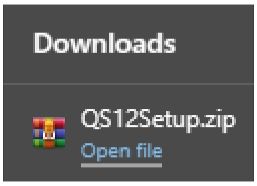
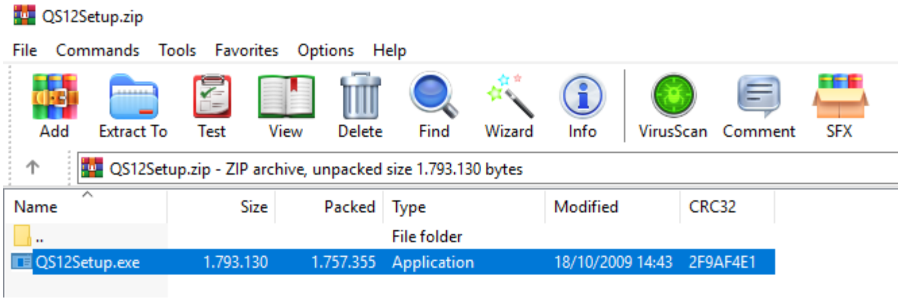
1. Download QS12 setup pada http://quickcrypto.com/products/QS12Setup.zip.



Downloads

QS12Setup.zip

2. Buka folder QS12Setup.zip pada WinRAR atau aplikasi pengekstrak file zip. Lalu ekstrak ke dalam folder lokal.

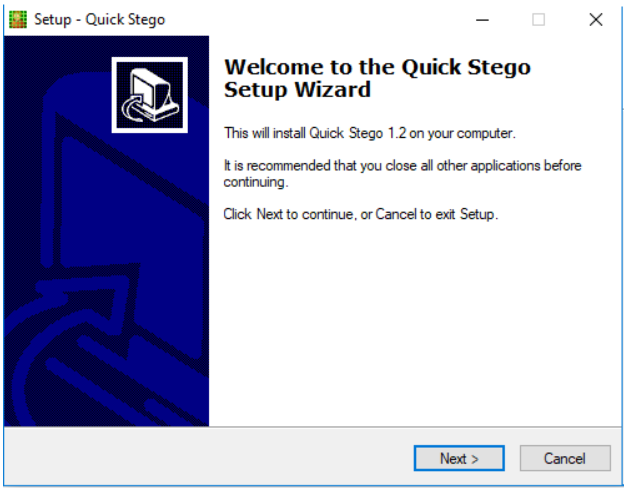


QS12Setup.zip

QS12Setup.zip - ZIP archive, unpacked size 1.793.130 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
QS12Setup.exe	1.793.130	1.757.355	Application	18/10/2009 14:43	2F9AF4E1

3. Buka file .exe dengan klik dua kali pada file. Klik Next.



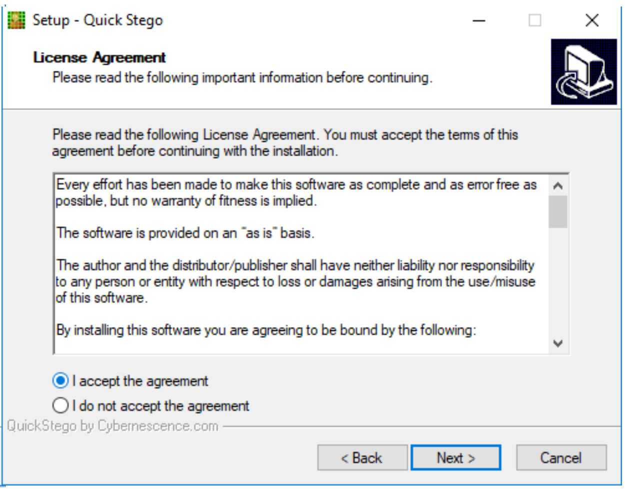
Setup - Quick Stego

Welcome to the Quick Stego Setup Wizard

This will install Quick Stego 1.2 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.



Setup - Quick Stego

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Every effort has been made to make this software as complete and as error free as possible, but no warranty of fitness is implied.

The software is provided on an "as is" basis.

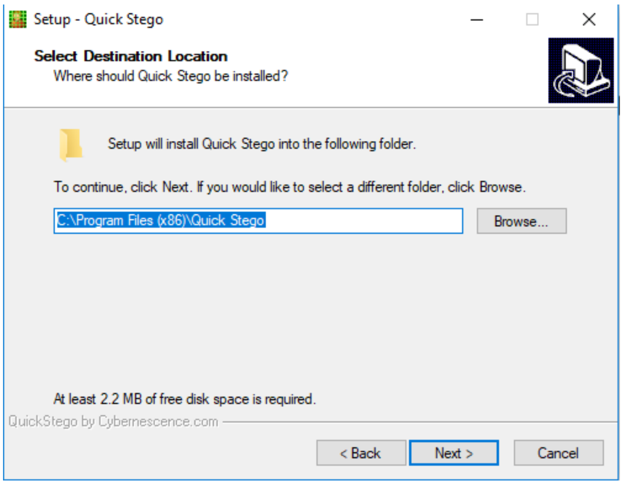
The author and the distributor/publisher shall have neither liability nor responsibility to any person or entity with respect to loss or damages arising from the use/misuse of this software.

By installing this software you are agreeing to be bound by the following:

● I accept the agreement

○ I do not accept the agreement

QuickStego by Cybernescence.com



Setup - Quick Stego

Select Destination Location

Where should Quick Stego be installed?

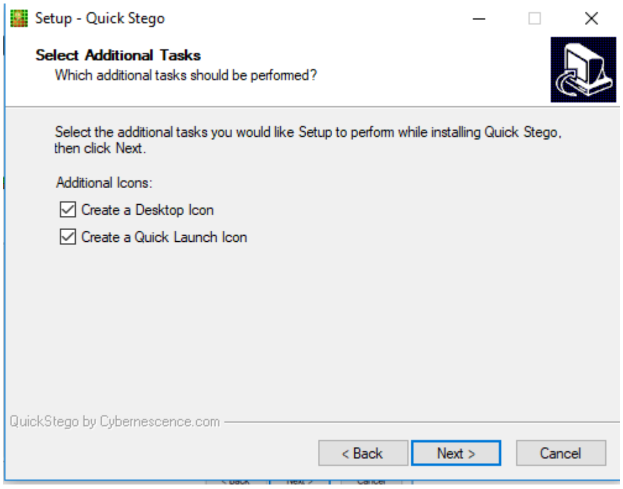
Setup will install Quick Stego into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\Quick Stego

At least 2.2 MB of free disk space is required.

QuickStego by Cybernescence.com



Setup - Quick Stego

Select Additional Tasks

Which additional tasks should be performed?

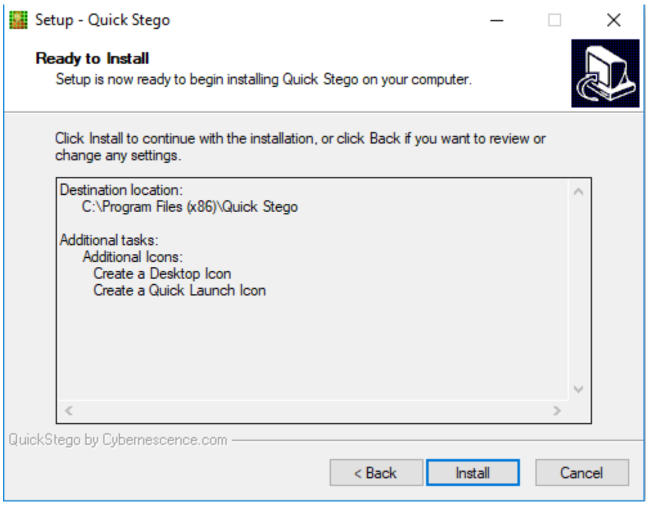
Select the additional tasks you would like Setup to perform while installing Quick Stego, then click Next.

Additional Icons:

☑ Create a Desktop Icon

☑ Create a Quick Launch Icon

QuickStego by Cybernescence.com



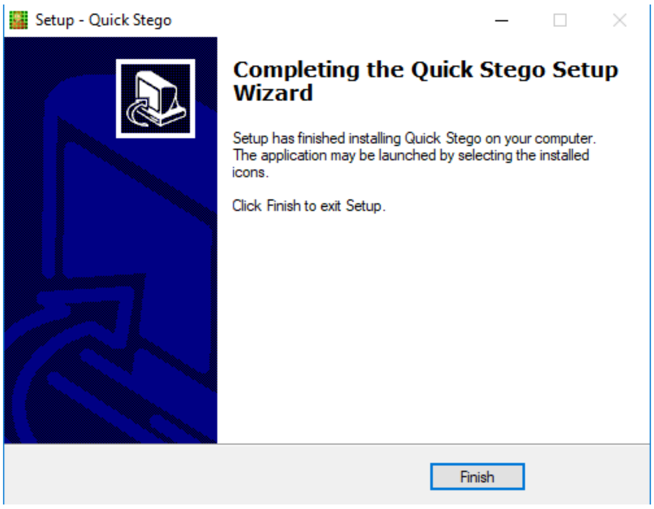
Setup - Quick Stego

Ready to Install

Setup is now ready to begin installing Quick Stego on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
    C:\Program Files (x86)\Quick Stego

Additional tasks:
    Additional Icons:
      Create a Desktop Icon
      Create a Quick Launch Icon
```



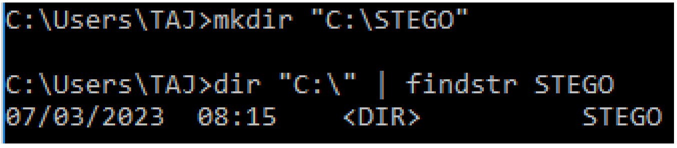
Setup - Quick Stego

Completing the Quick Stego Setup Wizard

Setup has finished installing Quick Stego on your computer. The application may be launched by selecting the installed icons.

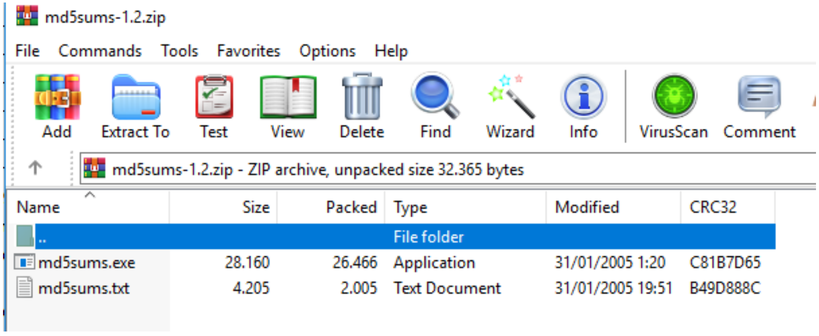
Click Finish to exit Setup.

4. Buka Command Prompt. Buat file STEGO melalui perintah mkdir "C:\STEGO". Temukan file tersebut dengan menggunakan perintah dir "C:\" | findstr STEGO.



