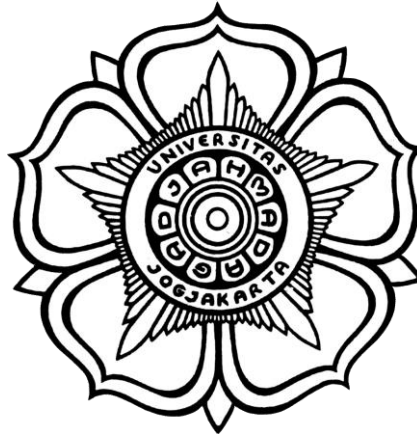


LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

UNIT 5 dan 6

Teknik Steganografi dan Analisis Log Server



Disusun Oleh :

Nama : Abu Alif Raharjo
NIM : 21/479770/SV/19537
Hari, tanggal : Selasa, 07 Maret 2023
Dosen Pengampu : Anni Karimatul Fauziyyah, S. Kom., M. Eng.

PROGRAM STUDI DIPLOMA IV TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

A. Tujuan

- Memahami Steganografi
- Memahami QuickStego
- Memahami MD5sums
- Membaca File Log dengan Cat, More, Less, dan Tail
- Memahami File Log dan Syslog
- Memahami File Log dan Jurnalctl

B. Latar Belakang

Steganografi adalah ilmu menulis pesan tersembunyi sedemikian rupa sehingga tidak ada seorang pun selain pengirim dan penerima yang dituju yang menyadari ada pesan tersembunyi. QuickStego memungkinkan anda menyembunyikan teks dalam gambar sehingga hanya pengguna QuickStego lain yang dapat mengambil dan membaca pesan rahasia yang tersembunyi. Setelah teks disembunyikan dalam gambar, gambar yang disimpan masih berupa 'gambar', itu akan dimuat seperti gambar lainnya dan muncul seperti sebelumnya. Gambar dapat disimpan, dikirim melalui email, diunggah ke web (, satu-satunya perbedaan adalah berisi teks tersembunyi. MD5sums 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.

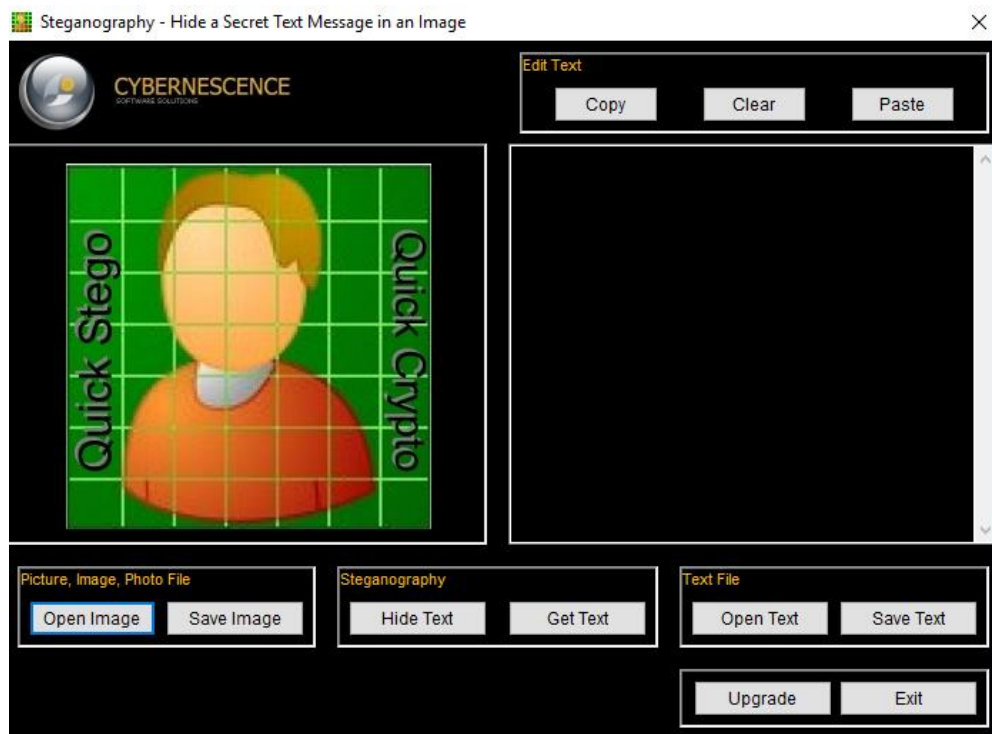
File Log adalah alat penting dalam pemecahan masalah dan pemantauan. Aplikasi yang berbeda menghasilkan file log yang berbeda, masing-masing berisi kumpulan bidang dan informasinya sendiri. Meskipun struktur bidang dapat berubah di antara file log, alat yang digunakan untuk membacanya sebagian besar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

C. Alat dan Bahan

- Software Quick Stego
- MD5sums
- CyberOps Workstation virtual machine
- VirtualBox

D. Instruksi Kerja

1. Install Quick Stego



2. Install md5sums

```

D:\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:\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
  
