connections. It provides information such as IP addresses, user agents, and date and time stamps.

Internet Information System Logs – Internet Information System, or IIS, logs keep track of IP addresses and user agents of systems connecting to Windows servers running Internet services, such as File transfer Protocol (FTP) and WWW (World Wide Web).

psloglist – Part of the PsTools suite, this file can dump Event Log information. The tool can be downloaded here: <http://download.sysinternals.com/files/PSTools.zip>

Lab Topology



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.

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		
DEFT Internal Machine	192.168.1.100		
Windows 7 External Machine	216.5.1.200	student	password

1 Examining Windows Event Logs, IIS Logs, and Scheduled Tasks

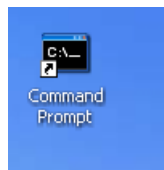
One of the first places to start when you are trying to determine what happened on a Microsoft Windows System is the Windows Event Viewer. Older Microsoft operating systems like Windows NT and 2000 did not log much by default, but newer operating systems like Windows 8 and Windows 2012 have more default logging enabled. Typically, a server operating system like Windows 2012 Server will have more logging enabled and have a large number of logs than a client operating system like Windows 8.

1.1 Windows Event Viewer

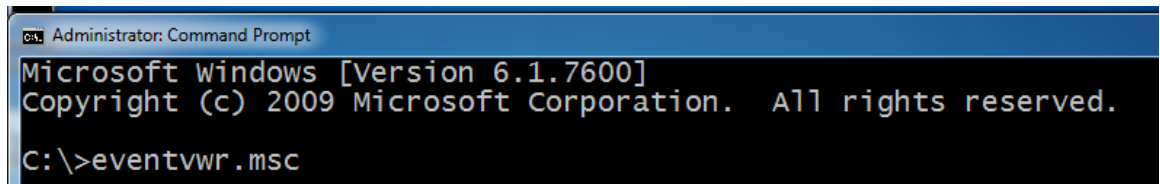
1. To log into the **Windows 7 External Machine**, click on the **Windows 7** icon on the topology.
2. If required, enter the username, **student**.
3. Type in the password, **password**, and press **Enter** to log in.



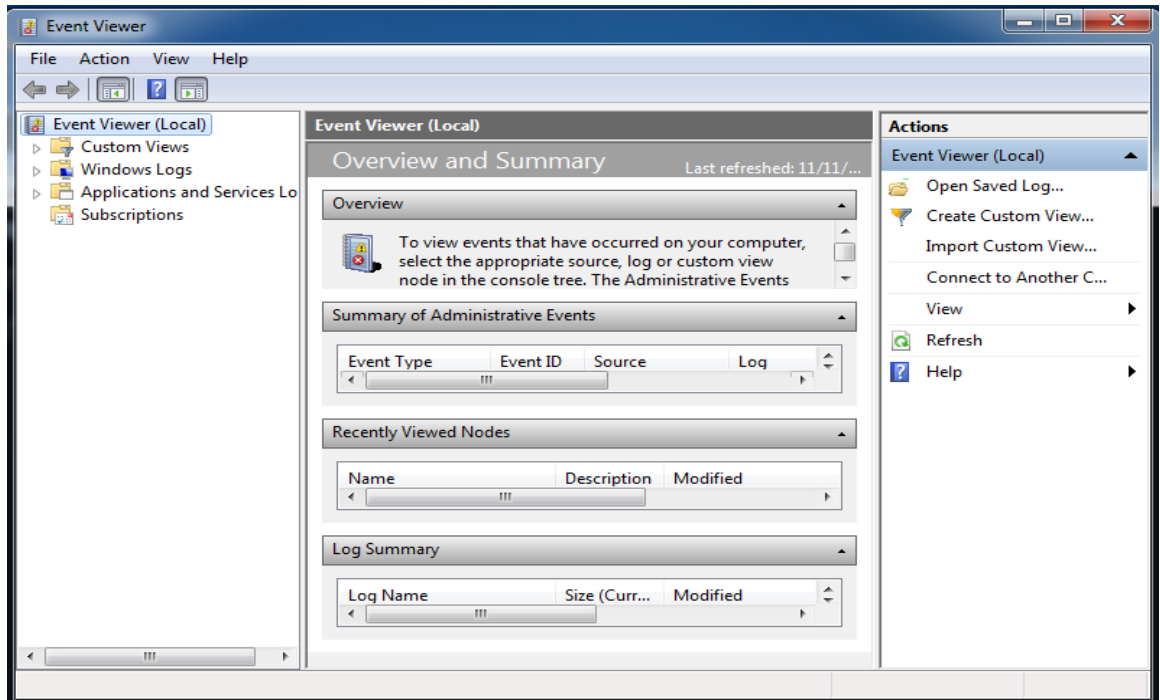
1. On **Windows 7**, open the Command Prompt by double-clicking on the shortcut.



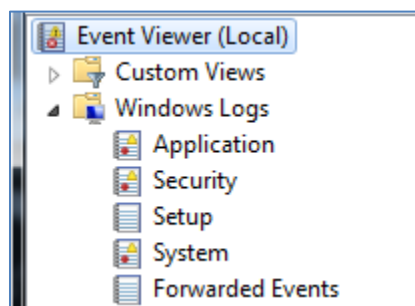
2. Type the following command to bring up the Event Viewer:
C:\>eventvwr.msc



3. After a short period, the Event Viewer window will appear.



4. Expand Windows Logs by clicking the arrow in front of the folder.

















There are three main logs within the Windows Event Viewer:



- Application Log - deals with issues related to the system's software
- Security Log - contains information about successful and failed attempts to access resources on the system
- System Log - contains information about the computer's hardware

There four message **Levels** within Microsoft's newer Event Viewer versions:

- Info
- Warning
- Error
- Critical

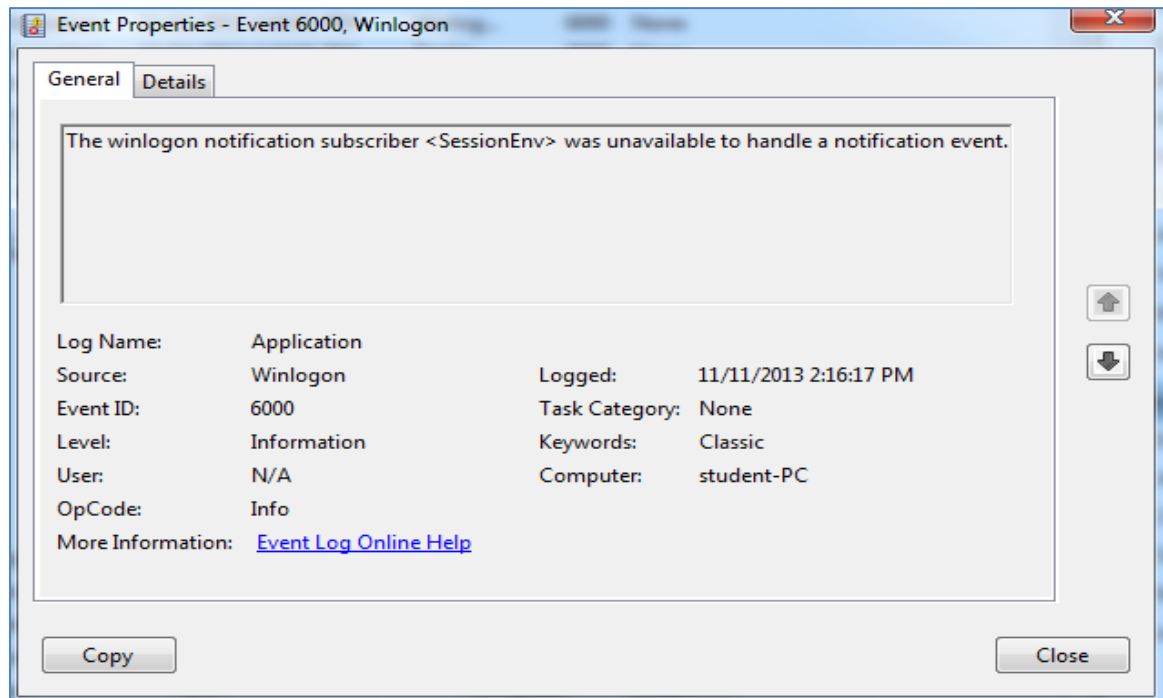
System Number of events: 2,233					
Level	Date and Time	Source	Event ID	Task Ca...	
 Information	7/11/2013 4:29:19 PM	Service ...	7036	None	
 Information	7/11/2013 4:29:18 PM	Service ...	7036	None	
 Information	7/11/2013 4:29:18 PM	Dhcp-C...	50036	Service ...	
 Information	7/11/2013 4:29:18 PM	Service ...	7036	None	
 Warning	9/23/2013 12:26:52 AM	Time-S...	134	None	
 Warning	8/13/2013 6:58:29 AM	Time-S...	134	None	
 Warning	11/11/2013 1:43:11 PM	Time-S...	134	None	
 Warning	7/8/2013 11:30:16 AM	Time-S...	134	None	
 Warning	7/8/2013 11:30:17 AM	Time-S...	134	None	
 Warning	10/22/2013 6:55:08 PM	Time-S...	36	None	
 Error	7/8/2013 7:52:55 PM	Service ...	7043	None	
 Error	11/11/2013 1:35:03 PM	EventLog	6008	None	
 Error	7/12/2013 3:38:59 PM	volsnap	36	None	
 Critical	11/11/2013 1:34:39 PM	Kernel-...	41	(63)	

For the Security Log, there are two keywords, Audit Success and Audit Failure.