```
C:\Users\TAJ>mkdir "C:\STEGO"

C:\Users\TAJ>dir "C:\" | findstr STEGO
07/03/2023  08:15    <DIR>          STEGO
```

5. Unduh ms5sums-1.2.zip pada http://www.pc-tools.net/files/win32/freeware/md5sums-1.2.zip. Buka menggunakan aplikasi pengekstrak zip.

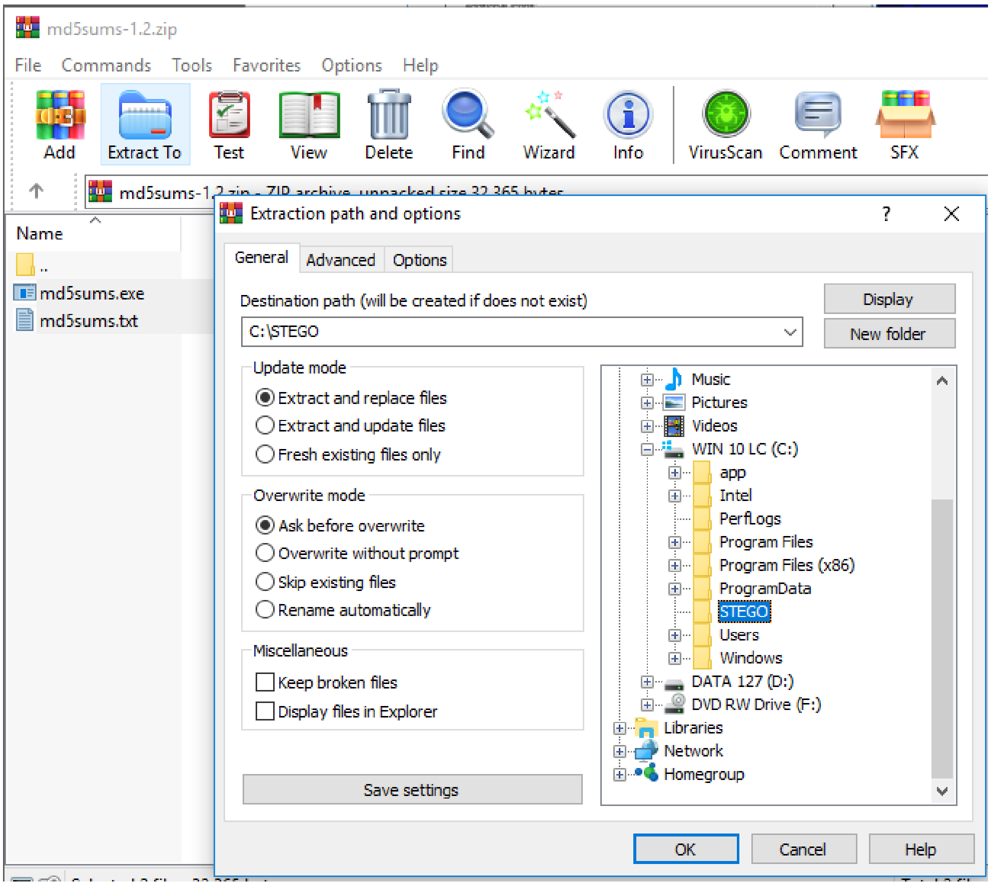


md5sums-1.2.zip

md5sums-1.2.zip - ZIP archive, unpacked size 32.365 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
md5sums.exe	28.160	26.466	Application	31/01/2005 1:20	C81B7D65
md5sums.txt	4.205	2.005	Text Document	31/01/2005 19:51	B49D888C

6. Ekstrak file ke dalam direktori STEGO yang telah dibuat sebelumnya.



Destination path (will be created if does not exist)

C:\STEGO

Update mode

● Extract and replace files

○ Extract and update files

○ Fresh existing files only

Overwrite mode

● Ask before overwrite

○ Overwrite without prompt

○ Skip existing files

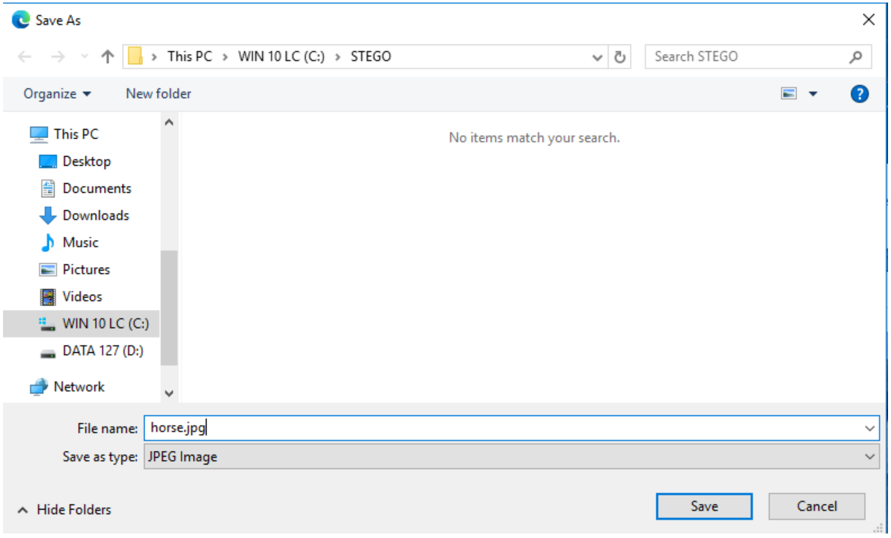
○ Rename automatically

Miscellaneous

□ Keep broken files

□ Display files in Explorer

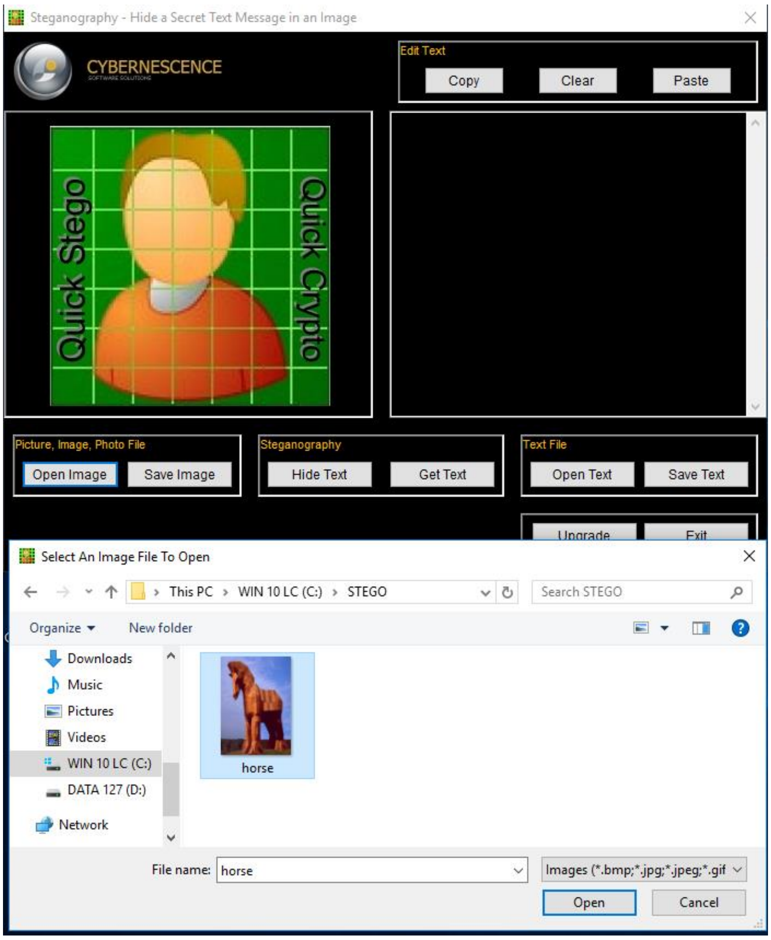
