

**LAPORAN PRAKTIKUM**  
**KEAMANAN INFORMASI 1**  
**STEGANOGRAFI DAN ANALISIS LOG SERVER**



**DISUSUN OLEH**

Nama : Fariansyah Permata Surya  
NIM : 21/473155/SV/18810  
Hari, Tanggal : Minggu, 12/03/2023  
Kelas : RI4AA

**SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET**  
**DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA**  
**SEKOLAH VOKASI**  
**UNIVERSITAS GADJAH MADA**  
**YOGYAKARTA**

**2023**

## A. Dasar Teori

Steganografi adalah seni menyembunyikan pesan atau informasi rahasia dalam media yang tampaknya tidak mencurigakan seperti gambar, audio, video, atau teks. Tujuannya adalah untuk membuat pesan yang tidak terdeteksi oleh orang yang tidak berwenang dan hanya dapat diakses oleh penerima yang dimaksud.

File Log adalah alat penting dalam pemecahan masalah dan pemantauan. Aplikasi yang berbeda menghasilkan file log yang berbeda, masing-masing berisi kumpulan bidang dan informasinya sendiri. Meskipun struktur bidang dapat berubah di antara file log, alat yang digunakan untuk membacanya sebagian besar sama. Di lab ini, Anda akan mempelajari tentang alat umum yang digunakan untuk membaca file log dan berlatih menggunakannya.

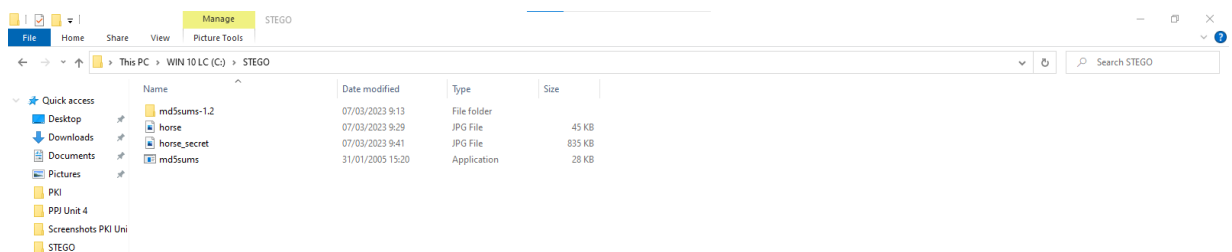
## B. Alat dan Bahan

1. PC Host dengan minimal RAM 8 GB dan Hardisk 40 GB
2. Koneksi Internet
3. CyberOps Workstation virtual machine
4. Quickstego
- 5.

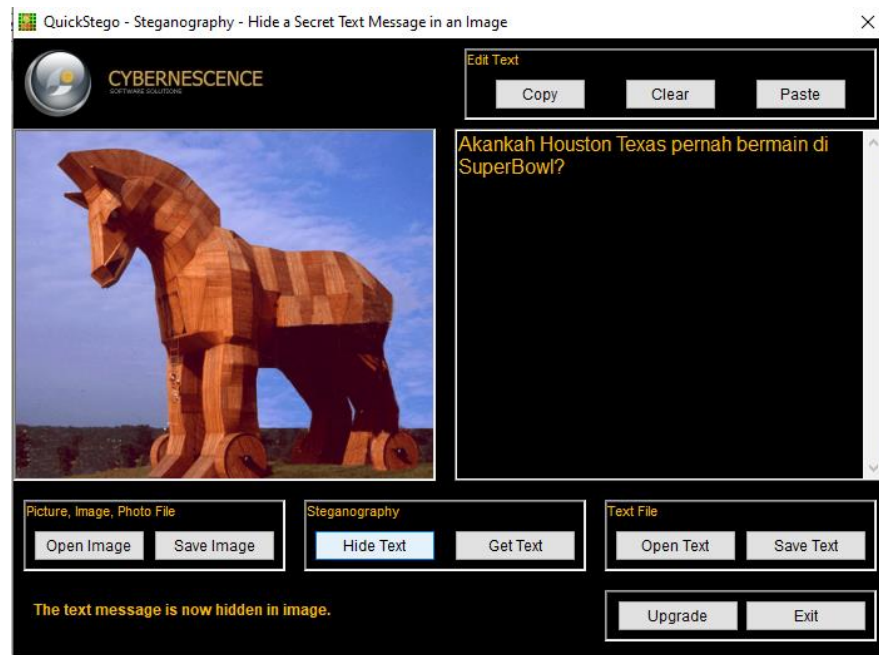
## C. Tugas dan Penyelesaian

### Unit Steganografi

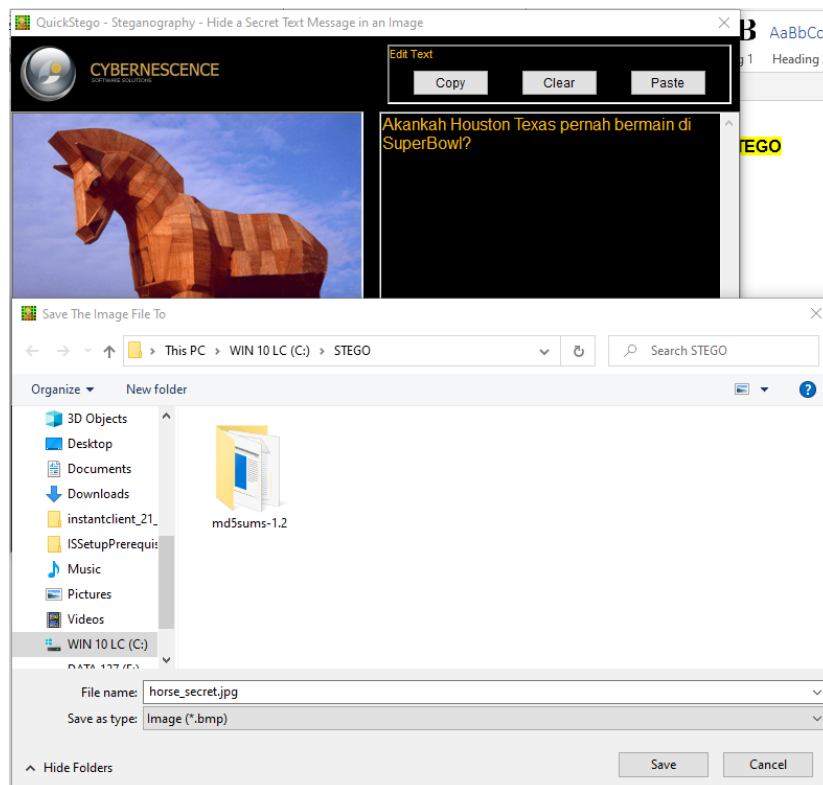
1. Mendownload dan meng install Quickstego dan MD5SUMS pada link :  
<http://quickcrypto.com/products/QS12Setup.zip>, <http://quickcrypto.com/free-steganography-software.html>.
2. Membuat sebuah folder kemudian memasukkan MD5SUMS.exe dan foto ke folder tersebut.



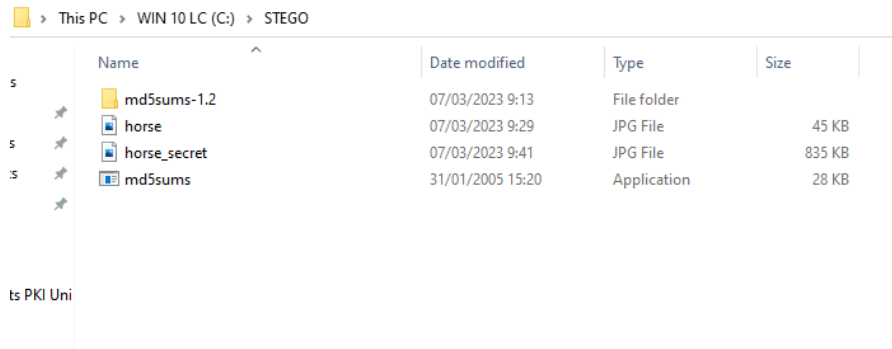
3. Buka aplikasi QuickStego dan kemudian memasukkan gambar yang diperintahkan kemudian menulis string pada bagian kiri dan klik Hide Text.



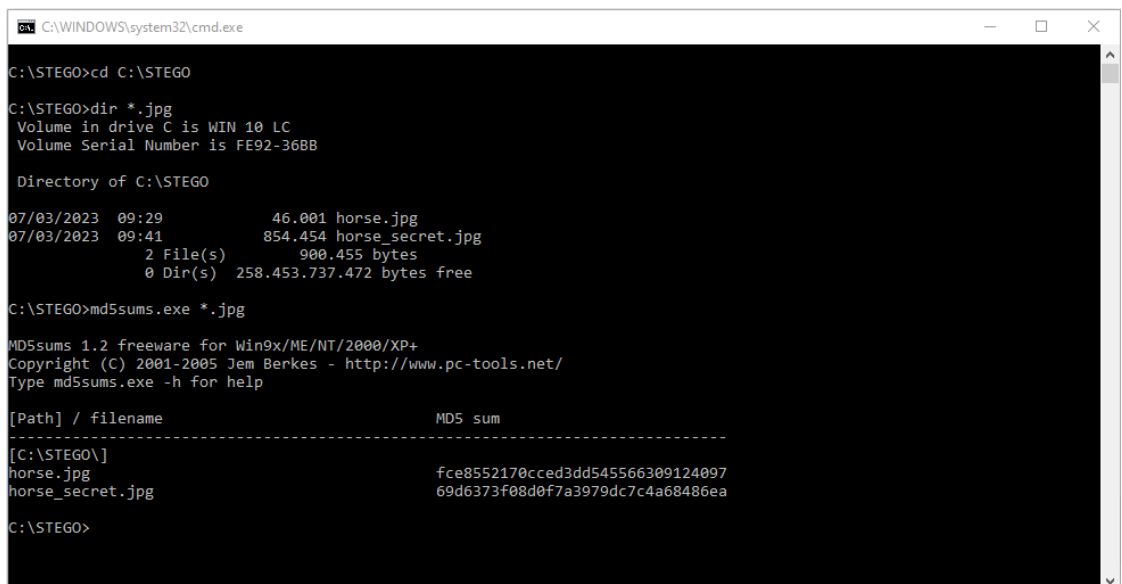
4. Setelah itu Save Image dan masukkan kedalam folder Stego yang sebelumnya dibuat dan tambahkan “.jpg”.