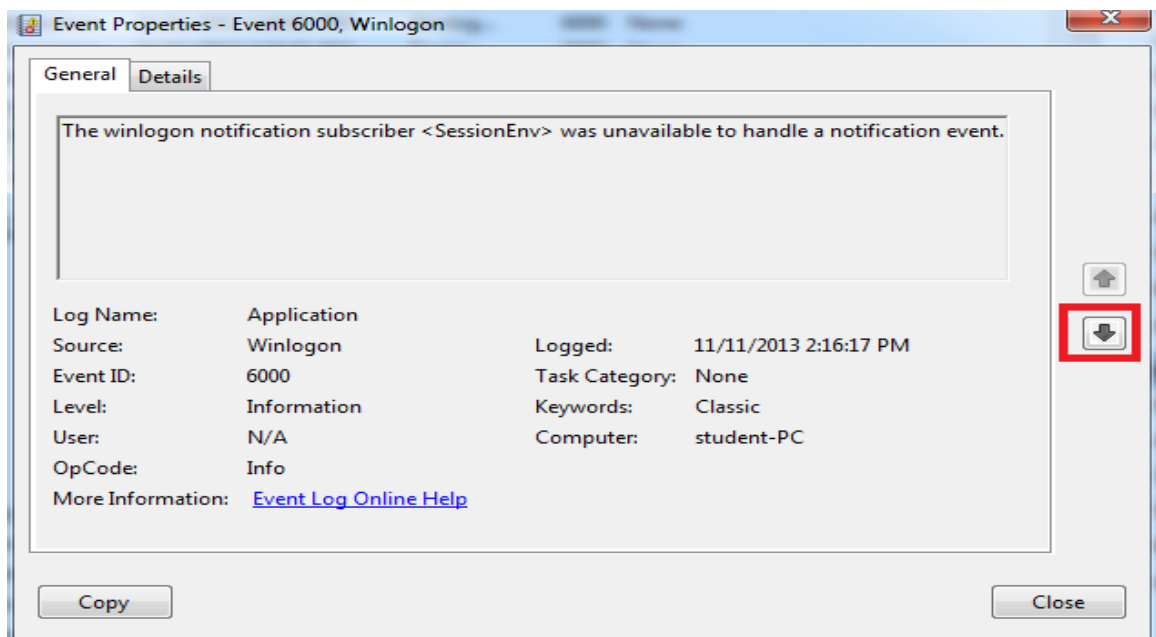
Security Number of events: 31,537 (!) New events available				
Keywords	Date and Time	Source	Event ID	Task C...
 Audit Success	3/30/2013 12:47:30 PM	Micros...	4907	Audit P...
 Audit Failure	10/21/2013 8:24:00 AM	Micros...	5038	System...

The user has the ability to further examine events. One important element for investigators is the date and time stamps that exist with each recorded incident.

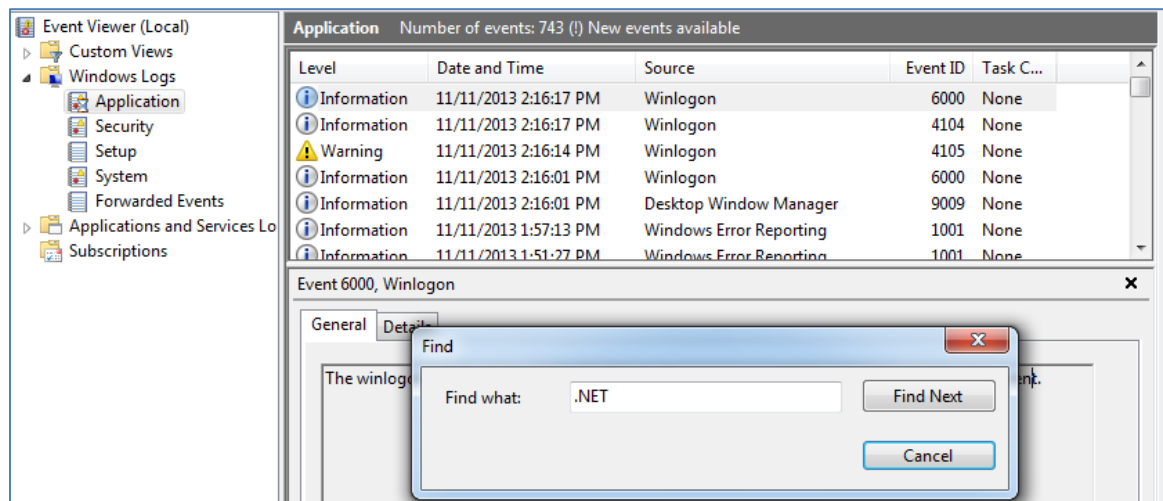
- Click on the Application Log. Click on the first event. View the date/time stamp.



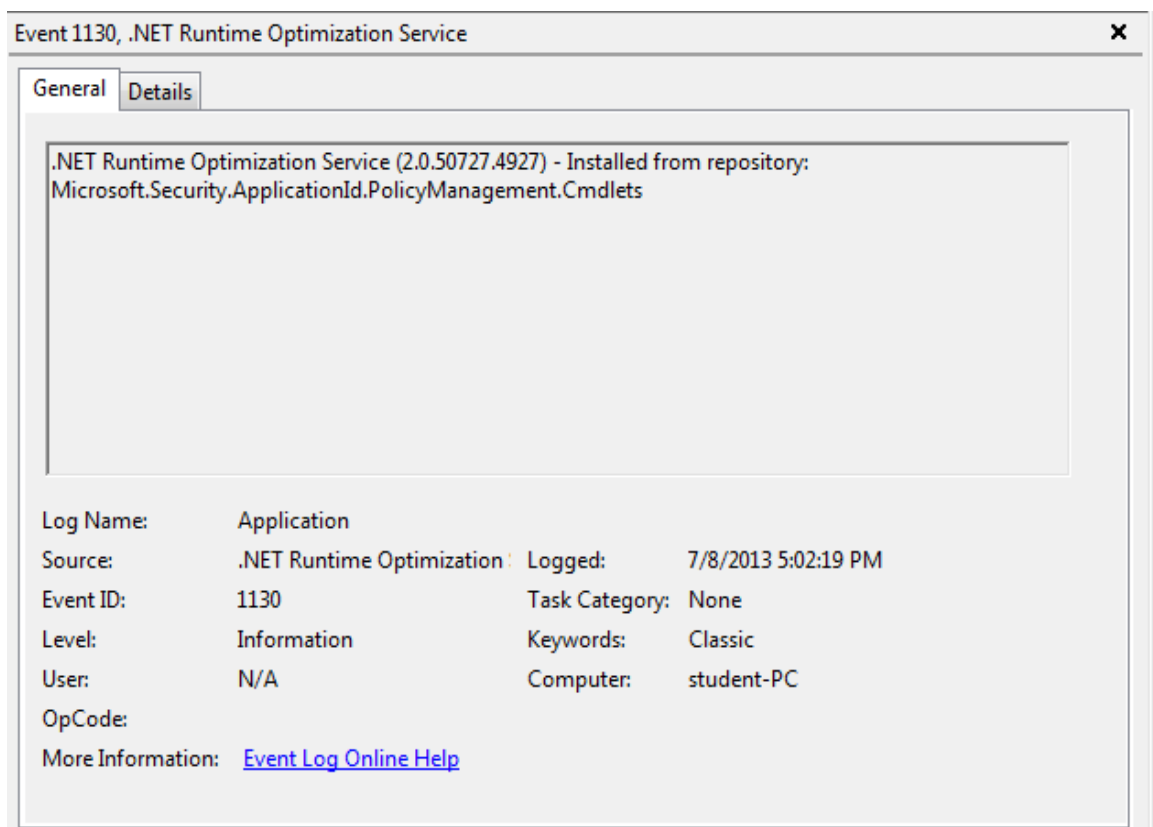
- Click the **down arrow** to view the next event in the list.