7. Unduh gambar kuda troya pada link https://elok.ugm.ac.id/mod/resource/view.php?id=349316. Klik kanan pada gambar > Save image as. Simpan dalam file direktori STEGO.



File name: horse.jpg

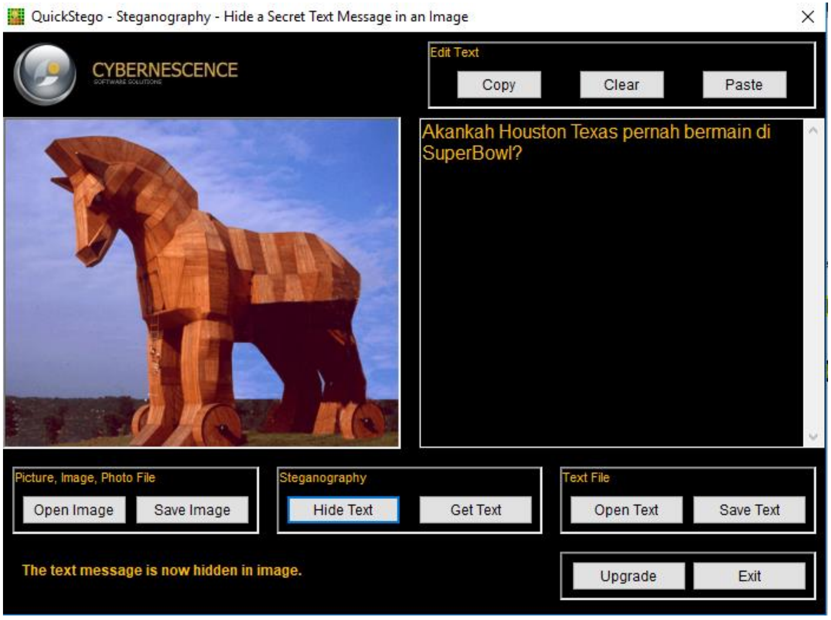
Save as type: JPEG Image

8. Jalankan Stego. Klik Open Image > pilih gambar horse.jpg > Open.



File name: horse

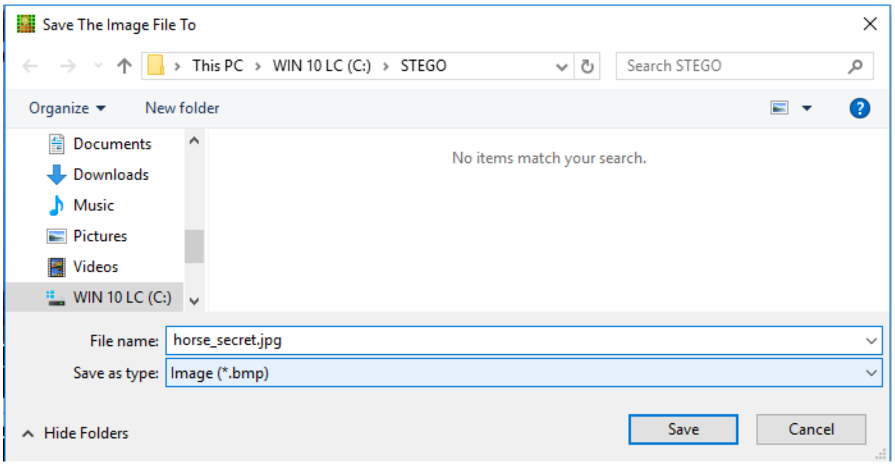
9. Berikan pesan tersembunyi lalu klik Hide Text.



Akankah Houston Texas pernah bermain di SuperBowl?

The text message is now hidden in image.

10. Simpan gambar dengan klik Save Image, arahkan ke dalam direktori STEGO dan simpan dengan nama horse_secret.jpg.



Save The Image File To

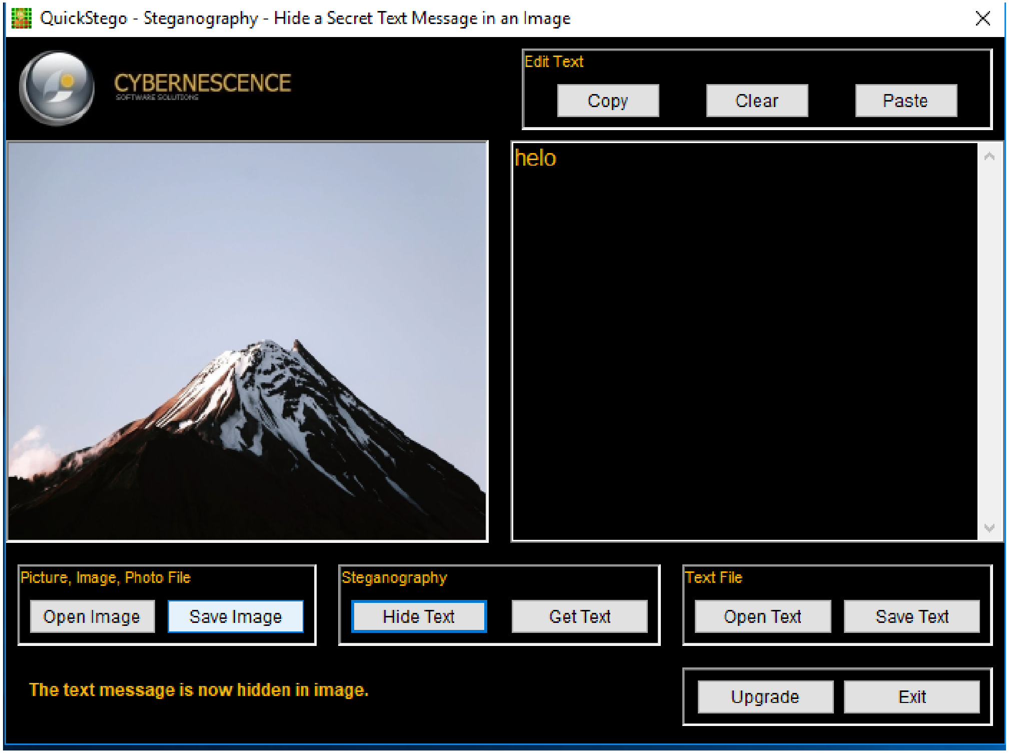
This PC › WIN 10 LC (C:) › STEGO

No items match your search.

File name: horse_secret.jpg

Save as type: Image (*.bmp)

11. Buka dan unduh file gambar kedua.



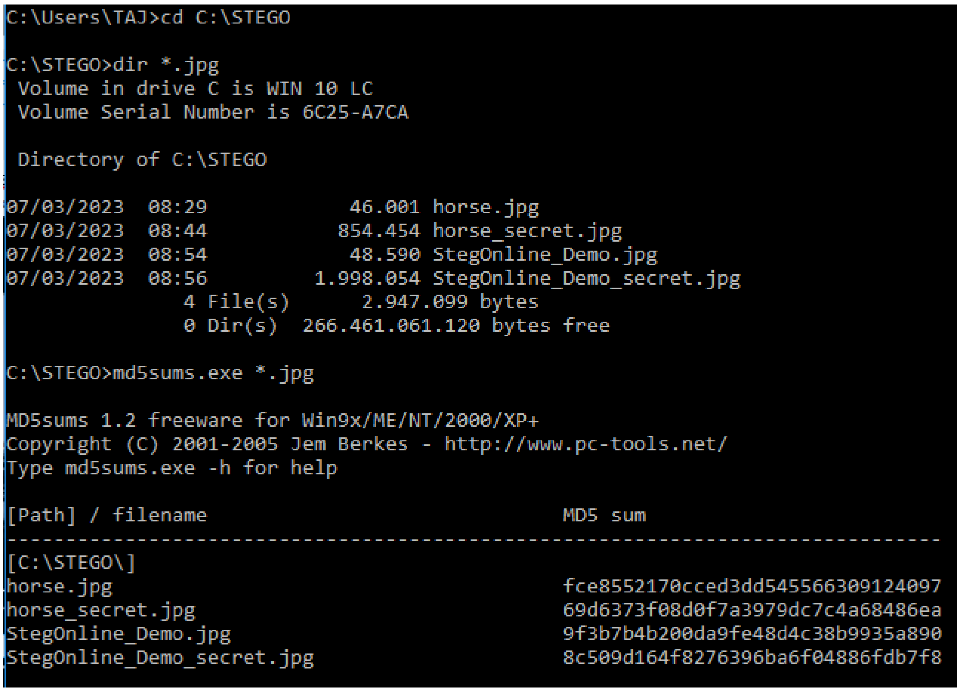
QuickStego - Steganography - Hide a Secret Text Message in an Image

helo

The text message is now hidden in image.

A. Pada md5sum

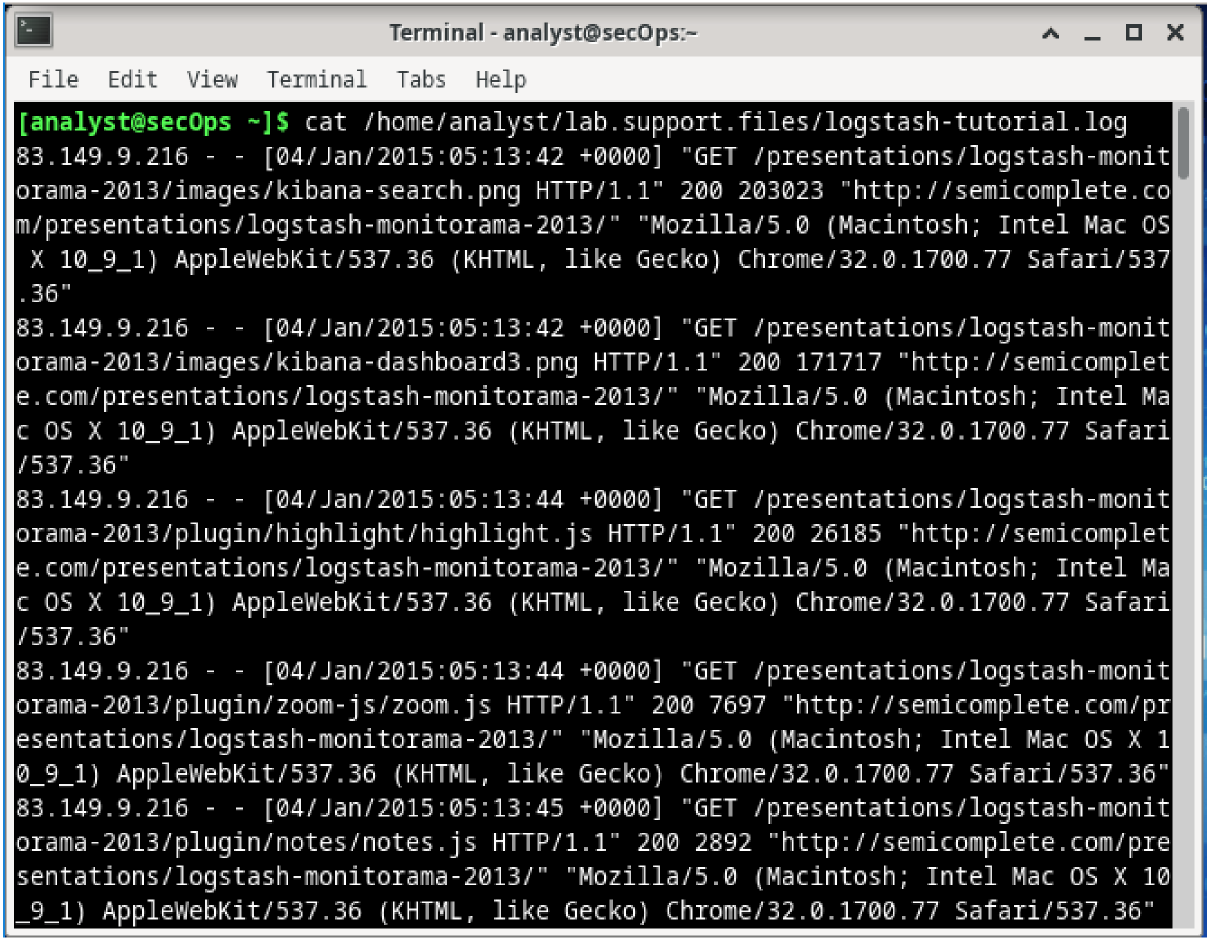
1. cd C:\STEGO
2. dir *.jpg
3. md5sums.exe *.jpg



