

LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1
Pertemuan 4 – Teknik Steganografi dan Analisis *Log Server*



DISUSUN OLEH

Nama : Sofiyanatul Munawaroh
NIM : 21/474781/SV/19035
Hari, Tanggal : Selasa, 7 Maret 2023
Kelas : RI4AA

LABORATORIUM PERANGKAT KERAS DAN LUNAK
PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI
REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

Praktikum Keamanan Informasi 1

Pertemuan 4 – Teknik Steganografi dan Analisis *Log Server*

I. Tujuan

- Mengeksplorasi steganografi.
- Membaca *File Log* dengan *Cat*, *More*, *Less*, dan *Tail*.
- Memahami *File Log* dan *Syslog*.
- Memahami *File Log* dan *Jurnalctl*.

II. Latar Belakang

Steganografi atau *Steganography* adalah sebuah ilmu, teknik atau seni menyembunyikan sebuah pesan rahasia dengan suatu cara sehingga pesan tersebut hanya akan diketahui oleh si pengirim dan si penerima pesan rahasia tersebut. Steganografi berasal dari Bahasa Yunani yaitu *Stegano* yang berarti “tersembunyi atau menyembunyikan” dan *graphy* yang berarti “Tulisan, jadi Steganografi adalah tulisan atau pesan yang disembunyikan. Steganografi kebalikannya kriptografi yang menyamarkan arti dari sebuah pesan rahasia saja, tetapi tidak menyembunyikan bahwa ada sebuah pesan. Kelebihan Steganografi dibandingkan dengan Kriptografi adalah pesan-pesannya akan dibuat tidak menarik perhatian dan tidak menimbulkan kecurigaan, berbeda dengan Kriptografi yang pesannya tidak disembunyikan, walaupun pesannya sulit untuk dipecahkan akan tetapi itu akan menimbulkan kecurigaan pesan tersebut.

Pesan rahasia yang akan disembunyikan akan disisipkan pada suatu media penampung seperti citra, suara, video dan sebagainya yang terlihat tidak mencurigakan untuk menyimpan pesan rahasia. Pesan rahasia akan memerlukan sebuah kunci rahasia yang dinamakan *stego-key* agar hanya pihak yang berhak saja yang dapat membuka atau mengekstrak pesan rahasia tersebut.

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.

III. Alat dan Bahan

- *Software Quick Stego*
- MD5SUMS
- *Cyberops Workstation Virtual Machine*
- Laptop
- Koneksi Internet

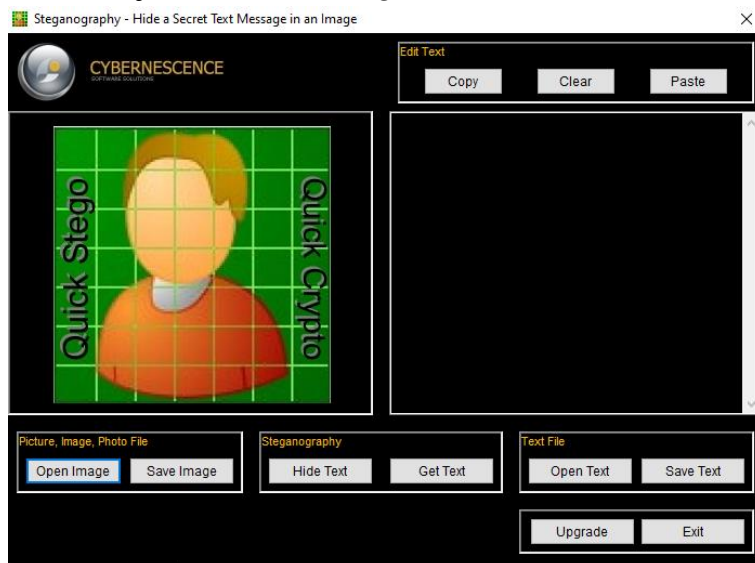
IV. Instruksi Kerja

a. Teknik Steganografi

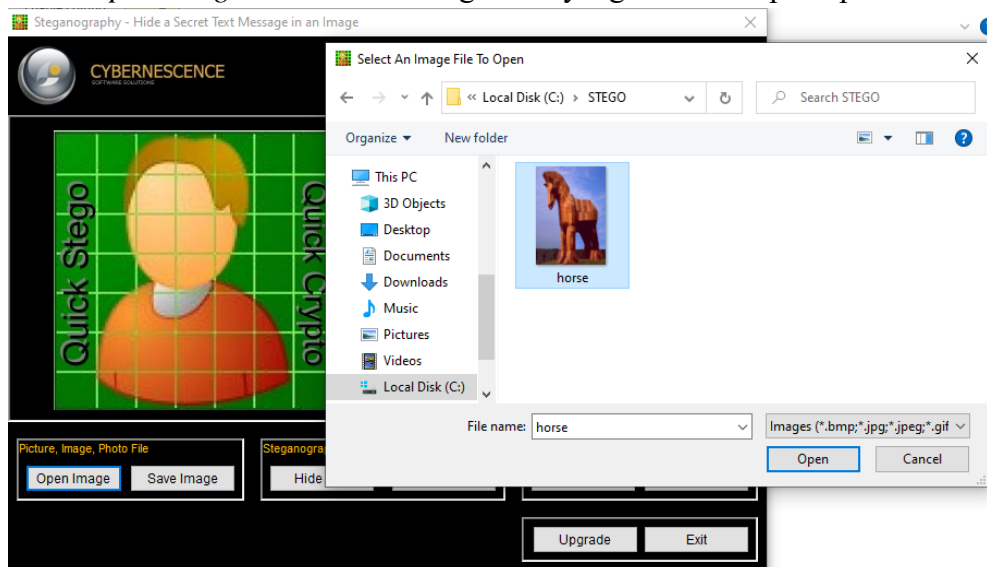
1. Unduh *software Quick Stego* melalui *link* di bawah ini.