```

3. Buat file pada file (C:) dengan nama “STEGO”

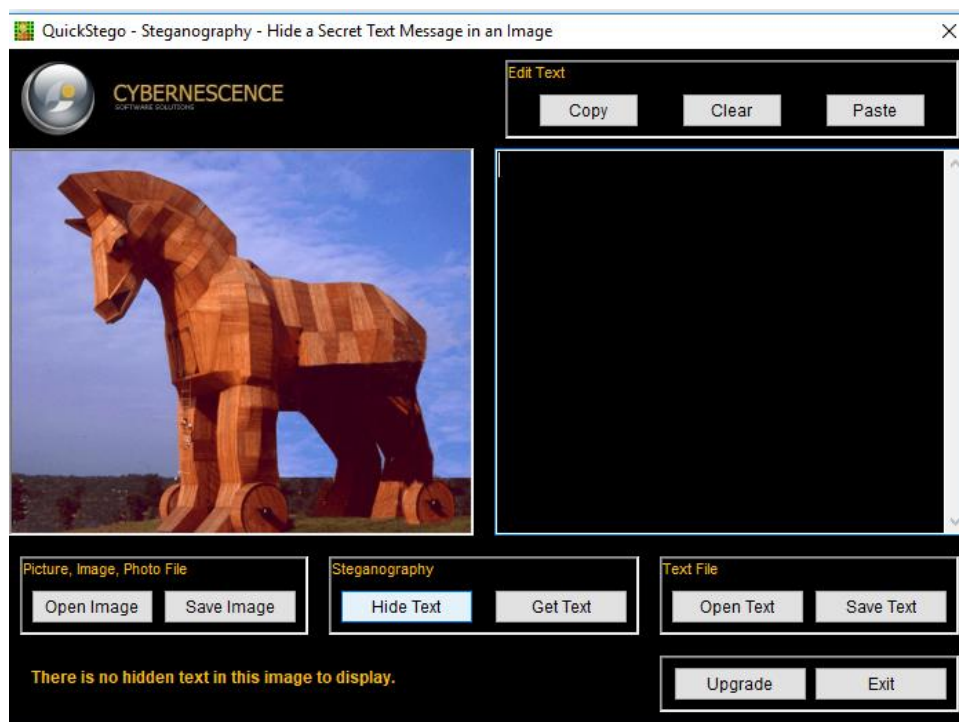
➤ This PC ➤ WIN 10 LC (C:) ➤ STEGO

4. Donwload gambar yang sudah disediakan pada elok.

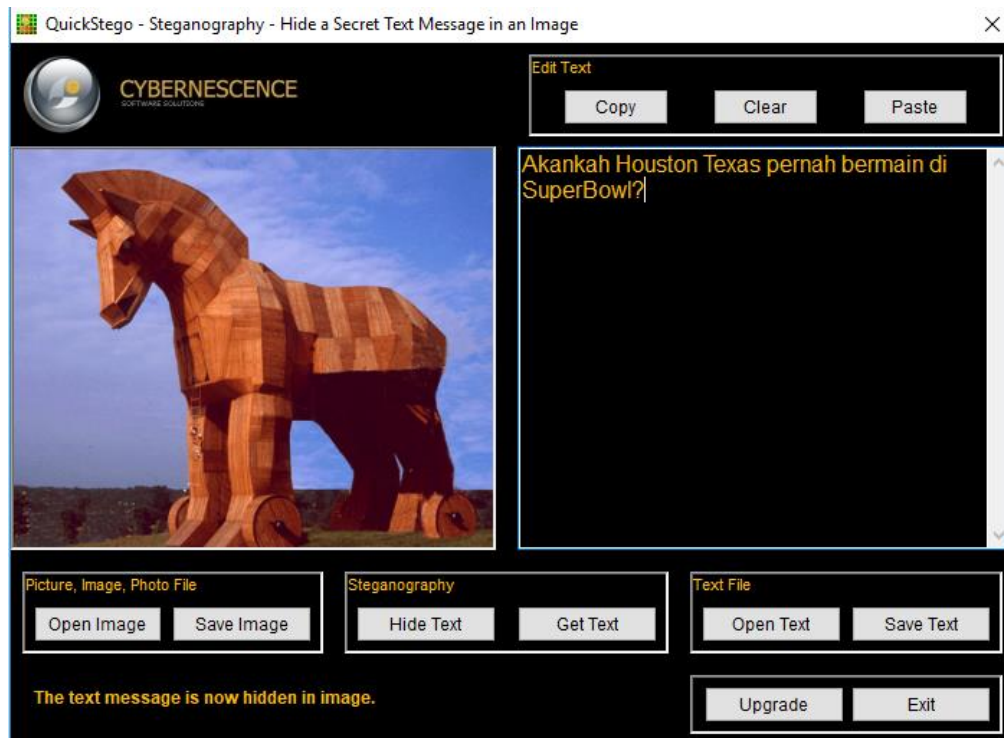
This PC ➤ WIN 10 LC (C:) ➤ STEGO				
Name	Date	Type	Size	Ta
horse	07/03/2023 8:17	JPG File	45 KB	



5. Klik open image, dan pilih gambar yang sudah didownload tadi.



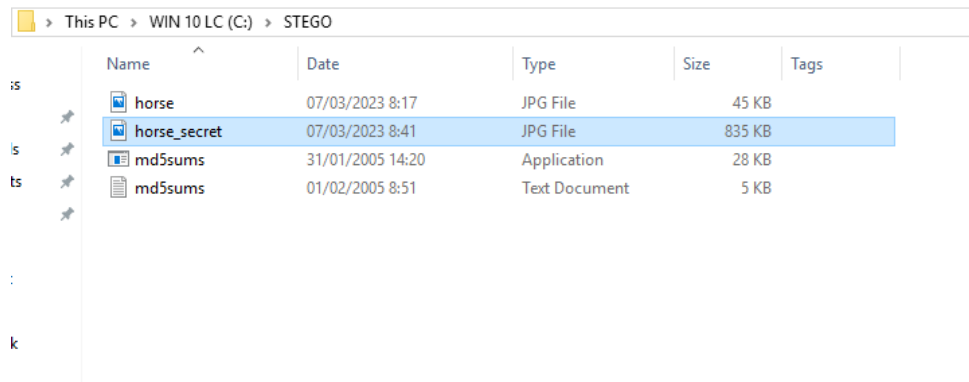
6. Berikan Pesan Tersembunyi Anda. Pesan tersembunyi saya ada di bawah.
(Lihat Gambar) **Akankah Houston Texas pernah bermain di SuperBowl?**