```
C:\Users\TAJ>cd C:\STEGO

C:\STEGO>dir *.jpg
 Volume in drive C is WIN 10 LC
 Volume Serial Number is 6C25-A7CA

 Directory of C:\STEGO

07/03/2023  08:29            46.001 horse.jpg
07/03/2023  08:44           854.454 horse_secret.jpg
07/03/2023  08:54            48.590 StegOnline_Demo.jpg
07/03/2023  08:56         1.998.054 StegOnline_Demo_secret.jpg
               4 File(s)      2.947.099 bytes
               0 Dir(s)  266.461.061.120 bytes free

C:\STEGO>md5sums.exe *.jpg

MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums.exe -h for help

[Path] / filename                              MD5 sum
-------------------------------------------------------------------------------
[C:\STEGO\]
horse.jpg                                      fce8552170cced3dd545566309124097
horse_secret.jpg                               69d6373f08d0f7a3979dc7c4a68486ea
StegOnline_Demo.jpg                            9f3b7b4b200da9fe48d4c38b9935a890
StegOnline_Demo_secret.jpg                     8c509d164f8276396ba6f04886fdb7f8
```

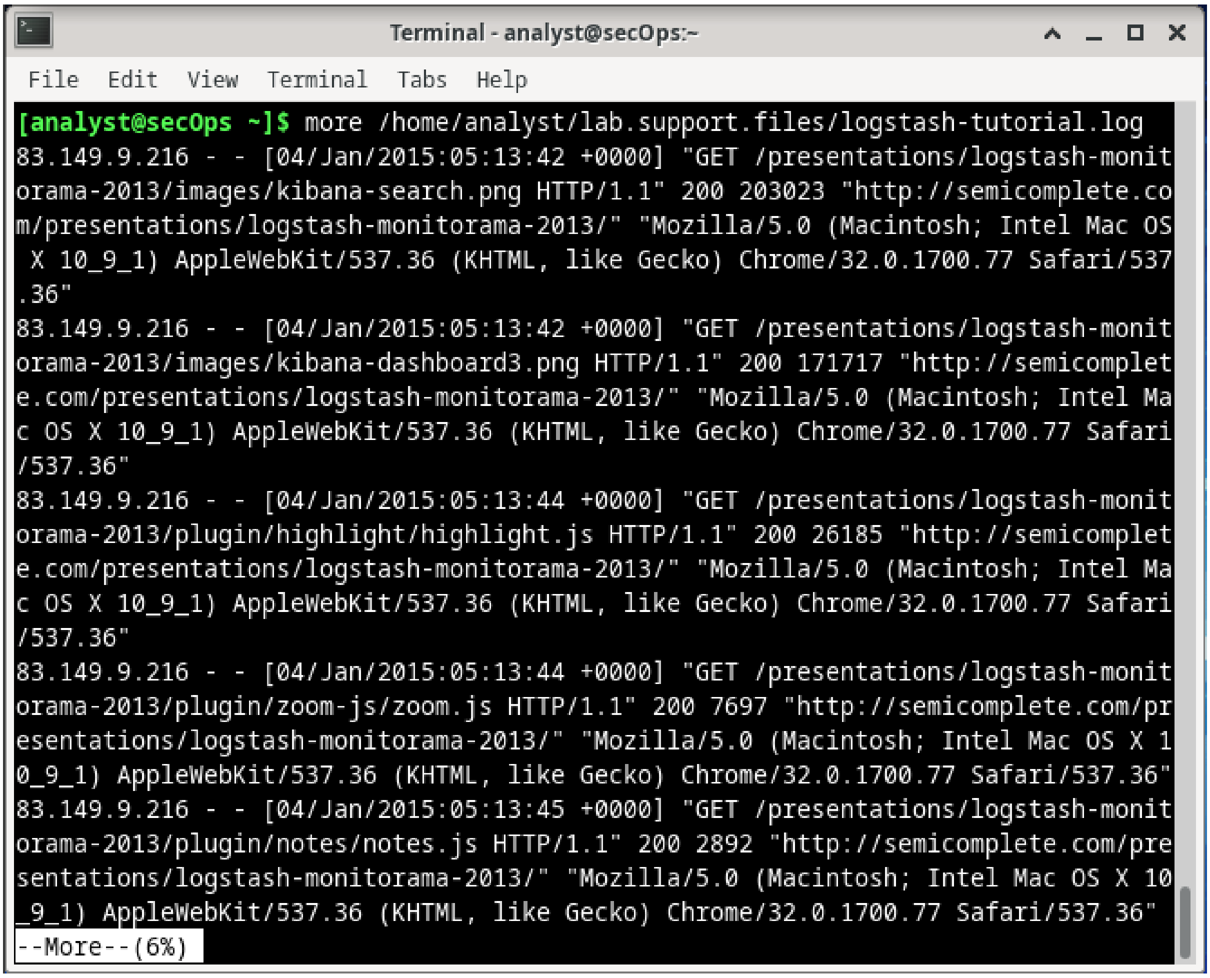
B. Analisis Log Server

1. Bukalah VM CyberOps Worstation dan jendela terminal. Jalankan perintah cat /home/analyst/lab.support.files/logstash-tutorial.log.


Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

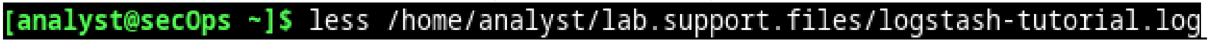
```
[analyst@secOps ~]$ cat /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.co
m/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
 X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537
.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/pr
esentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 1
0_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/pre
sentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10
_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
```

2. more /home/analyst/lab.support.files/logstash-tutorial.log

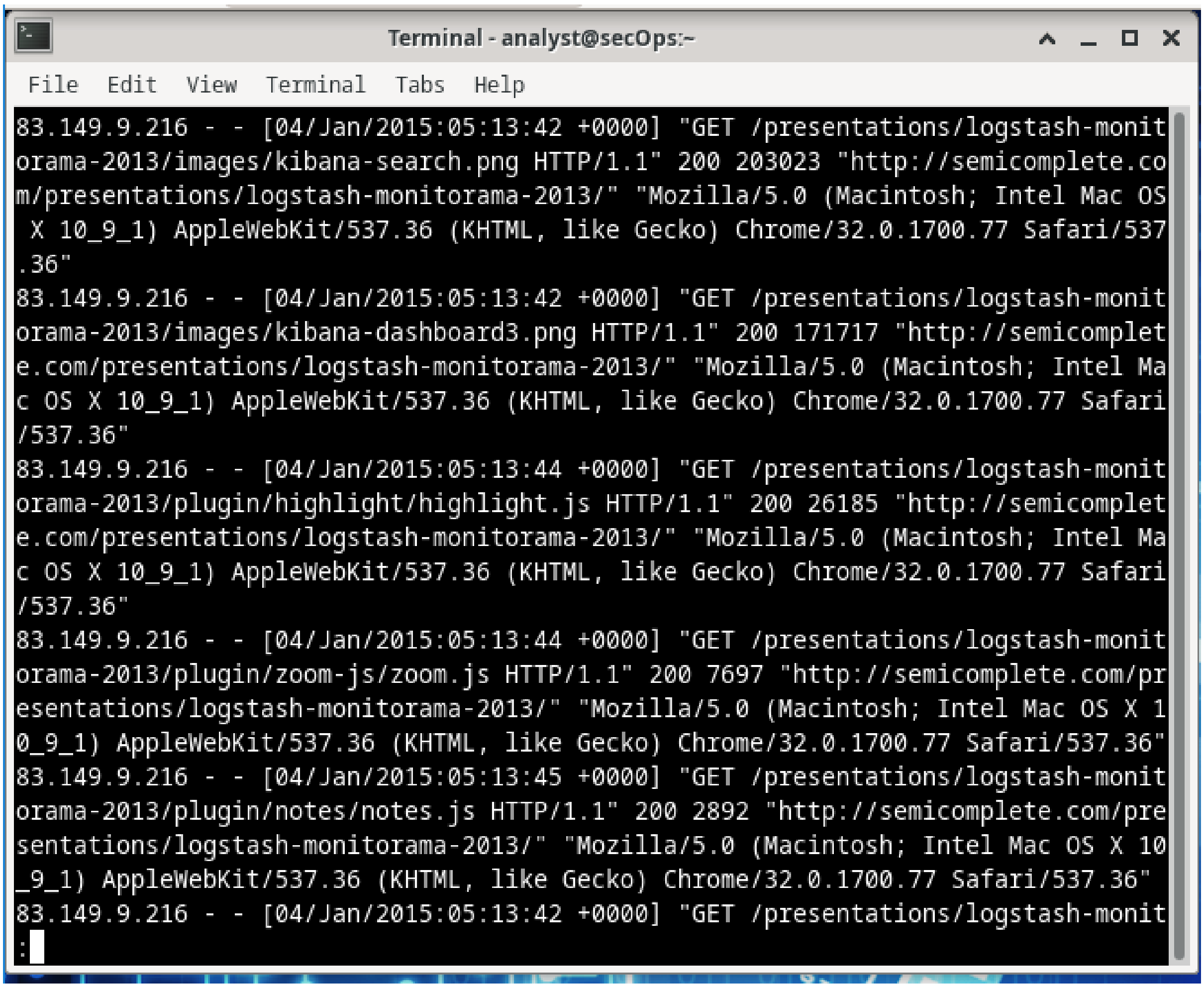

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ more /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.co
m/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
 X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537
.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/pr
esentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 1
0_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/pre
sentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10
_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
--More--(6%)
```

3. less /home/analyst/lab.support.files/logstash-tutorial.log

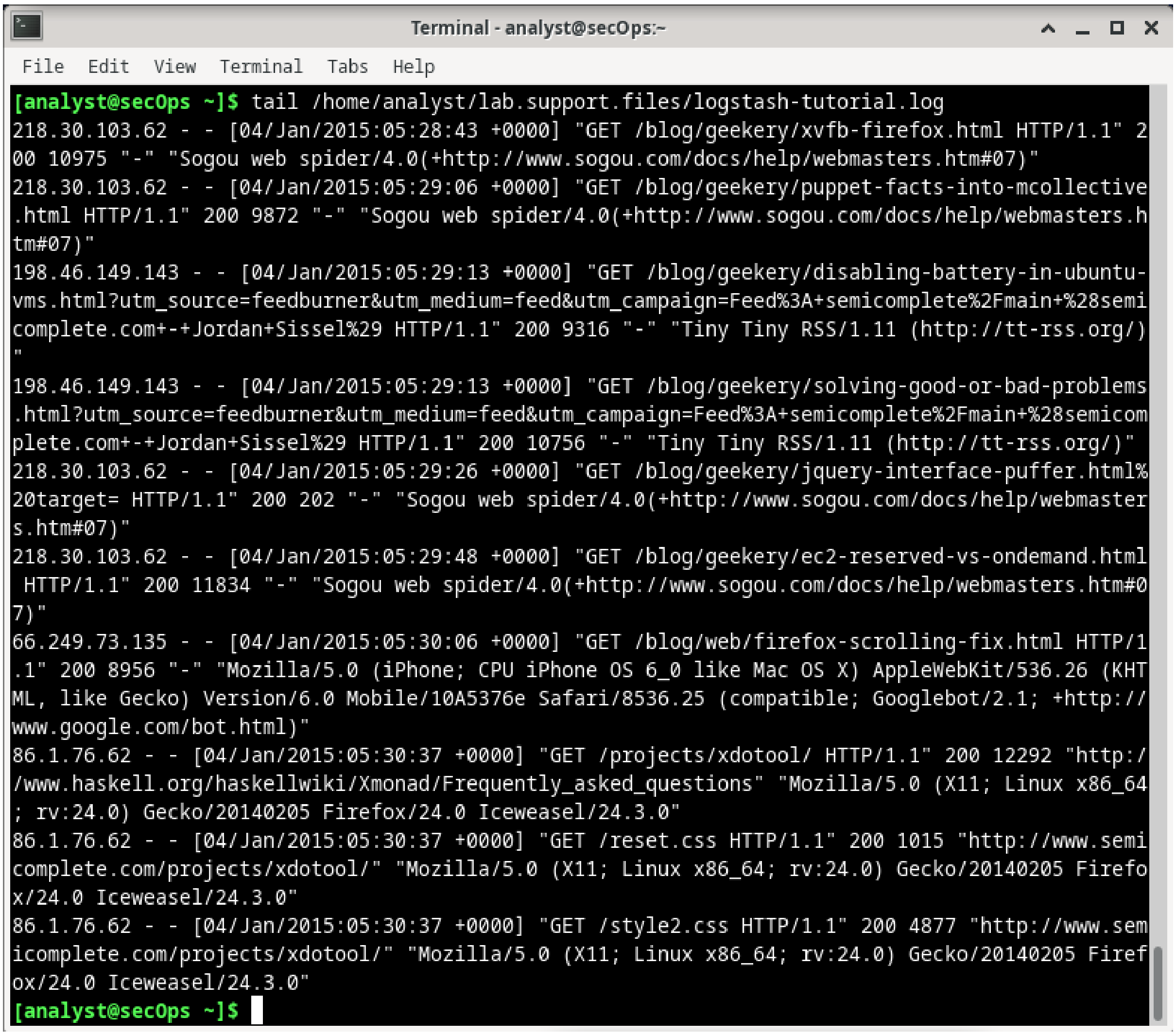


```
[analyst@secOps ~]$ less /home/analyst/lab.support.files/logstash-tutorial.log
```



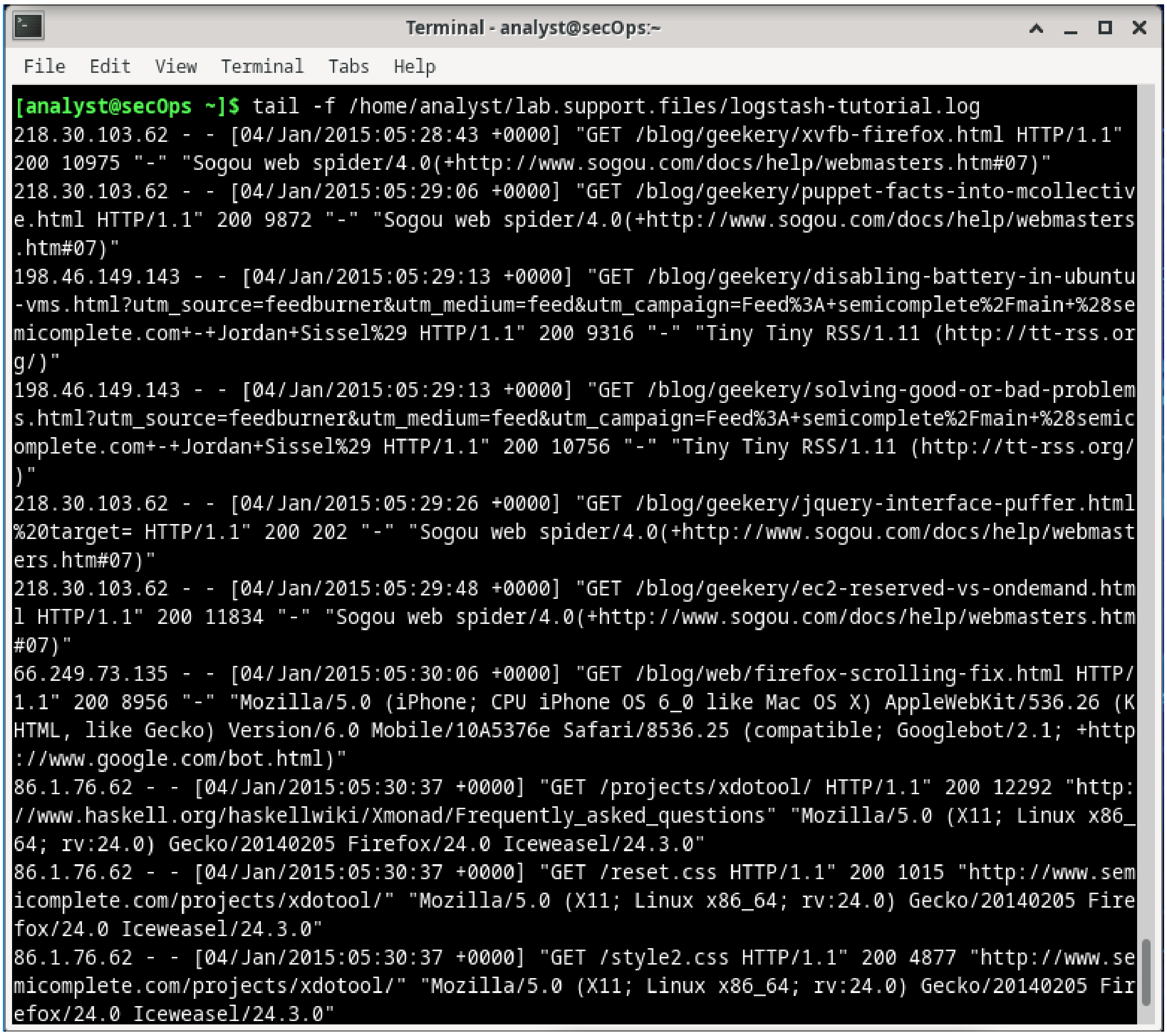
```
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.co
m/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
 X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537
.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/pr
esentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 1
0_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/pre
sentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10
_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
:
```