<http://quickcrypto.com/products/QS12Setup.zip>

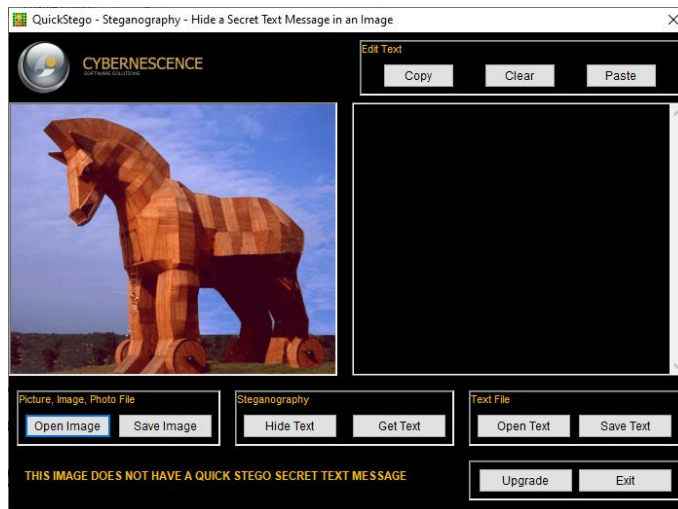
2. Buka *file* hasil unduhan, lalu *Extract File*.
3. Instal *Quick Stego*.
4. Buat *folder* khusus pada direktori C:\ dengan nama STEGO.
5. Unduh *tools* MD5SUM melalui *link* di bawah ini.
<http://www.pc-tools.net/files/win32/freeware/md5sums-1.2.zip>
6. Arahkan unduhan ke *folder* yang telah dibuat, lalu *Extract*.
7. Instal MD5SUMS.
8. Unduh gambar1 pada *link* yang telah disediakan.
9. Buka dan jalankan *Quick Stego*.



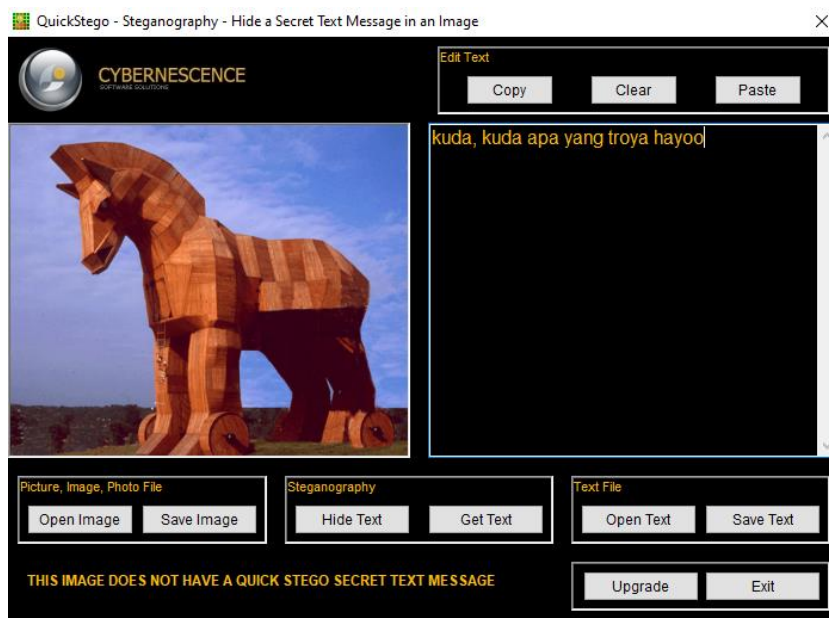
10. Pilih '*Open Image*' untuk memilih gambar yang akan disisipkan pesan rahasia.



11. Setelah klik '*Open*', gambar akan ter-upload.



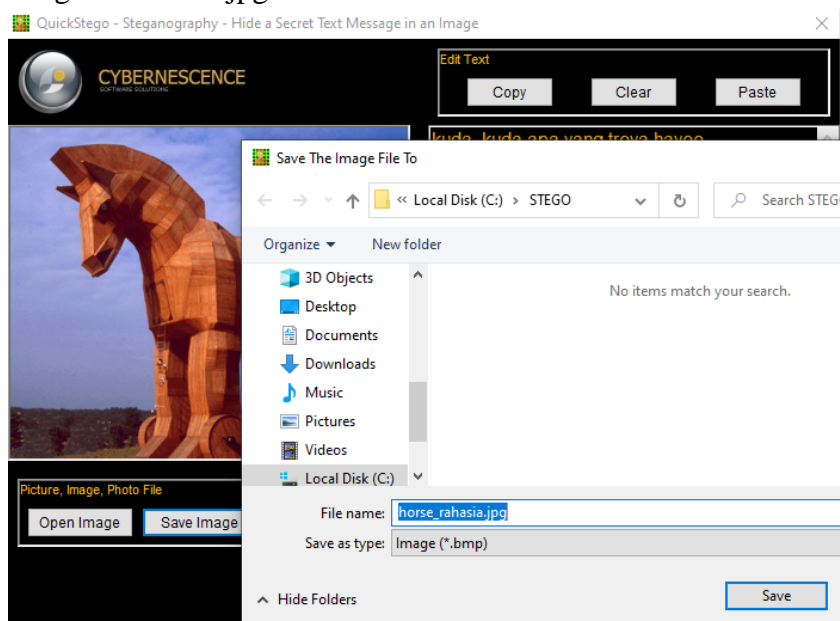
12. Tulis pesan rahasia yang akan disisipkan pada gambar di kolom hitam sebelah kanan.



13. Pilih 'Hide Text' untuk menyisipkan pesan rahasia ke dalam gambar. Jika sudah maka akan muncul notifikasi "The text message is now hidden in image".