7. Klik tombol Sembunyikan Teks
8. Perhatikan pesan yang menyatakan "Pesan teks sekarang tersembunyi di gambar".



9. Klik tombol Simpan Gambar
10. Arahkan ke direktori C:\STEGO
11. Nama file: horse_secret.jpg, pastikan menyertakan ekstensi .jpg.
12. Klik tombol Simpan



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

14. Klik **C:\Users\Dell>cd C:\STEGO** pada cmd

15. Lalu, klik **C:\STEGO>dir *.jpg**

16. Lanjutkan dengan **md5sums.exe *.jpg** pada cmd

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

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

C:\STEGO>dir *.jpg
Volume in drive C is WIN 10 LC
Volume Serial Number is 7BDC-4B5B

Directory of C:\STEGO

07/03/2023  08:17                46.001 horse.jpg
07/03/2023  08:41            854.454 horse_secret.jpg
               2 File(s)             900.455 bytes
               0 Dir(s)  265.561.919.488 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

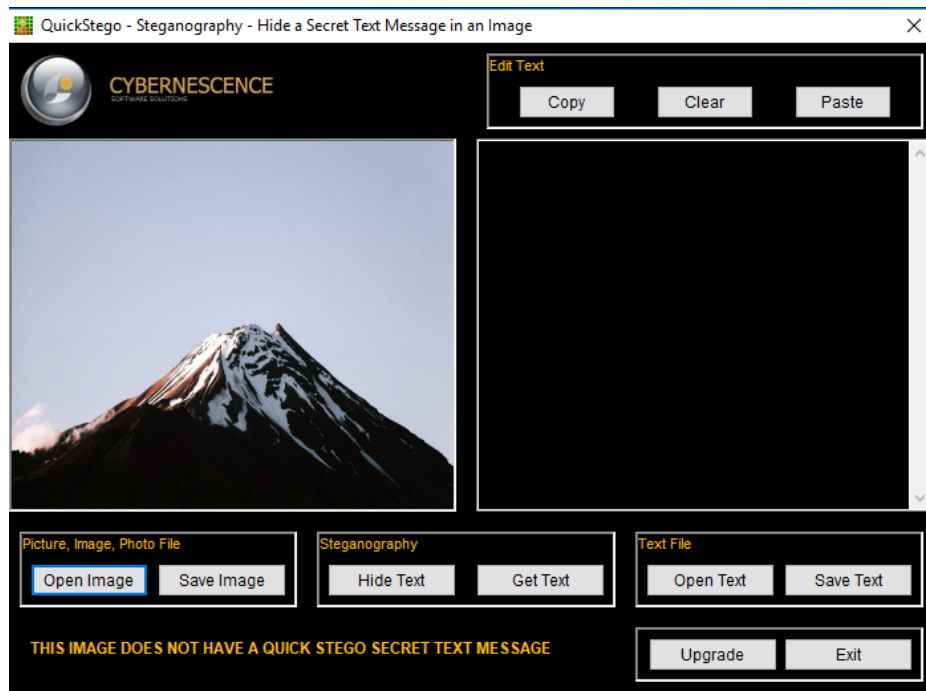
[Path] / filename                                MD5 sum
-----
[C:\STEGO\]
horse.jpg                                         fce8552170cccd3dd545566309124097
horse_secret.jpg                                69d6373f08d0f7a3979dc7c4a68486ea
C:\STEGO>

```

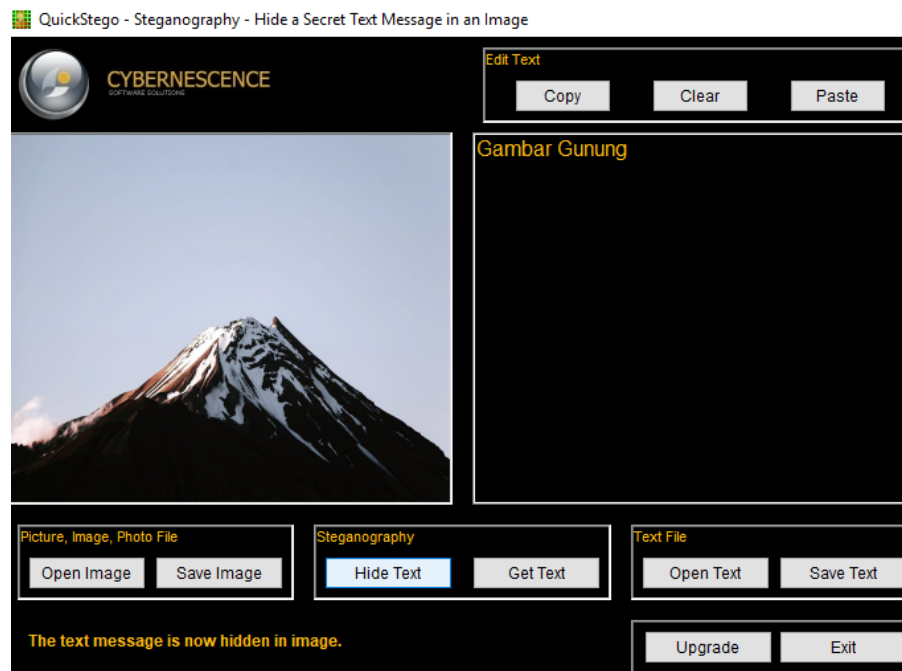
17. Setelah itu masukkan gambar kedua

18. Masukkan gambar tersebut pada file STEGO tadi

19. Upload gambar pada QuickStego



20. Tambahkan pesan, lalu klik Hide Text



21. Pada cmd masukkan perintah seperti sebelumnya. Maka akan muncul 4 gambar sesuai yang tersimpan pada folder STEGO