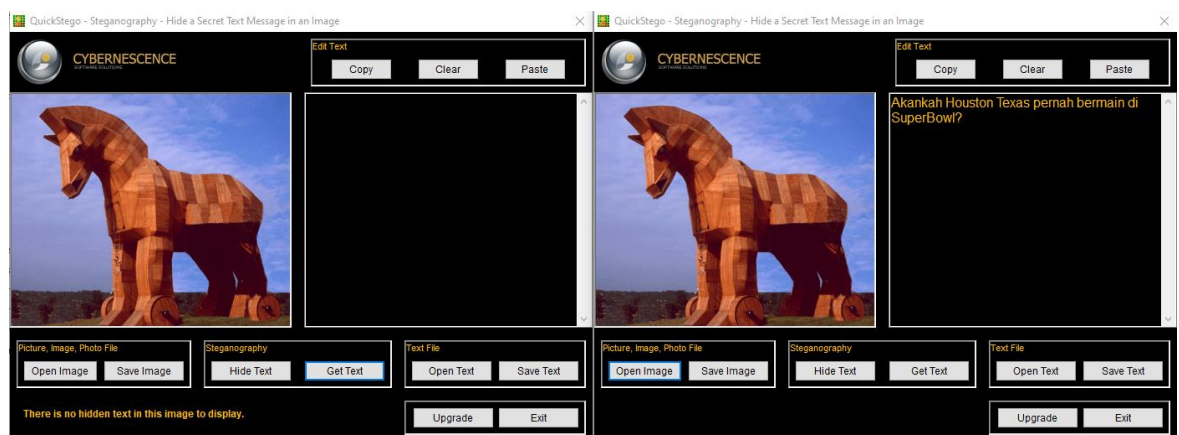
5. Isi folder Stego seperti gambar dibawah.



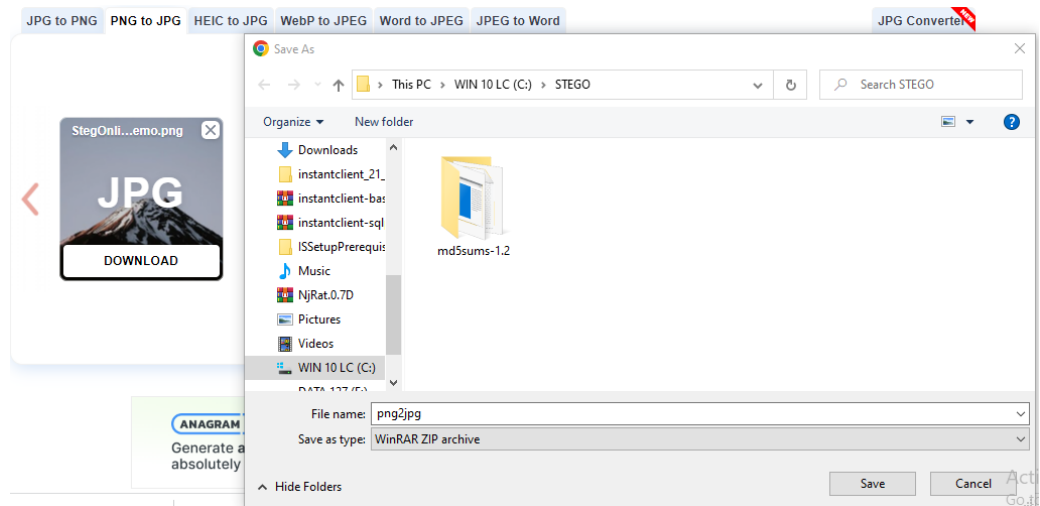
6. Buka Command Prompt kemudian pindah ke folder Stego, kemudian gunakan perintah “\*.jpg” untuk menampilkan semua file dengan format .jpg beserta size file tersebut, dan juga lakukan perintah “md5sums.exe \*.jpg” untuk menggunakan software md5sums.



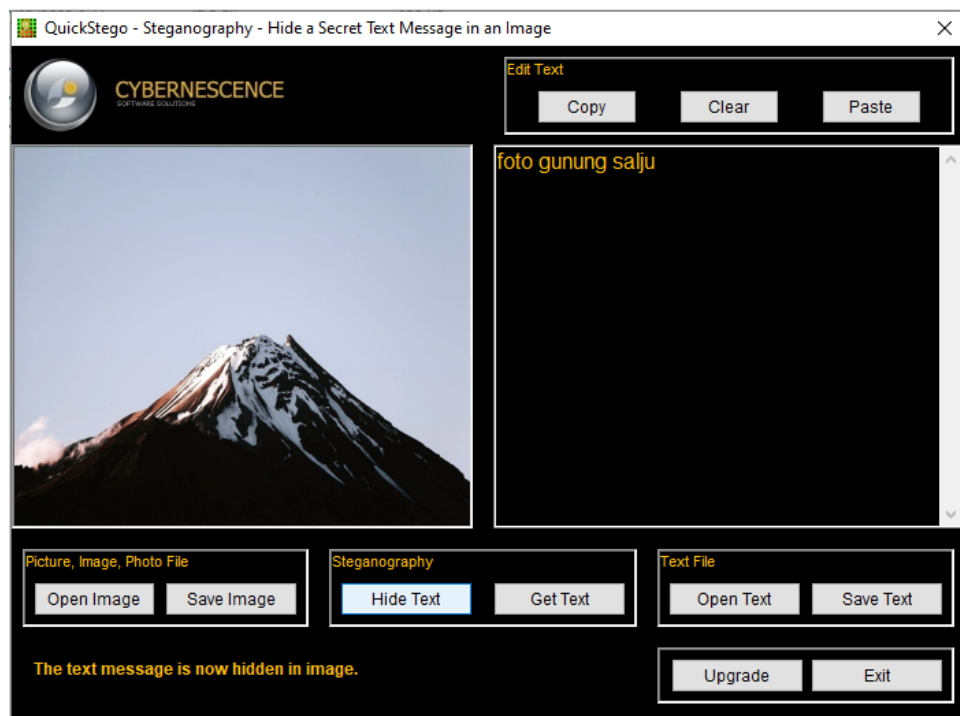
7. Pada aplikasi QuickStego juga dapat membedakan gambar biasa dengan gambar yang terdapat pesan string seperti gambar dibawah.



8. Kemudian lanjutkan dengan gambar ke 2. Karena gambar memiliki format .png maka harus di convert menjadi .jpg karena aplikasi QuickStego hanya bisa membaca file dengan format bmp, jpg, jpeg, gif.



9. Kemudian lakukan seperti langkah no. 2 sampai 3.



10. Kemudian gunakan Command Prompt untuk membuktikan perbedaan gambar dengan menggunakan md5sums dan dengan size gambar tersebut.

```
C:\WINDOWS\system32\cmd.exe
C:\STEGO>dir *.jpg
Volume in drive C is WIN 10 LC
Volume Serial Number is FE92-368B

Directory of C:\STEGO

07/03/2023  09:29             46.001 horse.jpg
07/03/2023  09:29             46.001 horse_copy.jpg
07/03/2023  09:41            854.454 horse_secret.jpg
07/03/2023  09:58            48.590 StegOnline_Demo_convert.jpg.jpg
07/03/2023  10:03            1.998.054 StegOnline_Demo_convert_secret.jpg
               5 File(s)          2.993.100 bytes
               0 Dir(s)        258.464.309.248 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                                         fce8552170cccd3dd545566309124097
horse_copy.jpg                                   fce8552170cccd3dd545566309124097
horse_secret.jpg                                 69d6373f08d0f7a3979dc7c4a68486ea
StegOnline_Demo_convert.jpg.jpg                 9f3b7b4b200da9fe48d4c38b9935a890
StegOnline_Demo_convert_secret.jpg              530fba1478ca32e4002c962dd4555456
C:\STEGO>
```

## Unit Analisis Log Server

1. Membuka CyberOps Workstation virtual machine, kemudian buka terminal dan jalankan perintah “cat /home/analyst/lab.support.files/logstash-tutorial.log” untuk menampilkan konten file logstash-tutorial.log, yang terletak di folder /home/analyst/lab.support.files/.

