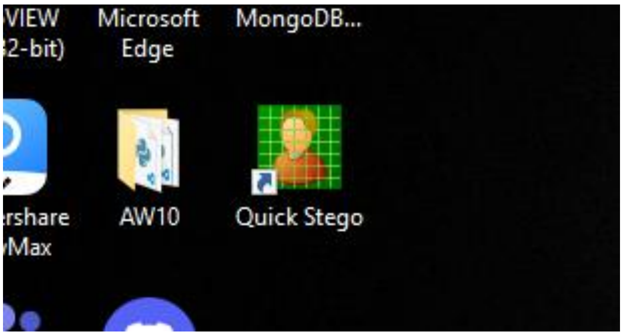
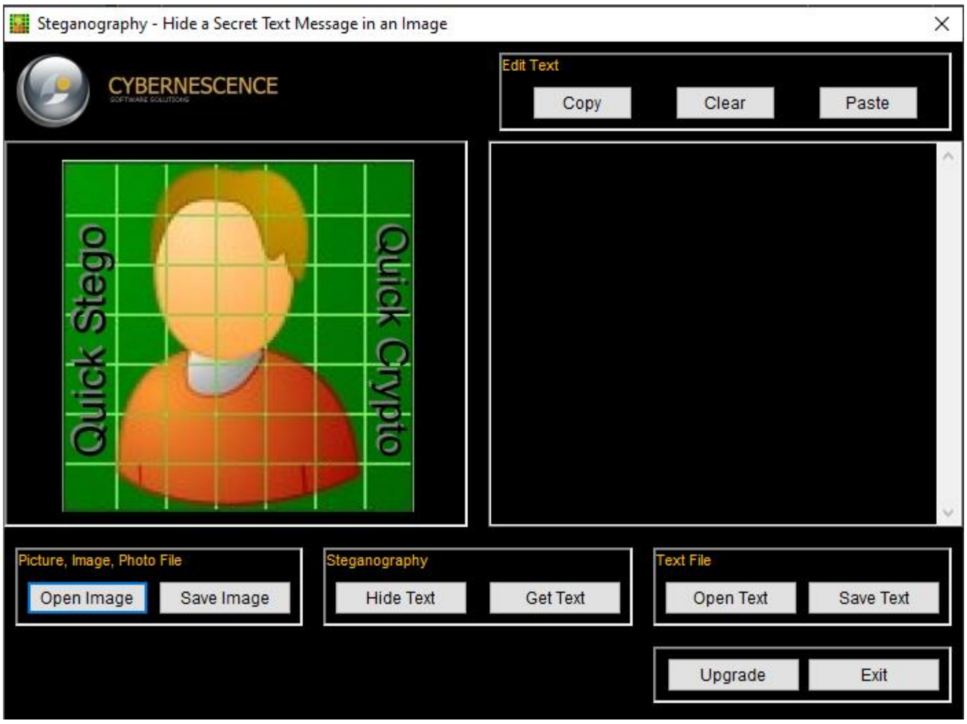
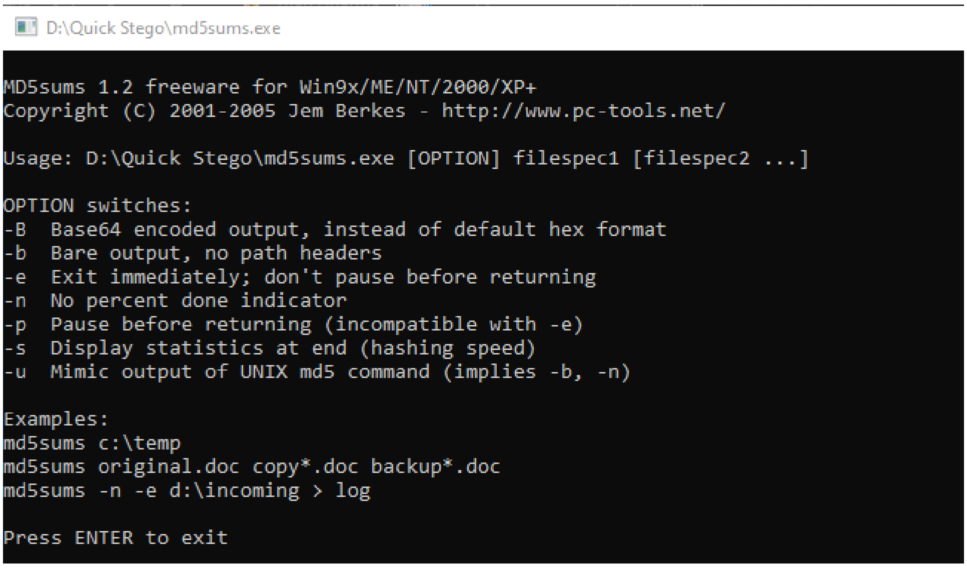
Praktikum Staganografi

1. Jalankan VM Windows OWASP
2. Install QuickStego





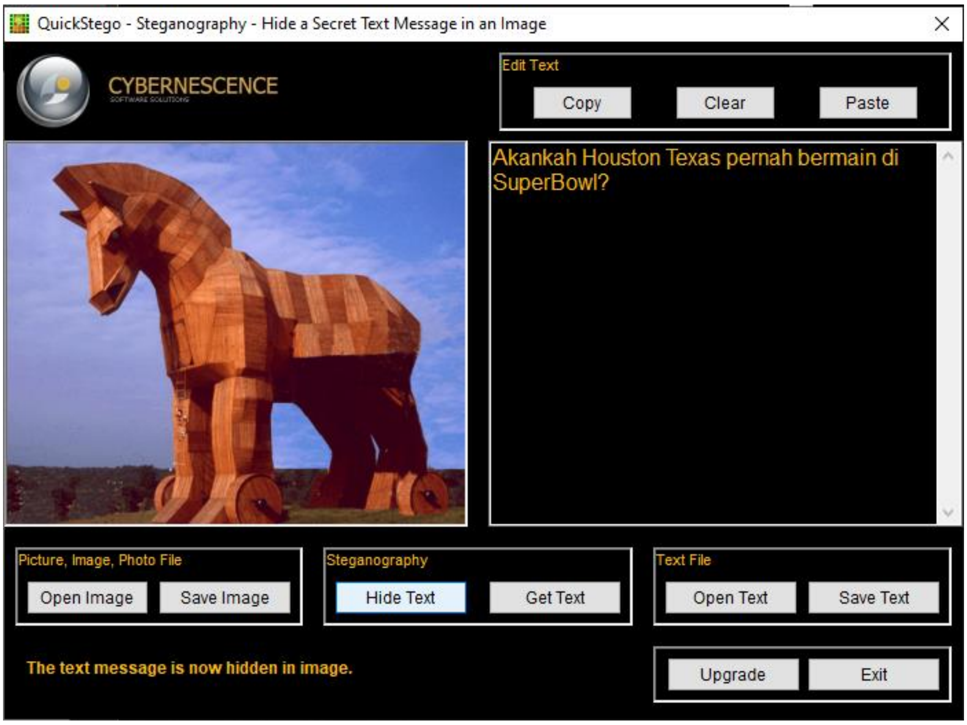
3. Install MD5SUMS



D:\Quick Stego\md5sums.exe

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

Usage: D:\Quick Stego\md5sums.exe [OPTION] filespec1 [filespec2 ...]

