

**LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
UNIT 5 & 6**



DI SUSUN OLEH:

Nama : Bintang Nur K
NIM : 21/481453/SV/19790
Kelas : RI4AA
Hari, tanggal : Selasa, 07 Maret 2023
Dosen Pengampu : Anni Karimatul Fauziyyah, S.Kom., M.Eng
Asisten Praktikum : Gabriella Alvera Chaterine

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

UNIT 5 & 6

TEKNIK STEGANOGRAFI DAN ANALISIS LOG SERVER

I. TUJUAN

- Memahami dan mempraktikkan steganografi
- Membaca File Log dengan Cat, More, Less, dan Tail
- Memahami File Log dan Syslog
- Memahami File Log dan Jurnalctl

II. LATAR BELAKANG

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.

Steganografi adalah ilmu, teknik atau seni menyembunyikan pesan rahasia “*hiding message*” atau tulisan rahasia “*covered writing*” sehingga keberadaan pesan tidak terdeteksi orang lain kecuali pengirim dan penerima pesan tersebut. Steganografi berasal dari bahasa Yunani yaitu steganos “tersembunyi/ menyembunyikan” dan graphy “tulisan”, sehingga secara lengkap bermakna tulisan yang disembunyikan.

III. ALAT DAN BAHAN

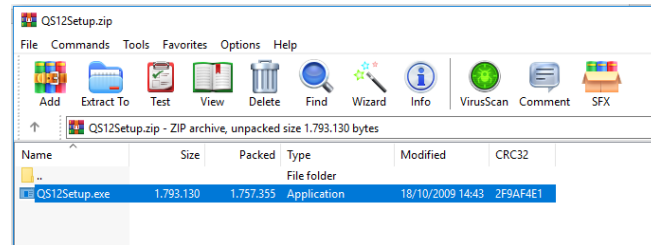
Alat dan Bahan yang dibutuhkan untuk melaksanakan praktikum adalah