```

C:\Windows\system32\cmd.exe
Volume in drive C is WIN 10 LC
Volume Serial Number is 7BDC-4B5B

Directory of C:\STEGO

07/03/2023  08:51          1.998.054 gambar_gunung.jpg
07/03/2023  08:17           46.001 horse.jpg
07/03/2023  08:41          854.454 horse_secret.jpg
07/03/2023  08:49          57.186 StegOnline_Demo.jpg
               4 File(s)      2.955.695 bytes
               0 Dir(s)    265.550.241.792 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\]
gambar_gunung.jpg                             529cbc046a051a7df4e902e1dee069e7
horse.jpg                                     fce8552170cced3dd545566309124097
horse_secret.jpg                             69d6373f08d0f7a3979dc7c4a68486ea
StegOnline_Demo.jpg                         8a030bc5730d020172f96c20bc32fb05

C:\STEGO>

```

Unit 6

1. Buka virtualBox, jalankan file CyberOps dan masuk ke 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.ort.files/:
`analis@secOps ~$ cat /home/analyst/lab.support.files/logstash-tutorial.log`

```

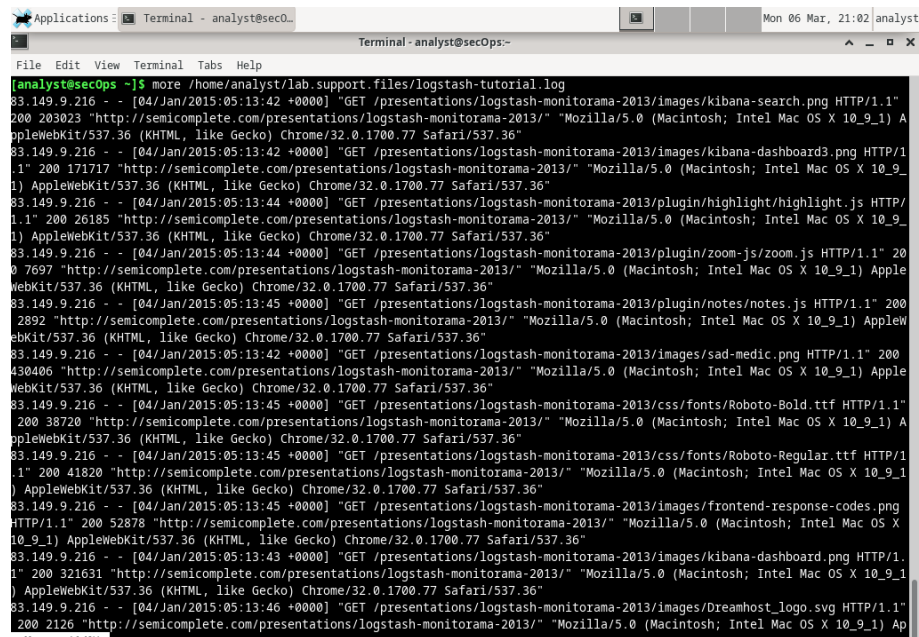
Applications: Terminal - analis@secOps...
Terminal - analis@secOps:~
File Edit View Terminal Tabs Help

[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-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/images/kibana-dashbaord.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 jendela terminal yang sama, gunakan perintah di bawah ini untuk menampilkan kembali isi file logstash-tutorial.log. Proses ini menggunakan `more:`

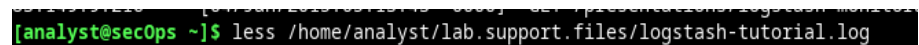
analis@secOps ~\$ more /home/analyst/lab.support.files/logstash-tutorial.log



```
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"
```

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



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

```
Applications Terminal - analyst@secOps... Mon 06 Mar, 21:05 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/2015:05:13:45 +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-dash-board.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"
[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_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-interface-puffer.html?target= 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-on-demand.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"
```

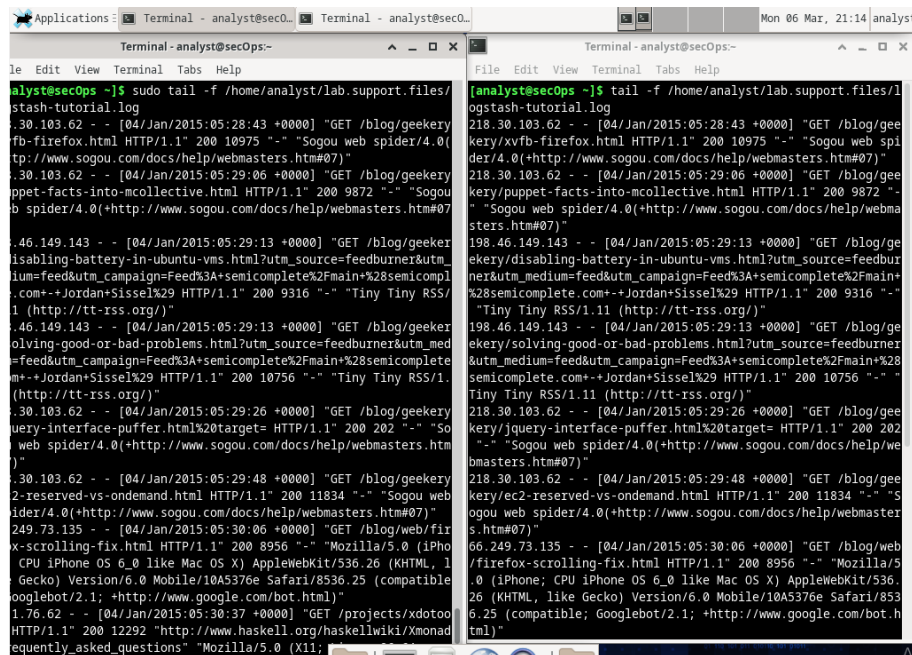
5. Perintah **tail** menampilkan akhir file teks. Secara default, tail menampilkan sepuluh baris terakhir file.