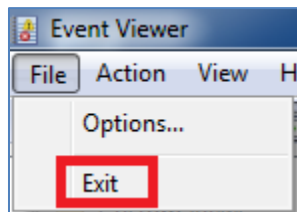
7. You also can search within a specific log for a specific event. Click the Find button in the right pane. Type **.NET** and click **Find Next**.



8. The event that has a match on the key word **.NET** will be displayed on the screen.

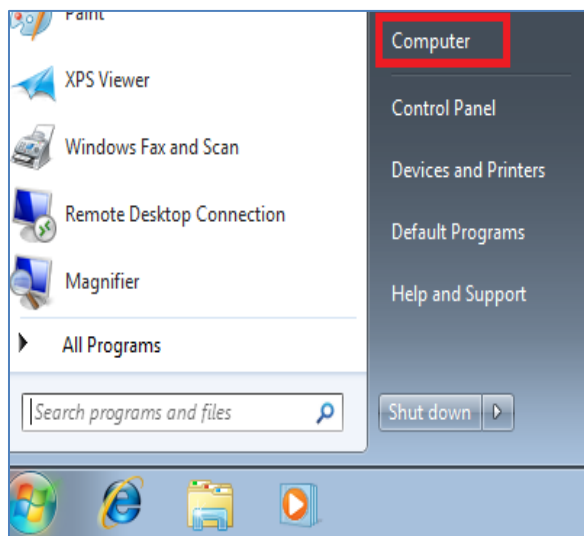


9. Select File from the Event Viewer menu bar and then press **Exit**.

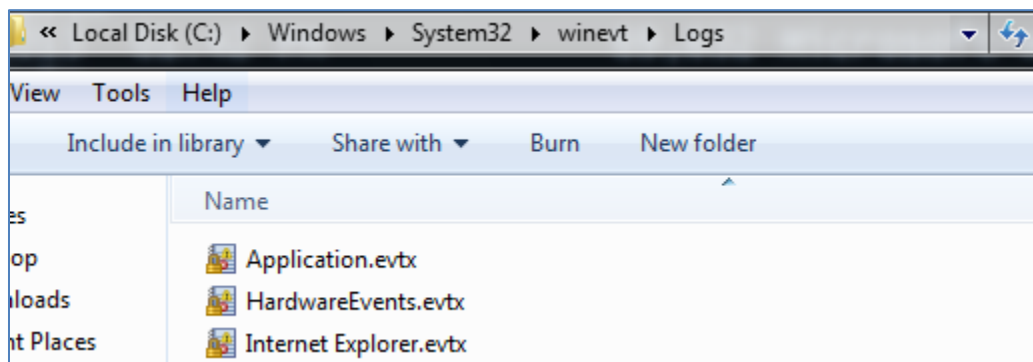


Next, we will examine the physical location of the Event Viewer files on the hard disk.

10. Click on the Start button and click the link to **Computer** on the right.



11. Double-click on C:, then select **Windows > System32 > winevt > Logs** to view the Event Viewer files.



With operating systems prior to Windows Vista (such as Windows 2003 Server, Windows XP, and Windows 2000), the Event Viewer files are stored in the EVT format. They can be converted to TXT or CSV files. They are stored in Windows\System32\config. It is important to note that the Windows registry files are also stored in this location.

Forensic Investigators usually examine the event viewer files using a forensic tool like FTK (Forensic Toolkit) from Access Data or EnCase (from Guidance Software).

Earlier versions of these forensic tools could not read Event Viewer files. However, the files in EVT format could be extracted from the image, and then opened with the Microsoft Event Viewer. The records could then be exported to a .TXT or CSV file. Newer versions of EnCase and FTK can read the files, so extraction is not necessary.

We can use a Sysinternals tool called PsLogList to read the Event Viewer Logs. This tool can be used during the incident response process to collect Event Viewer logs.

12. To dump the application log to a text file, type the following command:

```
C:\>psloglist -r "application" > application.txt
```

```
C:\>psloglist -r "application" > system.txt

PsLoglist v2.71 - local and remote event log viewer
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals - www.sysinternals.com
```

13. To view the dumped application log, type the following command:

```
C:\>notepad application.txt
```

```
C:\>notepad application.txt

application.txt - Notepad
File Edit Format View Help
Application log on \\STUDENT-PC:
[001] EventSystem
Type: INFORMATION
Computer: 37L4247D28-05
Time: 7/8/2013 10:27:09 AM ID: 4625
Message text not available. Insertion strings:
86400 SuppressDuplicateDuration Software\Microsoft\EventSystem\EventLog

[002] Microsoft-windows-user Profiles service
Type: INFORMATION
Computer: 37L4247D28-05
Time: 7/8/2013 10:27:08 AM ID: 1531
User: NT AUTHORITY\SYSTEM
The User Profile Service has started successfully.
```

14. Close the Notepad program when you are finished.

15. To dump the security log to a text file, type the following command:

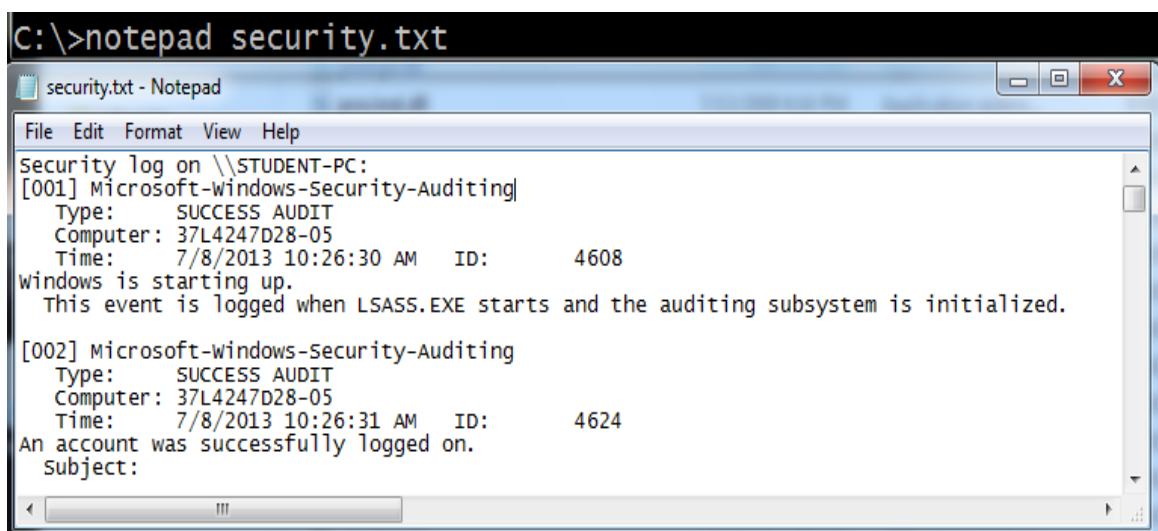
C:\>psloglist -r "security" > security.txt

```
C:\>psloglist -r "security" > security.txt

PsLoglist v2.71 - local and remote event log viewer
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals - www.sysinternals.com
```

16. To view the dumped application log, type the following command:

C:\>notepad security.txt



```
C:\>notepad security.txt

security.txt - Notepad
File Edit Format View Help
Security log on \\STUDENT-PC:
[001] Microsoft-Windows-Security-Auditing
    Type:      SUCCESS AUDIT
    Computer:  37L4247D28-05
    Time:      7/8/2013 10:26:30 AM    ID:      4608
    Windows is starting up.
    This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.

[002] Microsoft-Windows-Security-Auditing
    Type:      SUCCESS AUDIT
    Computer:  37L4247D28-05
    Time:      7/8/2013 10:26:31 AM    ID:      4624
    An account was successfully logged on.
    Subject:
```

17. Close the Notepad program when you are finished.

18. To dump the application log to a text file, type the following command:

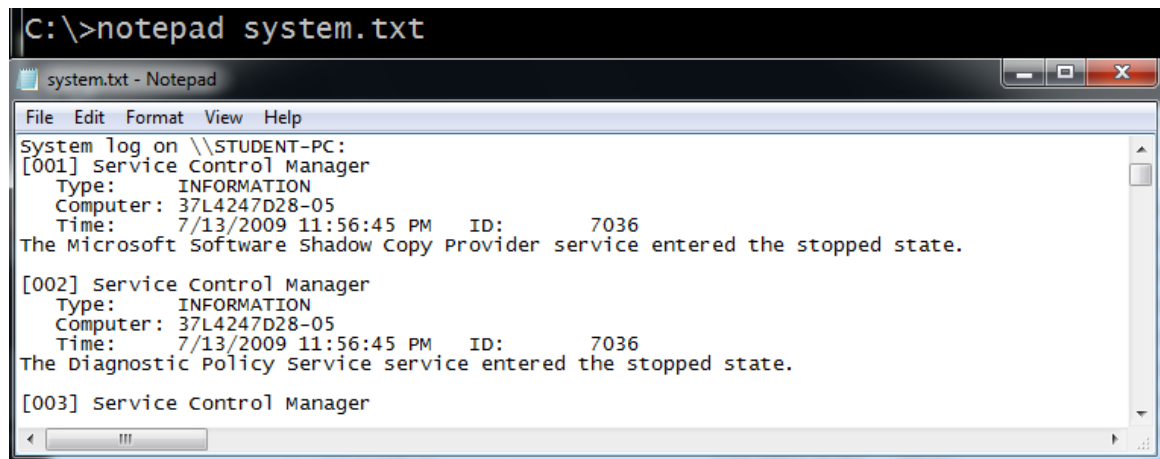
C:\>psloglist -r "system" > system.txt

```
C:\>psloglist -r "system" > system.txt

PsLoglist v2.71 - local and remote event log viewer
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals - www.sysinternals.com
```