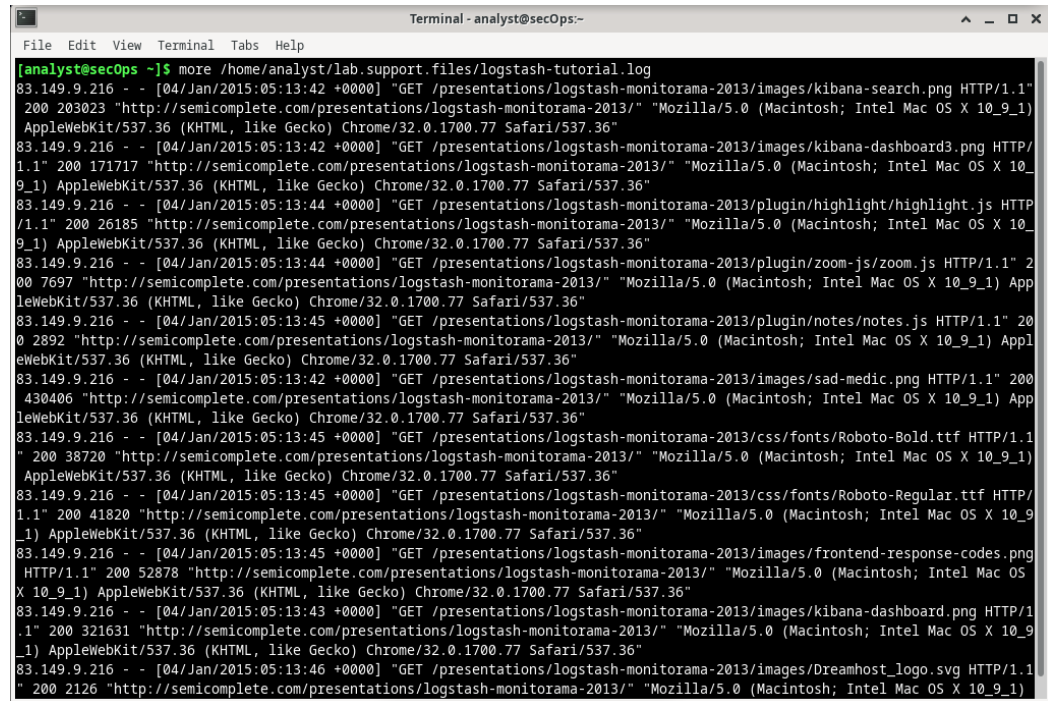
```
CyberOps Workstation [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Applications: Terminal - analyst@sec0...

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

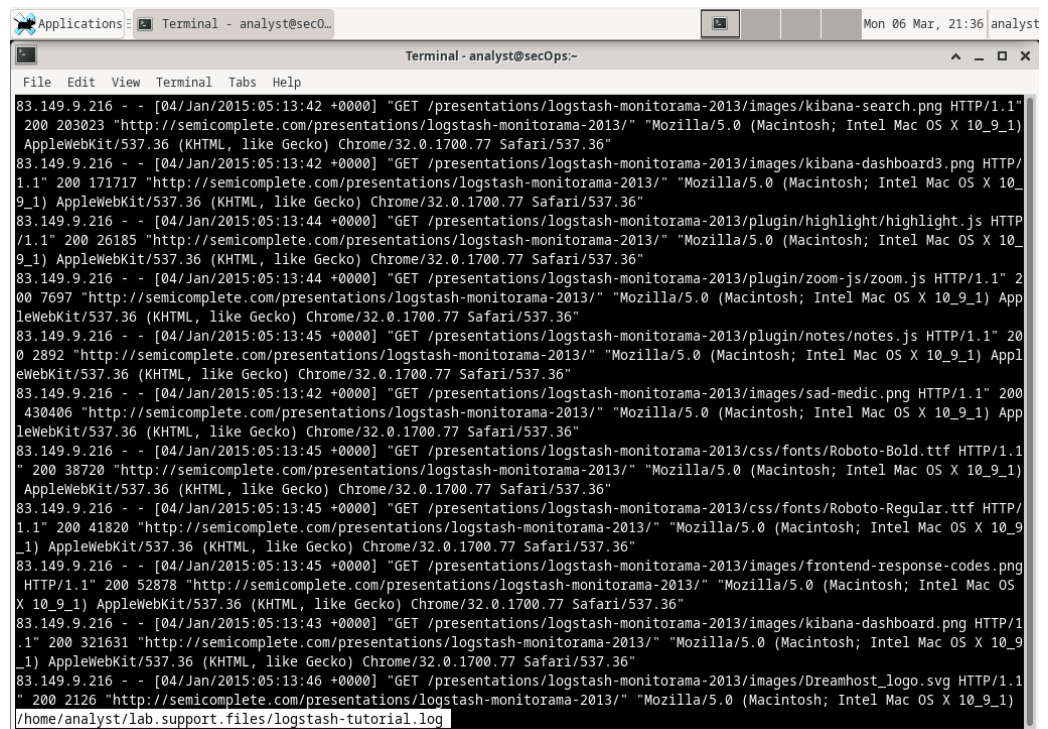
[analyst@secOps ~]$ cat /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.co
m/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; 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. Dari jendela terminal yang sama, gunakan perintah “more /home/analyst/lab.support.files/logstash-tutorial.log” untuk menampilkan kembali isi file logstash-tutorial.log.



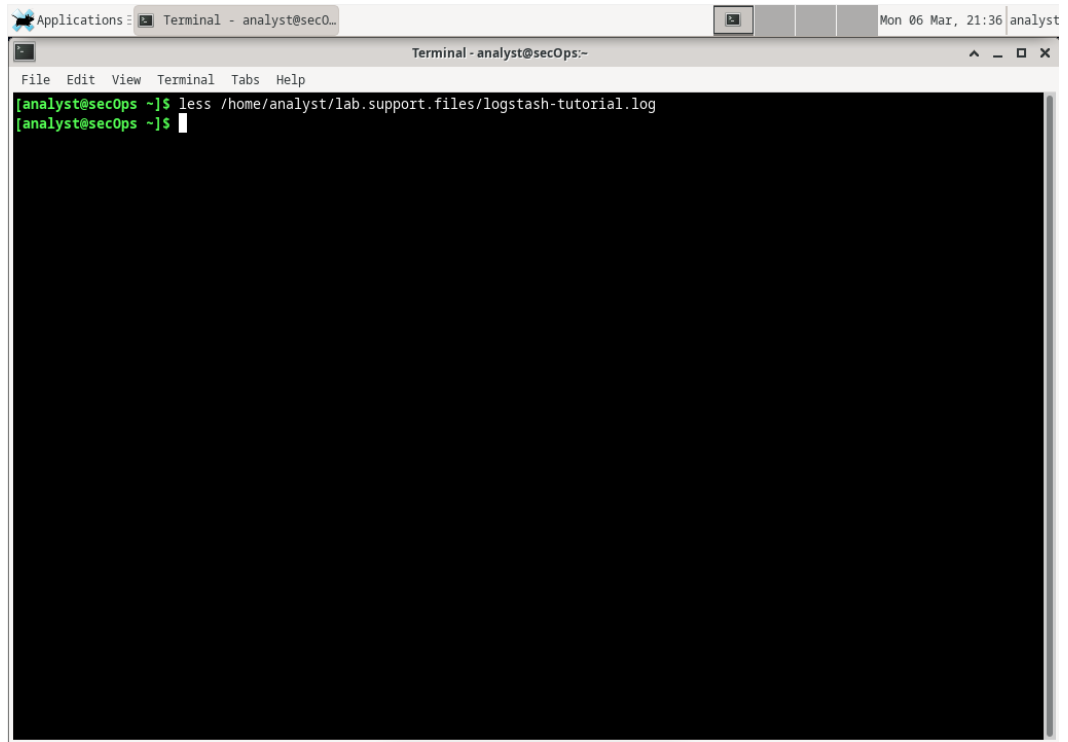
```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ more /home/analyst/lab.support.files/logstash-tutorial.log  
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "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-monitorama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplete.com/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/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplete.com/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/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/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/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/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-monitorama-2013/images/sad-medic.png HTTP/1.1" 200 430406 "http://semicomplete.com/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/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Bold.ttf HTTP/1.1" 200 38720 "http://semicomplete.com/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/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf HTTP/1.1" 200 41820 "http://semicomplete.com/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/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/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/2015:05:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard.png HTTP/1.1" 200 321631 "http://semicomplete.com/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/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/Dreamhost_logo.svg HTTP/1.1" 200 2126 "http://semicomplete.com/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"
```

3. Dari tampilan terminal yang sama, gunakan less untuk menampilkan konten file logstashtutorial.log lagi. Perintah yang digunakan “less /home/analyst/lab.support.files/logstash-tutorial.log”.



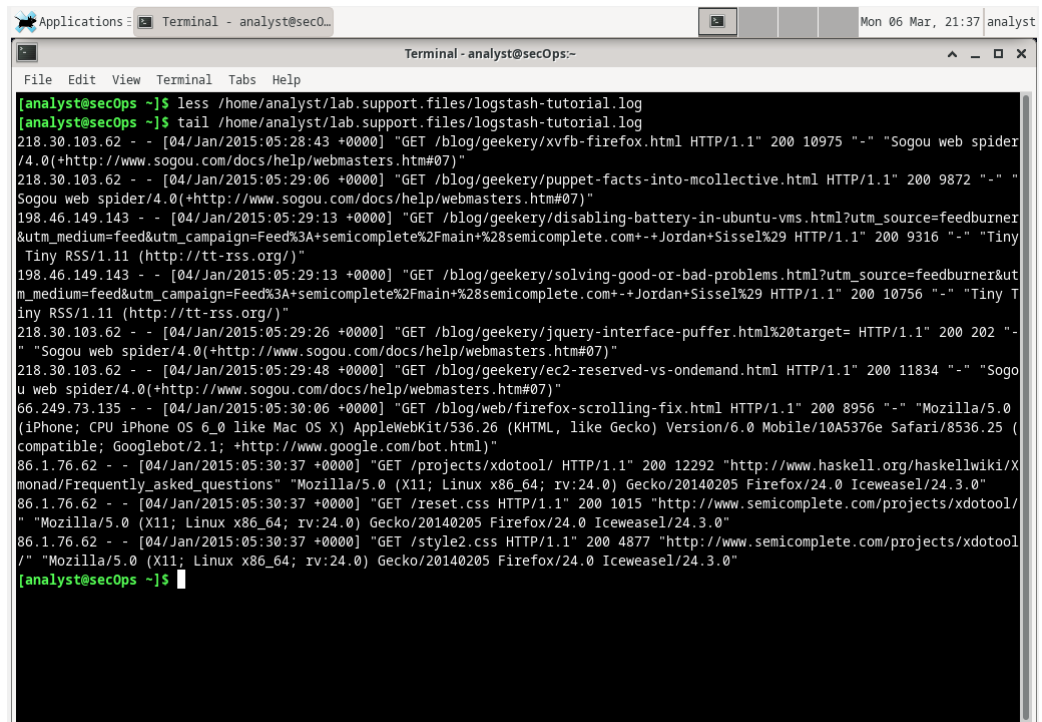
```
Applications: Terminal - analyst@sec0... Mon 06 Mar, 21:36 analyst  
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "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-monitorama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplete.com/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/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplete.com/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/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/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/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/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-monitorama-2013/images/sad-medic.png HTTP/1.1" 200 430406 "http://semicomplete.com/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/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Bold.ttf HTTP/1.1" 200 38720 "http://semicomplete.com/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/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf HTTP/1.1" 200 41820 "http://semicomplete.com/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/2015:05:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard.png HTTP/1.1" 200 321631 "http://semicomplete.com/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/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/Dreamhost_logo.svg HTTP/1.1" 200 2126 "http://semicomplete.com/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"  
/home/analyst/lab.support.files/logstash-tutorial.log
```





```
Applications: Terminal - analyst@sec0...
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ less /home/analyst/lab.support.files/logstash-tutorial.log
[analyst@secOps ~]$
```

- Gunakan `tail` untuk menampilkan sepuluh baris terakhir dari file `/home/analyst/lab.support.files/logstash-tutorial.log`. Perintah yang digunakan “`tail /home/analyst/lab.support.files/logstash-tutorial.log`”.

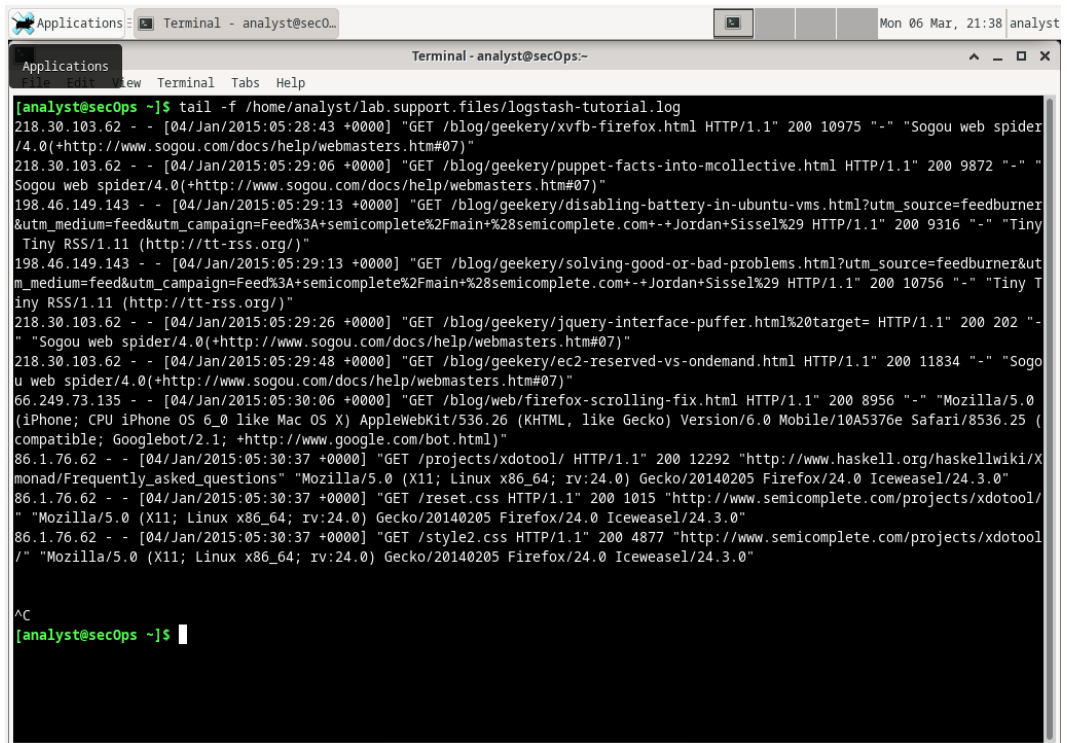