- PC
- Koneksi internet
- *Software* Steganografi
- CyberOps Workstation VM

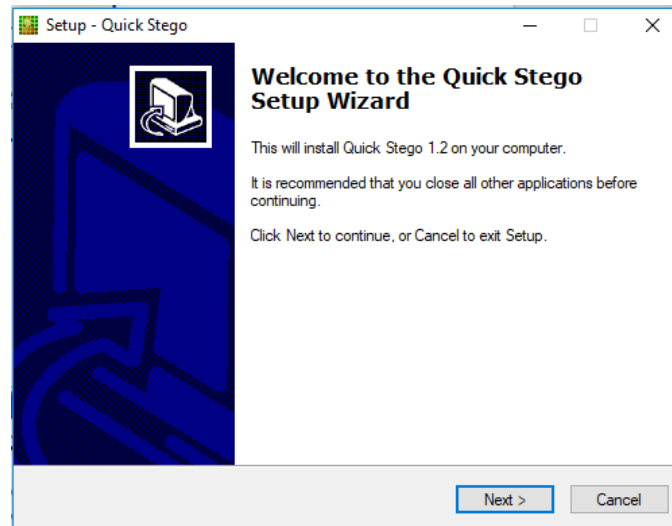
IV. LANGKAH KERJA DAN HASIL

Langkah kerja steganografi

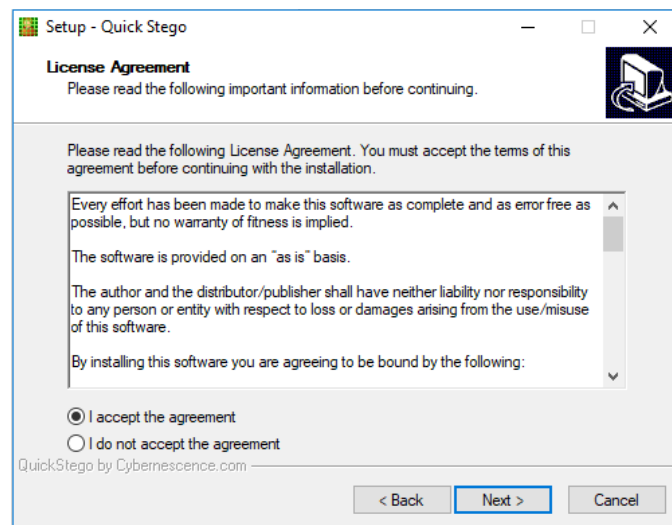
1. Buka windows



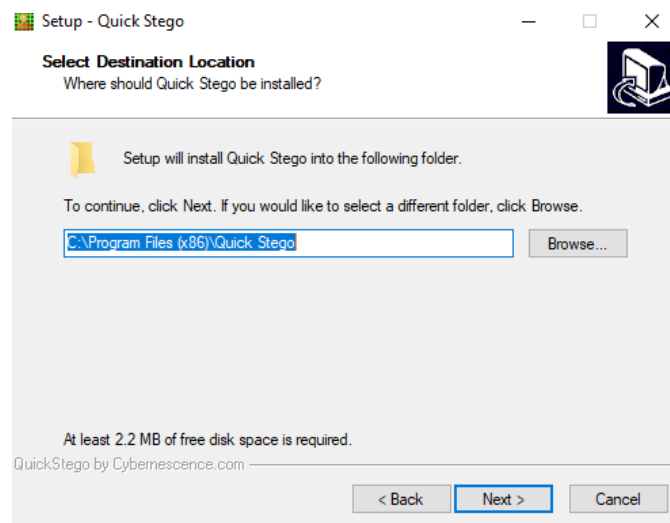
2. Instal quick stego



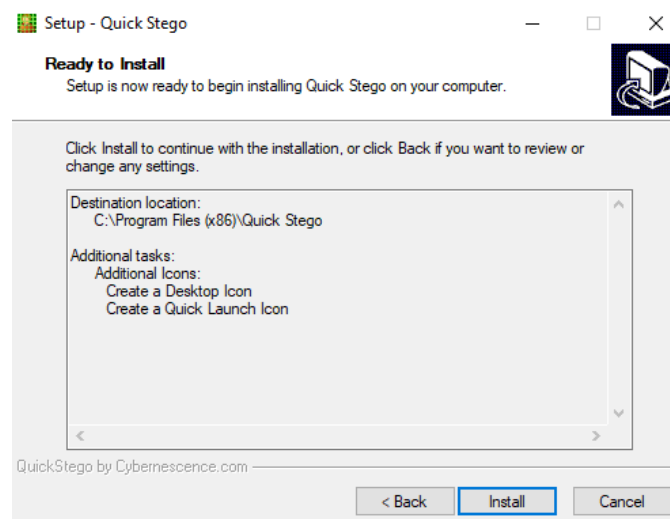
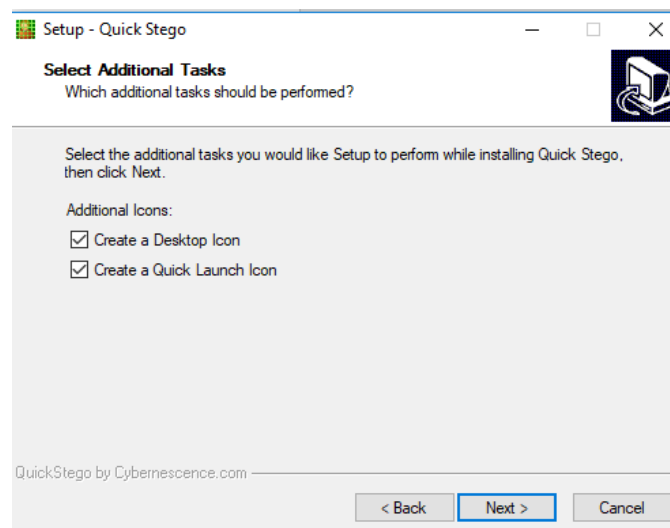
Pengaturan lisensi