14. Pilih 'Save Image' untuk menyimpan gambar yang telah disisipkan pesan rahasia dengan ekstensi .jpg.



15. Buka CMD, lalu arahkan ke direktori C:\STEGO. Lihat ukuran *byte files* pada *file* gambar yang belum dan sudah disisipkan pesan rahasia.

```

C:\> Command Prompt

Microsoft Windows [Version 10.0.19045.2604]
(c) Microsoft Corporation. All rights reserved.

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

C:\STEGO>dir *.jpg
Volume in drive C has no label.
Volume Serial Number is C0A7-7589

Directory of C:\STEGO

07/03/2023  08:31                46.001 horse.jpg
07/03/2023  08:37            854.454 horse_rahasia.jpg
               2 File(s)             900.455 bytes
               0 Dir(s)  274.577.670.144 bytes free
  
```

16. Lalu ketikkan `md5sums.exe *.jpg` untuk menampilkan semua *hashtag file* dengan ekstensi `.jpg`.

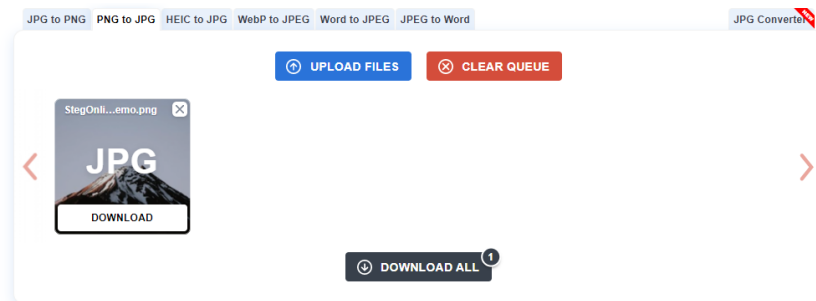
```
C:\STEGO>md5sums.exe *.jpg

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

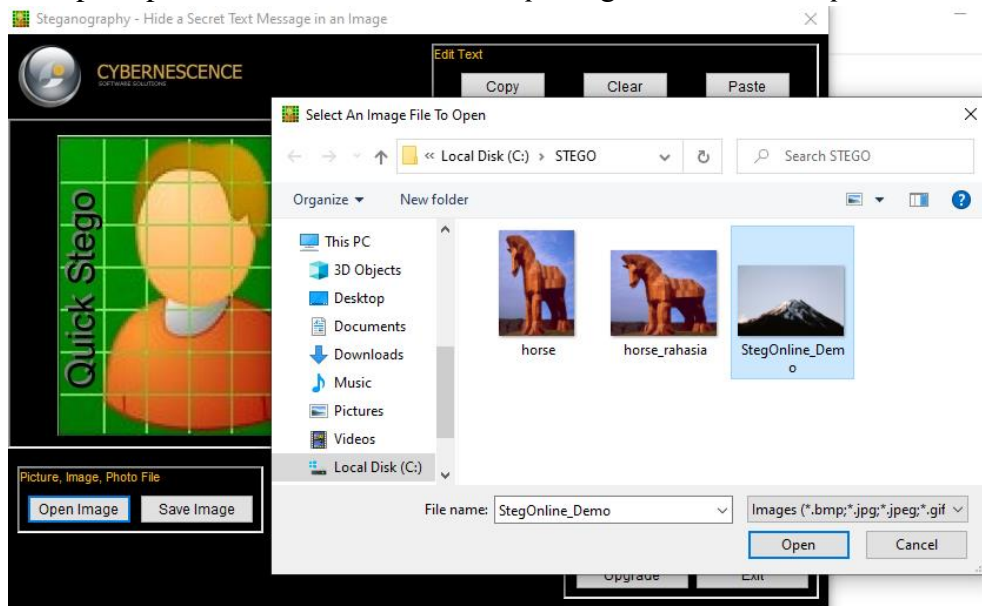
[Path] / filename                                MD5 sum
-----
[C:\STEGO\]
horse.jpg                                         fce8552170cccd3dd545566309124097
horse_rahasia.jpg                             98e91a4377e09a2533bb781674d4d1a1

C:\STEGO>
```

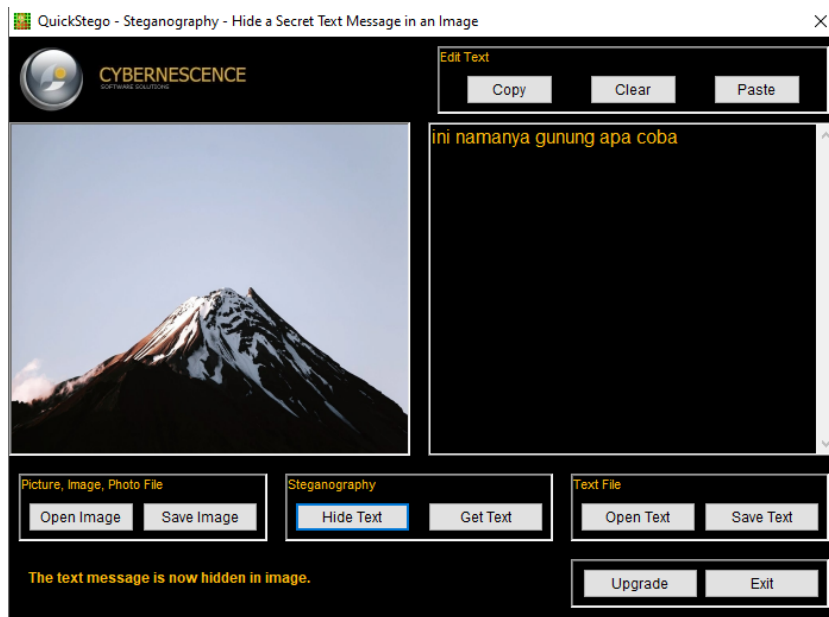
17. Lakukan hal yang sama pada gambar 2.
18. Unduh gambar2 pada *link* yang telah disediakan.
19. Karena gambar 2 merupakan format `.png`, maka *convert* terlebih dahulu ke `.jpg` agar bisa di-*upload*.



