FORENSICS
LAB SERIES

Lab 19: Log Analysis

Material in this Lab Aligns to the Following Certification Domains/Objectives	
GIAC Certified Forensics Examiner (GCFE) Domains	Computer Hacking Forensic Investigator (CHFI) Objectives
5: Log Analysis	16: Network Forensics, Investigating Logs, and Investigating Network Traffic

Document Version: 2016-08-17

Copyright © 2016 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition and NETLAB+ are registered trademarks of Network Development Group, Inc.

Contents

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

Introduction

This lab will introduce how to analyze logs, which is an important skill to have in order to curate information about the actions performed by an individual on a computer. In this lab, Linux logs and Windows event logs will be explored.

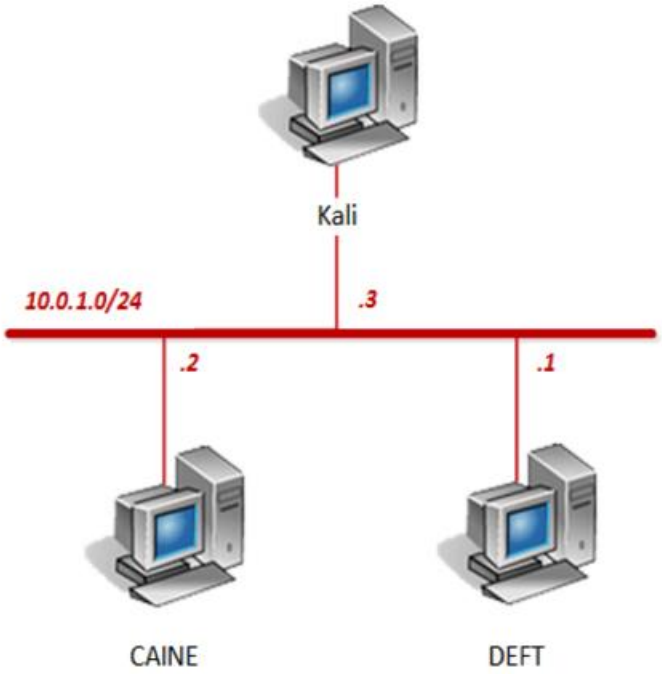
Objective

In this lab, you will be conducting forensic practices using various tools. You will be performing the following tasks:

1. Examining Linux Logs
2. Examining Windows Event Logs

Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

Pod Topology



 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

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)
DEFT	10.0.1.1	deft	password
CAINE	10.0.1.2	caine	
Kali	10.0.1.3	root	toor

Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

1 Examining Linux Logs

1. Click on the **Kali** graphic on the *topology page* to open the VM.
2. Login using `root` as the *username* and `toor` as the *password*.
3. Open a new terminal by clicking on the **Terminal** icon located in the left tool pane.

4. Using the terminal, enter the command below to change to the **/var/log/** directory.

```
cd /var/log
```

```
root@Kali2:~# cd /var/log
root@Kali2:/var/log#
```

5. List the files in the current directory by entering the command below.

```
ls
```

```
root@Kali2:/var/log# ls
alternatives.log       debug.4.gz      lynis.log           redis
alternatives.log.1     dmesg           lynis-report.dat    samba
alternatives.log.2.gz  dpkg.log        macchanger.log      speech-dispatcher
alternatives.log.3.gz  dpkg.log.1      macchanger.log.1.gz stunnel4
alternatives.log.4.gz  dpkg.log.2.gz   macchanger.log.2.gz syslog
apache2                dpkg.log.3.gz   macchanger.log.3.gz syslog.1
apt                    dpkg.log.4.gz   macchanger.log.4.gz syslog.2.gz
auth.log               dpkg.log.5.gz   messages            syslog.3.gz
auth.log.1             dpkg.log.6.gz   messages.1          syslog.4.gz
auth.log.2.gz          dpkg.log.7.gz   messages.2.gz       syslog.5.gz
auth.log.3.gz          dpkg.log.8.gz   messages.3.gz       syslog.6.gz
auth.log.4.gz          dradis          messages.4.gz       syslog.7.gz
bootstrap.log          exim4           mysql               user.log
btmp                   faillog         mysql.err           user.log.1
btmp.1                 fontconfig.log  mysql.log           user.log.2.gz
chkrootkit             fsck            mysql.log.1.gz      user.log.3.gz
daemon.log             gdm3            mysql.log.2.gz      user.log.4.gz
daemon.log.1           inetsim         mysql.log.3.gz      vsftpd.log
daemon.log.2.gz        installer       mysql.log.4.gz      vsftpd.log.1
daemon.log.3.gz        kern.log        mysql.log.5.gz      wtmp
daemon.log.4.gz        kern.log.1      mysql.log.6.gz      wtmp.1
debug                  kern.log.2.gz   mysql.log.7.gz      wvdialconf.log
debug.1                kern.log.3.gz   ntpstats            Xorg.0.log
debug.2.gz             kern.log.4.gz   openvas             Xorg.0.log.old
debug.3.gz             lastlog         postgresql          Xorg.1.log
root@Kali2:/var/log#
```