19. To view the dumped application log, type the following command:

C:\>notepad system.txt



```
C:\>notepad system.txt

system.txt - Notepad
File Edit Format View Help
System log on \\STUDENT-PC:
[001] Service Control Manager
Type:      INFORMATION
Computer:  37L4247D28-05
Time:      7/13/2009 11:56:45 PM  ID:      7036
The Microsoft Software Shadow Copy Provider service entered the stopped state.

[002] Service Control Manager
Type:      INFORMATION
Computer:  37L4247D28-05
Time:      7/13/2009 11:56:45 PM  ID:      7036
The Diagnostic Policy Service service entered the stopped state.

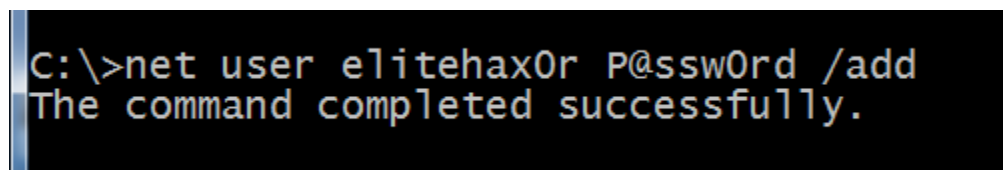
[003] Service Control Manager
```

20. Close the Notepad program when you are finished.

Next, we will perform actions that will cause the Windows operating system to generate events in the 3 logs.

21. First, we will generate an event in the security log by typing the following:

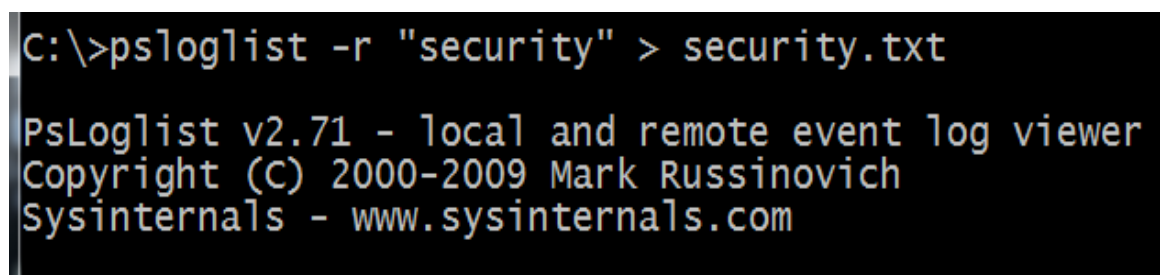
C:\>net user elitehax0r P@ssw0rd /add



```
C:\>net user elitehax0r P@ssw0rd /add
The command completed successfully.
```

22. To dump the security log to a text file, type the following command:

C:\>psloglist -r "security" > security.txt



```
C:\>psloglist -r "security" > security.txt

PsLoglist v2.71 - local and remote event log viewer
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals - www.sysinternals.com
```

23. To view part of the alert generated by the event, type the following command:

C:\>type security.txt | find "elite"

```
C:\>type security.txt | find "elite"
Account Name:      elitehax0r
SAM Account Name:  elitehax0r
Account Name:      elitehax0r
Account Name:      elitehax0r
SAM Account Name:  elitehax0r
Account Name:      elitehax0r
```

24. Next, we will generate an event in the system log by typing the following:

C:\>net stop "workstation"

```
C:\>net stop "workstation"
The Workstation service is stopping.
The Workstation service was stopped successfully.
```

25. To dump the security log to a text file, type the following command:

C:\>psloglist -r "system" > system.txt

```
C:\>psloglist -r "system" > system.txt

PsLoglist v2.71 - local and remote event log viewer
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals - www.sysinternals.com
```

26. To view part of the alert generated by the event, type the following command:

C:\> type system.txt | find "Workstation" | find "stop"

```
C:\>type system.txt | find "workstation" | find "stop"
The Workstation service entered the stopped state.
```

27. Next, we will generate an event in the system log by typing the following:

C:\>net stop themes

```
C:\>Net stop themes
The Themes service is stopping.
The Themes service was stopped successfully.
```

28. To dump the security log to a text file, type the following command:

```
C:\>psloglist -r "application" > application.txt
```

```
C:\>psloglist -r application > application.txt

PsLoglist v2.71 - local and remote event log viewer
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals - www.sysinternals.com
```

29. To view part of the alert generated by the event, type the following command:

```
C:\> type application.txt | find "theme"
```

```
C:\>type application.txt | find "theme"
The Desktop Window Manager was unable to start because a composited theme
```

1.2 Conclusion

When events are triggered on a Microsoft Windows system, there are artifacts that are generated on the system. Stopping and starting services generates logs in the Windows Event Viewer. The Psloglist tool can be used to dump the logs to a text file. After dumping the files, they can be examined for specific keywords generated by events.

1.3 Discussion Questions

1. Where is the location of the Event Viewer EVT files on a Windows 7 system?
2. Where is the location of the Event Viewer EVT files on a Windows XP system?
3. What is the syntax to dump the application log to a file called application.txt?
4. What is the syntax to dump the security log to a file called security.txt?

2 Examining Windows IIS Logs

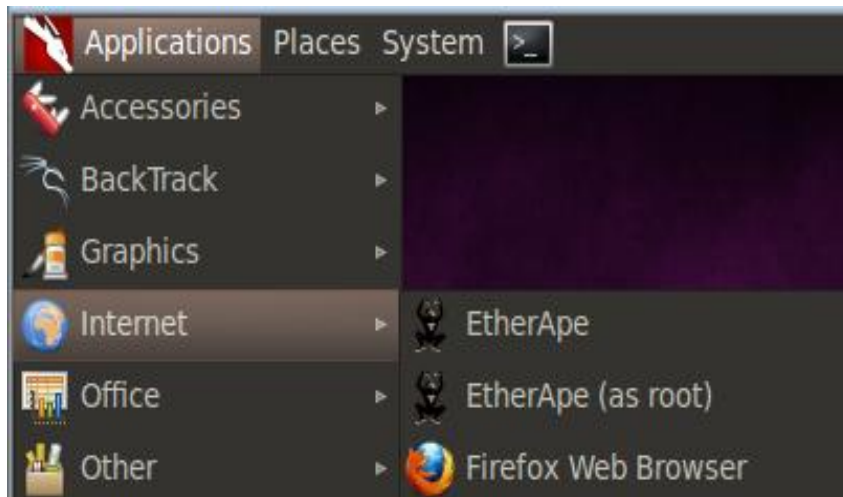
Log files contain information, including the IP addresses that have connected to your machine and will indicate which directories the machines attempted to access. Log files also include important date and time stamps that can be used as a timeline for an investigation. User Agents, which provide OS related information, also reside in web logs.

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

2.1 Connecting to the Windows 7 Website

We will connect to the default web page of the Windows 7 External Machine from 4 different machines, so that we can view the connection from 4 different IP addresses, as well as a variety of different user agents.