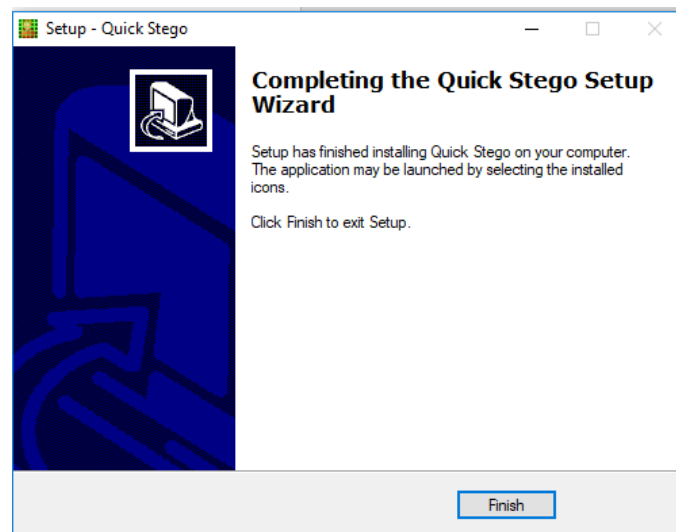


Pilih tujuan



Pilih tugas tambahan, lalu klik siap instal





Buka Command Prompt

Buat Direktori STEGO

```
mkdir "C:\STEGO"
```

```
dir "C:\" | temukanstr STEGO
```

catatan

mkdir, buat direktori. Dalam hal ini, buat direktori STEGO langsung di bawah Drive C.

dir "C:\", daftar semua direktori dan file langsung di bawah Drive C. Kemudian gunakan findstr untuk mencantumkan hanya file dan/atau direktori yang berisi string STEGO.