OPTION switches:
-B  Base64 encoded output, instead of default hex format
-b  Bare output, no path headers
-e  Exit immediately; don't pause before returning
-n  No percent done indicator
-p  Pause before returning (incompatible with -e)
-s  Display statistics at end (hashing speed)
-u  Mimic output of UNIX md5 command (implies -b, -n)

Examples:
md5sums c:\temp
md5sums original.doc copy*.doc backup*.doc
md5sums -n -e d:\incoming > log

Press ENTER to exit
```

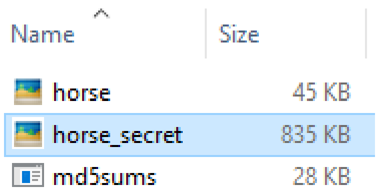
4. Sembunyikan pesan



Akankah Houston Texas pernah bermain di SuperBowl?

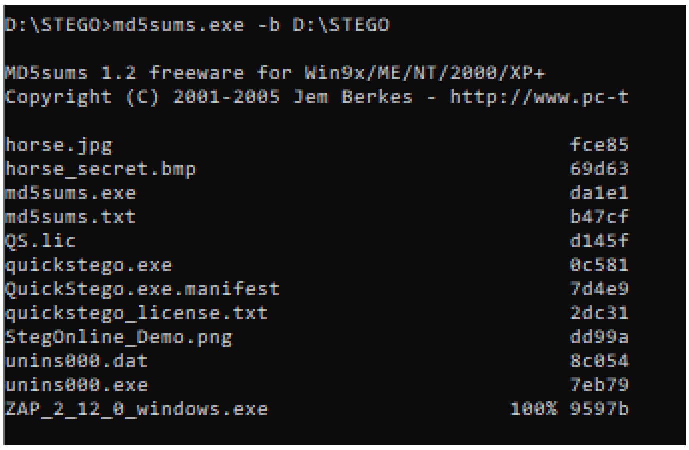
The text message is now hidden in image.

5. Melihat ukuran Byte files



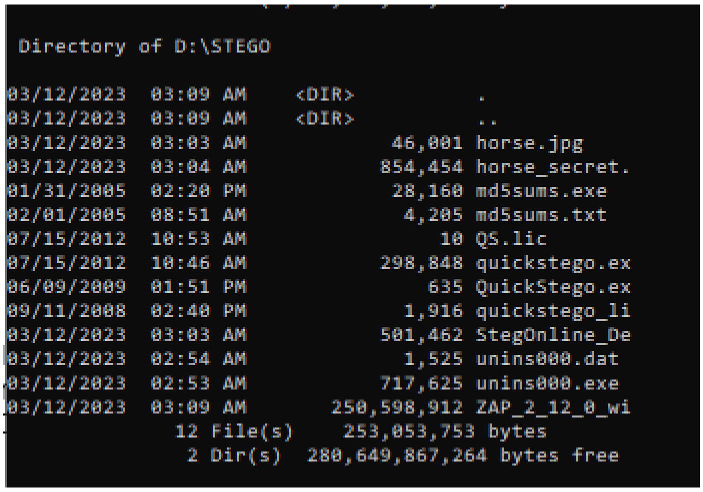
Name	Size
horse	45 KB
horse_secret	835 KB
md5sums	28 KB

6. Melihat MD5 checksum pada files



```
D:\STEGO>md5sums.exe -b D:\STEGO

MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-t

horse.jpg                                       fce85
horse_secret.bmp                                69d63
md5sums.exe                                     da1e1
md5sums.txt                                     b47cf
QS.lic                                          d145f
quickstego.exe                                  0c581
QuickStego.exe.manifest                         7d4e9
quickstego_license.txt                          2dc31
StegOnline_Demo.png                             dd99a
unins000.dat                                    8c054
unins000.exe                                    7eb79
ZAP_2_12_0_windows.exe                     100% 9597b
```

7. Hasil pembuktian dengan md5sum : buka command prompt , pastikan file md5sums.exe dalam satu folder dengan file gambar stego.