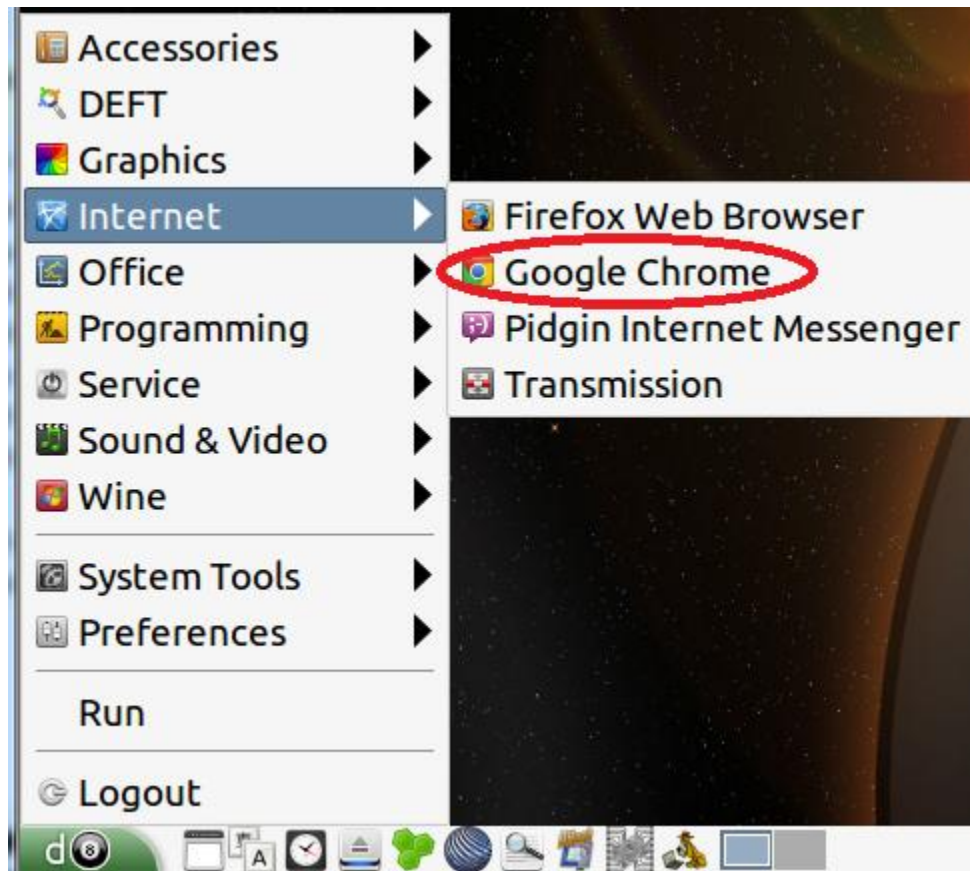
1. On the BackTrack 5 R3 Internal Machine , click **Applications > Internet > Firefox Web Browser**.



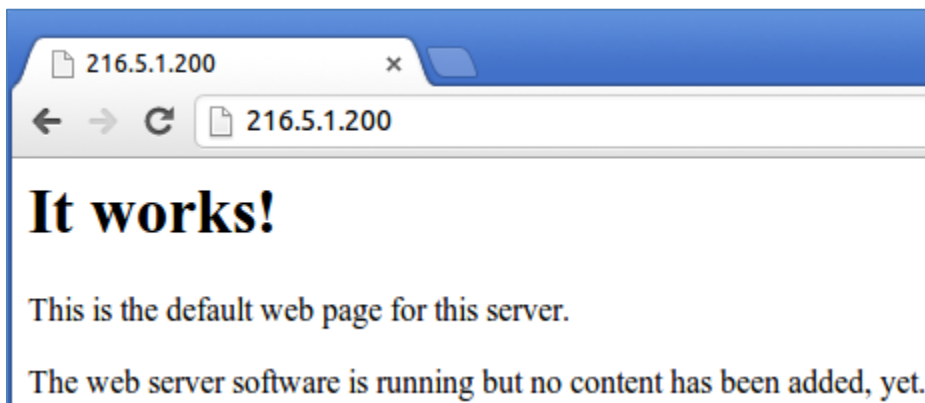
2. Type the following URL into the Firefox browser: **http://216.5.1.200**



3. On the DEFT Internal Machine, click on the **8 ball** > **Internet** > **Google Chrome**:



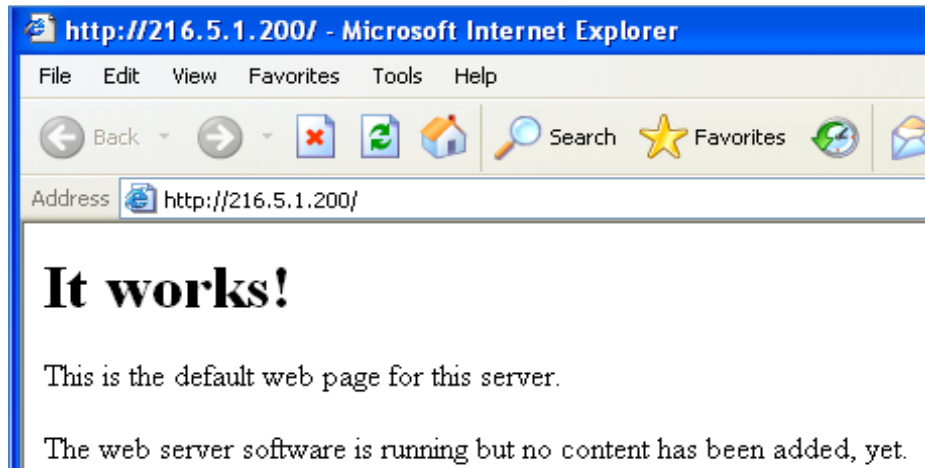
4. Type the following URL into the Chrome browser: **http://216.5.1.200**



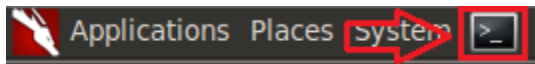
- On the Windows XP Pro Internal Machine, open Internet Explorer from the taskbar.



- Type the following URL into the Internet Explorer browser: **http://216.5.1.200**

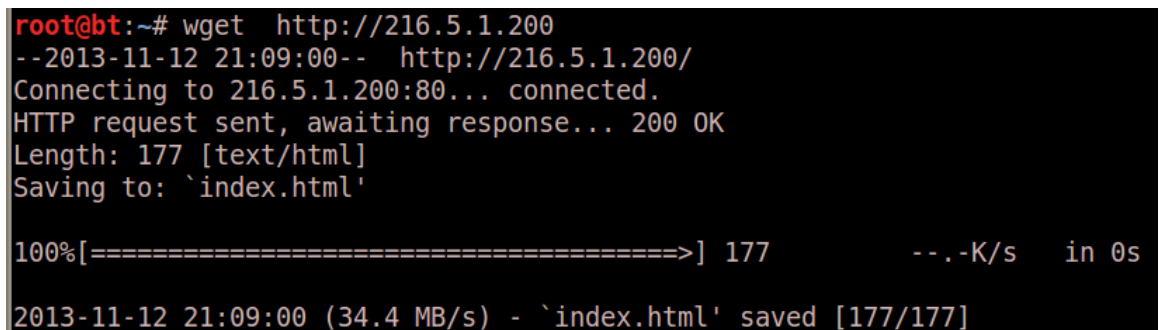


- Open the terminal from the top of the menu bar on the BackTrack 5 R3 Internal Machine.

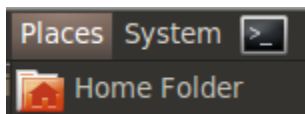


- Type the following command to download the web page using wget:

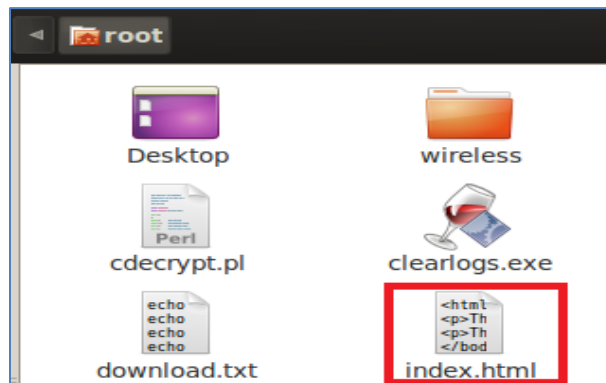
root@bt:~# **wget http://216.5.1.200**



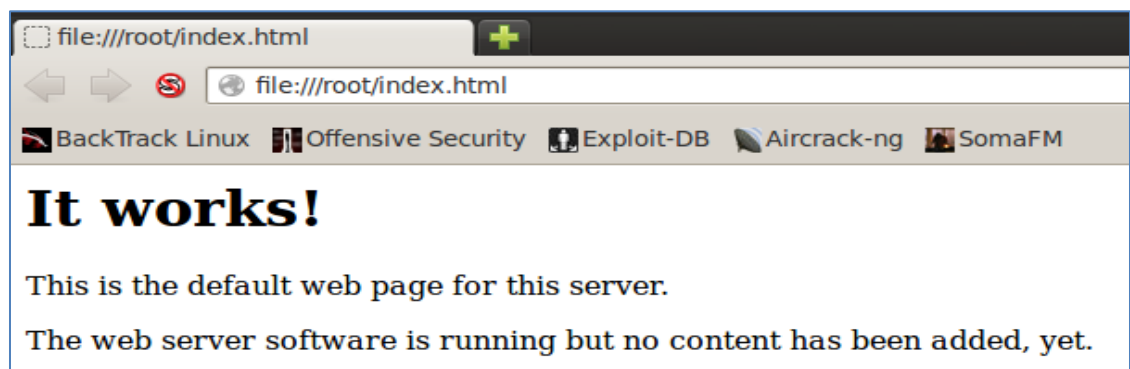
- Click **Places** from the BackTrack 5 R3 Internal Machine menu bar, and select the link for Home Folder.