```
Applications: Terminal - analyst@sec0...
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ less /home/analyst/lab.support.files/logstash-tutorial.log
[analyst@secOps ~]$ tail /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 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-mcollective.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+%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
m_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny T
iny 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/webmasters.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 "-" "Sogo
u 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/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/X
monad/Frequently_asked_questions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Icwaseasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/projects/xdotool/"
" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Icwaseasel/24.3.0"
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 Icwaseasel/24.3.0"
[analyst@secOps ~]$
```

- Dalam beberapa situasi, disarankan untuk memantau file log karena entri log ditulis ke file log. Untuk kasus tersebut, perintah `tail -f` sangat membantu.



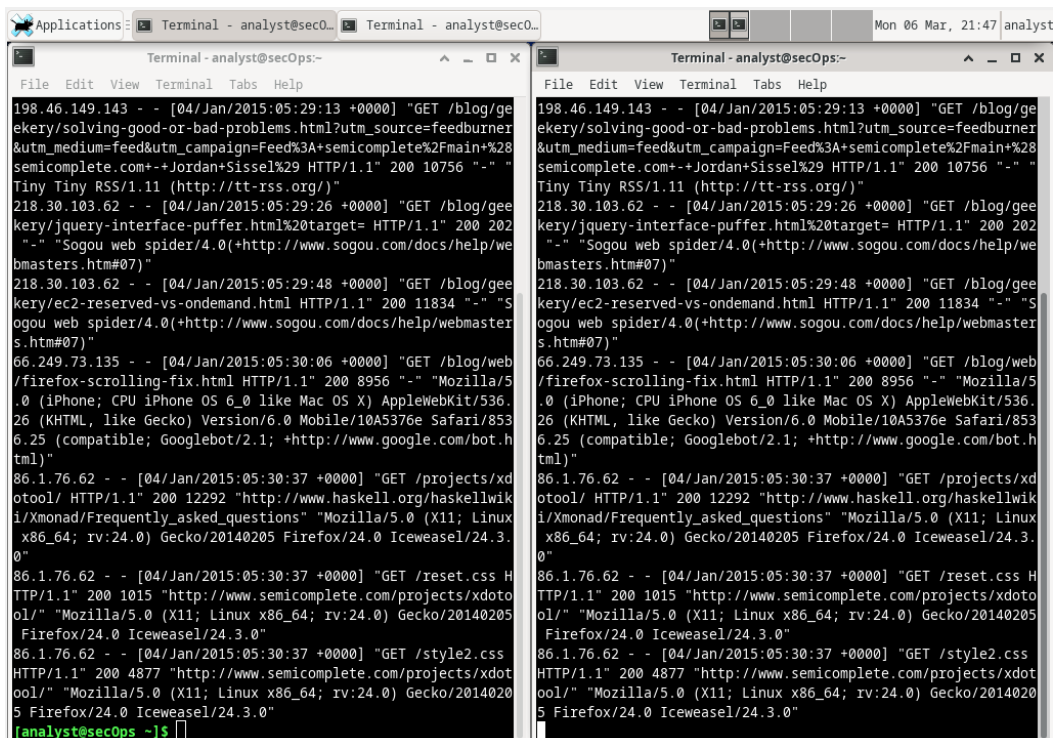
Gunakan perintah “`sudo tail -f /home/analyst/lab.support.files/logstash-tutorial.log`”.



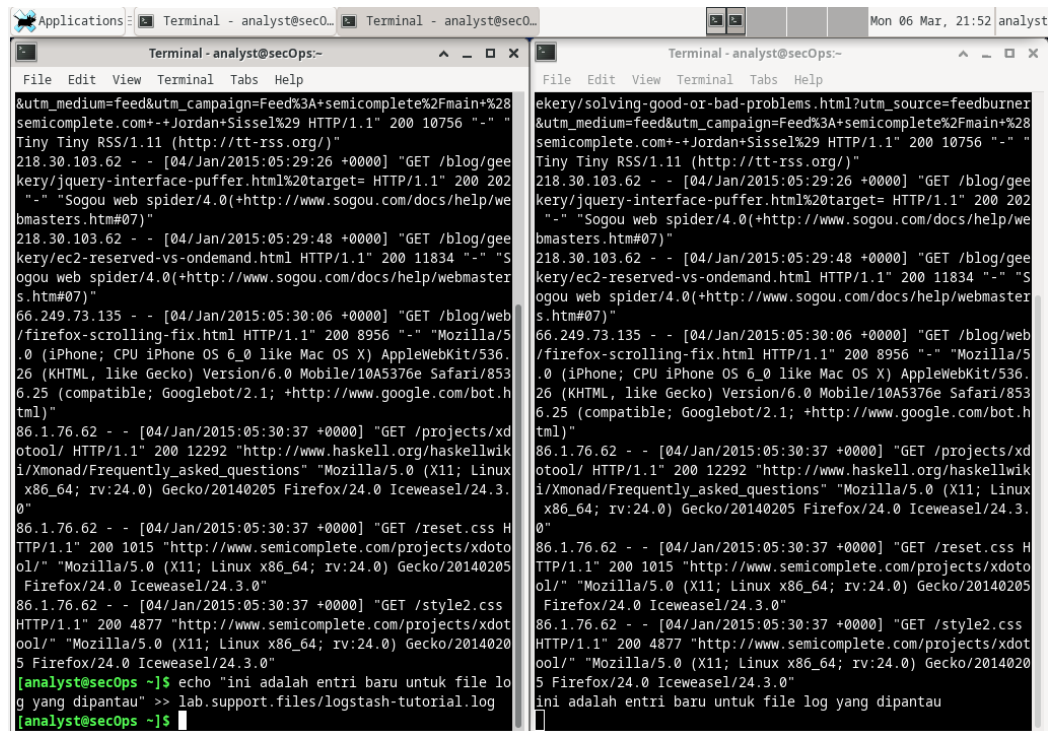
```
[analyst@secOps ~]$ tail -f /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.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+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "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 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/webmasters.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#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/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.semicomplete.com/projects/xdotool/" "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 /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"

^C
[analyst@secOps ~]$
```

6. Atur tampilan 2 buah terminal sehingga dapat melihat kedua jendela terminal. Ubah ukuran jendela terminal sehingga dapat melihat keduanya secara bersamaan.

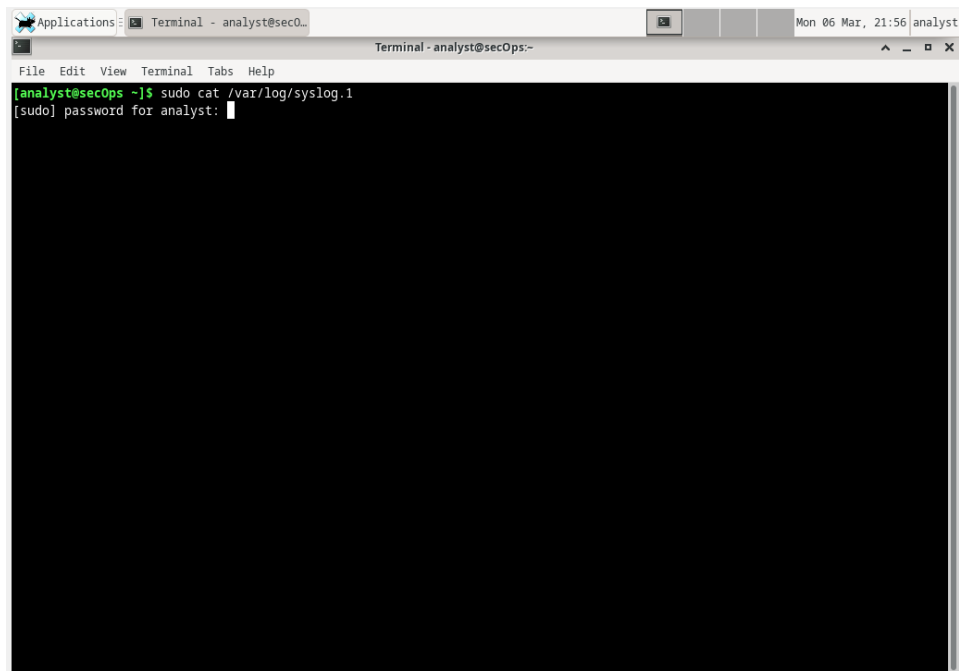


7. Pilihlah jendela terminal kanan dan masukkan perintah “echo "ini adalah entri baru untuk file log yang dipantau" >> lab.support.files/logstash-tutorial.log”.

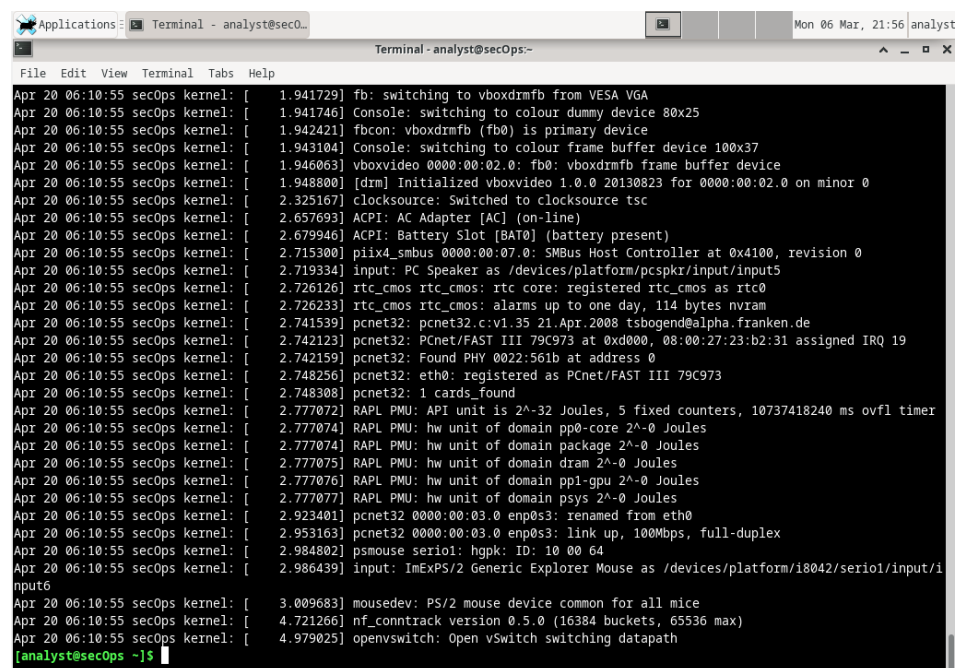


The image shows two terminal windows side-by-side. The left window displays a series of log entries, each starting with a timestamp and IP address, followed by a GET request and user-agent information. The right window shows the same log entries, but with a new entry at the bottom: `[analyst@secOps ~]$ echo "ini adalah entri baru untuk file log yang dipantau" >> lab.support.files/logstash-tutorial.log`. The prompt `[analyst@secOps ~]$` is visible at the bottom of the right window.

8. Tekan CTRL + C untuk menghentikan eksekusi tail -f dan kembali ke prompt shell. Tutup salah satu dari dua jendela terminal.
9. 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. Perintah yang digunakan “sudo cat /var/log/syslog.1”.