```
 Directory of D:\STEGO

03/12/2023  03:09 AM    <DIR>          .
03/12/2023  03:09 AM    <DIR>          ..
03/12/2023  03:03 AM            46,001 horse.jpg
03/12/2023  03:04 AM           854,454 horse_secret.
01/31/2005  02:20 PM            28,160 md5sums.exe
02/01/2005  08:51 AM             4,205 md5sums.txt
07/15/2012  10:53 AM                10 QS.lic
07/15/2012  10:46 AM           298,848 quickstego.ex
06/09/2009  01:51 PM               635 QuickStego.ex
09/11/2008  02:40 PM             1,916 quickstego_li
03/12/2023  03:03 AM           501,462 StegOnline_De
03/12/2023  02:54 AM             1,525 unins000.dat
03/12/2023  02:53 AM           717,625 unins000.exe
03/12/2023  03:09 AM       250,598,912 ZAP_2_12_0_wi
              12 File(s)    253,053,753 bytes
               2 Dir(s)  280,649,867,264 bytes free
```

Praktikum Analisis Log Server

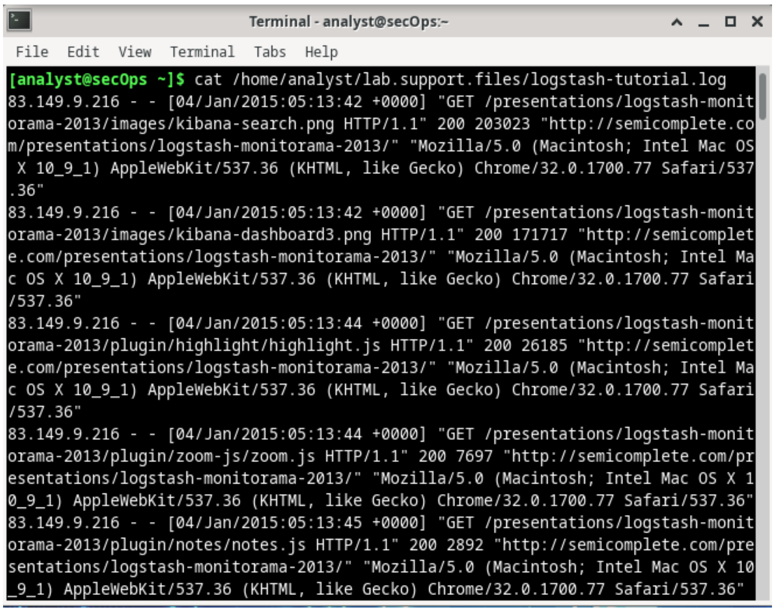
1. Membaca File Log dengan Cat, More, Less, dan Tail

   File log adalah file yang digunakan untuk merekam peristiwa tertentu yang dihasilkan oleh aplikasi, layanan, atau sistem operasi itu sendiri. Biasanya file log ini disimpan sebagai teks biasa. File log merupakan sumber yang sangat diperlukan untuk pemecahan masalah.

   File log biasanya berisi informasi teks biasa yang dapat dilihat oleh hampir semua program yang dapat menangani teks (editor teks, misalnya). Namun, karena kemudahan, kegunaan, dan kecepatan, beberapa alat lebih umum digunakan daripada yang lain. Bagian ini berfokus pada empat program berbasis baris perintah: **cat, more, less,** dan **tail.**

   Fitur cat, berasal dari kata 'concatenate', alat berbasis baris perintah yang digunakan untukmembaca dan menampilkan konten file di layar. Karena kemudahannya dan dapatmembuka file teks dan menampilkannya di terminal teks saja, cat banyak digunakan hingga hari ini. Bukalah VM CyberOps Worstation dan jendela terminal.

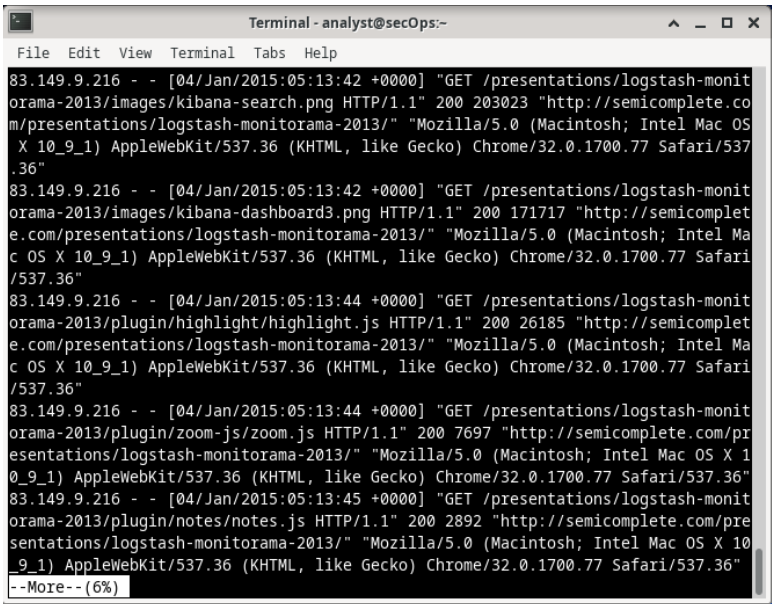
2. Dari jendela terminal, jalankan perintah di bawah ini untuk menampilkan konten file logstash-tutorial.log, yang terletak di folder /home/analyst/lab.support.files/
   analis@secOps ~$ cat /home/analyst/lab.support.files/logstash-tutorial.log


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"
```

   Apa kelemahan menggunakan cat dengan file teks besar?

3. Dari jendela terminal yang sama, gunakan perintah di bawah ini untuk menampilkan kembali isi file logstash-tutorial.log. Proses ini menggunakan more :
   analis@secOps ~$ more /home/analyst/lab.support.files/logstash-tutorial.log

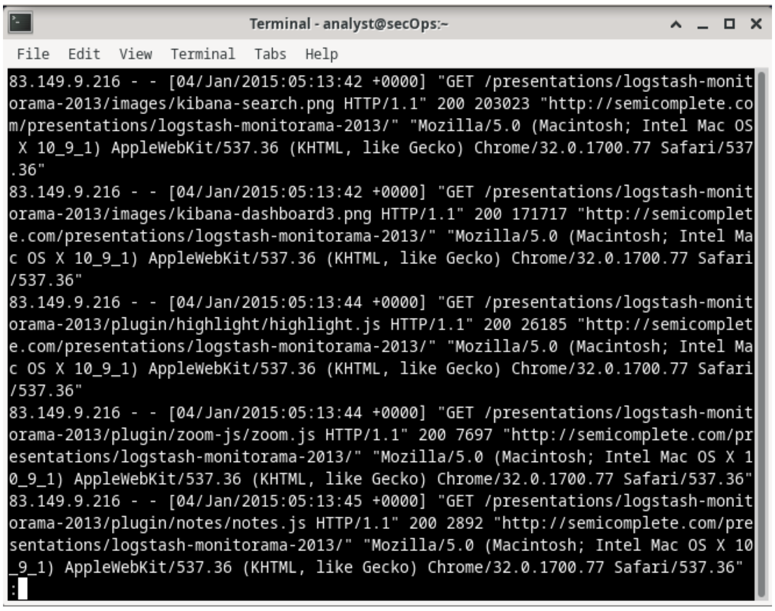

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
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%)
```

   Apa kelemahan menggunakan more?

4. Dari tampilan terminal yang sama, gunakan less untuk menampilkan konten file logstashtutorial.log lagi :

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

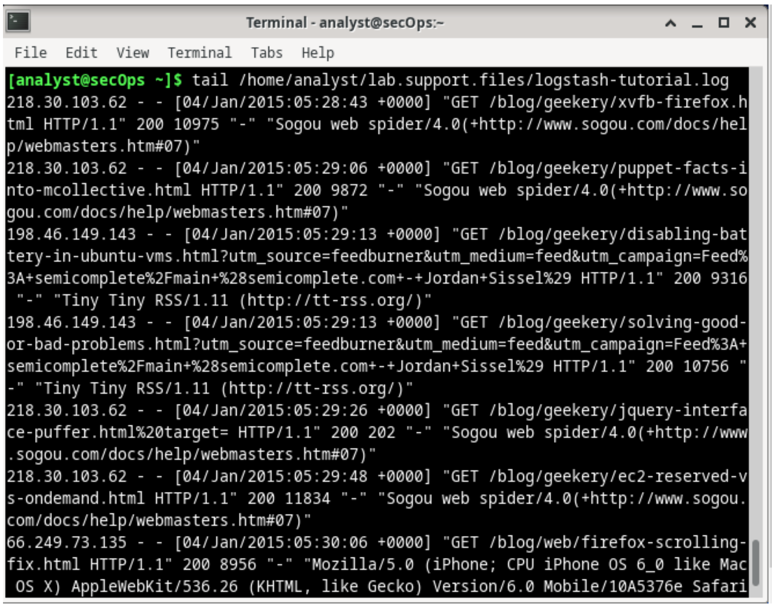


Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
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"
:
```

5. Perintah tail menampilkan akhir file teks. Secara default, tail menampilkan sepuluh baris terakhir file. Gunakan tail untuk menampilkan sepuluh baris terakhir dari file /home/analyst/lab.support.files/logstash-tutorial.log.