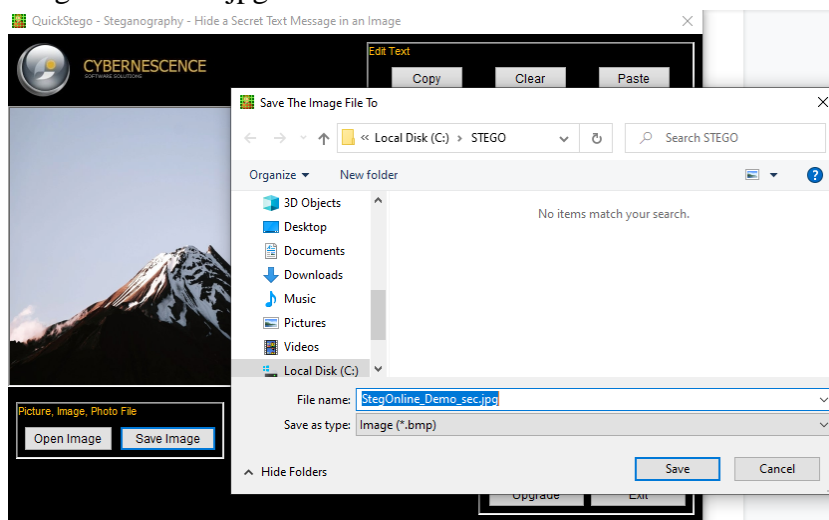
20. Jalankan *Quick Stego*. Pilih ‘*Open Image*’ untuk memilih gambar yang akan disisipkan pesan rahasia. Setelah klik ‘*Open*’, gambar akan ter-*upload*.



21. Tulis pesan rahasia yang akan disisipkan pada gambar di kolom hitam sebelah kanan. Pilih ‘*Hide Text*’ untuk menyisipkan pesan rahasia ke dalam gambar. Jika sudah maka akan muncul notifikasi “*The text message is now hidden in image*”.



22. Pilih 'Save Image' untuk menyimpan gambar yang telah disisipkan pesan rahasia dengan ekstensi .jpg.



23. Buka CMD, lalu arahkan ke direktori C:\STEGO. Lihat ukuran *byte files* pada *file* gambar yang belum dan sudah disisipkan pesan rahasia.

```
C:\STEGO>dir *.jpg
Volume in drive C has no label.
Volume Serial Number is C0A7-7589

Directory of C:\STEGO

07/03/2023  08:31             46.001 horse.jpg
07/03/2023  08:37          854.454 horse_rahasia.jpg
07/03/2023  08:45           48.590 StegOnline_Demo.jpg
07/03/2023  08:50        1.998.054 StegOnline_Demo_sec.jpg
               4 File(s)      2.947.099 bytes
               0 Dir(s)  274.574.901.248 bytes free
```

24. Lalu ketikkan md5sums.exe * .jpg untuk menampilkan semua *hashtag file* dengan ekstensi .jpg.


```
Command Prompt

C:\STEGO>md5sums.exe *.jpg

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

[Path] / filename                                MD5 sum
-----
[C:\STEGO\]
horse.jpg                                         fce8552170cced3dd545566309124097
horse_rahasia.jpg                               98e91a4377e09a2533bb781674d4d1a1
StegOnline_Demo.jpg                             9f3b7b4b200da9fe48d4c38b9935a890
StegOnline_Demo_sec.jpg                         ed37c39c1b447025f559c068f757955e
```

b. Log Server

1. Buka VM *CyberOps Workstation*.
2. Lakukan pengujian pembacaan *file log* dengan CAT.

```
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-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/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"
```

3. Lakukan pengujian pembacaan *file log* dengan *More*.


```
[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-monito
rama-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-monito
rama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplete.
com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac O
S 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-monito
rama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplete.
com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac O
S 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-monito
rama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/pres
entations/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-monito
rama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/prese
ntations/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-monito
--More-- (6%)
```

```
Mac OS X 10_8_2) App
ri/537.36"
71.212.224.97 - - [0
--More-- (84%)
```

4. Lakukan pengujian pembacaan *file log* dengan *Less*.

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

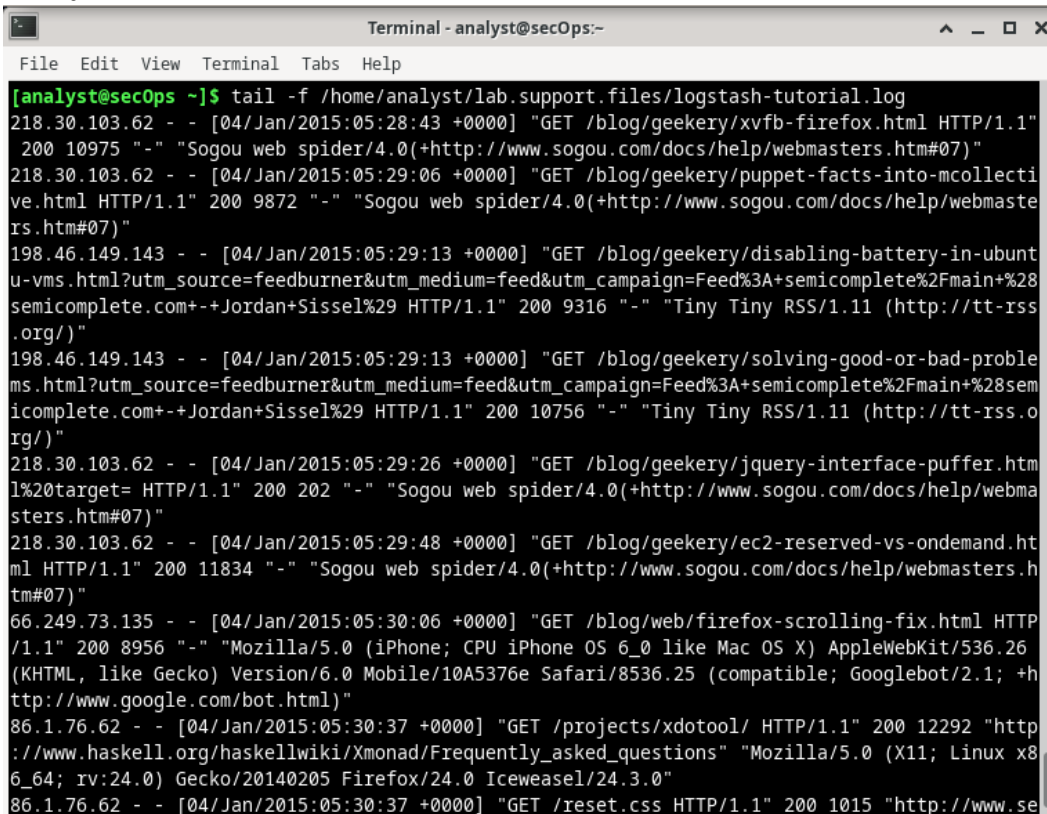
```
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monito
rama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.com/
presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X
10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monito
rama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplete.
com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac O
S 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-monito
rama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplete.
com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac O
S 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-monito
rama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/pres
entations/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-monito
rama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/prese
ntations/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-monito
rama-2013/images/sad-medic.png HTTP/1.1" 200 430406 "http://semicomplete.com/pres
entations/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-monito
/home/analyst/lab.support.files/logstash-tutorial.log
```