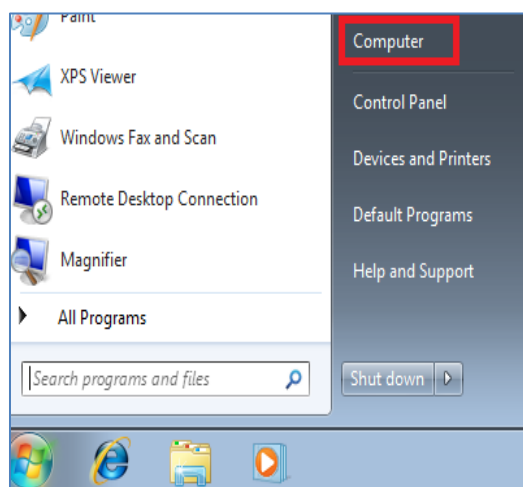
10. Double-click on the **Index.html** page listed within the root folder.



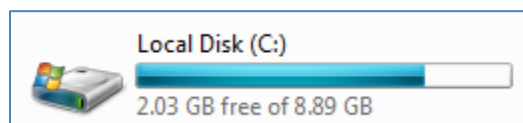
11. View the locally downloaded webpage.



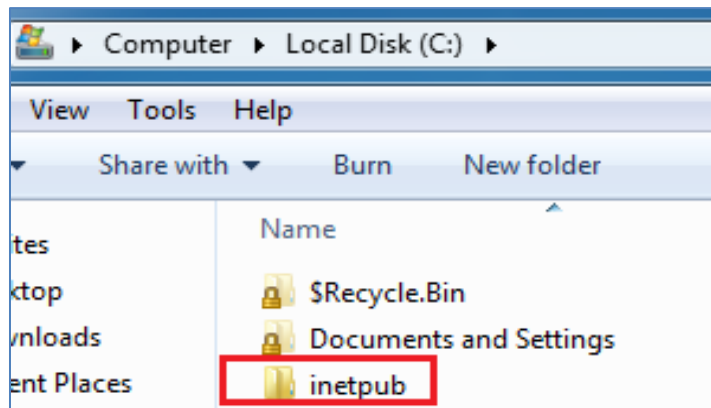
12. Click on the Start button and click the link to **Computer** on the right.



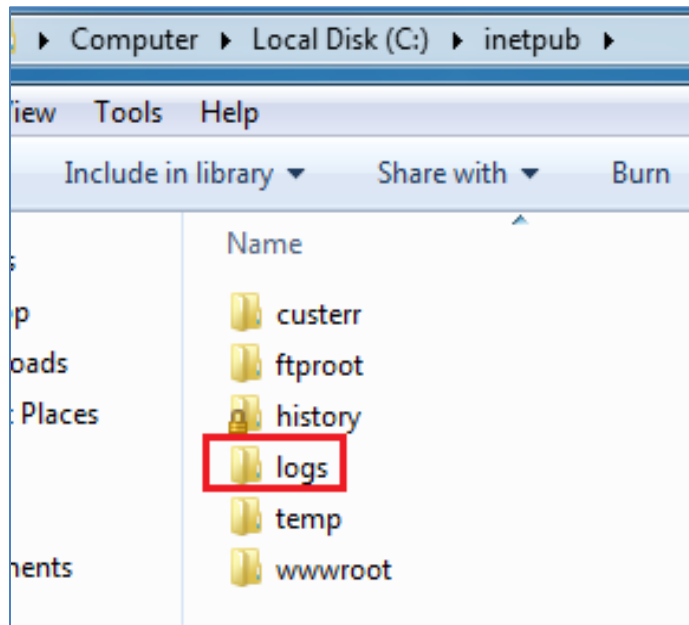
13. Double-click on Local Disk (C:).



14. Double-click on the **inetpub** directory.



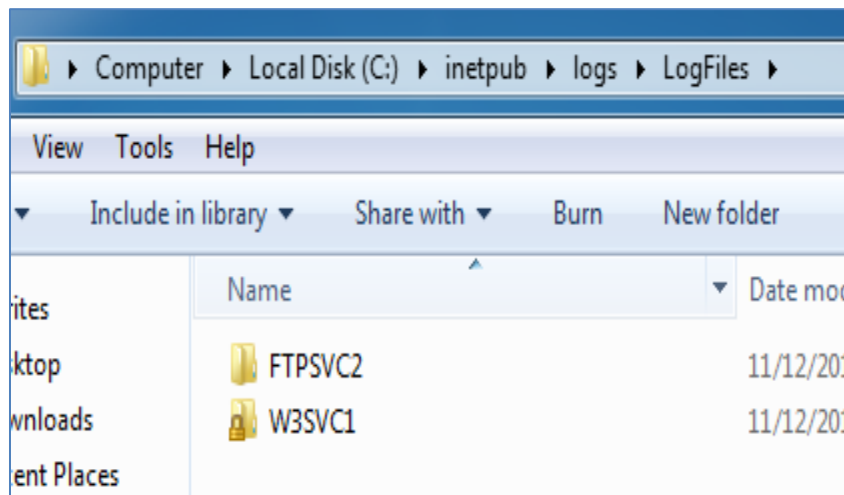
15. Double-click on the **Logs** directory.



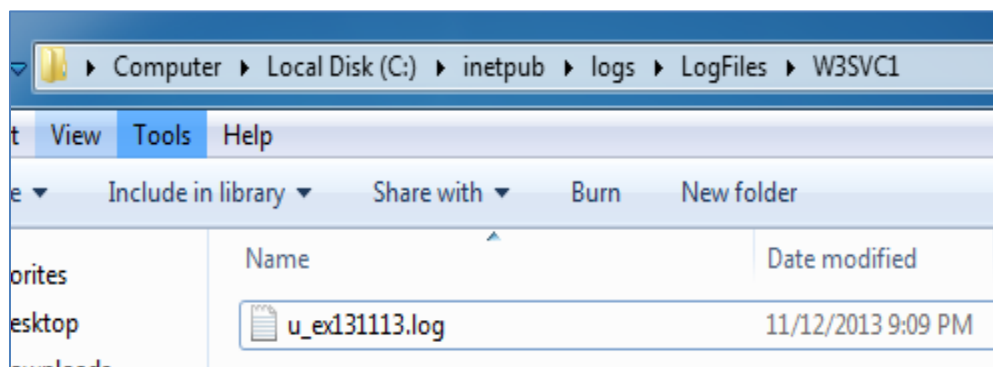
16. Double-click on the LogFiles directory.



17. Double-click on the **W3SVC1** folder. This is the log file for the web server hosted within Microsoft Internet Information Services (IIS).

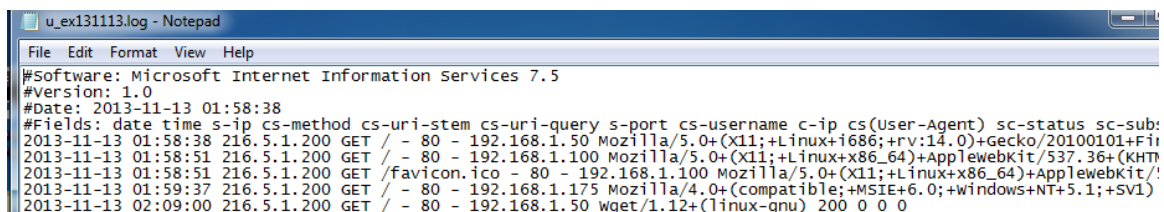


18. Double-click on the log file that indicates today's date as part of the file name. The filename format is: **u_exYYMMDD.log** (YYMMDD indicates today's date).



The log file will contain the IP address of the machine connecting to the system.

19. Double-click on the log file and examine the IP address information.



Common reasons Computer Forensics examiners might review web log files:

- Determining the IP addresses of connecting systems
- Looking for date and time stamps of connections
- Examining user agents or suspicious GET requests from foreign machines

2.2 Conclusion

When events are triggered on a Microsoft Windows system, there are artifacts that are generated on the system. When IP addresses connect to the IIS web server running on a Windows system, log entries are generated in the Internet Information Services logs. Additional information, such as the browser version, will also be present in the IIS logs. The Internet Information Services logs are located in the C:\inetpub\logs\LogFiles directory on Windows 7 and Windows 8 systems. FTP and Web logs are stored in different folders within the C:\inetpub\logs\LogFiles directory on Windows 7 and 8.