   analis@secOps ~$ tail /home/analyst/lab.support.files/logstash-tutorial.log

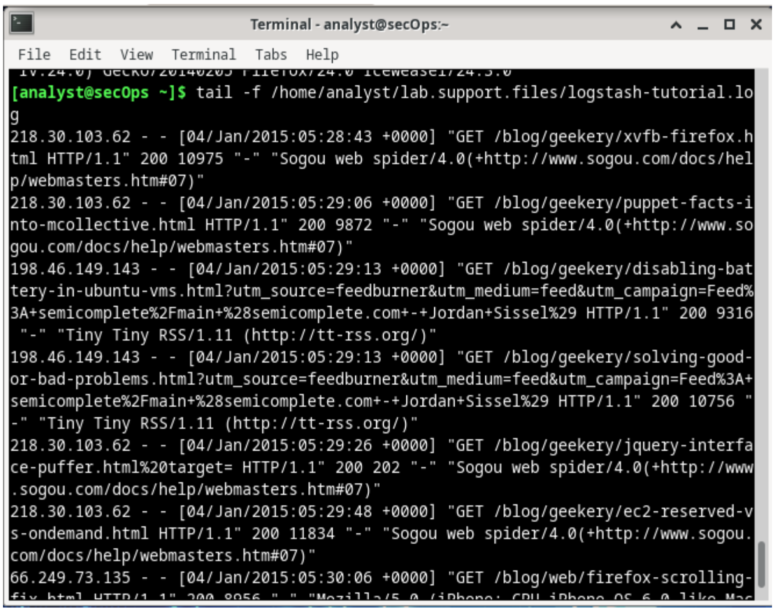


Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[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.h
tml HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/hel
p/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-i
nto-mcollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.so
gou.com/docs/help/webmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-bat
tery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%
3A+semicomplete%2Fmain+%28semicomplete.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+%28semicomplete.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-interfa
ce-puffer.html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www
.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-v
s-ondemand.html 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 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari
```

   Apa yang berbeda dalam output tail dan tail -f? Jelaskan

6. Atur tampilan Anda sehingga Anda dapat melihat kedua jendela terminal. Ubah ukuran jendela sehingga Anda dapat melihat keduanya secara bersamaan.

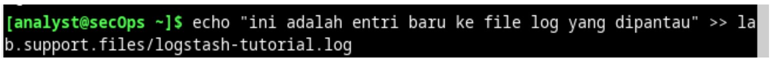


Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

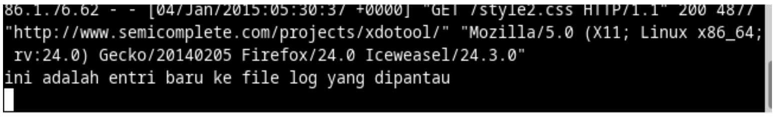
```
 rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
[analyst@secOps ~]$ tail -f /home/analyst/lab.support.files/logstash-tutorial.lo
g
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.h
tml HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/hel
p/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-i
nto-mcollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.so
gou.com/docs/help/webmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-bat
tery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%
3A+semicomplete%2Fmain+%28semicomplete.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+%28semicomplete.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-interfa
ce-puffer.html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www
.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-v
s-ondemand.html 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
```

7. Pilihlah jendela terminal bawah dan masukkan perintah berikut :

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



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

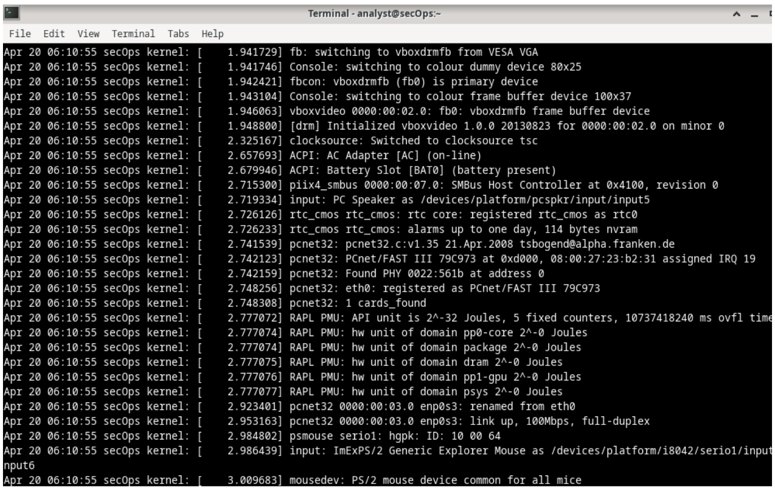


```
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877
"http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64;
 rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
ini adalah entri baru ke file log yang dipantau
```

8. Memahami File Log dan Syslog

   Gunakan perintah cat sebagai root untuk membuat daftar isi file /var/log/syslog.1. File ini menyimpan entri log yang dihasilkan oleh sistem operasi CyberOps Workstation VM dan dikirim ke layanan syslog.

   analis@secOps ~$ sudo cat /var/log/syslog.1



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