5. Lakukan pengujian pembacaan *file log* dengan *Tail* dan *Tail -f*.

Tail

```
[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-mcollecti
ve.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmaste
rs.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ubunt
u-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28
semicomplete.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-proble
ms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28sem
icomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.o
rg/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.htm
l%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webma
sters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand.ht
ml HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.h
tm#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; +h
ttp://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 x8
6_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
```

Tail -f



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

[analyst@secOps ~]$ tail -f /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1"
 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollecti
ve.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmaste
rs.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ubunt
u-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28
semicomplete.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-proble
ms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28sem
icomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.o
rg/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.htm
l%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webma
sters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand.ht
ml HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.h
tm#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; +h
ttp://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 x8
6_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.se
```

6. Buka 2 jendela terminal dan lakukan *split screen*. Lalu pada salah satu jendela, jalankan *tail -f /home/analyst/lab.support.files/logstash-tutorial.log*.

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

&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&ut
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 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"
[analyst@secOps ~]$
```

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

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 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"
[analyst@secOps ~]$
```

7. Kemudian pada jendela lain, jalankan `echo "ini adalah entri baru untuk file log yang dipantau tapi part 2" >> /home/analyst/lab.support.files/logstash-tutorial.log`.

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

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&ut
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 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"
ini adalah entri baru untuk file log yang dipantau
[analyst@secOps ~]$
```

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

(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 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"
^Z
[1]+  Stopped                  tail -f /home/analyst/lab.support.files/logstash-tutorial.log
[analyst@secOps ~]$ echo "ini adalah entri baru untuk file log yang dipantau" >> lab.support.files/logstash-tutorial.log
[analyst@secOps ~]$
```


8. Jalankan `sudo cat /var/log/syslog.1`

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
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 serio1: hgpk: ID: 10 00 64
Apr 20 06:10:55 secOps kernel: [ 2.986439] input: ImEXPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input/
input6
Apr 20 06:10:55 secOps kernel: [ 3.009683] mousedev: PS/2 mouse device common for all mice
Apr 20 06:10:55 secOps kernel: [ 4.721266] nf_conntrack version 0.5.0 (16384 buckets, 65536 max)
Apr 20 06:10:55 secOps kernel: [ 4.979025] openvswitch: Open vSwitch switching datapath
[analyst@secOps ~]$
```

Jalankan `sudo cat /var/log/syslog.2`

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
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/
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) relea
se 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 201
8
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 ~]$
```

Jalankan `sudo cat /var/log/syslog.3`

```
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
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 pp1-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) rele
ase 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 20
17
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/
input7
Mar 6 11:58:56 secOps kernel: [ 6.016025] openvswitch: Open vSwitch switching datapath
[analyst@secOps ~]$
```

Jalankan `sudo cat /var/log/syslog.4`

```
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
Nov 29 04:30:38 secOps kernel: [ 5.980014] input: Sleep Button as /devices/LNXSYSTM:00/LNXSLPBN:00/input/input5
Nov 29 04:30:38 secOps kernel: [ 5.985142] ACPI: Sleep Button [SLPF]
Nov 29 04:30:38 secOps kernel: [ 5.992292] openvswitch: Open vSwitch switching datapath
Nov 29 04:30:38 secOps kernel: [ 6.013723] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
Nov 29 04:30:38 secOps kernel: [ 6.014218] pcnet32: PCnet/FAST III 79C973 at 0xd000, 08:00:27:23:b2:31 assigned IRQ 19
Nov 29 04:30:38 secOps kernel: [ 6.014265] pcnet32: Found PHY 0022:561b at address 0
Nov 29 04:30:38 secOps kernel: [ 6.014587] pcnet32: eth0: registered as PCnet/FAST III 79C973
Nov 29 04:30:38 secOps kernel: [ 6.014605] pcnet32: 1 cards_found
Nov 29 04:30:38 secOps kernel: [ 6.064002] input: PC Speaker as /devices/platform/pcspkr/input/input6
Nov 29 04:30:38 secOps kernel: [ 6.142925] RAPL PMU: API unit is 2^32 Joules, 5 fixed counters, 10737418240 ms ovfl 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 pp1-gpu 2^0 Joules
Nov 29 04:30:38 secOps kernel: [ 6.142929] RAPL PMU: hw unit of domain psys 2^0 Joules
Nov 29 04:30:38 secOps kernel: [ 6.180343] VBoxService 5.1.18 r114002 (verbosity: 0) linux.x86 (Mar 16 2017 20:50:16) rele
ase 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 20
17
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/
input7
[analyst@secOps ~]$
```

9. Jalankan `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 20:56:29 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...
```