```
Applications: Terminal - analyst@sec0... Mon 06 Mar, 21:56 analyst
Terminal - analyst@secOps~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo cat /var/log/syslog.1
[sudo] password for analyst: 
```



```
Applications: Terminal - analyst@sec0... Mon 06 Mar, 21:56 analyst
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 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 ppl-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 serial: 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/input1
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
[analyst@secOps ~]$ 
```

10. 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
```

```
Applications: Terminal - analyst@sec0... Mon 06 Mar, 22:01 analyst
Terminal - analyst@secOps~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo cat /var/log/syslog.2
[sudo] password for analyst:
```

```
Applications: Terminal - analyst@sec0... Mon 06 Mar, 22:01 analyst
Terminal - analyst@secOps~
File Edit View Terminal Tabs Help
Mar 8 14:04:29 secOps kernel: [ 6.553467] RAPL PMU: hw unit of domain package 2^0 Joules
Mar 8 14:04:29 secOps kernel: [ 6.553468] RAPL PMU: hw unit of domain dram 2^0 Joules
Mar 8 14:04:29 secOps kernel: [ 6.553468] RAPL PMU: hw unit of domain pp1-gpu 2^0 Joules
Mar 8 14:04:29 secOps kernel: [ 6.553469] RAPL PMU: hw unit of domain psys 2^0 Joules
Mar 8 14:04:29 secOps kernel: [ 6.674042] pcnet32 0000:00:03.0 enp0s3: renamed from eth0
Mar 8 14:04:29 secOps kernel: [ 6.685876] ppdev: user-space parallel port driver
Mar 8 14:04:29 secOps kernel: [ 6.715010] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Mar 8 14:04:29 secOps kernel: [ 6.730560] psmouse serio1: hgpk: ID: 10 00 64
Mar 8 14:04:29 secOps kernel: [ 6.731557] input: ImExPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input/i
input6
Mar 8 14:04:29 secOps kernel: [ 6.763535] mousedev: PS/2 mouse device common for all mice
Mar 8 14:04:29 secOps kernel: [ 9.425608] nf_conntrack version 0.5.0 (16384 buckets, 65536 max)
Mar 8 14:04:29 secOps kernel: [ 9.449087] VBoxService 5.2.6 r120293 (verbosity: 0) linux.x86 (Jan 31 2018 10:18:27) releas
e log
Mar 8 14:04:29 secOps kernel: [ 9.449087] 00:00:00.000185 main Log opened 2018-03-08T14:04:28.251956000Z
Mar 8 14:04:29 secOps kernel: [ 9.449693] 00:00:00.000772 main OS Product: Linux
Mar 8 14:04:29 secOps kernel: [ 9.449853] 00:00:00.000980 main OS Release: 4.14.15-1.0-ARCH
Mar 8 14:04:29 secOps kernel: [ 9.449954] 00:00:00.001108 main OS Version: #1 SMP PREEMPT Fri Jan 26 00:21:11 CET 2018
Mar 8 14:04:29 secOps kernel: [ 9.450166] 00:00:00.001275 main Executable: /usr/bin/VBoxService
Mar 8 14:04:29 secOps kernel: [ 9.450166] 00:00:00.001277 main Process ID: 277
Mar 8 14:04:29 secOps kernel: [ 9.450166] 00:00:00.001277 main Package type: LINUX_32BITS_GENERIC (OSE)
Mar 8 14:04:29 secOps kernel: [ 9.453623] 00:00:00.004723 main 5.2.6 r120293 started. Verbose level = 0
Mar 8 14:04:29 secOps kernel: [ 9.653345] floppy0: no floppy controllers found
Mar 8 14:04:29 secOps kernel: [ 9.653375] work still pending
Mar 8 14:04:29 secOps kernel: [ 9.959610] openvswitch: Open vSwitch switching datapath
Mar 8 14:04:39 secOps kernel: [ 19.462057] 00:00:10.013104 timesync vgsvcTimeSyncWorker: Radical guest time change: 18 010
902 726 000ns (GuestNow=1 520 535 879 166 774 000 ns GuestLast=1 520 517 868 264 048 000 ns fSetTimeLastLoop=true )
Mar 8 15:04:50 secOps kernel: [ 3630.531995] 01:00:21.083323 control Guest control service stopped
Mar 8 15:04:50 secOps kernel: [ 3630.532030] 01:00:21.083346 control Guest control worker returned with rc=VINF_SUCCESS
Mar 8 15:04:50 secOps kernel: [ 3630.532401] 01:00:21.083710 main Session 0 is about to close ...
Mar 8 15:04:50 secOps kernel: [ 3630.532425] 01:00:21.083744 main Stopping all guest processes ...
Mar 8 15:04:50 secOps kernel: [ 3630.532445] 01:00:21.083765 main Closing all guest files ...
[analyst@secOps ~]$ sudo cat /var/log/syslog.3
```

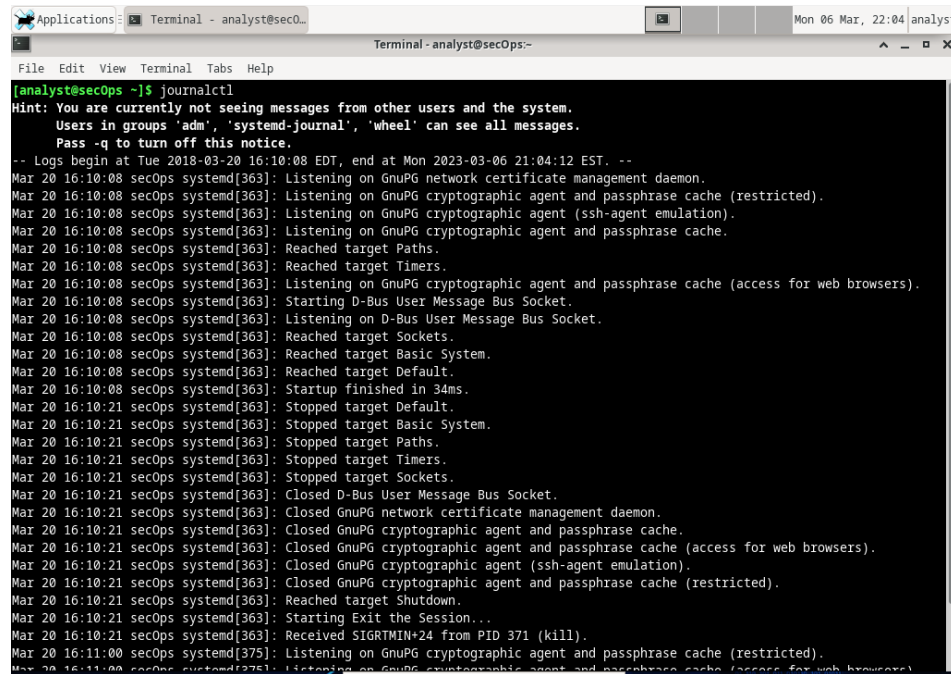
```
Applications: Terminal - analyst@sec0... Mon 06 Mar, 22:02 analyst
Terminal - analyst@secOps:~
Applications new Terminal Tabs Help
Mar 6 06:58:55 secOps kernel: [ 5.516986] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
Mar 6 06:58:55 secOps kernel: [ 5.517557] pcnet32: PCnet/FAST III 79C973 at 0xd000, 08:00:27:23:b2:31 assigned IRQ 19
Mar 6 06:58:55 secOps kernel: [ 5.517609] pcnet32: Found PHY 0022:561b at address 0
Mar 6 06:58:55 secOps kernel: [ 5.517956] pcnet32: eth0: registered as PCnet/FAST III 79C973
Mar 6 06:58:55 secOps kernel: [ 5.531118] ACPI: Battery Slot [BAT0] (battery present)
Mar 6 06:58:55 secOps kernel: [ 5.537314] piix4_smbus 0000:00:07:0: SMBus Host Controller at 0x4100, revision 0
Mar 6 06:58:55 secOps kernel: [ 5.552943] pcnet32: 1 cards_found
Mar 6 06:58:55 secOps kernel: [ 5.587936] mousedev: PS/2 mouse device common for all mice
Mar 6 06:58:55 secOps kernel: [ 5.660268] input: PC Speaker as /devices/platform/pcspkr/input/input6
Mar 6 06:58:55 secOps kernel: [ 5.707891] RAPL PMU: API unit is 2^32 Joules, 5 fixed counters, 10737418240 ms ovfl timer
Mar 6 06:58:55 secOps kernel: [ 5.707893] RAPL PMU: hw unit of domain pp0-core 2^0 Joules
Mar 6 06:58:55 secOps kernel: [ 5.707894] RAPL PMU: hw unit of domain package 2^0 Joules
Mar 6 06:58:55 secOps kernel: [ 5.707894] RAPL PMU: hw unit of domain dram 2^0 Joules
Mar 6 06:58:55 secOps kernel: [ 5.707895] RAPL PMU: hw unit of domain ppl-gpu 2^0 Joules
Mar 6 06:58:55 secOps kernel: [ 5.707895] RAPL PMU: hw unit of domain psys 2^0 Joules
Mar 6 06:58:55 secOps kernel: [ 5.776653] random: crng init done
Mar 6 06:58:55 secOps kernel: [ 5.788340] VBoxService 5.1.18 r114002 (verbosity: 0) linux.x86 (Mar 16 2017 20:50:16) relea
se log
Mar 6 06:58:55 secOps kernel: [ 5.788340] 00:00:00.000109 main Log opened 2018-03-06T11:58:55.458513000Z
Mar 6 06:58:55 secOps kernel: [ 5.796348] 00:00:00.008182 main OS Product: Linux
Mar 6 06:58:55 secOps kernel: [ 5.797354] 00:00:00.009188 main OS Release: 4.10.10-1-ARCH
Mar 6 06:58:55 secOps kernel: [ 5.798734] 00:00:00.010621 main OS Version: #1 SMP PREEMPT Wed Apr 12 19:10:48 CEST 201
7
Mar 6 06:58:55 secOps kernel: [ 5.800251] nf_conntrack version 0.5.0 (16384 buckets, 65536 max)
Mar 6 06:58:55 secOps kernel: [ 5.800739] 00:00:00.012568 main Executable: /usr/bin/VBoxService
Mar 6 06:58:55 secOps kernel: [ 5.800739] 00:00:00.012571 main Process ID: 251
Mar 6 06:58:55 secOps kernel: [ 5.800739] 00:00:00.012572 main Package type: LINUX_32BITS_GENERIC (OSE)
Mar 6 06:58:55 secOps kernel: [ 5.810851] 00:00:00.022706 main 5.1.18 r114002 started. Verbose level = 0
Mar 6 11:58:56 secOps kernel: [ 5.879268] psmouse serio1: hgpk: ID: 10 00 64
Mar 6 11:58:56 secOps kernel: [ 5.880529] input: ImExPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input/i
input7
Mar 6 11:58:56 secOps kernel: [ 6.016025] openvswitch: Open vSwitch switching datapath
[analyst@secOps ~]$ sudo cat /var/log/syslog.4
```

```
Applications: Terminal - analyst@sec0... Mon 06 Mar, 22:02 analyst
Terminal - analyst@secOps:~
Applications new 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/LNXLSPBN: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 timer
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 ppl-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) relea
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 201
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
Nov 29 11:30:39 secOps kernel: [ 6.302534] input: ImExPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input/i
input7
[analyst@secOps ~]$
```

11. Sistem manajemen log populer lainnya dikenal sebagai jurnal. Dikelola oleh daemon journald, sistem ini dirancang untuk memusatkan pengelolaan log terlepas dari mana pesan berasal. Dalam konteks lab ini, fitur yang paling jelas dari daemon sistem jurnal adalah penggunaan file biner khusus tambahan yang berfungsi sebagai file lognya.