```
Apr 20 06:10:55 secOps kernel: [    1.941729] fb: switching to vboxdrmfb from VESA VGA
Apr 20 06:10:55 secOps kernel: [    1.941746] Console: switching to colour dummy device 80x25
Apr 20 06:10:55 secOps kernel: [    1.942421] fbcon: vboxdrmfb (fb0) is primary device
Apr 20 06:10:55 secOps kernel: [    1.943104] Console: switching to colour frame buffer device 100x37
Apr 20 06:10:55 secOps kernel: [    1.946063] vboxvideo 0000:00:02.0: fb0: vboxdrmfb frame buffer device
Apr 20 06:10:55 secOps kernel: [    1.948800] [drm] Initialized vboxvideo 1.0.0 20130823 for 0000:00:02.0 on minor 0
Apr 20 06:10:55 secOps kernel: [    2.325167] clocksource: Switched to clocksource tsc
Apr 20 06:10:55 secOps kernel: [    2.657693] ACPI: AC Adapter [AC] (on-line)
Apr 20 06:10:55 secOps kernel: [    2.679946] ACPI: Battery Slot [BAT0] (battery present)
Apr 20 06:10:55 secOps kernel: [    2.715300] piix4_smbus 0000:00:07.0: SMBus Host Controller at 0x4100, revision 0
Apr 20 06:10:55 secOps kernel: [    2.719334] input: PC Speaker as /devices/platform/pcspkr/input/input5
Apr 20 06:10:55 secOps kernel: [    2.726126] rtc_cmos rtc_cmos: rtc core: registered rtc_cmos as rtc0
Apr 20 06:10:55 secOps kernel: [    2.726233] rtc_cmos rtc_cmos: alarms up to one day, 114 bytes nvram
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 time
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
nput6
Apr 20 06:10:55 secOps kernel: [    3.009683] mousedev: PS/2 mouse device common for all mice
```

Mengapa perintah cat harus dijalankan sebagai root?

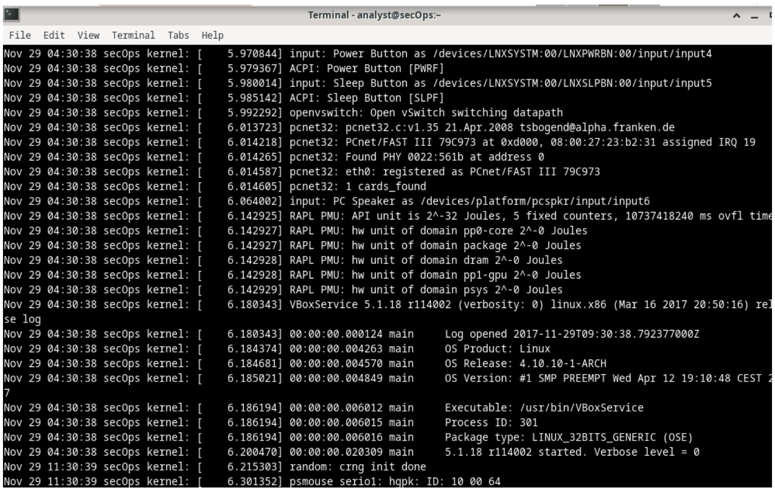
9. Perhatikan bahwa file /var/log/syslog hanya menyimpan entri log terbaru. Untuk menjaga agar file syslog tetap kecil, sistem operasi secara berkala merotasi file log, mengganti nama file log lama menjadi syslog.1, syslog.2, dan seterusnya.

   Gunakan perintah cat untuk membuat daftar file syslog yang lebih lama :

   analis@secOps ~$ sudo cat /var/log/syslog.2

   analis@secOps ~$ sudo cat /var/log/syslog.3

   analis@secOps ~$ sudo cat /var/log/syslog.4

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

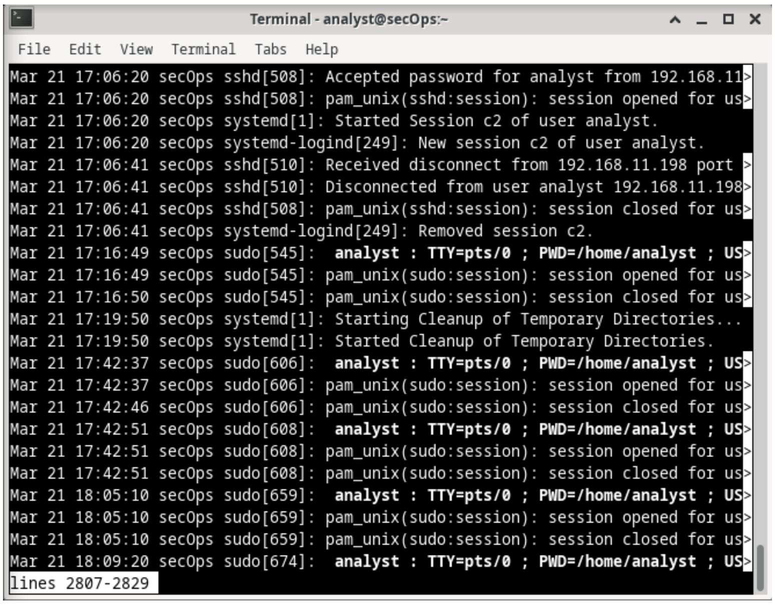
```
Nov 29 04:30:38 secOps kernel: [    5.970844] input: Power Button as /devices/LNXSYSTM:00/LNXPWRBN:00/input/input4
Nov 29 04:30:38 secOps kernel: [    5.979367] ACPI: Power Button [PWRF]
Nov 29 04:30:38 secOps kernel: [    5.980014] input: Sleep Button as /devices/LNXSYSTM:00/LNXSLPBN:00/input/input5
Nov 29 04:30:38 secOps kernel: [    5.985142] ACPI: Sleep Button [SLPF]
Nov 29 04:30:38 secOps kernel: [    5.992292] openvswitch: Open vSwitch switching datapath
Nov 29 04:30:38 secOps kernel: [    6.013723] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
Nov 29 04:30:38 secOps kernel: [    6.014218] pcnet32: PCnet/FAST III 79C973 at 0xd000, 08:00:27:23:b2:31 assigned IRQ 19
Nov 29 04:30:38 secOps kernel: [    6.014265] pcnet32: Found PHY 0022:561b at address 0
Nov 29 04:30:38 secOps kernel: [    6.014587] pcnet32: eth0: registered as PCnet/FAST III 79C973
Nov 29 04:30:38 secOps kernel: [    6.014605] pcnet32: 1 cards_found
Nov 29 04:30:38 secOps kernel: [    6.064002] input: PC Speaker as /devices/platform/pcspkr/input/input6
Nov 29 04:30:38 secOps kernel: [    6.142925] RAPL PMU: API unit is 2^-32 Joules, 5 fixed counters, 10737418240 ms ovfl time
Nov 29 04:30:38 secOps kernel: [    6.142927] RAPL PMU: hw unit of domain pp0-core 2^-0 Joules
Nov 29 04:30:38 secOps kernel: [    6.142927] RAPL PMU: hw unit of domain package 2^-0 Joules
Nov 29 04:30:38 secOps kernel: [    6.142928] RAPL PMU: hw unit of domain dram 2^-0 Joules
Nov 29 04:30:38 secOps kernel: [    6.142928] RAPL PMU: hw unit of domain pp1-gpu 2^-0 Joules