Kemudian jalankan *sudo journalctl -utc*

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ journalctl --utc
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 20:10:08 UTC, end at Tue 2023-03-07 01:56:29 UTC. --
Mar 20 20:10:08 secOps systemd[363]: Listening on GnuPG network certificate management daemon.
Mar 20 20:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 20:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Mar 20 20:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache.
Mar 20 20:10:08 secOps systemd[363]: Reached target Paths.
Mar 20 20:10:08 secOps systemd[363]: Reached target Timers.
Mar 20 20:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache (access for web browsers).
Mar 20 20:10:08 secOps systemd[363]: Starting D-Bus User Message Bus Socket.
Mar 20 20:10:08 secOps systemd[363]: Listening on D-Bus User Message Bus Socket.
Mar 20 20:10:08 secOps systemd[363]: Reached target Sockets.
Mar 20 20:10:08 secOps systemd[363]: Reached target Basic System.
Mar 20 20:10:08 secOps systemd[363]: Reached target Default.
Mar 20 20:10:08 secOps systemd[363]: Startup finished in 34ms.
Mar 20 20:10:21 secOps systemd[363]: Stopped target Default.
Mar 20 20:10:21 secOps systemd[363]: Stopped target Basic System.
Mar 20 20:10:21 secOps systemd[363]: Stopped target Paths.
Mar 20 20:10:21 secOps systemd[363]: Stopped target Timers.
Mar 20 20:10:21 secOps systemd[363]: Stopped target Sockets.
Mar 20 20:10:21 secOps systemd[363]: Closed D-Bus User Message Bus Socket.
Mar 20 20:10:21 secOps systemd[363]: Closed GnuPG network certificate management daemon.
Mar 20 20:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache.
Mar 20 20:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache (access for web browsers).
Mar 20 20:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent (ssh-agent emulation).
Mar 20 20:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 20:10:21 secOps systemd[363]: Reached target Shutdown.
Mar 20 20:10:21 secOps systemd[363]: Starting Exit the Session...
```

Jalankan juga *sudo journalctl -b*


```
[analyst@secOps ~]$ journalctl -b
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 20:56:29 EST. --
Mar 06 20:56:19 secOps systemd[373]: Reached target Paths.
Mar 06 20:56:19 secOps systemd[373]: Reached target Timers.
Mar 06 20:56:19 secOps systemd[373]: Starting D-Bus User Message Bus Socket.
Mar 06 20:56:19 secOps systemd[373]: Listening on GnuPG network certificate management daemon.
Mar 06 20:56:19 secOps systemd[373]: Listening on GnuPG cryptographic agent and passphrase cache (access for web browsers).
Mar 06 20:56:19 secOps systemd[373]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Mar 06 20:56:19 secOps systemd[373]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Mar 06 20:56:19 secOps systemd[373]: Listening on GnuPG cryptographic agent and passphrase cache.
Mar 06 20:56:19 secOps systemd[373]: Listening on p11-kit server.
Mar 06 20:56:19 secOps systemd[373]: Listening on D-Bus User Message Bus Socket.
Mar 06 20:56:19 secOps systemd[373]: Reached target Sockets.
Mar 06 20:56:19 secOps systemd[373]: Reached target Basic System.
Mar 06 20:56:19 secOps systemd[373]: Reached target Main User Target.
Mar 06 20:56:19 secOps systemd[373]: Startup finished in 144ms.
Mar 06 20:56:19 secOps systemd[373]: Started D-Bus User Message Bus.
Mar 06 20:56:19 secOps dbus-daemon[383]: [session uid=1000 pid=383] Activating via systemd: service name='org.a11y.Bus' unit=
Mar 06 20:56:19 secOps systemd[373]: Starting Accessibility services bus...
Mar 06 20:56:19 secOps dbus-daemon[383]: [session uid=1000 pid=383] Successfully activated service 'org.a11y.Bus'
Mar 06 20:56:19 secOps systemd[373]: Started Accessibility services bus.
Mar 06 20:56:19 secOps dbus-daemon[383]: [session uid=1000 pid=383] Activating service name='org.xfce.Xfconf' requested by
Mar 06 20:56:19 secOps dbus-daemon[383]: [session uid=1000 pid=383] Successfully activated service 'org.xfce.Xfconf'
Mar 06 20:56:19 secOps at-spi-bus-launcher[398]: dbus-daemon[398]: Activating service name='org.a11y.atspi.Registry' request
Mar 06 20:56:19 secOps at-spi-bus-launcher[398]: dbus-daemon[398]: Successfully activated service 'org.a11y.atspi.Registry'
Mar 06 20:56:20 secOps at-spi-bus-launcher[407]: SpiRegistry daemon is running with well-known name - org.a11y.atspi.Registry
Mar 06 20:56:20 secOps systemd[373]: Started GnuPG cryptographic agent and passphrase cache.
Mar 06 20:56:20 secOps gpg-agent[424]: gpg-agent (GnuPG) 2.2.20 starting in supervised mode.
```

10. Jalankan `sudo journalctl -u nginx.service -since today`