Gunakan **tail** untuk menampilkan sepuluh baris terakhir dari file `/home/analyst/lab.support.files/logstash-tutorial.log`.

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

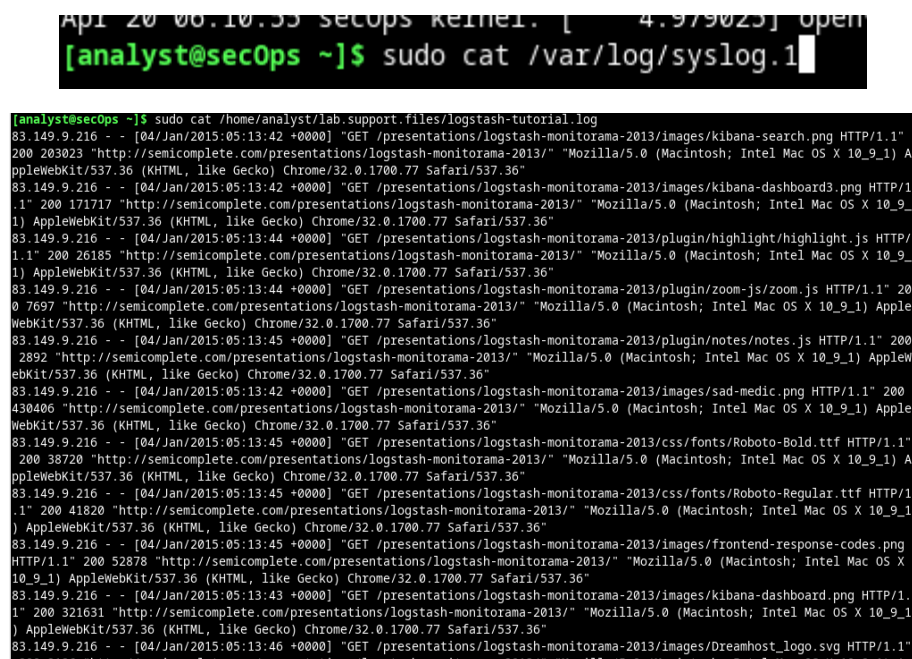
```
[analyst@secOps ~]$ sudo tail -f /home/analyst/lab.support.files/logstash-tutorial.log
[sudo] password for analyst:
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0 (+http://www.sogou.com/docs/help/webmasters.htm#07)"
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_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-interface-puffer.html?target= 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-on-demand.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"
```

6. Atur tampilan Anda sehingga Anda dapat melihat kedua jendela terminal. Ubah ukuran jendela sehingga Anda dapat melihat keduanya secara bersamaan. Pada jendela terminal tersebut, jalankanlah **tail -f** untuk melihat file `/home/analyst/lab.support.files/logstash-tutorial.log`.



```
analyst@secOps ~]$ sudo 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 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-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/firx-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)"
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; Ubuntu; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0"
```

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



```
analyst@secOps ~]$ sudo cat /var/log/syslog.1
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 2136 "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"
```

8. Gunakan perintah cat untuk membuat daftar file syslog yang lebih lama:
analis@secOps ~\$ sudo cat /var/log/syslog.2

```
[analyst@secOps ~]$ sudo cat /var/log/syslog.2

) ) #1 SMP PREEMPT Wed Apr 12 19:10:48 CEST 2017
Mar 6 07:27:19 secOps kernel: [ 0.000000] -----[ cut here ]-----
Mar 6 07:27:19 secOps kernel: [ 0.000000] WARNING: CPU: 0 PID: 0 at arch/x86/kernel/fpu/xstate.c:595 fpu__init_system_xstate+0x465/0x7b2
Mar 6 07:27:19 secOps kernel: [ 0.000000] XSAVE consistency problem, dumping leaves
Mar 6 07:27:19 secOps kernel: [ 0.000000] Modules linked in:
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPU: 0 PID: 0 Comm: swapper Not tainted 4.10.10-1-ARCH #1
Mar 6 07:27:19 secOps kernel: [ 0.000000] Call Trace:
Mar 6 07:27:19 secOps kernel: [ 0.000000] dump_stack+0x58/0x74
Mar 6 07:27:19 secOps kernel: [ 0.000000] __warn+0xea/0x110
Mar 6 07:27:19 secOps kernel: [ 0.000000] ? fpu__init_system_xstate+0x465/0x7b2
Mar 6 07:27:19 secOps kernel: [ 0.000000] warn_slowpath_fmt+0x46/0x60
Mar 6 07:27:19 secOps kernel: [ 0.000000] fpu__init_system_xstate+0x465/0x7b2
Mar 6 07:27:19 secOps kernel: [ 0.000000] fpu__init_system+0x18c/0x1b1
Mar 6 07:27:19 secOps kernel: [ 0.000000] early_cpu_init+0x110/0x113
Mar 6 07:27:19 secOps kernel: [ 0.000000] setup_arch+0xe4/0xbb6
Mar 6 07:27:19 secOps kernel: [ 0.000000] start_kernel+0x8f/0x3ce
Mar 6 07:27:19 secOps kernel: [ 0.000000] i386_start_kernel+0x91/0x95
Mar 6 07:27:19 secOps kernel: [ 0.000000] startup_32_smp+0x16b/0x16d
Mar 6 07:27:19 secOps kernel: [ 0.000000] ---[ end trace 8bb55a17cbc12e3d ]---
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 00]: eax=00000007 ebx=00000440 ecx=00000440 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 01]: eax=00000000 ebx=000003c0 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 02]: eax=00000100 ebx=00000240 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 03]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 04]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 05]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 06]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 07]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 08]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 09]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 0a]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 0b]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 0c]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 0d]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
```