These are the main log files in a Linux operating system.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

6. Enter the command below using the *last* command to view the contents of the *utmp* file.

```
last -f /var/run/utmp
```

```
root@Kali2:/var/log# last -f /var/run/utmp
root     pts/0        :0               Fri Aug  5 13:19   still logged in
root     :0           :0               Fri Aug  5 13:19   still logged in
reboot   system boot  4.0.0-kali1-amd6 Fri Aug  5 07:48 - 13:35  (05:47)

utmp begins Fri Aug  5 07:48:36 2016
root@Kali2:/var/log#
```

Notice the *utmp* file shows who is currently logged onto the system with a time and date stamp.

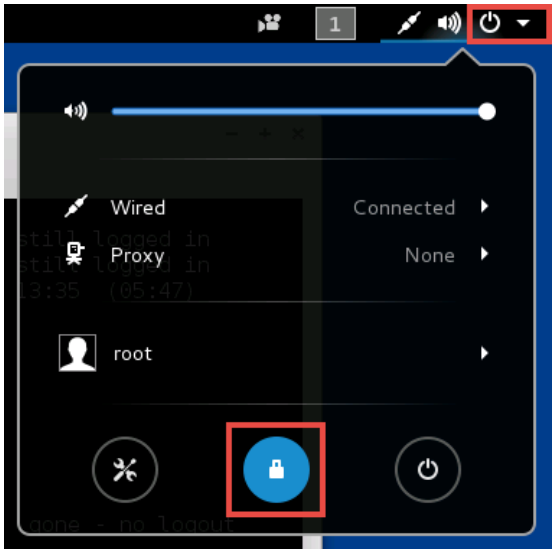
7. Enter the command below to view the contents of the *btmp* file.

```
last -f btmp
```

```
root@Kali2:/var/log# last -f btmp

btmp begins Fri Aug  5 07:48:44 2016
root@Kali2:/var/log#
```

The *btmp* file records failed login attempts but notice no information is available.

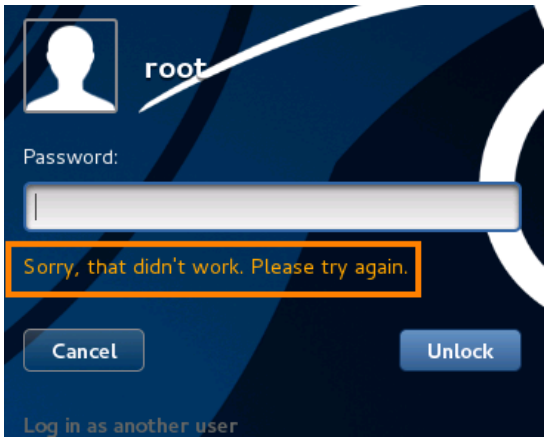
8. Logout of the system by clicking on the **power** icon located in the upper-right corner, followed by clicking on the **lock** icon.



9. Once the time and date appears on the screen, press the **Enter** key to bring up the login prompt.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

10. Type `root` into the *Password* field, press **Enter**.



Notice the message stating that the password was incorrect.