```
[analyst@secOps ~]$ sudo journalctl -u nginx.service --since today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 22:00:07 EST. --
-- No entries --
[analyst@secOps ~]$
```

11. Jalankan `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 22:01:20 EST. --
Mar 06 20:56:00 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 20:56:00 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 ip=
Mar 06 20:56:00 secOps kernel: KERNEL supported cpus:
Mar 06 20:56:00 secOps kernel: Intel GenuineIntel
Mar 06 20:56:00 secOps kernel: AMD AuthenticAMD
Mar 06 20:56:00 secOps kernel: Hygon HygonGenuine
Mar 06 20:56:00 secOps kernel: Centaur CentaurHauls
Mar 06 20:56:00 secOps kernel: zhaoxin Shanghai
Mar 06 20:56:00 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 20:56:00 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 20:56:00 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 20:56:00 secOps kernel: BIOS-provided physical RAM map:
Mar 06 20:56:00 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable
Mar 06 20:56:00 secOps kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
Mar 06 20:56:00 secOps kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Mar 06 20:56:00 secOps kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000003ffff] usable
Mar 06 20:56:00 secOps kernel: BIOS-e820: [mem 0x0000000003ffff000-0x0000000003ffffffffff] ACPI data
Mar 06 20:56:00 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 20:56:00 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 20:56:00 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 06 20:56:00 secOps kernel: NX (Execute Disable) protection: active
Mar 06 20:56:00 secOps kernel: SMBIOS 2.5 present.
Mar 06 20:56:00 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 20:56:00 secOps kernel: Hypervisor detected: KVM
Mar 06 20:56:00 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 20:56:00 secOps kernel: kvm-clock: cpu 0, msr 5e01001, primary cpu clock
Mar 06 20:56:00 secOps kernel: kvm-clock: using sched offset of 10651588185 cycles
Mar 06 20:56:00 secOps kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 8815>
```

12. Jalankan `sudo journalctl -f`


```
[analyst@secOps ~]$ sudo journalctl -f
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Mar 06 22:02:06 secOps kernel: audit: type=1106 audit(1678158126.846:109): pid=713 uid=0 auid=1000 ses=2 msg='op=PAM:session_
close grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succe
ss'
Mar 06 22:02:06 secOps kernel: audit: type=1104 audit(1678158126.846:110): pid=713 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 22:02:10 secOps audit[720]: USER_ACCT pid=720 uid=0 auid=1000 ses=2 msg='op=PAM:accounting grantors=pam_unix,pam_pe
rmit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 22:02:10 secOps sudo[720]: analyst : TTY=pts/0 ; PWD=/home/analyst ; USER=root ; COMMAND=/usr/bin/journalctl -f
Mar 06 22:02:10 secOps audit[720]: CRED_REFR pid=720 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 22:02:10 secOps sudo[720]: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 06 22:02:10 secOps audit[720]: USER_START pid=720 uid=0 auid=1000 ses=2 msg='op=PAM:session_open grantors=pam_limits,pam_
unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 22:02:10 secOps kernel: audit: type=1101 audit(1678158130.946:111): pid=720 uid=1000 auid=1000 ses=2 msg='op=PAM:accou
nting grantors=pam_unix,pam_permit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succ
ess'
Mar 06 22:02:10 secOps kernel: audit: type=1110 audit(1678158130.946:112): pid=720 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 22:02:10 secOps kernel: audit: type=1105 audit(1678158130.946:113): pid=720 uid=0 auid=1000 ses=2 msg='op=PAM:session_
open grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succes
s'
```

V. Hasil dan Pembahasan

Pada praktikum ini terdapat 2 modul praktikum, yaitu Teknik Steganografi dan Analisis Log Server. Praktikum pertama yaitu Teknik Steganografi, steganografi sendiri merupakan sebuah ilmu menulis sekaligus seni untuk menyembunyikan suatu pesan rahasia sehingga keberadaan pesan tersebut menjadi tidak dapat diketahui. Dimana pada praktikum ini, mahasiswa akan melakukan pengujian untuk menyembunyikan informasi atau pesan rahasia dalam sebuah gambar. *Tools* yang digunakan adalah *Quick Stego* dan MD5SUM. *Quick Stego* adalah *software* yang digunakan untuk menyembunyikan pesan dalam media gambar berekstensi .bmp, .jpg, .jpeg, dan .gif. Sehingga ketika ingin menyembunyikan pesan pada gambar dengan ekstensi yang berbeda, maka harus di-*convert* terlebih dahulu dengan ekstensi yang sesuai seperti yang dilakukan pada gambar 2.

Sedangkan MD5SUM digunakan untuk menampilkan *hash* dari suatu *file*. Dari hasil praktikum yang telah dilaksanakan dapat dilihat bahwa ketika terdapat tambahan informasi atau pesan rahasia yang disembunyikan menggunakan *software Quick Stego*, maka *hash* dari *file* gambar yang telah disisipkan pesan rahasia akan berbeda dengan *file* aslinya.

```
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 - Copy.jpg                                fce8552170cced3dd545566309124097
horse.jpg                                       fce8552170cced3dd545566309124097
horse_rahasia.jpg                             98e91a4377e09a2533bb781674d4d1a1
StegOnline_Demo.jpg                           9f3b7b4b200da9fe48d4c38b9935a890
StegOnline_Demo_sec.jpg                       ed37c39c1b447025f559c068f757955e
```

Dapat dilihat juga bahwa ketika hanya melakukan *copy – paste* terhadap suatu *file*, maka *hash* dari kedua *file* tersebut tetap sama karena tidak ada informasi dari *file* yang diubah. Seperti pada *file* horse.jpg dan horse – Copy.jpg, kedua *file* tersebut memiliki *hash* yang sama.

Selanjutnya praktikum kedua adalah menjalankan dan membaca *file log server* dengan beberapa perintah seperti *cat*, *more*, *less*, atau *tail*. Pengujian pertama adalah membaca menggunakan *cat*. *Cat* sendiri merupakan akronim dari *concatenate* yang berfungsi untuk mencantumkan, menggabungkan, dan menulis konten atau isi *file* dalam *output* standar. Untuk menjalankan *command* ini, ketik *cat* diikuti nama dan ekstensi *file*. Kelemahan perintah ini yaitu jika digunakan untuk *preview* isi *file* yang memiliki banyak tulisan atau *file* teks besar, karena *cat* akan melakukan *review* semua isi *file* hingga teks atau karakter terakhir, sehingga jika digunakan untuk mengoreksi hasil tulisan akan mengalami kendala. Hal ini karena pengguna kesulitan dalam melihat isi *file* awal.