2.3 Discussion Questions

1. Where are the IIS logfiles stored on a Windows 7 or Windows 8 system?
2. Where are the FTP logfiles stored on a Windows 7 or Windows 8 system?
3. Where are the WWW logfiles stored on a Windows 7 or Windows 8 system?
4. Explain the naming format for Logfiles within Windows 7 or Windows 8

3 Examining Linux Log Files

Linux includes a large number of log files that keep track of events on the system. One of the most important log files is the secure file, which logs security incidents. The secure file is located in /var/log on a Red Hat system. The Ubuntu equivalent to secure is auth.log. This log file tracks SSH, or Secure Shell, connections. It provides information such as IP addresses, and date and time stamps. It also tracks other events related to security, such as the creation of new user accounts and new group accounts. Another important file on a Linux system is the access_log file, which keeps track of web server connections.

3.1 Examining access_log and auth_log

1. To start the webserver on the BackTrack 5 R3 Internal Machine, type the following:

```
root@bt:~# apache2ctl start
```

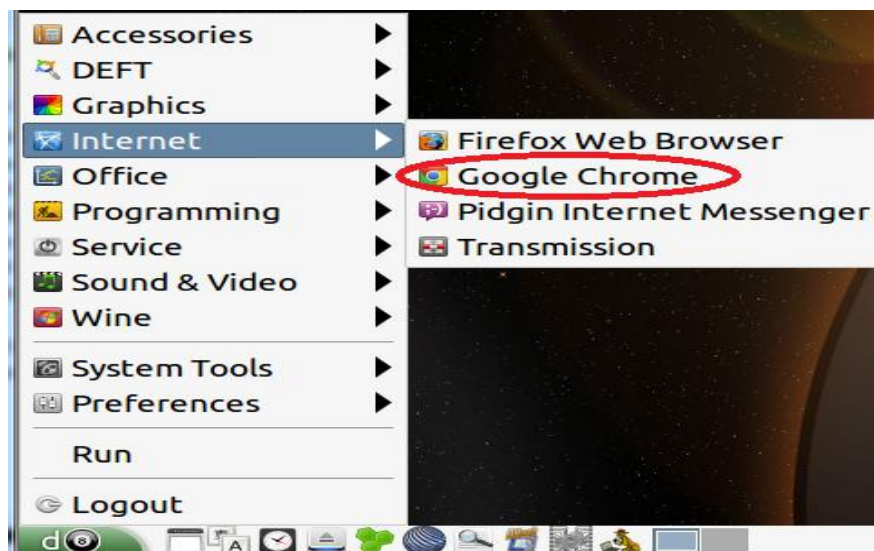
```
root@bt:~# apache2ctl start
```

2. To verify the webserver is listening on port 80, type the following:

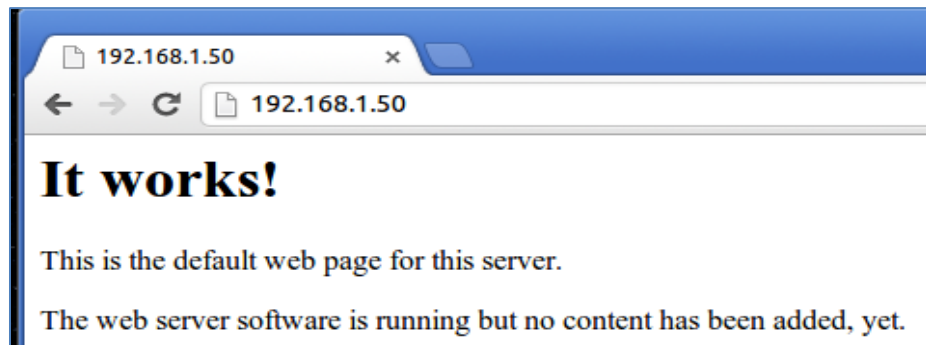
```
root@bt:~# netstat -tan | grep 80
```

```
root@bt:~# netstat -tan | grep 80
tcp        0      0 0.0.0.0:80 0.0.0.0:*    LISTEN
```

3. On the DEFT Internal Machine, click on the **8 ball** > **Internet** > **Google Chrome**.



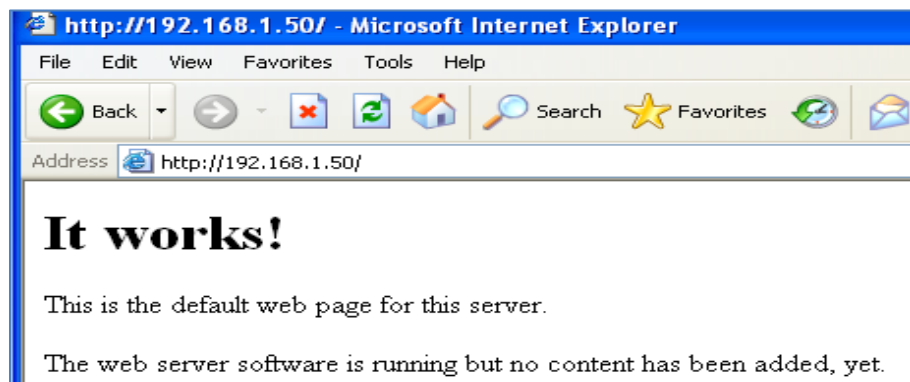
4. Type the following URL in the Chrome browser: **http://192.168.1.50**



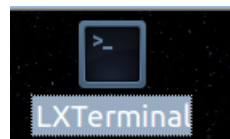
5. On the Windows XP system, open Internet Explorer from the taskbar.



6. Type the following URL in the Internet Explorer Browser: **http://192.168.1.50**



7. On the DEFT Internal Machine, click on the **LXTerminal** icon on the desktop.



8. Type the following command to download the web page using wget:
deft-virtual-machine ~ % **wget <http://192.168.1.50>**

```
deft-virtual-machine ~ % wget http://192.168.1.50
--2013-11-13 12:35:26--  http://192.168.1.50/
Connecting to 192.168.1.50:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 177 [text/html]
Saving to: `index.html'

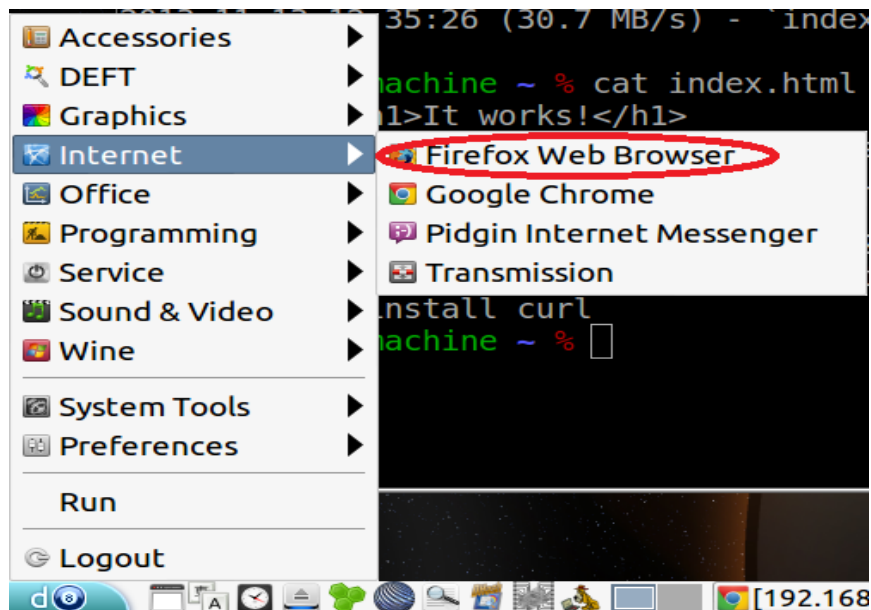
100%[=====>] 177      --.-K/s   in 0s

2013-11-13 12:35:26 (30.7 MB/s) - `index.html' saved [177/177]
```