11. This time type `toor` into the *Password* field, press **Enter**.
12. Using the same terminal, enter the command below once more.

```
last -f btmp
```

```
root@Kali2:/var/log# last -f btmp
root     :0           :0               Fri Aug  5 13:39    gone - no logout

btmp begins Fri Aug  5 13:39:40 2016
root@Kali2:/var/log#
```

Notice now that *btmp* is able to report a failed login attempt for the *root* account.

13. Enter the command below to view the contents of the *wtmp* file.

```
last -f wtmp
```

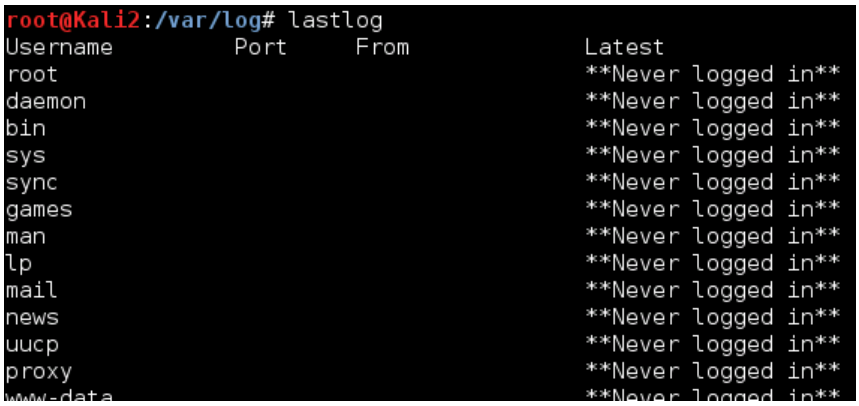
```
root@Kali2:/var/log# last -f wtmp
root     pts/0        :0               Fri Aug  5 13:19   still logged in
root     :0           :0               Fri Aug  5 13:19   still logged in
(unknown :0           :0               Fri Aug  5 07:49 - 13:19  (05:30)
reboot   system boot  4.0.0-kali1-amd6 Fri Aug  5 07:48 - 13:48  (05:59)
root     pts/0        :0               Thu Aug  4 14:09 - 18:20  (04:10)
root     :0           :0               Thu Aug  4 14:02 - 18:20  (04:18)

wtmp begins Thu Aug  4 14:02:07 2016
root@Kali2:/var/log#
```

The *wtmp* file is a historical record of the *utmp* file.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

14. Enter the command below to see if any user logged in remotely over the network.

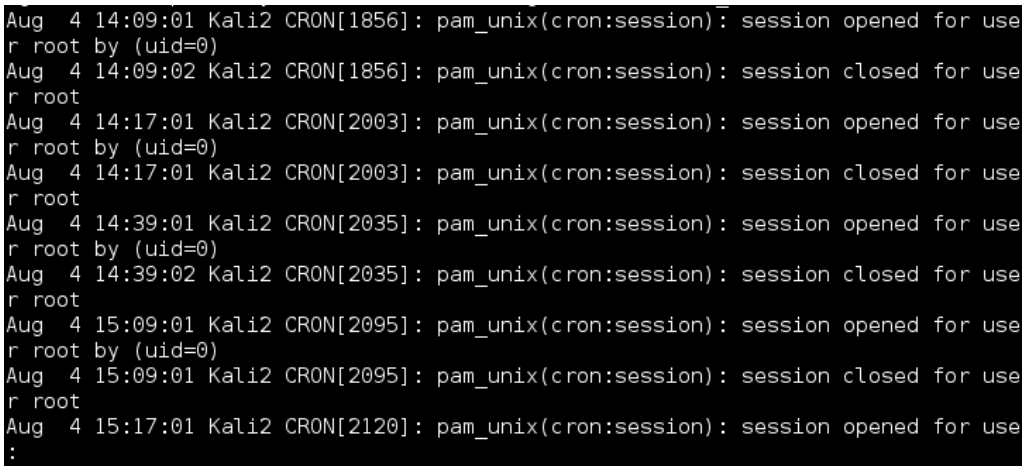
```
lastlog
```



After briefly analyzing through the list, notice no user logged in remotely.