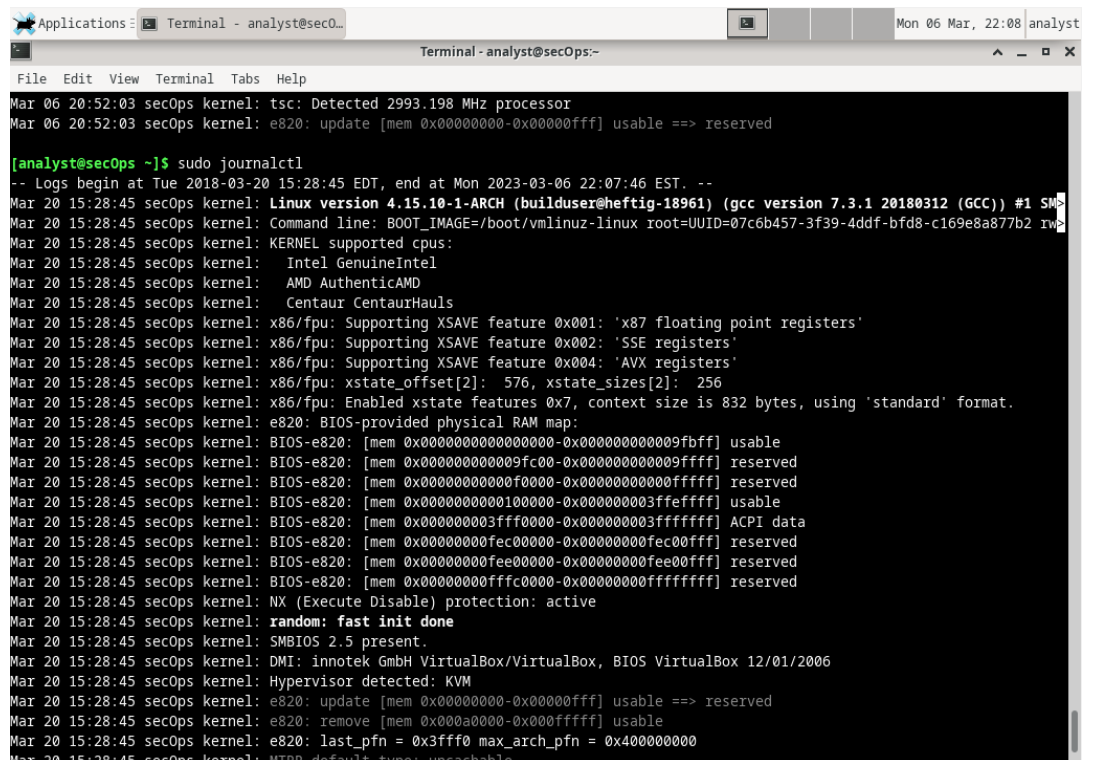


Untuk melihat log journald, gunakan perintah journalctl. Alat journalctl menginterpretasikan dan menampilkan entri log yang sebelumnya disimpan dalam file log biner jurnal. Perintah yang digunakan “journalctl”.



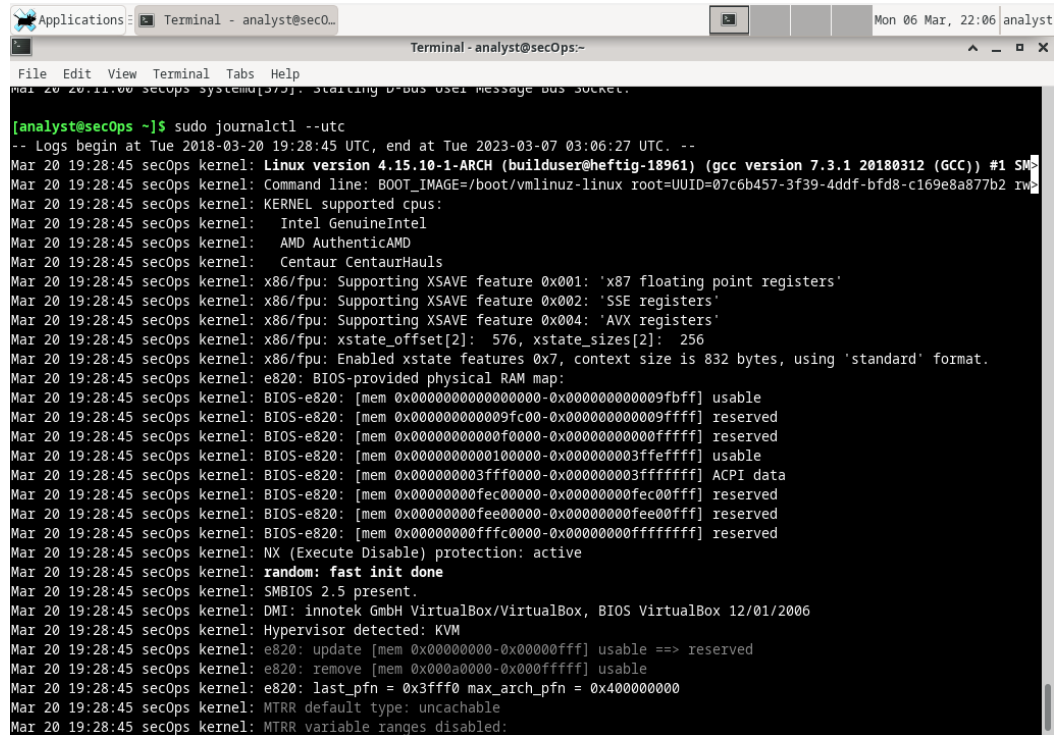
```
Applications: Terminal - analyst@sec0... Mon 06 Mar, 22:04 analyst
Terminal - analyst@secOps:-
[analyst@secOps ~]$ journalctl
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal', 'wheel' can see all messages.
      Pass -q to turn off this notice.
-- Logs begin at Tue 2018-03-20 16:10:08 EDT, end at Mon 2023-03-06 21:04:12 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).
Mar 20 16:11:00 secOps systemd[375]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 16:11:00 secOps systemd[375]: Listening on GnuPG cryptographic agent and passphrase cache (access for web browsers).
```

12. Menjalankan journalctl sebagai root akan menampilkan informasi yang lebih detail. Gunakan CTRL+C untuk keluar dari tampilan. Perintah yang digunakan “sudo journalctl”.



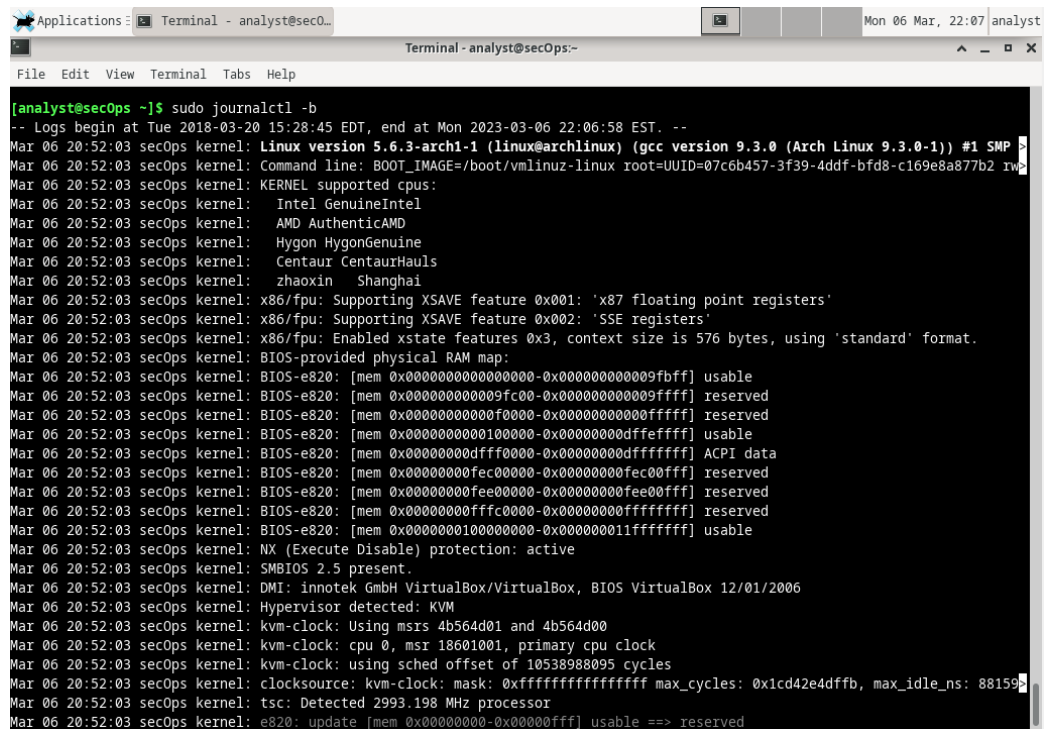
```
Applications: Terminal - analyst@sec0... Mon 06 Mar, 22:08 analyst
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
Mar 06 20:52:03 secOps kernel: tsc: Detected 2993.198 MHz processor
Mar 06 20:52:03 secOps kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[analyst@secOps ~]$ sudo journalctl
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 22:07:46 EST. --
Mar 20 15:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builduser@heftig-18961) (gcc version 7.3.1 20180312 (GCC)) #1 SMP
Mar 20 15:28:45 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 20 15:28:45 secOps kernel: KERNEL supported cpus:
Mar 20 15:28:45 secOps kernel: Intel GenuineIntel
Mar 20 15:28:45 secOps kernel: AMD AuthenticAMD
Mar 20 15:28:45 secOps kernel: Centaur CentaurHauls
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Mar 20 15:28:45 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Mar 20 15:28:45 secOps kernel: e820: BIOS-provided physical RAM map:
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000] usable
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000] ACPI data
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000-0x00000000] reserved
Mar 20 15:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 15:28:45 secOps kernel: random: fast init done
Mar 20 15:28:45 secOps kernel: SMBIOS 2.5 present.
Mar 20 15:28:45 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 20 15:28:45 secOps kernel: Hypervisor detected: KVM
Mar 20 15:28:45 secOps kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Mar 20 15:28:45 secOps kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
Mar 20 15:28:45 secOps kernel: e820: last_pfn = 0x3fff0 max_arch_pfn = 0x400000000
Mar 20 15:28:45 secOps kernel: MTDP: default: type: uncacheable
```