4. tail /home/analyst/lab.support.files/logstash-tutorial.log


Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ tail /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 2
00 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective
.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.h
tm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ubuntu-
vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semi
complete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)
"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-problems
.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicom
plete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.html%
20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmaster
s.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand.html
 HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#0
7)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html HTTP/1
.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHT
ML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://
www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "http:/
/www.haskell.org/haskellwiki/Xmonad/Frequently_asked_questions" "Mozilla/5.0 (X11; Linux x86_64
; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semi
complete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefo
x/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.sem
icomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firef
ox/24.0 Iceweasel/24.3.0"
[analyst@secOps ~]$
```

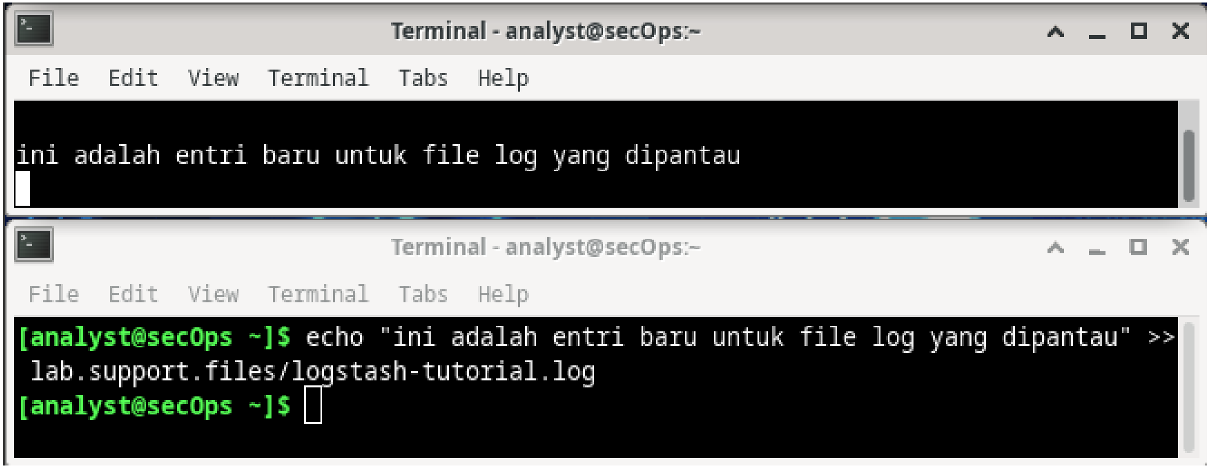
5. tail -f



Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ tail -f /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1"
200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollectiv
e.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters
.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ubuntu
-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28se
micomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.or
g/)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-problem
s.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semic
omplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/
)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.html
%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmast
ers.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand.htm
l HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm
#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html HTTP/
1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (K
HTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http
://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "http:
//www.haskell.org/haskellwiki/Xmonad/Frequently_asked_questions" "Mozilla/5.0 (X11; Linux x86_
64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.sem
icomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Fire
fox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.se
micomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Fir
efox/24.0 Iceweasel/24.3.0"
```

6. echo "ini adalah entri baru untuk file log yang dipantau" >> lab.support.files/logstash-tutorial.log



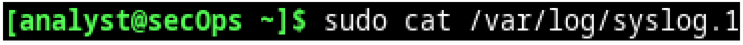
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
ini adalah entri baru untuk file log yang dipantau
```

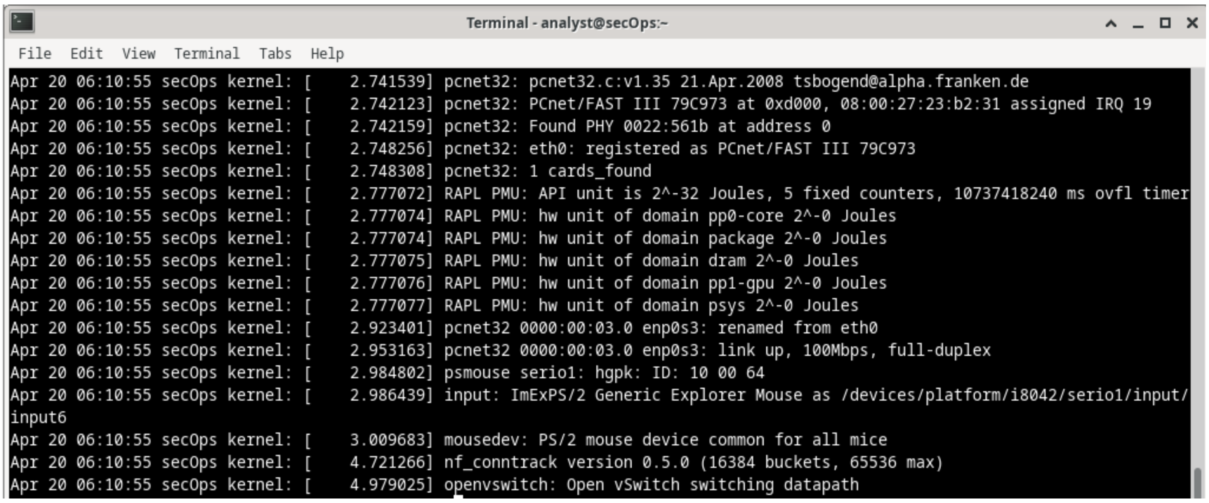
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ echo "ini adalah entri baru untuk file log yang dipantau" >>
 lab.support.files/logstash-tutorial.log
[analyst@secOps ~]$ 
```

7. sudo cat /var/log/syslog.1

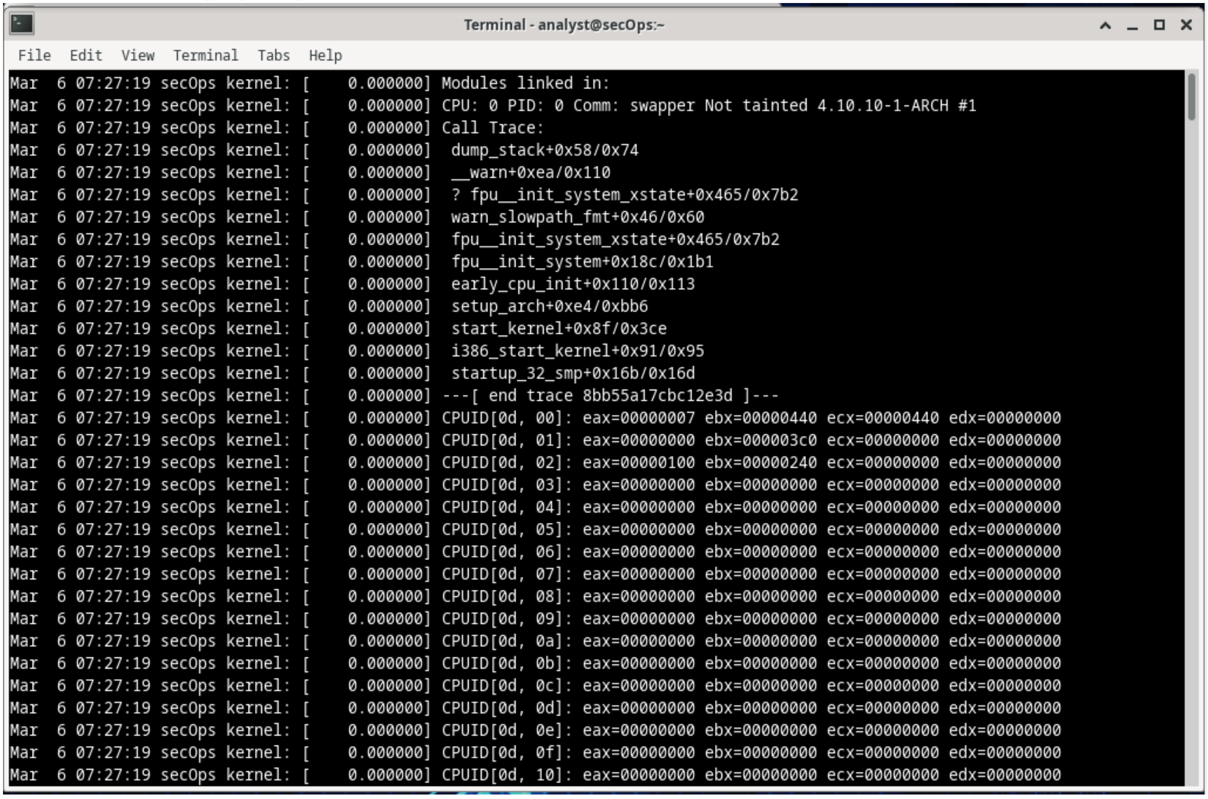


```
[analyst@secOps ~]$ sudo cat /var/log/syslog.1
```


Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

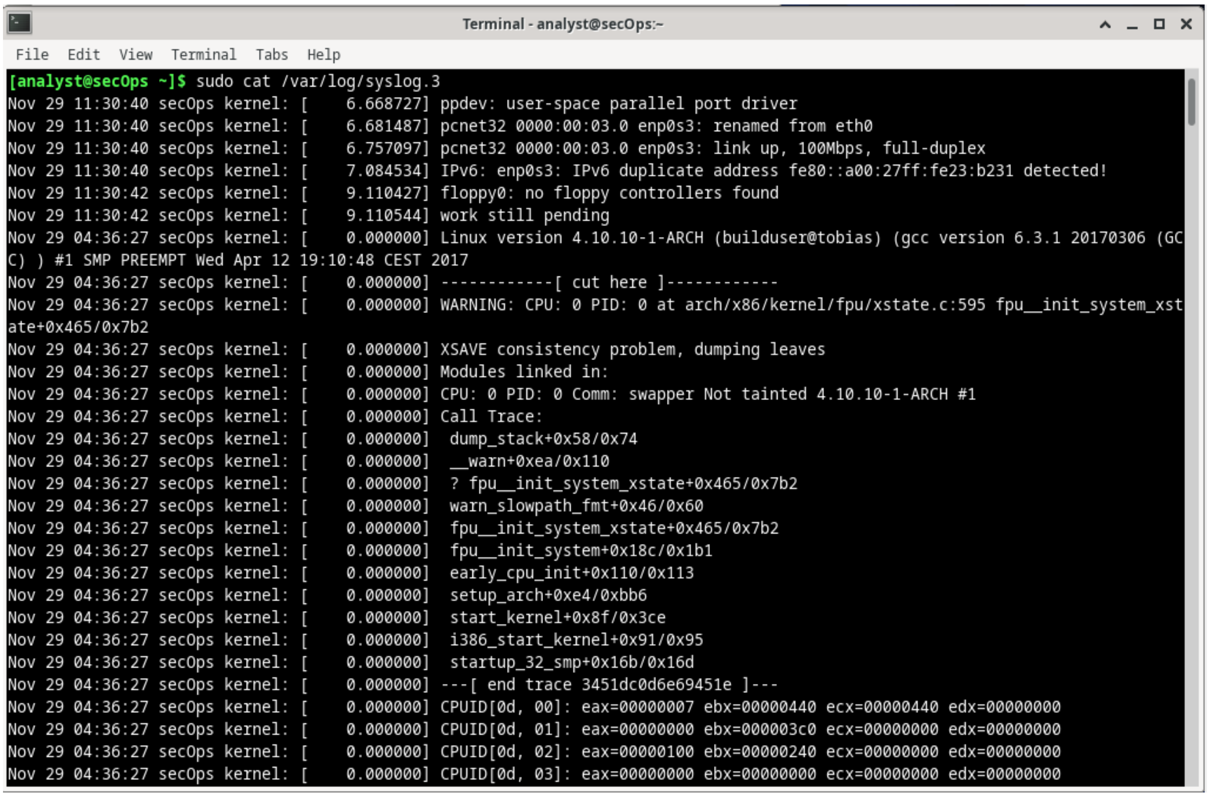
```
Apr 20 06:10:55 secOps kernel: [    2.741539] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
Apr 20 06:10:55 secOps kernel: [    2.742123] pcnet32: PCnet/FAST III 79C973 at 0xd000, 08:00:27:23:b2:31 assigned IRQ 19
Apr 20 06:10:55 secOps kernel: [    2.742159] pcnet32: Found PHY 0022:561b at address 0
Apr 20 06:10:55 secOps kernel: [    2.748256] pcnet32: eth0: registered as PCnet/FAST III 79C973
Apr 20 06:10:55 secOps kernel: [    2.748308] pcnet32: 1 cards_found
Apr 20 06:10:55 secOps kernel: [    2.777072] RAPL PMU: API unit is 2^-32 Joules, 5 fixed counters, 10737418240 ms ovfl timer
Apr 20 06:10:55 secOps kernel: [    2.777074] RAPL PMU: hw unit of domain pp0-core 2^-0 Joules
Apr 20 06:10:55 secOps kernel: [    2.777074] RAPL PMU: hw unit of domain package 2^-0 Joules
Apr 20 06:10:55 secOps kernel: [    2.777075] RAPL PMU: hw unit of domain dram 2^-0 Joules
Apr 20 06:10:55 secOps kernel: [    2.777076] RAPL PMU: hw unit of domain pp1-gpu 2^-0 Joules
Apr 20 06:10:55 secOps kernel: [    2.777077] RAPL PMU: hw unit of domain psys 2^-0 Joules
Apr 20 06:10:55 secOps kernel: [    2.923401] pcnet32 0000:00:03.0 enp0s3: renamed from eth0
Apr 20 06:10:55 secOps kernel: [    2.953163] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Apr 20 06:10:55 secOps kernel: [    2.984802] psmouse serio1: hgpk: ID: 10 00 64
Apr 20 06:10:55 secOps kernel: [    2.986439] input: ImExPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input/
input6
Apr 20 06:10:55 secOps kernel: [    3.009683] mousedev: PS/2 mouse device common for all mice
Apr 20 06:10:55 secOps kernel: [    4.721266] nf_conntrack version 0.5.0 (16384 buckets, 65536 max)
Apr 20 06:10:55 secOps kernel: [    4.979025] openvswitch: Open vSwitch switching datapath
```

8. sudo cat /var/log/syslog.2


Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
Mar  6 07:27:19 secOps kernel: [    0.000000] Modules linked in:
Mar  6 07:27:19 secOps kernel: [    0.000000] CPU: 0 PID: 0 Comm: swapper Not tainted 4.10.10-1-ARCH #1
Mar  6 07:27:19 secOps kernel: [    0.000000] Call Trace:
Mar  6 07:27:19 secOps kernel: [    0.000000]  dump_stack+0x58/0x74
Mar  6 07:27:19 secOps kernel: [    0.000000]  __warn+0xea/0x110
Mar  6 07:27:19 secOps kernel: [    0.000000]  ? fpu__init_system_xstate+0x465/0x7b2
Mar  6 07:27:19 secOps kernel: [    0.000000]  warn_slowpath_fmt+0x46/0x60
Mar  6 07:27:19 secOps kernel: [    0.000000]  fpu__init_system_xstate+0x465/0x7b2
Mar  6 07:27:19 secOps kernel: [    0.000000]  fpu__init_system+0x18c/0x1b1
Mar  6 07:27:19 secOps kernel: [    0.000000]  early_cpu_init+0x110/0x113
Mar  6 07:27:19 secOps kernel: [    0.000000]  setup_arch+0xe4/0xbb6
Mar  6 07:27:19 secOps kernel: [    0.000000]  start_kernel+0x8f/0x3ce
Mar  6 07:27:19 secOps kernel: [    0.000000]  i386_start_kernel+0x91/0x95
Mar  6 07:27:19 secOps kernel: [    0.000000]  startup_32_smp+0x16b/0x16d
Mar  6 07:27:19 secOps kernel: [    0.000000] ---[ end trace 8bb55a17cbc12e3d ]---
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 00]: eax=00000007 ebx=00000440 ecx=00000440 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 01]: eax=00000000 ebx=000003c0 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 02]: eax=00000100 ebx=00000240 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 03]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 04]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 05]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 06]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 07]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 08]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 09]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 0a]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 0b]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 0c]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 0d]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 0e]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 0f]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 10]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
```

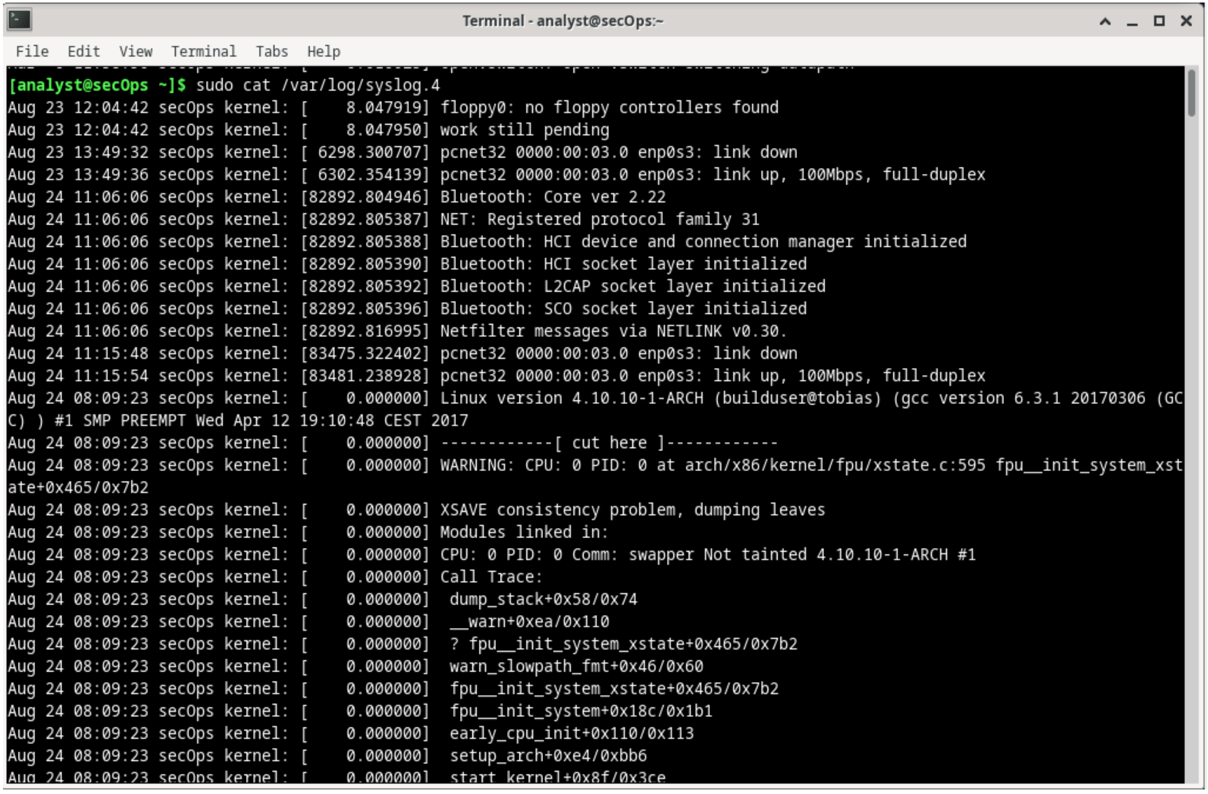
9. sudo cat /var/log/syslog.3



Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ sudo cat /var/log/syslog.3
Nov 29 11:30:40 secOps kernel: [    6.668727] ppdev: user-space parallel port driver
Nov 29 11:30:40 secOps kernel: [    6.681487] pcnet32 0000:00:03.0 enp0s3: renamed from eth0
Nov 29 11:30:40 secOps kernel: [    6.757097] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Nov 29 11:30:40 secOps kernel: [    7.084534] IPv6: enp0s3: IPv6 duplicate address fe80::a00:27ff:fe23:b231 detected!
Nov 29 11:30:42 secOps kernel: [    9.110427] floppy0: no floppy controllers found
Nov 29 11:30:42 secOps kernel: [    9.110544] work still pending
Nov 29 04:36:27 secOps kernel: [    0.000000] Linux version 4.10.10-1-ARCH (builduser@tobias) (gcc version 6.3.1 20170306 (GC
C) ) #1 SMP PREEMPT Wed Apr 12 19:10:48 CEST 2017
Nov 29 04:36:27 secOps kernel: [    0.000000] ------------[ cut here ]------------
Nov 29 04:36:27 secOps kernel: [    0.000000] WARNING: CPU: 0 PID: 0 at arch/x86/kernel/fpu/xstate.c:595 fpu__init_system_xst
ate+0x465/0x7b2
Nov 29 04:36:27 secOps kernel: [    0.000000] XSAVE consistency problem, dumping leaves
Nov 29 04:36:27 secOps kernel: [    0.000000] Modules linked in:
Nov 29 04:36:27 secOps kernel: [    0.000000] CPU: 0 PID: 0 Comm: swapper Not tainted 4.10.10-1-ARCH #1
Nov 29 04:36:27 secOps kernel: [    0.000000] Call Trace:
Nov 29 04:36:27 secOps kernel: [    0.000000]  dump_stack+0x58/0x74
Nov 29 04:36:27 secOps kernel: [    0.000000]  __warn+0xea/0x110
Nov 29 04:36:27 secOps kernel: [    0.000000]  ? fpu__init_system_xstate+0x465/0x7b2
Nov 29 04:36:27 secOps kernel: [    0.000000]  warn_slowpath_fmt+0x46/0x60
Nov 29 04:36:27 secOps kernel: [    0.000000]  fpu__init_system_xstate+0x465/0x7b2
Nov 29 04:36:27 secOps kernel: [    0.000000]  fpu__init_system+0x18c/0x1b1
Nov 29 04:36:27 secOps kernel: [    0.000000]  early_cpu_init+0x110/0x113
Nov 29 04:36:27 secOps kernel: [    0.000000]  setup_arch+0xe4/0xbb6
Nov 29 04:36:27 secOps kernel: [    0.000000]  start_kernel+0x8f/0x3ce
Nov 29 04:36:27 secOps kernel: [    0.000000]  i386_start_kernel+0x91/0x95
Nov 29 04:36:27 secOps kernel: [    0.000000]  startup_32_smp+0x16b/0x16d
Nov 29 04:36:27 secOps kernel: [    0.000000] ---[ end trace 3451dc0d6e69451e ]---
Nov 29 04:36:27 secOps kernel: [    0.000000] CPUID[0d, 00]: eax=00000007 ebx=00000440 ecx=00000440 edx=00000000
Nov 29 04:36:27 secOps kernel: [    0.000000] CPUID[0d, 01]: eax=00000000 ebx=000003c0 ecx=00000000 edx=00000000
Nov 29 04:36:27 secOps kernel: [    0.000000] CPUID[0d, 02]: eax=00000100 ebx=00000240 ecx=00000000 edx=00000000
Nov 29 04:36:27 secOps kernel: [    0.000000] CPUID[0d, 03]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
```