15. The *auth.log* is a log file that shows authorization information including user's logins and the services the operating system used. Enter the command below to view the contents of the **auth.log** file.

```
less auth.log
```

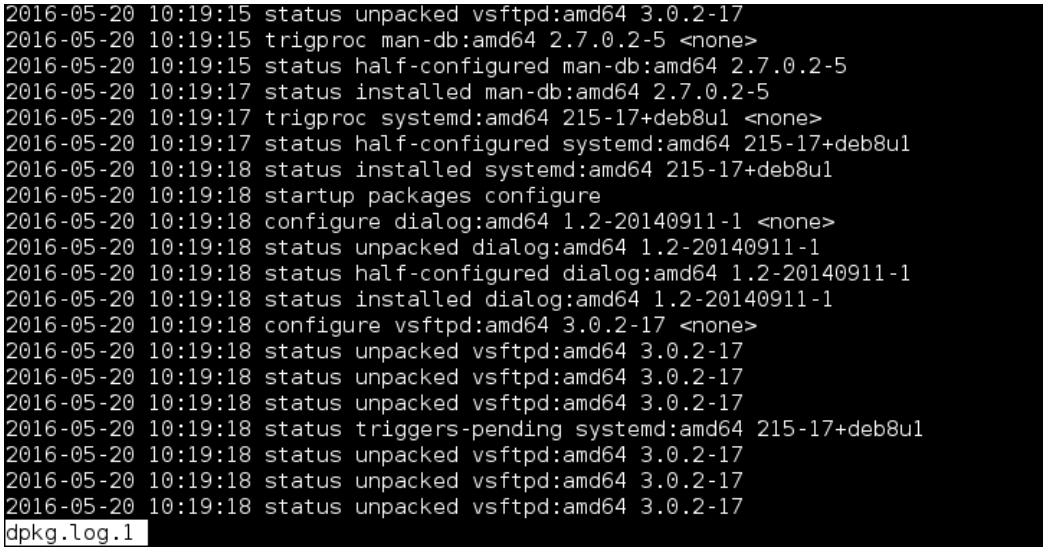


With the *less* command, use the **Enter** key to skip to the next line item of the list or use the **spacebar** to skip by page. When finished analyzing the file, press the **q** character to quit.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

16. Another log that may be useful to examine is the *dpkg* log, which shows what software was installed. It is snapshotted during each reboot of the system. Enter the command below to view the contents of the archived **dpkg.log.1** file.

```
less dpkg.log.1
```



With the *less* command, use the **Enter** key to skip to the next line item of the list or use the **spacebar** to skip by page. When finished analyzing the file, press the **q** character to quit.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

2 Examining Windows Event Logs

1. Click on the **CAINE** graphic on the *topology page* to open the VM.
2. Open a new terminal by clicking on the **Mate Terminal** icon located on the bottom tool pane.

3. Using the terminal, navigate to **/home/caine/Downloads/Parse-Evtx-1.1.1** by entering the command below.

```
cd Downloads/Parse-Evtx-1.1.1
```

```
caine@Caine01:~$ cd Downloads/Parse-Evtx-1.1.1
caine@Caine01:~/Downloads/Parse-Evtx-1.1.1$
```

4. Enter the command below to list the files in the current directory.

```
ls
```

```
caine@Caine01:~/Downloads/Parse-Evtx-1.1.1$ ls
blib          lib          MANIFEST     MYMETA.yml  scripts
CHANGELOG.txt Makefile     META.yml     pm_to_blib
gpl-2.0.txt   Makefile.PL  MYMETA.json  README.txt
caine@Caine01:~/Downloads/Parse-Evtx-1.1.1$
```