13. Kelebihan menggunakan journalctl terletak pada banyaknya pilihan. Gunakan journalctl --utc untuk menampilkan semua cap waktu dalam waktu UTC. Perintah yang digunakan “sudo journalctl --utc”.



```
Applications: Terminal - analyst@sec0...
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
Mar 20 20:11:00 secOps systemd[37]: Starting D-Bus User Message Bus Socket.
[analyst@secOps ~]$ sudo journalctl --utc
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Tue 2023-03-07 03:06:27 UTC. --
Mar 20 19:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builder@heftig-18961) (gcc version 7.3.1 20180312 (GCC)) #1 SMP
Mar 20 19:28:45 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
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 floating point registers'
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 20 19:28:45 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Mar 20 19:28:45 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Mar 20 19:28:45 secOps kernel: e820: BIOS-provided physical RAM map:
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000003fffff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000003ffff000-0x000000003fffffff] ACPI data
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 20 19:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 19:28:45 secOps kernel: random: fast init done
Mar 20 19:28:45 secOps kernel: SMBIOS 2.5 present.
Mar 20 19:28:45 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 20 19:28:45 secOps kernel: Hypervisor detected: KVM
Mar 20 19:28:45 secOps kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Mar 20 19:28:45 secOps kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Mar 20 19:28:45 secOps kernel: e820: last_pfn = 0x3ffff max_arch_pfn = 0x40000000
Mar 20 19:28:45 secOps kernel: MTRR default type: uncachable
Mar 20 19:28:45 secOps kernel: MTRR variable ranges disabled:
```

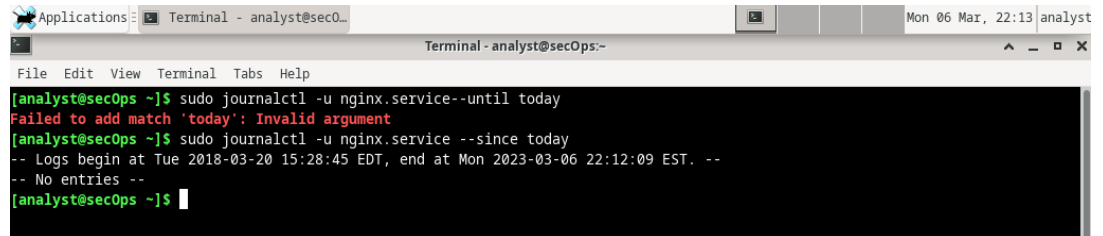
14. Gunakan journalctl -b untuk menampilkan entri log yang direkam selama boot terakhir. Perintah yang digunakan “sudo journalctl -b”.



```
Applications: Terminal - analyst@sec0...
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
Mar 06 20:52:03 secOps systemd[37]: Starting D-Bus User Message Bus Socket.
[analyst@secOps ~]$ sudo journalctl -b
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 22:06:58 EST. --
Mar 06 20:52:03 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (gcc version 9.3.0 (Arch Linux 9.3.0-1)) #1 SMP
Mar 06 20:52:03 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 06 20:52:03 secOps kernel: KERNEL supported cpus:
Mar 06 20:52:03 secOps kernel: Intel GenuineIntel
Mar 06 20:52:03 secOps kernel: AMD AuthenticAMD
Mar 06 20:52:03 secOps kernel: Hygon HygonGenuine
Mar 06 20:52:03 secOps kernel: Centaur CentaurHauls
Mar 06 20:52:03 secOps kernel: zhaoxin Shanghai
Mar 06 20:52:03 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 20:52:03 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 20:52:03 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 20:52:03 secOps kernel: BIOS-provided physical RAM map:
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000000fffff] usable
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x00000000000fffc000-0x00000000000fffff] ACPI data
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffff] usable
Mar 06 20:52:03 secOps kernel: NX (Execute Disable) protection: active
Mar 06 20:52:03 secOps kernel: SMBIOS 2.5 present.
Mar 06 20:52:03 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 20:52:03 secOps kernel: Hypervisor detected: KVM
Mar 06 20:52:03 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 20:52:03 secOps kernel: kvm-clock: cpu 0, msr 18601001, primary cpu clock
Mar 06 20:52:03 secOps kernel: kvm-clock: using sched offset of 10538988095 cycles
Mar 06 20:52:03 secOps kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 88159
Mar 06 20:52:03 secOps kernel: tsc: Detected 2993.198 MHz processor
Mar 06 20:52:03 secOps kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
```

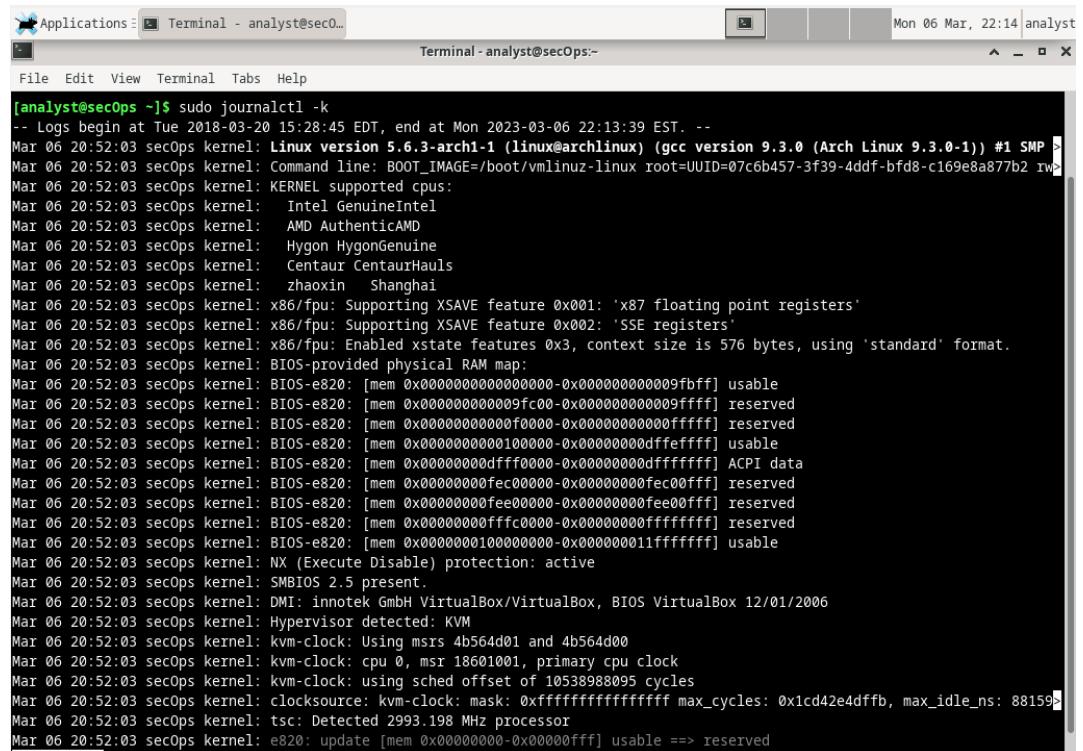


15. Gunakan `journalctl` untuk menentukan layanan dan kerangka waktu untuk entri log. Perintah “`sudo journalctl -u nginx.service --since today`” menunjukkan semua log layanan nginx yang direkam hari ini.



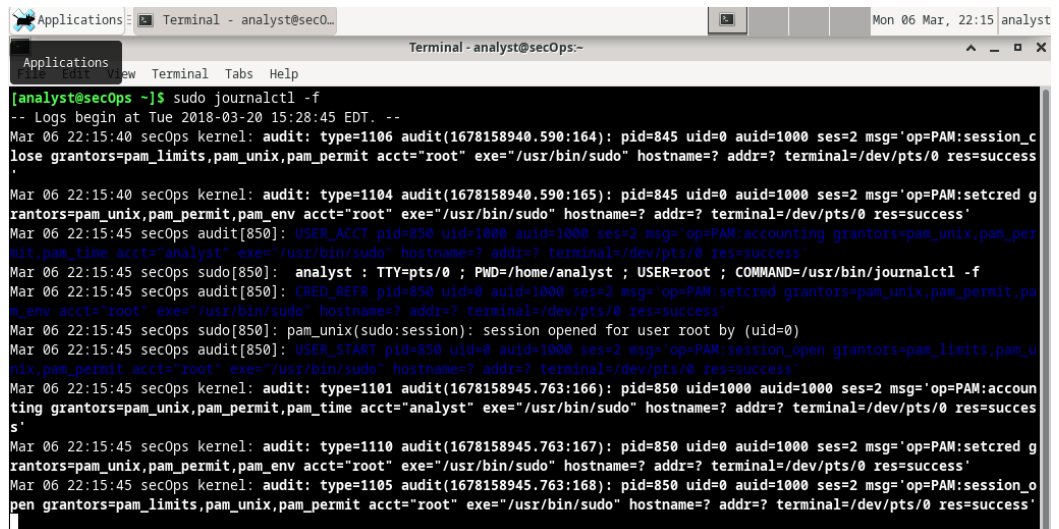
```
Applications: Terminal - analyst@sec0...
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo journalctl -u nginx.service--until today
Failed to add match 'today': Invalid argument
[analyst@secOps ~]$ sudo journalctl -u nginx.service --since today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 22:12:09 EST. --
-- No entries --
[analyst@secOps ~]$
```

16. Gunakan `-k` switch untuk hanya menampilkan pesan yang dihasilkan oleh kernel. Perintah yang digunakan “`sudo journalctl -k`”.



```
Applications: Terminal - analyst@sec0...
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 2023-03-06 22:13:39 EST. --
Mar 06 20:52:03 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (gcc version 9.3.0 (Arch Linux 9.3.0-1)) #1 SMP
Mar 06 20:52:03 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 06 20:52:03 secOps kernel: KERNEL supported cpus:
Mar 06 20:52:03 secOps kernel: Intel GenuineIntel
Mar 06 20:52:03 secOps kernel: AMD AuthenticAMD
Mar 06 20:52:03 secOps kernel: Hygon HygonGenuine
Mar 06 20:52:03 secOps kernel: Centaur CentaurHauls
Mar 06 20:52:03 secOps kernel: zhaoxin Shanghai
Mar 06 20:52:03 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 20:52:03 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 20:52:03 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 20:52:03 secOps kernel: BIOS-provided physical RAM map:
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009fbff] usable
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x00000000000009fc00-0x00000000000009ffff] reserved
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x0000000000000f0000-0x0000000000000fffff] reserved
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x000000000000100000-0x0000000000000dffff] usable
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x000000000dffff0000-0x00000000dffffffffff] ACPI data
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffffff] reserved
Mar 06 20:52:03 secOps kernel: BIOS-e820: [mem 0x0000000010000000-0x0000000011ffffff] usable
Mar 06 20:52:03 secOps kernel: NX (Execute Disable) protection: active
Mar 06 20:52:03 secOps kernel: SMBIOS 2.5 present.
Mar 06 20:52:03 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 20:52:03 secOps kernel: Hypervisor detected: KVM
Mar 06 20:52:03 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 20:52:03 secOps kernel: kvm-clock: cpu 0, msr 18601001, primary cpu clock
Mar 06 20:52:03 secOps kernel: kvm-clock: using sched offset of 10538988095 cycles
Mar 06 20:52:03 secOps kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 88159
Mar 06 20:52:03 secOps kernel: tsc: Detected 2993.198 MHz processor
Mar 06 20:52:03 secOps kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
```