Nov 29 04:30:38 secOps kernel: [    6.142929] RAPL PMU: hw unit of domain psys 2^-0 Joules
Nov 29 04:30:38 secOps kernel: [    6.180343] VBoxService 5.1.18 r114002 (verbosity: 0) linux.x86 (Mar 16 2017 20:50:16) rel
se log
Nov 29 04:30:38 secOps kernel: [    6.180343] 00:00:00.000124 main     Log opened 2017-11-29T09:30:38.792377000Z
Nov 29 04:30:38 secOps kernel: [    6.184374] 00:00:00.004263 main     OS Product: Linux
Nov 29 04:30:38 secOps kernel: [    6.184681] 00:00:00.004570 main     OS Release: 4.10.10-1-ARCH
Nov 29 04:30:38 secOps kernel: [    6.185021] 00:00:00.004849 main     OS Version: #1 SMP PREEMPT Wed Apr 12 19:10:48 CEST 2
7
Nov 29 04:30:38 secOps kernel: [    6.186194] 00:00:00.006012 main     Executable: /usr/bin/VBoxService
Nov 29 04:30:38 secOps kernel: [    6.186194] 00:00:00.006015 main     Process ID: 301
Nov 29 04:30:38 secOps kernel: [    6.186194] 00:00:00.006016 main     Package type: LINUX_32BITS_GENERIC (OSE)
Nov 29 04:30:38 secOps kernel: [    6.200470] 00:00:00.020309 main     5.1.18 r114002 started. Verbose level = 0
Nov 29 11:30:39 secOps kernel: [    6.215303] random: crng init done
Nov 29 11:30:39 secOps kernel: [    6.301352] psmouse serio1: hgpk: ID: 10 00 64
```

   Jelaskan kenapa harus mensinkronkan waktu dan tanggal komputer dengan benar?

10. Memahami File Log dan Jurnalctl

    Untuk melihat log journald, gunakan perintah journalctl. Alat journalctl menafsirkan dan menampilkan entri log yang sebelumnya disimpan dalam file log biner jurnal.

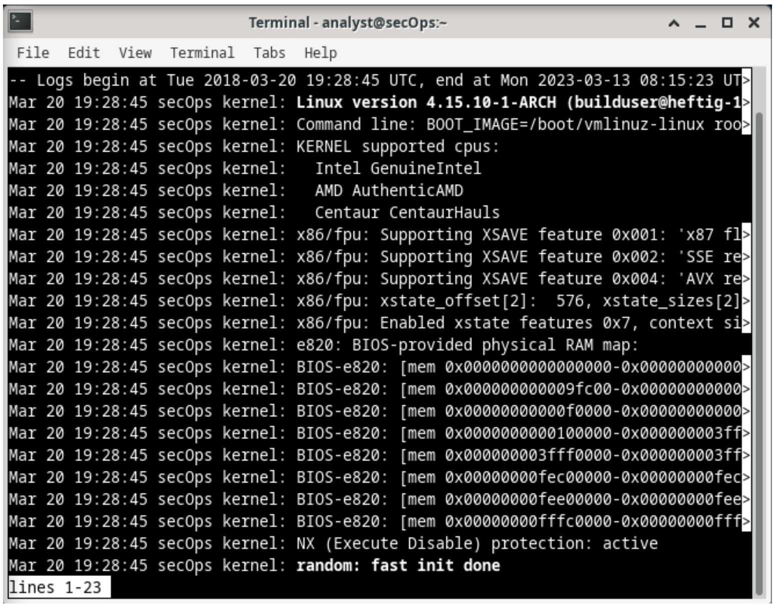
    analis@secOps ~$ journalctl

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

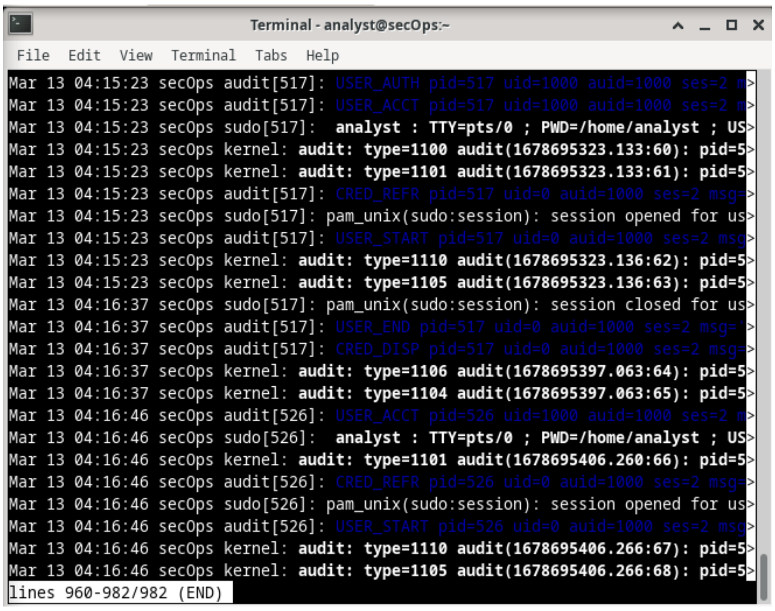
```
Mar 21 17:06:20 secOps sshd[508]: Accepted password for analyst from 192.168.11>
Mar 21 17:06:20 secOps sshd[508]: pam_unix(sshd:session): session opened for us>
Mar 21 17:06:20 secOps systemd[1]: Started Session c2 of user analyst.
Mar 21 17:06:20 secOps systemd-logind[249]: New session c2 of user analyst.
Mar 21 17:06:41 secOps sshd[510]: Received disconnect from 192.168.11.198 port >
Mar 21 17:06:41 secOps sshd[510]: Disconnected from user analyst 192.168.11.198>
Mar 21 17:06:41 secOps sshd[508]: pam_unix(sshd:session): session closed for us>
Mar 21 17:06:41 secOps systemd-logind[249]: Removed session c2.
Mar 21 17:16:49 secOps sudo[545]:  analyst : TTY=pts/0 ; PWD=/home/analyst ; US>
Mar 21 17:16:49 secOps sudo[545]: pam_unix(sudo:session): session opened for us>
Mar 21 17:16:50 secOps sudo[545]: pam_unix(sudo:session): session closed for us>
Mar 21 17:19:50 secOps systemd[1]: Starting Cleanup of Temporary Directories...
Mar 21 17:19:50 secOps systemd[1]: Started Cleanup of Temporary Directories.
Mar 21 17:42:37 secOps sudo[606]:  analyst : TTY=pts/0 ; PWD=/home/analyst ; US>
Mar 21 17:42:37 secOps sudo[606]: pam_unix(sudo:session): session opened for us>
Mar 21 17:42:46 secOps sudo[606]: pam_unix(sudo:session): session closed for us>
Mar 21 17:42:51 secOps sudo[608]:  analyst : TTY=pts/0 ; PWD=/home/analyst ; US>
Mar 21 17:42:51 secOps sudo[608]: pam_unix(sudo:session): session opened for us>
Mar 21 17:42:51 secOps sudo[608]: pam_unix(sudo:session): session closed for us>
Mar 21 18:05:10 secOps sudo[659]:  analyst : TTY=pts/0 ; PWD=/home/analyst ; US>
Mar 21 18:05:10 secOps sudo[659]: pam_unix(sudo:session): session opened for us>
Mar 21 18:05:10 secOps sudo[659]: pam_unix(sudo:session): session closed for us>
Mar 21 18:09:20 secOps sudo[674]:  analyst : TTY=pts/0 ; PWD=/home/analyst ; US>
lines 2807-2829
```

analis@secOps ~$ sudo journalctl –utc


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