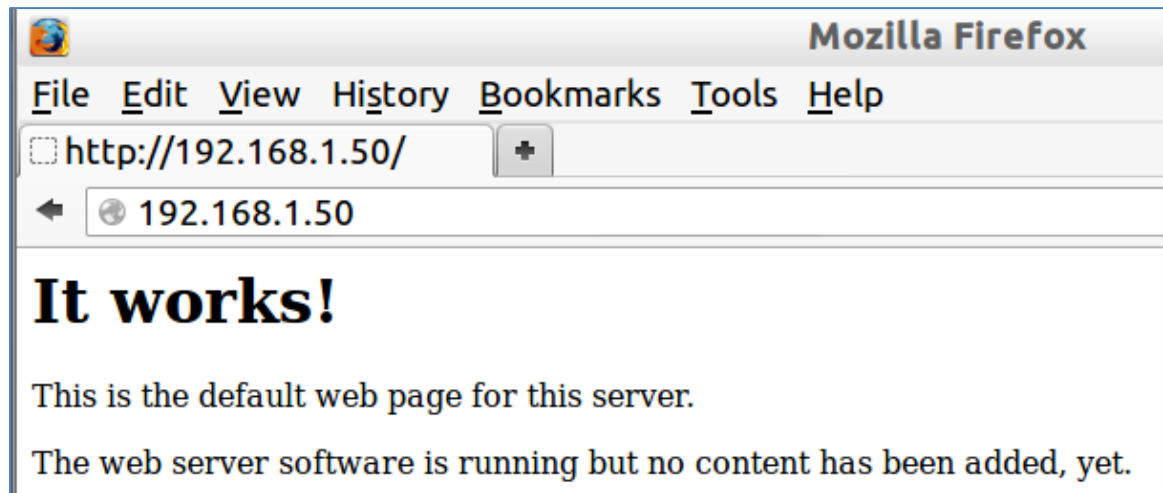
9. Type the following command to view the webpage downloaded with wget:
deft-virtual-machine ~ % **cat index.html**

```
deft-virtual-machine ~ % cat index.html
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
</body></html>
```

10. On the DEFT Internal Machine, click on the **8 ball** > **Internet** > **Google Chrome**.



11. Type the following URL in the Chrome browser: **http://192.168.1.50**



The Apache Server keeps records of the connections made to the website, including:

- IP addresses
- User Agents
- Date/Time Stamps

The access_log is located in the /var/log/httpd directory and will have evidence of:

- The connection made with Chrome
- The connection made with Internet Explorer
- The connection made with wget
- The connection made with Firefox
- The connection made with the curl command

12. To view, the access_log, type the following command on the BackTrack 5 R3 Internal Machine:

```
[root@rhel ~]# cd /var/log/apache2
```

```
root@bt:~# cd /var/log/apache2/
```

13. To view the connections in the log file, type the following command:

```
root@bt:/var/log/apache2# ls
```

```
root@bt:/var/log/apache2# ls
access.log  error.log  other_vhosts_access.log
```

14. To view the connections with Firefox, type the following command:

```
root@bt:/var/log/apache2# cat access_log | grep Firefox
```

```
root@bt:/var/log/apache2# cat access.log | grep Firefox
192.168.1.100 - - [13/Nov/2013:12:44:57 -0500] "GET / HTTP/1.1" 200 484 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:22.0) Gecko/20100101 Firefox/22.0"
192.168.1.100 - - [13/Nov/2013:12:44:57 -0500] "GET /favicon.ico HTTP/1.1" 404 503 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:22.0) Gecko/20100101 Firefox/22.0"
192.168.1.100 - - [13/Nov/2013:12:44:57 -0500] "GET /favicon.ico HTTP/1.1" 404 503 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:22.0) Gecko/20100101 Firefox/22.0"
```

15. To generate the keys that will be needed for an SSH connection, type:

```
root@bt:/var/log/apache2# sshd-generate
```

```
root@bt:/var/log/apache2# sshd-generate
Generating public/private rsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_key.
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
The key fingerprint is:
f2:9b:c9:5e:6b:46:cb:3c:59:67:73:3c:47:7d:97:a2 root@bt
The key's randomart image is:
+--[RSA 2048]-----+
|
|             o|
|      .  .  .|=|
|    . S    . .00|
|    o  .E.  .+.|
|    .+.  o 00|
|    . =0.  |
|    .*0..  |
|
+-----+
Generating public/private rsa key pair.
```

16. To start the SSH server on the , BackTrack 5 R3 Internal Machine type:

```
root@bt:~# service ssh start
```

```
root@bt:/var/log/apache2# service ssh start
ssh start/running, process 4311
```

17. To verify that the SSH server service is running on the machine, type:

```
root@bt:/var/log/apache2# netstat -tan | grep 22
```

```
root@bt:/var/log/apache2# netstat -tan | grep 22
tcp        0      0 0.0.0.0:22          0.0.0.0:*          LISTEN
tcp6       0      0 :::22              :::*                LISTEN
```

18. From the terminal is Backtrack, type the following command to add a user:
 root@bt:/var/log/apache2# **useradd forensicuser**

```
root@bt:/var/log/apache2# useradd forensicuser
```

19. Set forensicuser's password to forensic by typing **forensic** twice after typing:
 root@bt:/var/log/apache2# **passwd forensic**

```
root@bt:/var/log/apache2# passwd forensicuser
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

20. Next, examine the alterations to the shadow file by typing the following:
 root@bt:/var/log/apache2# **tail -n 1 /etc/shadow**

```
root@bt:/var/log/apache2# tail -n 1 /etc/shadow
forensicuser:$6$vjXvZ62R$d7iDtntRg4EYBz3YCVzCn6SMA2ou748mUCLTg3uiKSKJrHBtfHFVV4kpA9
/u5WmGh3/plGe1B8aJQiQnRna021:16022:0:99999:7:::
```

21. In the terminal on the Deft 8 machine, type the following command:
 deft-virtual-machine ~ % **ssh 192.168.1.50 -l forensicuser**
 22. Type **yes** in response to the question about continuing to connect.

```
deft-virtual-machine ~ % ssh 192.168.1.50 -l forensicuser
The authenticity of host '192.168.1.50 (192.168.1.50)' can't be established.
RSA key fingerprint is 60:90:fe:99:00:7f:e5:44:55:05:c0:68:1d:2a:d9:c7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.50' (RSA) to the list of known hosts.
```

23. Type **forensic** for the password. The SSH connection should be established.

```
forensicuser@192.168.1.50's password:
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

System information as of Wed Nov 13 13:08:23 EST 2013

System load:  0.0                Processes:            128
Usage of /:   60.1% of 19.06GB    Users logged in:     1
Memory usage: 19%                IP address for eth0: 192.168.1.50
Swap usage:   0%
```

24. Type forensic for the password. The SSH connection should be established.

```
forensicuser@192.168.1.50's password:
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

System information as of Wed Nov 13 13:08:23 EST 2013

System load:  0.0                Processes:            128
Usage of /:   60.1% of 19.06GB    Users logged in:     1
Memory usage: 19%                IP address for eth0: 192.168.1.50
Swap usage:   0%
```

When you perform administrative tasks that are directly related to the security on a Linux system, they will show up in the auth.log in the /var/log directory.

Examples of security incidents that will be recorded to the secure log include the following:

- Adding a User
- Logging on from a Remote System
- Adding a Group
- Changing a User's Password.

25. To switch to the log directory, type the following command on the system
root@bt:/var/log/apache2# **cd /var/log**

```
root@bt:/var/log/apache2# cd /var/log
```

26. To view auth.log for forensicuser, type the following on the BackTrack 5 R3 Internal Machine:

root@bt:/var/log# **cat auth.log | grep forensicuser**

```
root@bt:/var/log# cat auth.log | grep forensicuser
Nov 13 13:04:30 bt useradd[4367]: new group: name=forensicuser, GID=1002
Nov 13 13:04:30 bt useradd[4367]: new user: name=forensicuser, UID=1002, GID=1002,
home=/home/forensicuser, shell=/bin/sh
Nov 13 13:04:44 bt passwd[4372]: pam_unix(passwd:chauthtok): password changed for
forensicuser
Nov 13 13:08:23 bt sshd[4394]: pam_sm_authenticate: username = [forensicuser]
Nov 13 13:08:23 bt sshd[4394]: Accepted password for forensicuser from 192.168.1.1
0 port 34495 ssh2
Nov 13 13:08:23 bt sshd[4394]: pam_unix(sshd:session): session opened for user for
nsicuser by (uid=0)
```

3.2 Conclusion

Linux keeps a large number of log files that keep track of events on the system. One of the most important log files is the `auth.log`, which logs security incidents. This log file tracks SSH, or Secure Shell, connections. It provides information such as IP addresses, and Date and Time Stamps. It also tracks other events related to security, such as the creation of new user accounts and new group accounts. Another important file on a Linux system is the `access_log` file, which keeps track of web server connections.

3.3 Discussion Questions

1. Where is the `auth.log` file located?
2. What is the `auth.log` file referred to on a Red Hat system?
3. Where is the `access log` located?
4. What command can be utilized to verify that the SSH or Apache is running?

References

1. The auth.log file:
<http://www.thegeekstuff.com/2011/08/linux-var-log-files/>
2. Psloglist:
<http://technet.microsoft.com/en-us/sysinternals/bb897544.aspx>
3. The access_log file:
<http://httpd.apache.org/docs/2.2/logs.html>
4. Windows Event Viewer:
<http://support.microsoft.com/kb/308427>
5. IIS Log Overview:
[http://msdn.microsoft.com/en-us/library/ms525410\(v=vs.90\).aspx](http://msdn.microsoft.com/en-us/library/ms525410(v=vs.90).aspx)