Perintah kedua adalah *more*. *More* memiliki kesamaan fungsi dengan perintah *cat*. Perbedaannya terdapat saat melakukan *review* isi *file*. Pada *more* untuk melihat isi *file* dilakukan secara bertahap dengan dibatasi setiap 1 halaman. Untuk melihat isi *file* berikutnya dapat dengan *enter* untuk tiap 1 baris selanjutnya atau dengan spasi untuk tiap 1 halaman selanjutnya. Kelemahan dari perintah ini adalah hanya dapat melihat isi *file* selanjutnya dan tidak dapat melihat kembali isi *file* di halaman sebelumnya.

Perintah ketiga adalah *less*, dimana perintah ini juga memiliki fungsi yang sama seperti dua perintah sebelumnya. Bedanya *less* memungkinkan isi *file* ditampilkan halaman demi halaman, serta dapat melihat kembali isi *file* pada halaman sebelum ataupun setelahnya.

Perintah keempat adalah *tail* yang berfungsi untuk menampilkan 10 baris terakhir secara *default* dari satu atau lebih *file* atau data yang disalurkan. Perintah ini juga dapat digunakan untuk memantau perubahan *file* secara *real time* hanya dengan menambahkan opsi *-f* (*--follow*) setelah *command tail*. Opsi ini sangat berguna untuk memonitor *file log*. Pada pengujiannya, dicoba untuk menambahkan teks menggunakan *command echo* ke *file* dan saat dibaca menggunakan opsi *-f* isi *file* otomatis ter-update.

Selanjutnya adalah memahami *syslog* atau *System Logging Protocol* merupakan protokol standar yang digunakan untuk mengirim pesan peristiwa atau *log* sistem ke server tertentu. Untuk menampilkan isi *file syslog* pada praktikum ini menggunakan *cat* dan harus dijalankan sebagai *root* karena direktori */var/log/syslog* berada dalam direktori *root*. Untuk menghindari *file syslog* yang terlalu besar, sistem operasi secara berkala biasanya akan mengganti nama *file syslog*. Agar dapat diketahui waktu aktivitas dari suatu *file syslog*, maka kita perlu melakukan sinkronisasi waktu dan tanggal dengan benar.

Kemudian terdapat *tools journald* yang memiliki perintah dasar *journalctl*. *Journald* adalah program sistem dari *systemd* yaitu alat yang mengumpulkan data dari beberapa *log* dalam format biner. Perintah ini digunakan untuk menampilkan semua catatan *log* jurnal dari entri terlama. Kelebihan menggunakan *journalctl* yaitu perintah ini memiliki banyak pilihan (*option*) untuk menjalankan perintah tersebut. Salah satunya adalah opsi *-utc* untuk menampilkan semua cap waktu dalam waktu UTC. Lalu ada opsi *-b* untuk menampilkan entri *log* yang direkam selama *boot* terakhir.

Perintah *journalctl* juga dapat dikombinasikan dengan opsi *filtering* agar hanya menampilkan pesan tertentu. Seperti memungkinkan pengguna untuk mendapatkan catatan *log* dari periode tertentu, misalnya jika ingin mendapatkan catatan *log* hari ini maka tambahkan opsi *--since today* setelah *command*. Selanjutnya terdapat opsi *-k* untuk

hanya menampilkan pesan yang dihasilkan oleh kernel. Serta jika ingin menampilkan *log* jurnal secara *real-time* dapat menggunakan opsi -f.

VI. Kesimpulan

1. Teknik steganografi berguna untuk menyembunyikan pesan rahasia pada sebuah *file*.
2. Saat meng-*upload* gambar pada *Quick Stego* harus menyesuaikan format yang dapat diterima oleh *software*.
3. *File* yang telah disisipkan pesan rahasia dan *file* aslinya akan memiliki *hash* yang berbeda karena terdapat perubahan informasi di dalamnya.
4. Terdapat berbagai perintah untuk menampilkan isi *file log*.
5. Saat akan menampilkan isi *syslog*, perintah yang digunakan harus dijalankan sebagai *root* karena *syslog* disimpan pada direktori yang ada pada sistem *root*.
6. Untuk melakukan pemantauan *file log* maupun *journalctl* secara *real-time* dapat menggunakan opsi -f.

VII. Daftar Pustaka

- Immersa Lab. (2018). *PENGERTIAN STEGANOGRAFI, JENIS-JENIS, DAN PRINSIP KERJA*. Diakses pada 12 Maret 2023 dari <https://www.immersa-lab.com/pengertian-steganografi-jenis-jenis-dan-prinsip-kerja.htm>
- pakdosen. (2023). *Steganografi adalah*. Diakses pada 12 Maret 2023 dari <https://pakdosen.co.id/steganografi-adalah/>
- Pangestu, Fredi. (2019). *Implementasi Steganografi Pada Aplikasi Quick Stego*. Diakses pada 12 Maret 2023 dari <https://tutorsbs.wordpress.com/2019/12/02/implementasi-steganografi-pada-aplikasi-quick-stego/>
- C, Ariata. (2023). *40 Perintah Dasar Linux yang Perlu Anda Tahu*. Diakses pada 12 Maret 2023 dari <https://www.hostinger.co.id/tutorial/perintah-dasar-linux#:~:text=cat%20%28akronim%20dari%20concatenate%29%20adalah%20salah%20satu%20perintah,ini%2C%20ketik%20cat%20diikuti%20nama%20dan%20ekstensi%20file.>
- Linuxcent0s. (2017). *Perintah Cat Pada Linux*. Diakses pada 12 Maret 2023 dari <https://linuxcent0s.blogspot.com/2017/09/perintah-cat-pada-linux.html>
- LinuxID. (Tanpa Tahun). *Memahami Perintah Tail Pada Linux Terminal*. Diakses pada 12 Maret 2023 dari <https://www.linuxid.net/24803/memahami-perintah-tail-pada-linux-terminal/#:~:text=Memahami%20Perintah%20Tail%20Pada%20Linux%20Terminal%20Perintah%20tail,digunakan%20untuk%20memantau%20perubahan%20file%20secara%20real%20time.>