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

```
[analyst@secOps ~]$ sudo cat /var/log/syslog.3

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

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


```
[analyst@secOps ~]$ sudo cat /var/log/syslog.4
Aug 23 12:04:42 secOps kernel: [ 8.047919] floppy0: no floppy controllers found
Aug 23 12:04:42 secOps kernel: [ 8.047950] work still pending
Aug 23 13:49:32 secOps kernel: [ 6298.300707] pcnet32 0000:00:03.0 enp0s3: link down
Aug 23 13:49:36 secOps kernel: [ 6302.354139] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Aug 24 11:06:06 secOps kernel: [82892.804946] Bluetooth: Core ver 2.22
Aug 24 11:06:06 secOps kernel: [82892.805387] NET: Registered protocol family 31
Aug 24 11:06:06 secOps kernel: [82892.805388] Bluetooth: HCI device and connection manager initialized
Aug 24 11:06:06 secOps kernel: [82892.805390] Bluetooth: HCI socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.805392] Bluetooth: L2CAP socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.805396] Bluetooth: SCO socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.816995] Netfilter messages via NETLINK v0.30.
Aug 24 11:15:48 secOps kernel: [83475.322402] pcnet32 0000:00:03.0 enp0s3: link down
Aug 24 11:15:54 secOps kernel: [83481.238928] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Aug 24 08:09:23 secOps kernel: [ 0.000000] Linux version 4.10.10-1-ARCH (builduser@tobias) (gcc version 6.3.1 20170306 (GCC
) ) #1 SMP PREEMPT Wed Apr 12 19:10:48 CEST 2017
Aug 24 08:09:23 secOps kernel: [ 0.000000] -----[ cut here ]-----
Aug 24 08:09:23 secOps kernel: [ 0.000000] WARNING: CPU: 0 PID: 0 at arch/x86/kernel/fpu/xstate.c:595 fpu__init_system_xsta
te+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [ 0.000000] XSAVE consistency problem, dumping leaves
Aug 24 08:09:23 secOps kernel: [ 0.000000] Modules linked in:
Aug 24 08:09:23 secOps kernel: [ 0.000000] CPU: 0 PID: 0 Comm: swapper Not tainted 4.10.10-1-ARCH #1
Aug 24 08:09:23 secOps kernel: [ 0.000000] Call Trace:
Aug 24 08:09:23 secOps kernel: [ 0.000000] dump_stack+0x58/0x74
Aug 24 08:09:23 secOps kernel: [ 0.000000] __warn+0xea/0x110
Aug 24 08:09:23 secOps kernel: [ 0.000000] ? fpu__init_system_xstate+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [ 0.000000] warn_slowpath_fmt+0x46/0x60
Aug 24 08:09:23 secOps kernel: [ 0.000000] fpu__init_system_xstate+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [ 0.000000] fpu__init_system+0x18c/0x1b1
Aug 24 08:09:23 secOps kernel: [ 0.000000] early_cpu_init+0x110/0x113
Aug 24 08:09:23 secOps kernel: [ 0.000000] setup_arch+0xe4/0xbb6
Aug 24 08:09:23 secOps kernel: [ 0.000000] start_kernel+0x8f/0x3ce
Aug 24 08:09:23 secOps kernel: [ 0.000000] i386_start_kernel+0x91/0x95
```

- 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

```
[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 20:54:08 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).
```

- Kelebihan menggunakan journalctl terletak pada banyaknya pilihan. Gunakan journalctl -utc untuk menampilkan semua cap waktu dalam waktu UTC:

analis@secOps ~\$ sudo journalctl -utc

```
[analyst@secOps ~]$ sudo journalctl --utc
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Tue 2023-03-07 02:33:44 UTC. --
Mar 20 19:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builduser@heftig-18961) (gcc version 7.3.1 20180312 (GCC)) #1 SMP
Mar 20 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 0x0000000003ffff0000-0x0000000003ffffff] 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 0x000a0000-0x0000ffff] usable
Mar 20 19:28:45 secOps kernel: e820: last_pfn = 0x3ffff max_arch_pfn = 0x400000000
Mar 20 19:28:45 secOps kernel: UTPN default type: unresizable
```

11. Gunakan journalctl -b untuk menampilkan entri log yang direkam selama boot terakhir

```
[analyst@secOps ~]$ sudo journalctl -b
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:34:52 EST. --
Mar 06 20:53:40 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 20:53:40 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 06 20:53:40 secOps kernel: KERNEL supported cpus:
Mar 06 20:53:40 secOps kernel: Intel GenuineIntel
Mar 06 20:53:40 secOps kernel: AMD AuthenticAMD
Mar 06 20:53:40 secOps kernel: Hygon HygonGenuine
Mar 06 20:53:40 secOps kernel: Centaur CentaurHauls
Mar 06 20:53:40 secOps kernel: zhaoxin Shanghai
Mar 06 20:53:40 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 20:53:40 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 20:53:40 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 20:53:40 secOps kernel: BIOS-provided physical RAM map:
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000003fffff] usable
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x0000000003ffff0000-0x0000000003ffffff] ACPI data
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011ffffff] usable
Mar 06 20:53:40 secOps kernel: NX (Execute Disable) protection: active
Mar 06 20:53:40 secOps kernel: SMBIOS 2.5 present.
Mar 06 20:53:40 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 20:53:40 secOps kernel: Hypervisor detected: KVM
Mar 06 20:53:40 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 20:53:40 secOps kernel: kvm-clock: cpu 0, msr ad201001, primary cpu clock
Mar 06 20:53:40 secOps kernel: kvm-clock: using sched offset of 10493752944 cycles
Mar 06 20:53:40 secOps kernel: clocksource: kvm clock: mask: 0xffffffffffffff max_cycles: 0x1d423d4fff, max_idle_ns: 89150
```

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