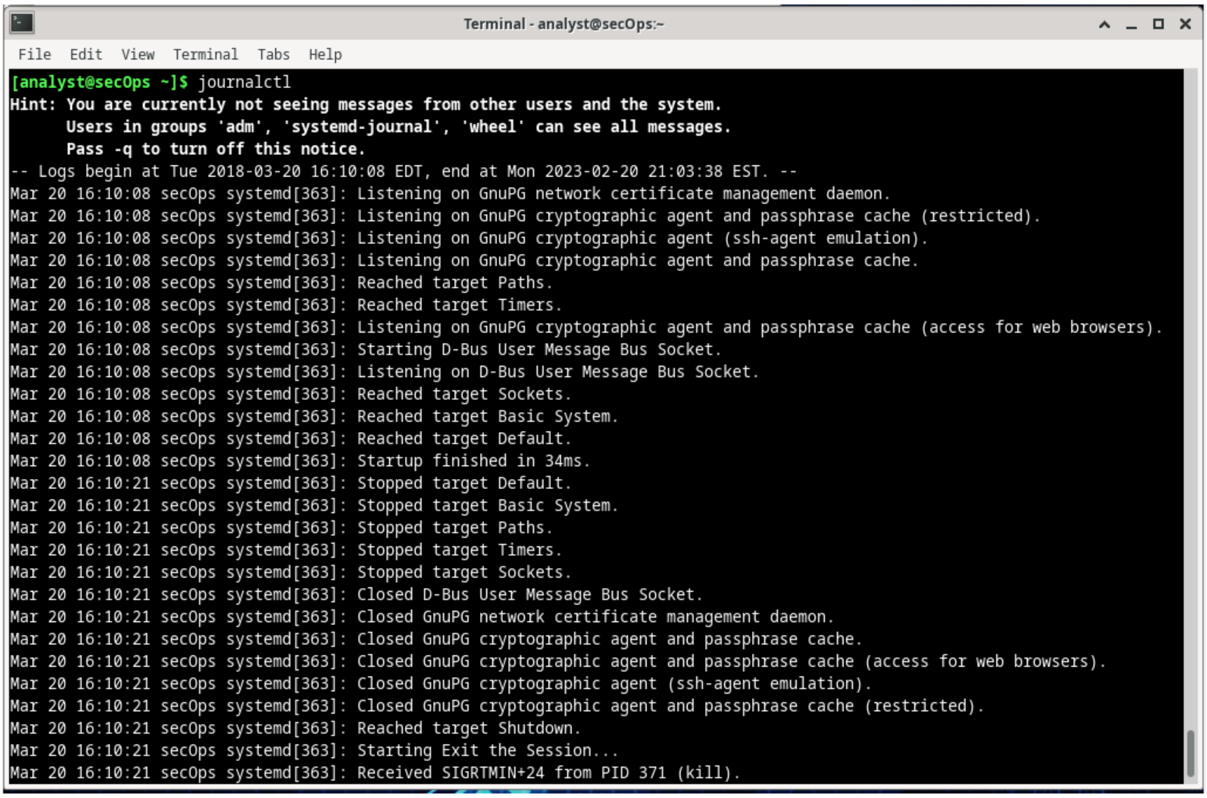
10. sudo cat /var/log/syslog.4



Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ sudo cat /var/log/syslog.4
Aug 23 12:04:42 secOps kernel: [    8.047919] floppy0: no floppy controllers found
Aug 23 12:04:42 secOps kernel: [    8.047950] work still pending
Aug 23 13:49:32 secOps kernel: [ 6298.300707] pcnet32 0000:00:03.0 enp0s3: link down
Aug 23 13:49:36 secOps kernel: [ 6302.354139] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Aug 24 11:06:06 secOps kernel: [82892.804946] Bluetooth: Core ver 2.22
Aug 24 11:06:06 secOps kernel: [82892.805387] NET: Registered protocol family 31
Aug 24 11:06:06 secOps kernel: [82892.805388] Bluetooth: HCI device and connection manager initialized
Aug 24 11:06:06 secOps kernel: [82892.805390] Bluetooth: HCI socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.805392] Bluetooth: L2CAP socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.805396] Bluetooth: SCO socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.816995] Netfilter messages via NETLINK v0.30.
Aug 24 11:15:48 secOps kernel: [83475.322402] pcnet32 0000:00:03.0 enp0s3: link down
Aug 24 11:15:54 secOps kernel: [83481.238928] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Aug 24 08:09:23 secOps kernel: [    0.000000] Linux version 4.10.10-1-ARCH (builduser@tobias) (gcc version 6.3.1 20170306 (GC
C) ) #1 SMP PREEMPT Wed Apr 12 19:10:48 CEST 2017
Aug 24 08:09:23 secOps kernel: [    0.000000] ------------[ cut here ]------------
Aug 24 08:09:23 secOps kernel: [    0.000000] WARNING: CPU: 0 PID: 0 at arch/x86/kernel/fpu/xstate.c:595 fpu__init_system_xst
ate+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [    0.000000] XSAVE consistency problem, dumping leaves
Aug 24 08:09:23 secOps kernel: [    0.000000] Modules linked in:
Aug 24 08:09:23 secOps kernel: [    0.000000] CPU: 0 PID: 0 Comm: swapper Not tainted 4.10.10-1-ARCH #1
Aug 24 08:09:23 secOps kernel: [    0.000000] Call Trace:
Aug 24 08:09:23 secOps kernel: [    0.000000]  dump_stack+0x58/0x74
Aug 24 08:09:23 secOps kernel: [    0.000000]  __warn+0xea/0x110
Aug 24 08:09:23 secOps kernel: [    0.000000]  ? fpu__init_system_xstate+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [    0.000000]  warn_slowpath_fmt+0x46/0x60
Aug 24 08:09:23 secOps kernel: [    0.000000]  fpu__init_system_xstate+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [    0.000000]  fpu__init_system+0x18c/0x1b1
Aug 24 08:09:23 secOps kernel: [    0.000000]  early_cpu_init+0x110/0x113
Aug 24 08:09:23 secOps kernel: [    0.000000]  setup_arch+0xe4/0xbb6
Aug 24 08:09:23 secOps kernel: [    0.000000]  start_kernel+0x8f/0x3ce
```

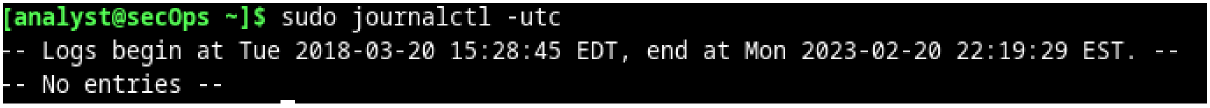
11. journalctl



Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

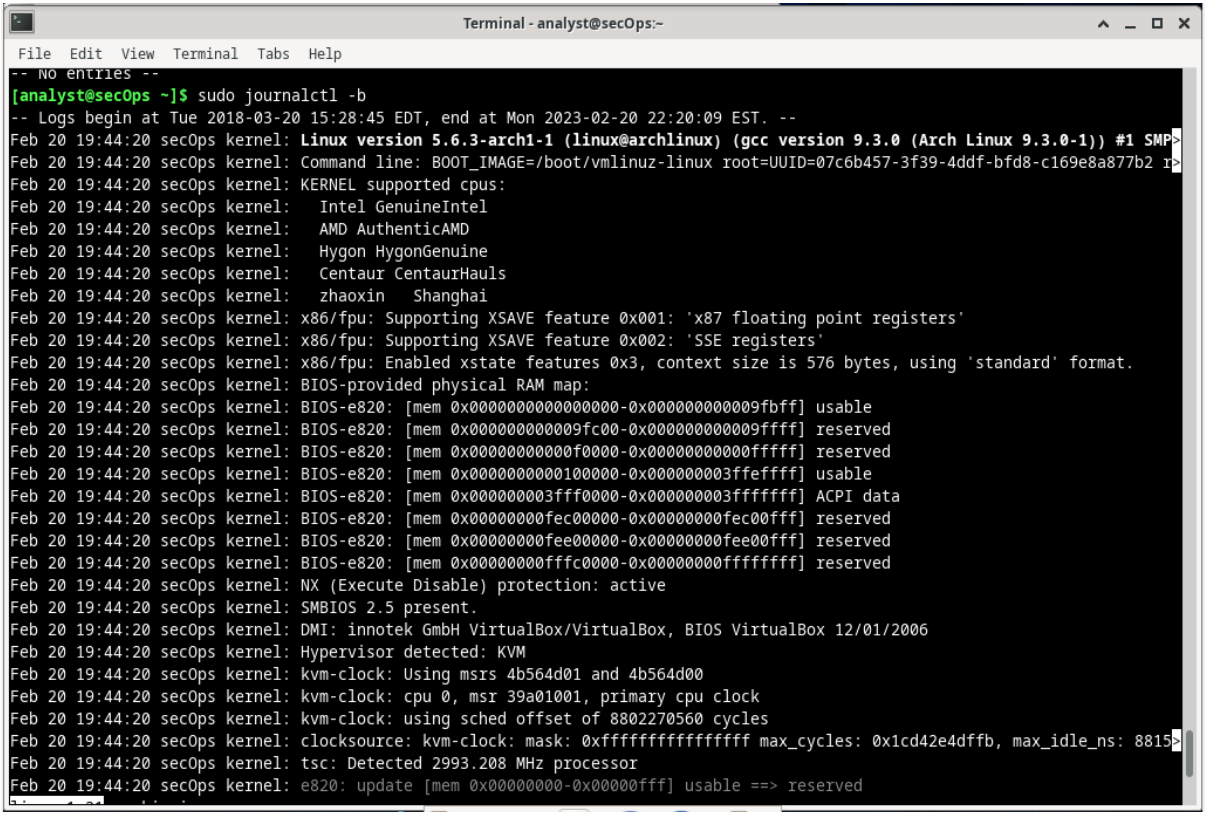
```
[analyst@secOps ~]$ journalctl
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal', 'wheel' can see all messages.
      Pass -q to turn off this notice.
-- Logs begin at Tue 2018-03-20 16:10:08 EDT, end at Mon 2023-02-20 21:03:38 EST. --
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG network certificate management daemon.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache.
Mar 20 16:10:08 secOps systemd[363]: Reached target Paths.
Mar 20 16:10:08 secOps systemd[363]: Reached target Timers.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache (access for web browsers).
Mar 20 16:10:08 secOps systemd[363]: Starting D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Listening on D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Reached target Sockets.
Mar 20 16:10:08 secOps systemd[363]: Reached target Basic System.
Mar 20 16:10:08 secOps systemd[363]: Reached target Default.
Mar 20 16:10:08 secOps systemd[363]: Startup finished in 34ms.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Default.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Basic System.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Paths.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Timers.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Sockets.
Mar 20 16:10:21 secOps systemd[363]: Closed D-Bus User Message Bus Socket.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG network certificate management daemon.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache (access for web browsers).
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent (ssh-agent emulation).
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 16:10:21 secOps systemd[363]: Reached target Shutdown.
Mar 20 16:10:21 secOps systemd[363]: Starting Exit the Session...
Mar 20 16:10:21 secOps systemd[363]: Received SIGRTMIN+24 from PID 371 (kill).
```

12. sudo journalctl –utc