```
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Mon 2023-03-13 08:15:23 UT>
Mar 20 19:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builduser@heftig-1>
Mar 20 19:28:45 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux roo>
Mar 20 19:28:45 secOps kernel: KERNEL supported cpus:
Mar 20 19:28:45 secOps kernel:   Intel GenuineIntel
Mar 20 19:28:45 secOps kernel:   AMD AuthenticAMD
Mar 20 19:28:45 secOps kernel:   Centaur CentaurHauls
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 fl>
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE re>
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX re>
Mar 20 19:28:45 secOps kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]>
Mar 20 19:28:45 secOps kernel: x86/fpu: Enabled xstate features 0x7, context si>
Mar 20 19:28:45 secOps kernel: e820: BIOS-provided physical RAM map:
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x00000000000>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ff>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003ff>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000fff>
Mar 20 19:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 19:28:45 secOps kernel: random: fast init done
lines 1-23
```

analis@secOps ~$ sudo journalctl –b

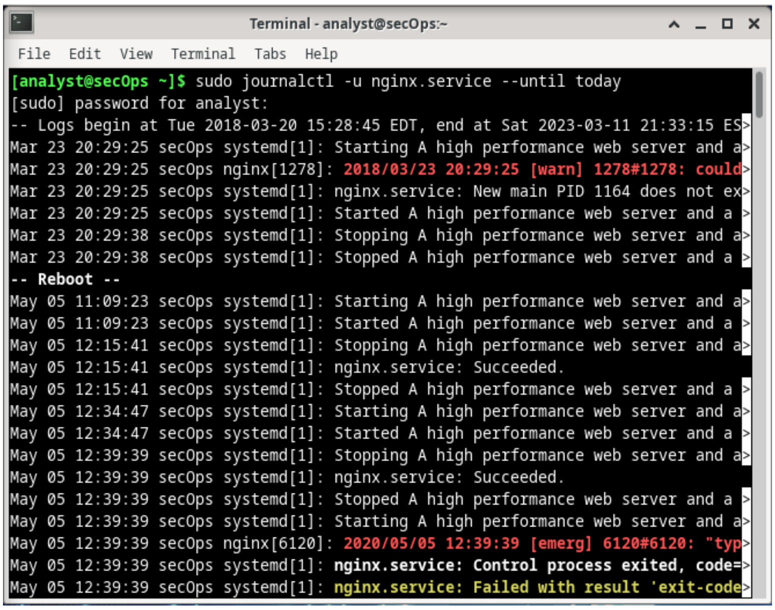

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
Mar 13 04:15:23 secOps audit[517]: USER_AUTH pid=517 uid=1000 auid=1000 ses=2 m>
Mar 13 04:15:23 secOps audit[517]: USER_ACCT pid=517 uid=1000 auid=1000 ses=2 m>
Mar 13 04:15:23 secOps sudo[517]:  analyst : TTY=pts/0 ; PWD=/home/analyst ; US>
Mar 13 04:15:23 secOps kernel: audit: type=1100 audit(1678695323.133:60): pid=5>
Mar 13 04:15:23 secOps kernel: audit: type=1101 audit(1678695323.133:61): pid=5>
Mar 13 04:15:23 secOps audit[517]: CRED_REFR pid=517 uid=0 auid=1000 ses=2 msg=>
Mar 13 04:15:23 secOps sudo[517]: pam_unix(sudo:session): session opened for us>
Mar 13 04:15:23 secOps audit[517]: USER_START pid=517 uid=0 auid=1000 ses=2 msg>
Mar 13 04:15:23 secOps kernel: audit: type=1110 audit(1678695323.136:62): pid=5>
Mar 13 04:15:23 secOps kernel: audit: type=1105 audit(1678695323.136:63): pid=5>
Mar 13 04:16:37 secOps sudo[517]: pam_unix(sudo:session): session closed for us>
Mar 13 04:16:37 secOps audit[517]: USER_END pid=517 uid=0 auid=1000 ses=2 msg='>
Mar 13 04:16:37 secOps audit[517]: CRED_DISP pid=517 uid=0 auid=1000 ses=2 msg=>
Mar 13 04:16:37 secOps kernel: audit: type=1106 audit(1678695397.063:64): pid=5>
Mar 13 04:16:37 secOps kernel: audit: type=1104 audit(1678695397.063:65): pid=5>
Mar 13 04:16:46 secOps audit[526]: USER_ACCT pid=526 uid=1000 auid=1000 ses=2 m>
Mar 13 04:16:46 secOps sudo[526]:  analyst : TTY=pts/0 ; PWD=/home/analyst ; US>
Mar 13 04:16:46 secOps kernel: audit: type=1101 audit(1678695406.260:66): pid=5>
Mar 13 04:16:46 secOps audit[526]: CRED_REFR pid=526 uid=0 auid=1000 ses=2 msg=>
Mar 13 04:16:46 secOps sudo[526]: pam_unix(sudo:session): session opened for us>
Mar 13 04:16:46 secOps audit[526]: USER_START pid=526 uid=0 auid=1000 ses=2 msg>
Mar 13 04:16:46 secOps kernel: audit: type=1110 audit(1678695406.266:67): pid=5>
Mar 13 04:16:46 secOps kernel: audit: type=1105 audit(1678695406.266:68): pid=5>
lines 960-982/982 (END)
```