17. Mirip dengan `tail -f` yang dijelaskan di atas, gunakan `-f` untuk secara aktif mengikuti log saat sedang ditulis. Perintah yang digunakan “`sudo journalctl -f`”.



```
Applications Terminal - analyst@sec0... Mon 06 Mar, 22:15 analyst
Terminal - analyst@secOps--
Applications new Terminal Tabs Help
[analyst@secOps ~]$ sudo journalctl -f
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Mar 06 22:15:40 secOps kernel: audit: type=1106 audit(1678158940.590:164): pid=845 uid=0 auid=1000 ses=2 msg='op=PAM:session_c
lose grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success
'
Mar 06 22:15:40 secOps kernel: audit: type=1104 audit(1678158940.590:165): pid=845 uid=0 auid=1000 ses=2 msg='op=PAM:setcred g
rantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 22:15:45 secOps audit[850]: USER_ACCT pid=850 uid=1000 auid=1000 ses=2 msg='op=PAM:accounting grantors=pam_unix,pam_per
mit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 22:15:45 secOps sudo[850]: analyst : TTY=pts/0 ; PWD=/home/analyst ; USER=root ; COMMAND=/usr/bin/journalctl -f
Mar 06 22:15:45 secOps audit[850]: CRED_REFR pid=850 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'
Mar 06 22:15:45 secOps sudo[850]: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 06 22:15:45 secOps audit[850]: USER_START pid=850 uid=0 auid=1000 ses=2 msg='op=PAM:session_open grantors=pam_limits,pam_u
nix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 22:15:45 secOps kernel: audit: type=1101 audit(1678158945.763:166): pid=850 uid=0 auid=1000 ses=2 msg='op=PAM:account
ing grantors=pam_unix,pam_permit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succes
s'
Mar 06 22:15:45 secOps kernel: audit: type=1110 audit(1678158945.763:167): pid=850 uid=0 auid=1000 ses=2 msg='op=PAM:setcred g
rantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 22:15:45 secOps kernel: audit: type=1105 audit(1678158945.763:168): pid=850 uid=0 auid=1000 ses=2 msg='op=PAM:session_o
pen grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
```

## D. Analisis

Pada praktikum Keamanan Informasi 1 pertemuan 4 membahas tentang Teknik Steganografi dan Analisis Log server. Teknik steganografi adalah sebuah teknik untuk menyembunyikan pesan rahasia di dalam media seperti gambar, video, atau audio dengan cara mengubah sedikit atau sebagian informasi dalam media tersebut, sehingga pesan rahasia tersebut tidak terlihat oleh orang yang tidak berwenang. Dalam teknik steganografi, pesan rahasia tersebut disisipkan ke dalam media dengan cara yang tidak mencolok, sehingga orang yang melihat atau mendengar media tersebut tidak akan curiga bahwa terdapat pesan rahasia yang disembunyikan di dalamnya. Pada unit steganografi aplikasi yang digunakan adalah QuickStego dimana aplikasi yang digunakan untuk menyembunyikan pesan rahasia di dalam media seperti gambar atau audio menggunakan teknik steganografi. QuickStego merupakan salah satu perangkat lunak yang cukup populer dan mudah digunakan untuk menyembunyikan pesan rahasia. Dan untuk menguji sebuah gambar yang disisipi sebuah string digunakan software bernama MD5SUMS dimana menghitung intisari pesan MD5 untuk satu atau beberapa file (termasuk persen tampilan selesai untuk file besar). Dengan membandingkan intisari MD5 dari file dengan nilai yang diberikan oleh pengirim asli, Anda dapat memastikan bahwa file yang Anda unduh bebas dari kerusakan dan gangguan.

Saat menggunakan QuickStego setelah mengimport gambar dapat disisipkan sebuah string pada bagian kiri aplikasi kemudian klik Hide Text dimana untuk menyembunyikan sebuah text kedalam gambar dan kemudian gambar yang telah disisipi text dan gambar asli

dapat di simpan pada sebuah folder dimana juga berisi MD5SUMS.exe. Setelah itu buka CMD dan pindah ke direktori folder yang berisi MD5SUMS dan gambar kemudian gunakan perintah “md5sums.exe \*.jpg”. Perbedaan antara gambar asli dengan gambar yang telah disisipi text dapat terlihat pada besar size yang berbeda satu sama lain dimana gambar yang disisipi text memiliki size penyimpanan yang lebih besar serta dapat dilihat juga pada MD5SUMS dimana hasil kodenya berbeda gambar asli dengan gambar yang disisipi text.

Pada unit analisis server log dimana File Log adalah alat penting dalam pemecahan masalah dan pemantauan. File log juga merupakan 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. Aplikasi yang berbeda menghasilkan file log yang berbeda, masing-masing berisi kumpulan bidang dan informasinya sendiri. Meskipun struktur bidang dapat berubah di antara file log, alat yang digunakan untuk membacanya sebagian besar sama. 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.

Pada unit ini menggunakan VM CyberOps Workstation dimana disini perintah yang digunakan antara lain :

- Perintah "cat" pada sistem operasi Linux merupakan singkatan dari "concatenate" yang berfungsi untuk menampilkan atau menggabungkan isi dari satu atau beberapa file teks dan menampilkannya ke layar konsol. Fungsi utama dari perintah "cat" adalah untuk membaca atau menampilkan isi dari satu atau beberapa file teks yang ada pada sistem.
- Perintah "more" pada sistem operasi Linux merupakan perintah yang berfungsi untuk menampilkan isi dari satu atau beberapa file teks secara berurutan pada layar konsol. Fungsi utama dari perintah "more" adalah untuk membaca isi dari file teks yang terlalu panjang untuk ditampilkan pada satu layar konsol.
- Fitur "less" pada sistem operasi Linux digunakan untuk melihat isi file teks secara berurutan dalam terminal atau konsol. Fitur ini mirip dengan perintah "more", namun memiliki beberapa tambahan fitur yang lebih canggih. Tekan spasi untuk maju ke halaman berikutnya. Tekan enter untuk menampilkan baris teks

berikutnya. Gunakan tombol panah atas dan bawah untuk bergerak maju mundur melalui file teks. Gunakan tombol q pada keyboard untuk keluar.

- Fitur "tail" pada sistem operasi Linux digunakan untuk melihat konten terakhir dari sebuah file teks atau output dari sebuah program yang sedang berjalan. Secara default, tail menampilkan sepuluh baris terakhir file.

Berikut adalah jawaban dari pertanyaan yang ada pada modul Analisis Log Server.

- Apa kelemahan menggunakan cat dengan file teks besar? Awal file mungkin hilang karena cat tidak mendukung pemecahan halaman.
- Apa kelemahan menggunakan more? Bergantung pada aplikasi terminal yang digunakan, mungkin tidak mudah untuk menampilkan kembali halaman yang sudah ditampilkan.
- Apa yang berbeda dalam output tail dan tail -f? Setelah perintah tail -f dikeluarkan, terminal tampak terkunci dan tidak menerima perintah lagi. Ini terjadi karena tail masih berjalan, menonton file log dan akan mencetak setiap perubahan yang tertulis di layar.
- Mengapa perintah cat harus dijalankan sebagai root? Di VM CyberOps Workstation, /var/log/syslog merupakan milik root dan hanya dapat dibaca oleh root.
- Jelaskan kenapa harus mensinkronkan waktu dan tanggal komputer dengan benar? Sistem log menggunakan file log untuk merekam dan menyimpan peristiwa dan tanggal/waktu terjadinya. Jika jam sistem salah atau tidak sinkron, maka akan mempersulit proses pemecahan masalah.

Perbandingan Syslog dengan Journald adalah Syslog adalah solusi standar untuk logging. Ini menggunakan file plaintext tetapi memiliki kekurangan struktur. Informasi tidak terpusat, dan mungkin perlu mencari banyak informasi yang tidak terkait untuk menemukan informasi yang relevan. Syslog tidak menyediakan cara untuk memisahkan pesan dengan aplikasi terkait. Selain itu, file plaintext mungkin memerlukan rotasi agar tidak menjadi terlalu besar. Journald mengganti file log teks biasa dengan format file khusus untuk pesan log. Ini membuatnya lebih mudah untuk menemukan pesan log yang relevan.

## E. Kesimpulan

Berdasarkan data diatas dapat disimpulkan Dengan menggunakan teknik steganografi, pesan atau informasi rahasia dapat dikirim secara aman dan rahasia tanpa menarik perhatian dari pihak yang tidak berwenang. Namun, teknik steganografi juga dapat disalahgunakan untuk tujuan ilegal atau kriminal, seperti menyembunyikan informasi teroris atau melanggar privasi orang lain. Oleh karena itu, penggunaan teknik steganografi haruslah dilakukan dengan penuh tanggung jawab dan etika yang baik.

Beberapa kesimpulan penting tentang file log pada Linux server adalah:

1. File log dapat digunakan untuk memantau kinerja server dan mengidentifikasi masalah dalam sistem.
2. File log dapat membantu dalam penelusuran sumber masalah, termasuk pemecahan masalah yang terkait dengan keamanan, kesalahan konfigurasi, dan masalah performa.
3. File log juga dapat membantu dalam mendeteksi dan mencegah serangan keamanan, seperti serangan Brute Force, serangan DDoS, atau serangan malware.
4. Penting untuk memperhatikan pengaturan rotasi log untuk memastikan file log tidak menghabiskan ruang disk yang berlebihan dan berpotensi membuat server menjadi tidak stabil.
5. Para administrator sistem harus secara teratur memeriksa file log untuk mengidentifikasi aktivitas yang mencurigakan atau aneh yang mungkin mengindikasikan masalah atau serangan keamanan.

## F. Daftar Pustaka

1. Biniasz, K. (2017). *What are Linux Logs? Code Examples, Tutorials & More*. [online] Stackify. Available at: <https://stackify.com/linux-logs/>.
2. Lakukan sulap dengan log Linux Anda dengan Log Management. (2019, July 2). Motadata. <https://www.motadata.com/id/blog/do-magic-with-your-linux-logs-with-log-management/>
3. Pangestu, F. (2019, December 2). Implementasi Steganografi Pada Aplikasi Quick Stego. Freeday's SBS. <https://tutorsbs.wordpress.com/2019/12/02/implementasi-steganografi-pada-aplikasi-quick-stego/>