```
[analyst@secOps ~]$ sudo journalctl -utc
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-02-20 22:19:29 EST. --
-- No entries --
```

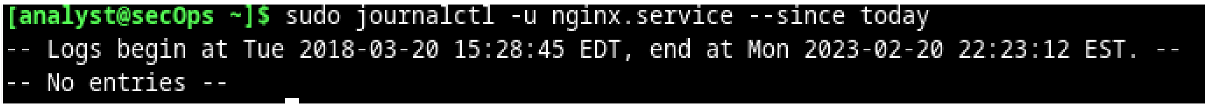
13. sudo journalctl –b



Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

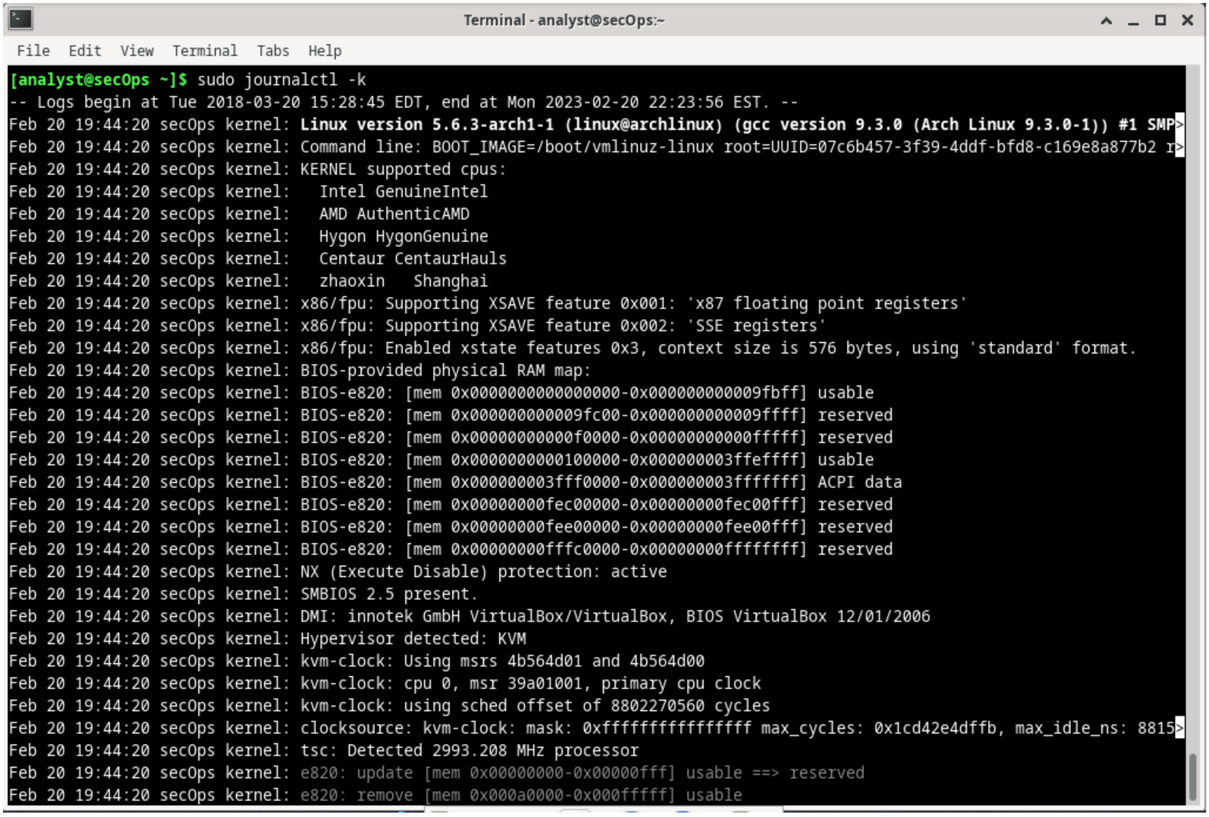
```
-- No entries --
[analyst@secOps ~]$ sudo journalctl -b
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-02-20 22:20:09 EST. --
Feb 20 19:44:20 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (gcc version 9.3.0 (Arch Linux 9.3.0-1)) #1 SMP>
Feb 20 19:44:20 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 r>
Feb 20 19:44:20 secOps kernel: KERNEL supported cpus:
Feb 20 19:44:20 secOps kernel:   Intel GenuineIntel
Feb 20 19:44:20 secOps kernel:   AMD AuthenticAMD
Feb 20 19:44:20 secOps kernel:   Hygon HygonGenuine
Feb 20 19:44:20 secOps kernel:   Centaur CentaurHauls
Feb 20 19:44:20 secOps kernel:   zhaoxin   Shanghai
Feb 20 19:44:20 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Feb 20 19:44:20 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Feb 20 19:44:20 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Feb 20 19:44:20 secOps kernel: BIOS-provided physical RAM map:
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usable
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACPI data
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Feb 20 19:44:20 secOps kernel: NX (Execute Disable) protection: active
Feb 20 19:44:20 secOps kernel: SMBIOS 2.5 present.
Feb 20 19:44:20 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Feb 20 19:44:20 secOps kernel: Hypervisor detected: KVM
Feb 20 19:44:20 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Feb 20 19:44:20 secOps kernel: kvm-clock: cpu 0, msr 39a01001, primary cpu clock
Feb 20 19:44:20 secOps kernel: kvm-clock: using sched offset of 8802270560 cycles
Feb 20 19:44:20 secOps kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 8815>
Feb 20 19:44:20 secOps kernel: tsc: Detected 2993.208 MHz processor
Feb 20 19:44:20 secOps kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
```

14. sudo journalctl -u nginx.service --since today



```
[analyst@secOps ~]$ sudo journalctl -u nginx.service --since today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-02-20 22:23:12 EST. --
-- No entries --
```

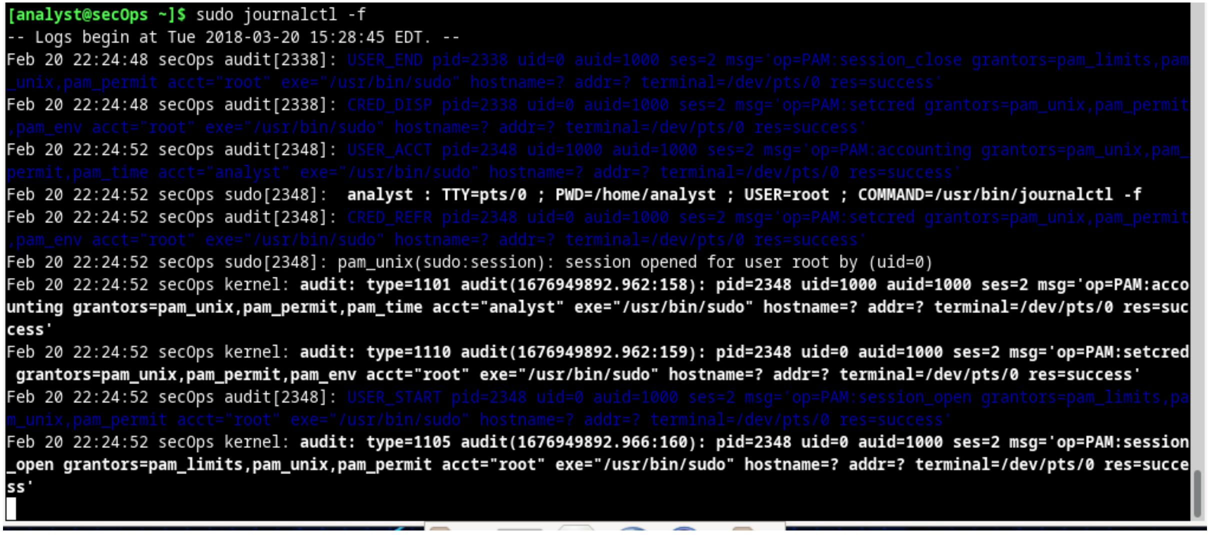
15. sudo journalctl –k



Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ sudo journalctl -k
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-02-20 22:23:56 EST. --
Feb 20 19:44:20 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (gcc version 9.3.0 (Arch Linux 9.3.0-1)) #1 SMP>
Feb 20 19:44:20 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 r>
Feb 20 19:44:20 secOps kernel: KERNEL supported cpus:
Feb 20 19:44:20 secOps kernel:   Intel GenuineIntel
Feb 20 19:44:20 secOps kernel:   AMD AuthenticAMD
Feb 20 19:44:20 secOps kernel:   Hygon HygonGenuine
Feb 20 19:44:20 secOps kernel:   Centaur CentaurHauls
Feb 20 19:44:20 secOps kernel:   zhaoxin   Shanghai
Feb 20 19:44:20 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Feb 20 19:44:20 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Feb 20 19:44:20 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Feb 20 19:44:20 secOps kernel: BIOS-provided physical RAM map:
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usable
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACPI data
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Feb 20 19:44:20 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Feb 20 19:44:20 secOps kernel: NX (Execute Disable) protection: active
Feb 20 19:44:20 secOps kernel: SMBIOS 2.5 present.
Feb 20 19:44:20 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Feb 20 19:44:20 secOps kernel: Hypervisor detected: KVM
Feb 20 19:44:20 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Feb 20 19:44:20 secOps kernel: kvm-clock: cpu 0, msr 39a01001, primary cpu clock
Feb 20 19:44:20 secOps kernel: kvm-clock: using sched offset of 8802270560 cycles
Feb 20 19:44:20 secOps kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 8815>
Feb 20 19:44:20 secOps kernel: tsc: Detected 2993.208 MHz processor
Feb 20 19:44:20 secOps kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Feb 20 19:44:20 secOps kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
```

16. sudo journalctl –f



```
[analyst@secOps ~]$ sudo journalctl -f
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Feb 20 22:24:48 secOps audit[2338]: USER_END pid=2338 uid=0 auid=1000 ses=2 msg='op=PAM:session_close grantors=pam_limits,pam
_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Feb 20 22:24:48 secOps audit[2338]: CRED_DISP pid=2338 uid=0 auid=1000 ses=2 msg='op=PAM:setcred grantors=pam_unix,pam_permit
,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Feb 20 22:24:52 secOps audit[2348]: USER_ACCT pid=2348 uid=1000 auid=1000 ses=2 msg='op=PAM:accounting grantors=pam_unix,pam_
permit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Feb 20 22:24:52 secOps sudo[2348]:  analyst : TTY=pts/0 ; PWD=/home/analyst ; USER=root ; COMMAND=/usr/bin/journalctl -f
Feb 20 22:24:52 secOps audit[2348]: CRED_REFR pid=2348 uid=0 auid=1000 ses=2 msg='op=PAM:setcred grantors=pam_unix,pam_permit
,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Feb 20 22:24:52 secOps sudo[2348]: pam_unix(sudo:session): session opened for user root by (uid=0)
Feb 20 22:24:52 secOps kernel: audit: type=1101 audit(1676949892.962:158): pid=2348 uid=1000 auid=1000 ses=2 msg='op=PAM:acco
unting grantors=pam_unix,pam_permit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=suc
cess'
Feb 20 22:24:52 secOps kernel: audit: type=1110 audit(1676949892.962:159): pid=2348 uid=0 auid=1000 ses=2 msg='op=PAM:setcred
 grantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Feb 20 22:24:52 secOps audit[2348]: USER_START pid=2348 uid=0 auid=1000 ses=2 msg='op=PAM:session_open grantors=pam_limits,pa
m_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Feb 20 22:24:52 secOps kernel: audit: type=1105 audit(1676949892.966:160): pid=2348 uid=0 auid=1000 ses=2 msg='op=PAM:session
_open grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succe
ss'
```