5. Navigate to the **scripts/** folder by entering the command below.

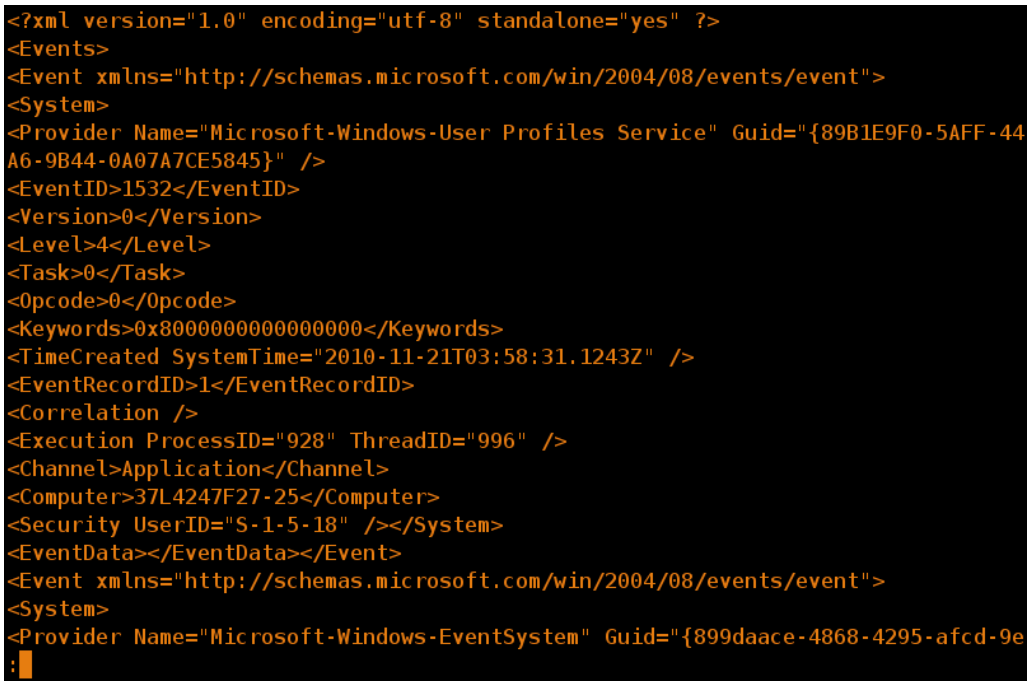
```
cd scripts
```

```
caine@Caine01:~/Downloads/Parse-Evtx-1.1.1$ cd scripts
caine@Caine01:~/Downloads/Parse-Evtx-1.1.1/scripts$
```

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

6. Using the *evtxdump.pl Perl* script, view the contents of the **Application.evtx** log by entering the command below.

```
./evtxdump.pl /home/caine/Downloads/Application.evtx | less
```



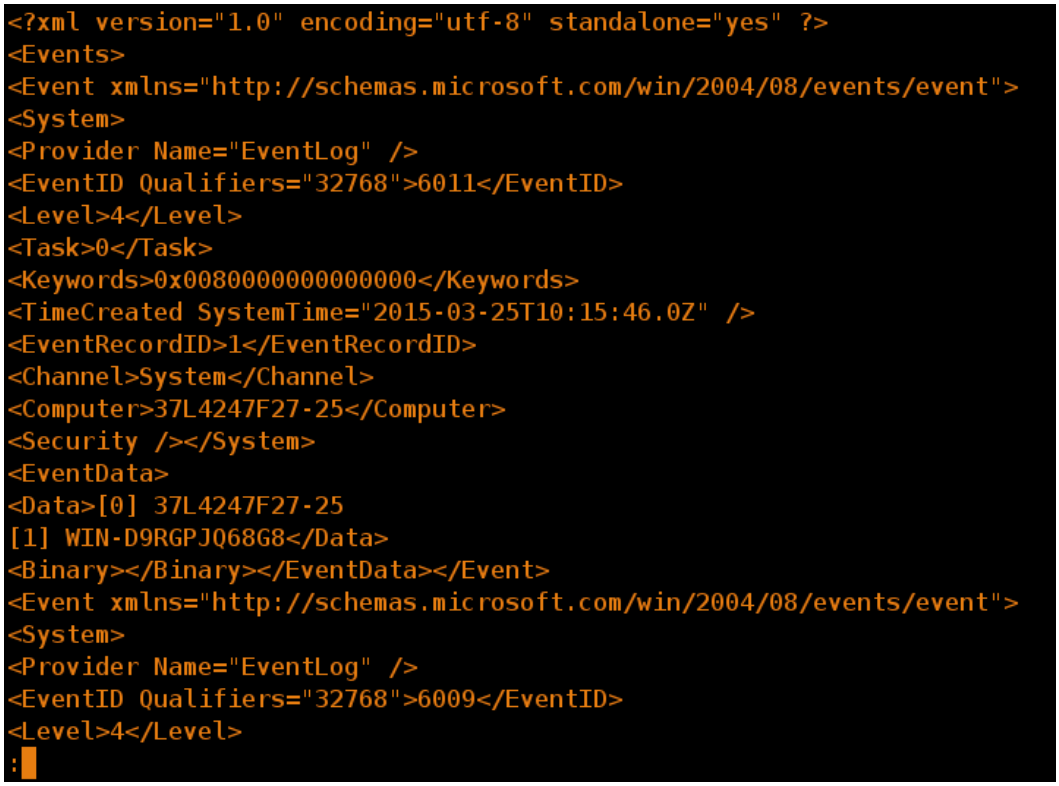
The *Perl* script helps translate the original file format of the *Application.evtx* file, which is in *XML* format into human readable *ASCII* format. Briefly analyze the log file for installed software or problems with software.