```

[analyst@secOps ~]$ sudo journalctl -u nginx.service --until today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:42:46 EST. --
Mar 23 20:29:25 secOps systemd[1]: Starting A high performance web server and a reverse proxy server...
Mar 23 20:29:25 secOps nginx[1278]: 2018/03/23 20:29:25 [warn] 1278#1278: could not build optimal types_hash, you should inc
Mar 23 20:29:25 secOps systemd[1]: nginx.service: New main PID 1164 does not exist or is a zombie.
Mar 23 20:29:25 secOps systemd[1]: Started A high performance web server and a reverse proxy server.
Mar 23 20:29:38 secOps systemd[1]: Stopping A high performance web server and a reverse proxy server...
Mar 23 20:29:38 secOps systemd[1]: Stopped A high performance web server and a reverse proxy server.
-- Reboot --
May 05 11:09:23 secOps systemd[1]: Starting A high performance web server and a reverse proxy server...
May 05 11:09:23 secOps systemd[1]: Started A high performance web server and a reverse proxy server.
May 05 12:15:41 secOps systemd[1]: Stopping A high performance web server and a reverse proxy server...
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 reverse proxy server.
May 05 12:34:47 secOps systemd[1]: Starting A high performance web server and a reverse proxy server...
May 05 12:34:47 secOps systemd[1]: Started A high performance web server and a reverse proxy server.
May 05 12:39:39 secOps systemd[1]: Stopping A high performance web server and a reverse proxy server...
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 reverse proxy server.
May 05 12:39:39 secOps systemd[1]: Starting A high performance web server and a reverse proxy server...
May 05 12:39:39 secOps nginx[6120]: 2020/05/05 12:39:39 [emerg] 6120#6120: "types_hash_max_size" directive is duplicate in /e
May 05 12:39:39 secOps systemd[1]: nginx.service: Control process exited, code=exited, status=1/FAILURE
May 05 12:39:39 secOps systemd[1]: nginx.service: Failed with result 'exit-code'.
May 05 12:39:39 secOps systemd[1]: Failed to start A high performance web server and a reverse proxy server.
May 05 12:39:52 secOps systemd[1]: Starting A high performance web server and a reverse proxy server...
May 05 12:39:52 secOps nginx[6127]: 2020/05/05 12:39:52 [emerg] 6127#6127: "types_hash_max_size" directive is duplicate in /e
May 05 12:39:52 secOps systemd[1]: nginx.service: Control process exited, code=exited, status=1/FAILURE
May 05 12:39:52 secOps systemd[1]: nginx.service: Failed with result 'exit-code'.
May 05 12:39:52 secOps systemd[1]: Failed to start A high performance web server and a reverse proxy server.
May 05 12:40:45 secOps systemd[1]: Starting A high performance web server and a reverse proxy server...
May 05 12:40:45 secOps systemd[1]: Started A high performance web server and a reverse proxy server.
May 05 12:40:46 secOps nginx[6145]: 2020/05/05 12:40:46 [emerg] 6145#6145: "types_hash_max_size" directive is duplicate in /e

```

13. Gunakan sakelar k untuk hanya menampilkan pesan yang dihasilkan oleh kernel: `analis@secOps ~$ sudo journalctl -k`

```

[analyst@secOps ~]$ sudo journalctl -k
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:45:31 EST. --
Mar 06 20:53:40 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 20:53:40 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 06 20:53:40 secOps kernel: KERNEL supported cpus:
Mar 06 20:53:40 secOps kernel: Intel GenuineIntel
Mar 06 20:53:40 secOps kernel: AMD AuthenticAMD
Mar 06 20:53:40 secOps kernel: Hygon HygonGenuine
Mar 06 20:53:40 secOps kernel: Centaur CentaurHauls
Mar 06 20:53:40 secOps kernel: zhaoxin Shanghai
Mar 06 20:53:40 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 20:53:40 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 20:53:40 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 20:53:40 secOps kernel: BIOS-provided physical RAM map:
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000000ffff] reserved
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x0000000000dfffff] usable
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x000000000dffff0000-0x000000000dffffffffff] ACPI data
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 06 20:53:40 secOps kernel: BIOS-e820: [mem 0x0000000010000000-0x000000001fffffffff] usable
Mar 06 20:53:40 secOps kernel: NX (Execute Disable) protection: active
Mar 06 20:53:40 secOps kernel: SMBIOS 2.5 present.
Mar 06 20:53:40 secOps kernel: DMI: Innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 20:53:40 secOps kernel: Hypervisor detected: KVM
Mar 06 20:53:40 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 20:53:40 secOps kernel: kvm-clock: cpu 0, msr ad201001, primary cpu clock
Mar 06 20:53:40 secOps kernel: kvm-clock: using sched offset of 10493752944 cycles

```

14. Mirip dengan tail k f yang dijelaskan di atas, gunakan saat sedang ditulis: `analis@secOps ~$ sudo journalctl -f`