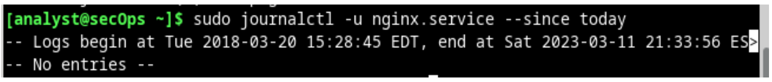
11. Gunakan journalctl untuk menentukan layanan dan kerangka waktu untuk entri log.

    Perintah di bawah ini menunjukkan semua log layanan nginx yang direkam hari ini:

    analis@secOps ~$ sudo journalctl -u nginx.service --since today


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

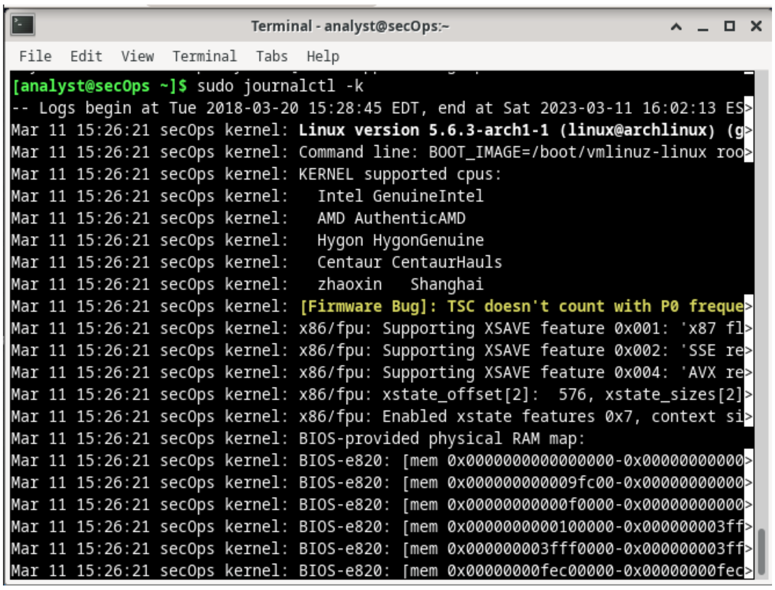
```
[analyst@secOps ~]$ sudo journalctl -u nginx.service --until today
[sudo] password for analyst:
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Sat 2023-03-11 21:33:15 ES>
Mar 23 20:29:25 secOps systemd[1]: Starting A high performance web server and a>
Mar 23 20:29:25 secOps nginx[1278]: 2018/03/23 20:29:25 [warn] 1278#1278: could>
Mar 23 20:29:25 secOps systemd[1]: nginx.service: New main PID 1164 does not ex>
Mar 23 20:29:25 secOps systemd[1]: Started A high performance web server and a >
Mar 23 20:29:38 secOps systemd[1]: Stopping A high performance web server and a>
Mar 23 20:29:38 secOps systemd[1]: Stopped A high performance web server and a >
-- Reboot --
May 05 11:09:23 secOps systemd[1]: Starting A high performance web server and a>
May 05 11:09:23 secOps systemd[1]: Started A high performance web server and a >
May 05 12:15:41 secOps systemd[1]: Stopping A high performance web server and a>
May 05 12:15:41 secOps systemd[1]: nginx.service: Succeeded.
May 05 12:15:41 secOps systemd[1]: Stopped A high performance web server and a >
May 05 12:34:47 secOps systemd[1]: Starting A high performance web server and a>
May 05 12:34:47 secOps systemd[1]: Started A high performance web server and a >
May 05 12:39:39 secOps systemd[1]: Stopping A high performance web server and a>
May 05 12:39:39 secOps systemd[1]: nginx.service: Succeeded.
May 05 12:39:39 secOps systemd[1]: Stopped A high performance web server and a >
May 05 12:39:39 secOps systemd[1]: Starting A high performance web server and a>
May 05 12:39:39 secOps nginx[6120]: 2020/05/05 12:39:39 [emerg] 6120#6120: "typ>
May 05 12:39:39 secOps systemd[1]: nginx.service: Control process exited, code=>
May 05 12:39:39 secOps systemd[1]: nginx.service: Failed with result 'exit-code>
```



```
[analyst@secOps ~]$ sudo journalctl -u nginx.service --since today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Sat 2023-03-11 21:33:56 ES>
-- No entries --
```

12. Gunakan sakelar -k untuk hanya menampilkan pesan yang dihasilkan oleh kernel:

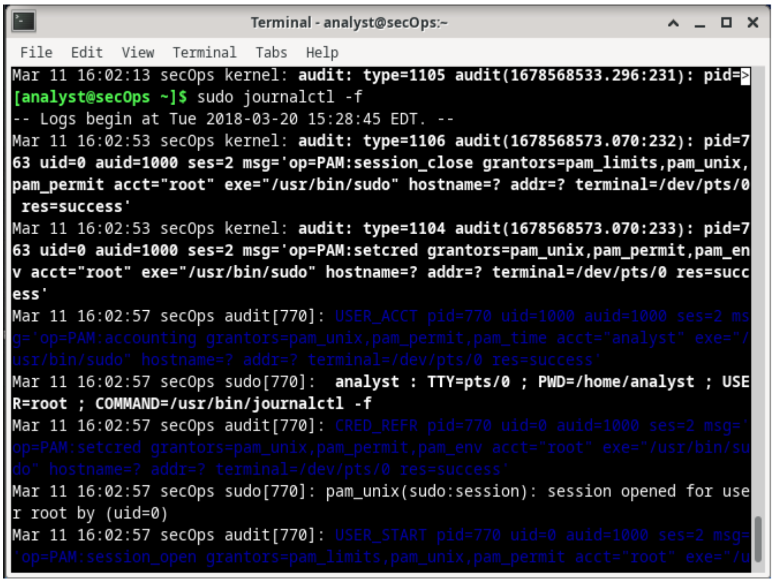
analis@secOps ~$ sudo journalctl –k


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 Sat 2023-03-11 16:02:13 ES>
Mar 11 15:26:21 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (g>
Mar 11 15:26:21 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux roo>
Mar 11 15:26:21 secOps kernel: KERNEL supported cpus:
Mar 11 15:26:21 secOps kernel:   Intel GenuineIntel
Mar 11 15:26:21 secOps kernel:   AMD AuthenticAMD
Mar 11 15:26:21 secOps kernel:   Hygon HygonGenuine
Mar 11 15:26:21 secOps kernel:   Centaur CentaurHauls
Mar 11 15:26:21 secOps kernel:   zhaoxin   Shanghai
Mar 11 15:26:21 secOps kernel: [Firmware Bug]: TSC doesn't count with P0 freque>
Mar 11 15:26:21 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 fl>
Mar 11 15:26:21 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE re>
Mar 11 15:26:21 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX re>
Mar 11 15:26:21 secOps kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]>
Mar 11 15:26:21 secOps kernel: x86/fpu: Enabled xstate features 0x7, context si>
Mar 11 15:26:21 secOps kernel: BIOS-provided physical RAM map:
Mar 11 15:26:21 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000>
Mar 11 15:26:21 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x00000000000>
Mar 11 15:26:21 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000>
Mar 11 15:26:21 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ff>
Mar 11 15:26:21 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003ff>
Mar 11 15:26:21 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec>
```

13. Mirip dengan tail -f yang dijelaskan di atas, gunakan -f untuk secara aktif mengikuti log saat sedang ditulis:

analis@secOps ~$ sudo journalctl –f



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

```
Mar 11 16:02:13 secOps kernel: audit: type=1105 audit(1678568533.296:231): pid=>
[analyst@secOps ~]$ sudo journalctl -f
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Mar 11 16:02:53 secOps kernel: audit: type=1106 audit(1678568573.070:232): pid=7
63 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'
Mar 11 16:02:53 secOps kernel: audit: type=1104 audit(1678568573.070:233): pid=7
63 uid=0 auid=1000 ses=2 msg='op=PAM:setcred grantors=pam_unix,pam_permit,pam_en
v acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succ
ess'
Mar 11 16:02:57 secOps audit[770]: USER_ACCT pid=770 uid=1000 auid=1000 ses=2 ms
g='op=PAM:accounting grantors=pam_unix,pam_permit,pam_time acct="analyst" exe="/
usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 11 16:02:57 secOps sudo[770]:  analyst : TTY=pts/0 ; PWD=/home/analyst ; USE
R=root ; COMMAND=/usr/bin/journalctl -f
Mar 11 16:02:57 secOps audit[770]: CRED_REFR pid=770 uid=0 auid=1000 ses=2 msg='
op=PAM:setcred grantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/su
do" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 11 16:02:57 secOps sudo[770]: pam_unix(sudo:session): session opened for use
r root by (uid=0)
Mar 11 16:02:57 secOps audit[770]: USER_START pid=770 uid=0 auid=1000 ses=2 msg=
'op=PAM:session_open grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/u
```

14. Buatlah laporan tentang pengerjaan anda ini kemudian dikumpulkan melalui elok.