With the *less* command, use the **Enter** key to skip to the next line item of the list or use the **spacebar** to skip by page. When finished analyzing the file, press the **q** character to quit.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

7. View the contents of the **System.evtx** log file by entering the command below.

```
./evtxdump.pl /home/caine/Downloads/System.evtx | less
```



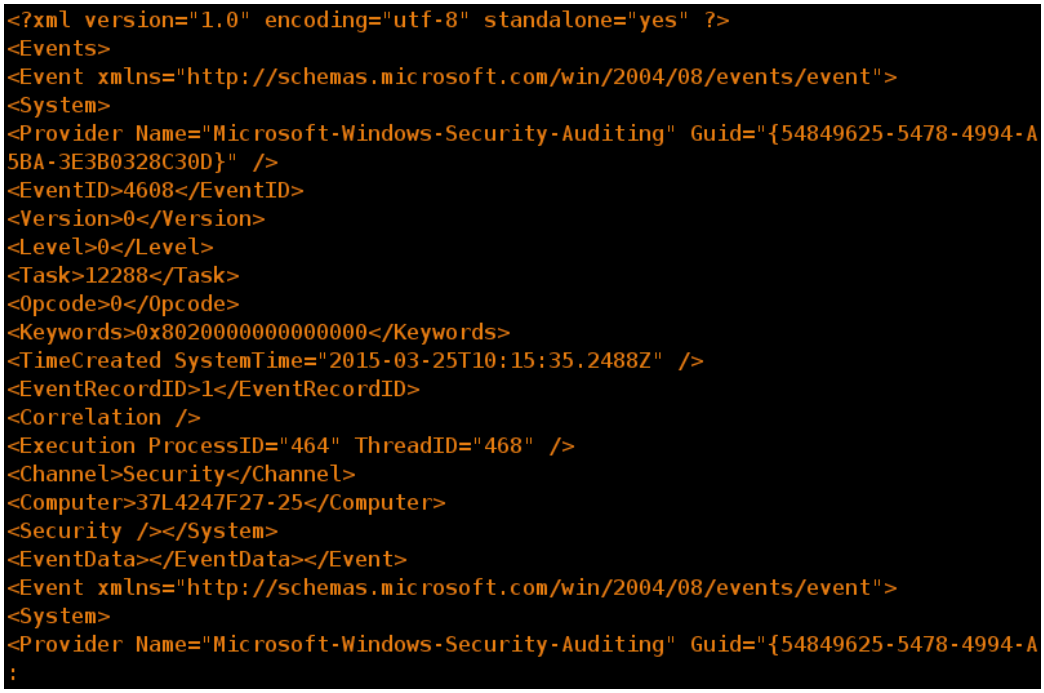
The *System.evtx* log file shows events to Windows and Window services.

With the *less* command, use the **Enter** key to skip to the next line item of the list or use the **spacebar** to skip by page. When finished analyzing the file, press the **q** character to quit.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

8. View the contents of the **Security.evtx** log file by entering the command below.

```
./evtxdump.pl /home/caine/Downloads/Security.evtx | less
```



With the *less* command, use the **Enter** key to skip to the next line item of the list or use the **spacebar** to skip by page. When finished analyzing the file, press the **q** character to quit.

9. Close all **PC Viewers** and end the reservation to complete the lab.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com