```

[analyst@secOps ~]$ sudo journalctl -f
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Mar 06 21:45:58 secOps kernel: audit: type=1106 audit(1678157158.063:162): pid=803 uid=0 auid=1000 ses=2 msg='op=PAM:session_c
close grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success
Mar 06 21:45:58 secOps kernel: audit: type=1104 audit(1678157158.063:163): pid=803 uid=0 auid=1000 ses=2 msg='op=PAM:setcred g
rants=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 21:46:08 secOps audit[812]: USER_ACCT pid=812 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 21:46:08 secOps sudo[812]: analyst : TTY=pts/0 ; PWD=/home/analyst ; USER=root ; COMMAND=/usr/bin/journalctl -f
Mar 06 21:46:08 secOps kernel: audit: type=1101 audit(1678157168.603:164): pid=812 uid=1000 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=success
s'
Mar 06 21:46:08 secOps audit[812]: CRED_REFR pid=812 uid=0 auid=1000 ses=2 msg='op=PAM:setcred grantors=pam_unix,pam_permit,p
am_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 21:46:08 secOps sudo[812]: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 06 21:46:08 secOps audit[812]: USER_START pid=812 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 21:46:08 secOps kernel: audit: type=1110 audit(1678157168.606:165): pid=812 uid=0 auid=1000 ses=2 msg='op=PAM:setcred g
rants=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 21:46:08 secOps kernel: audit: type=1105 audit(1678157168.606:166): pid=812 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'

```

E. Pembahasan

Pada praktikum kali ini yang membahas tentang Steganografi yang merupakan ilmu menulis pesan tersembunyi sedemikian rupa sehingga tidak ada seorang pun selain pengirim dan penerima yang dituju yang menyadari ada pesan tersembunyi. Praktikum kali ini menggunakan aplikasi QuickStego yang memungkinkan kita menyembunyikan teks dalam gambar sehingga hanya pengguna QuickStego lain yang dapat mengambil dan membaca pesan rahasia yang tersembunyi. Setelah teks disembunyikan dalam gambar, gambar yang disimpan masih berupa 'gambar', itu akan dimuat seperti gambar lainnya dan muncul seperti sebelumnya. Gambar dapat disimpan, dikirim melalui email, diunggah ke web (, satu-satunya perbedaan adalah berisi teks tersembunyi. Kita juga menginstall file MD5sum yang menghitung intisari pesan MD5 untuk stau atau beberapa file. 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. Setelah menginstall, kita memasukkan gambar dan masukkan pesan dan klik hide text dan save gambar yang sudah dimasukkan text tersembunyi. Nantinya pada command prompt melalui md5sums kita dapat mengetahui gambar mana yang mempunyai pesan teks tersembunyi dari ukuran filenya yang lebih besar dibandingkan aslinya.

Unit 6

Pada praktikum kali ini yaitu 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 untuk membaca dan menampilkan konten file di layar. Karena kemudahannya dan dapat membuka file teks dan menampilkannya di terminal teks saja, maka **cat** banyak digunakan. Kelemahan menggunakan **cat** yaitu datar kata tidak dapat diubah. Perbedaan utama antara **cat** dan **more** adalah lebih mendukung page break, memungkinkan pengguna untuk melihat konten file, satu halaman dalam satu waktu. Ini dapat dilakukan dengan menggunakan tombol spasi untuk menampilkan halaman berikutnya. Kelemahan menggunakan **more**. Membangun fungsionalitas **cat** dan lebih banyak lagi, alat yang lebih sedikit memungkinkan konten file ditampilkan halaman demi halaman, sementara juga memungkinkan pengguna memilih untuk melihat halaman yang ditampilkan sebelumnya. Perintah **less** adalah perintah yang digunakan untuk menampilkan isi file secara paginated di terminal. Ini berguna jika file terlalu besar

untuk ditampilkan sekaligus di terminal, sehingga Anda dapat menelusuri isi file secara per page. Perintah **tail** menampilkan akhir file teks. Secara default, tail menampilkan sepuluh baris terakhir file. Untuk memudahkan visualisasi, pilih jendela terminal atas (yang menjalankan tail -f) dan tekan enter beberapa kali. Ini akan menambahkan beberapa baris antara konten file saat ini dan informasi baru yang akan ditambahkan. Perintah echo digunakan untuk menambahkan pesan pada file yang ingin kita tambahkan.

File log dapat dijadikan dalam satu server agar lebih mudah dalam pemantauannya. Syslog adalah sistem yang dirancang agar perangkat dapat mengirim file log ke server, yang dikenal sebagai server syslog. Klien berkomunikasi ke server syslog menggunakan protokol syslog. Gunakan perintah cat sebagai root untuk membuat daftar isi file. File ini menyimpan entri log yang dihasilkan oleh sistem operasi CyberOps Workstation VM dan dikirim ke layanan syslog. 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. 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 menafsirkan dan menampilkan entri log yang sebelumnya disimpan dalam file log biner jurnal. Kelebihan menggunakan journalctl terletak pada banyaknya pilihan. Gunakan journalctl -b untuk menampilkan entri log yang direkam selama boot terakhir. Gunakan journalctl untuk menentukan layanan dan kerangka waktu untuk entri log. Lalu gunakan sakelar -k untuk hanya menampilkan pesan yang dihasilkan oleh kernel, dan gunakan -f untuk secara aktif mengikuti log saat sedang ditulis.

F. Kesimpulan

Kesimpulan pada praktikum kali ini antara lain :

1. Steganografi yang merupakan ilmu menulis pesan tersembunyi sedemikian rupa sehingga tidak ada seorang pun selain pengirim dan penerima yang dituju yang menyadari ada pesan tersembunyi.
2. MD5sum yang menghitung intisari pesan MD5 untuk stau atau beberapa file. 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.
3. File log adalah file yang digunakan untuk merekam peristiwa tertentu yang dihasilkan oleh aplikasi, layanan, atau sistem operasi itu sendiri.
4. Fitur cat, berasal dari kata 'concatenate', alat berbasis baris perintah yang digunakan untuk membaca dan menampilkan konten file di layar.

G. Daftar Pustaka

Free Steganography Software - QuickStego. (2017). Quickcrypto.com.

<http://quickcrypto.com/free-steganography-software.html>

MD5sums for Windows. (n.d.). Wwww.pc-Tools.net. Retrieved March 12, 2023,

from <http://www.pc-tools.net/win32/md5sums/>