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

C:\Users\TAJ>dir "C:\" | findstr STEGO
07/03/2023  08:22    <DIR>          STEGO

C:\Users\TAJ>
```

3. Install MD5SUMS

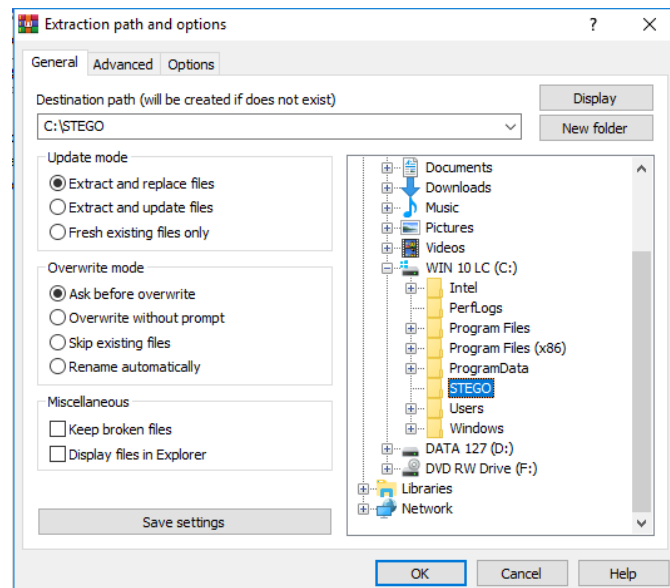
Unduh md5sums-1.2

Arahkan ke URL berikut

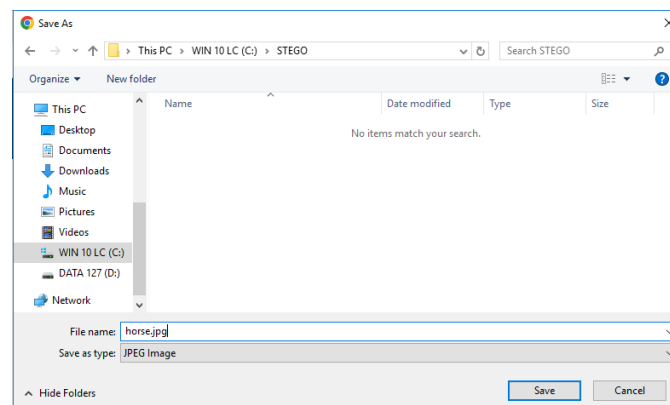
<http://www.pc-tools.net/files/win32/freeware/md5sums-1.2.zip>

Klik tombol Simpan File Radio

Klik tombol **OK**



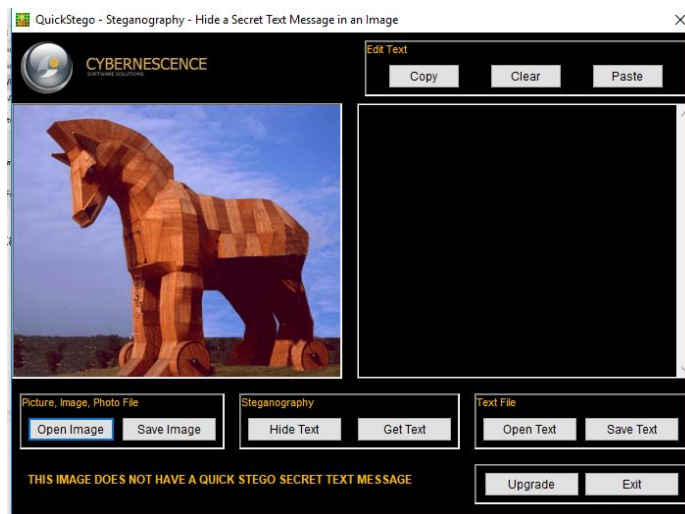
Beri nama dengan jenis file jpg



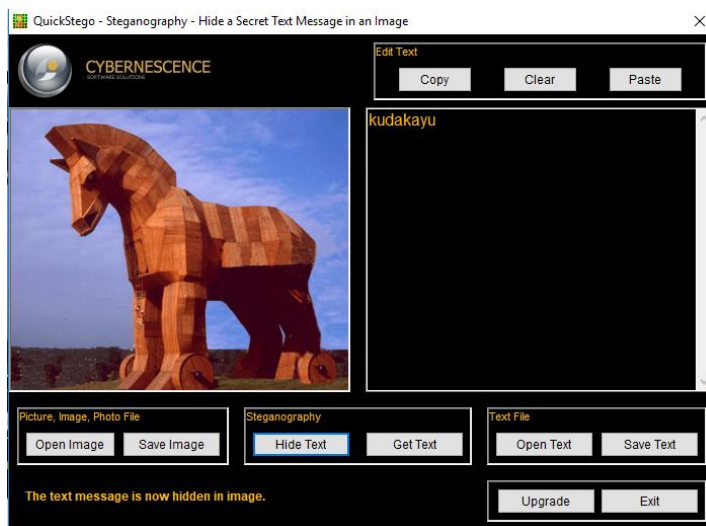
Jalankan Stego Cepat



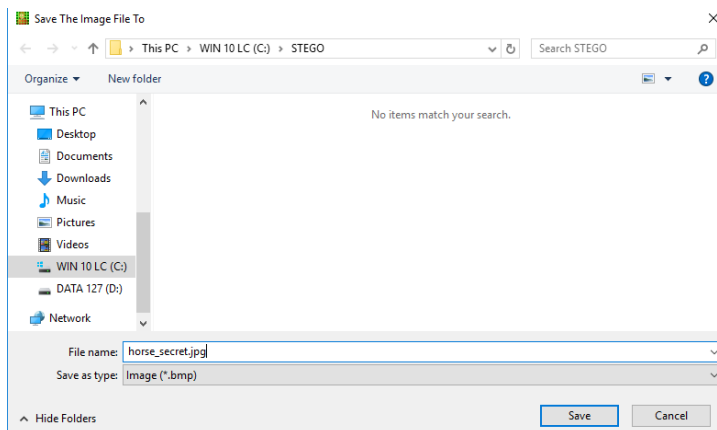
Masukkan gambar yang ingin diberi kata tersembunyi



Sembunyikan Teks



Simpan gambar dengan nama file “horse_secret.jpg”



Buka Command Prompt

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

C:\Users\TAJ>dir "C:\\" | findstr STEGO
07/03/2023  08:22    <DIR>          STEGO

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

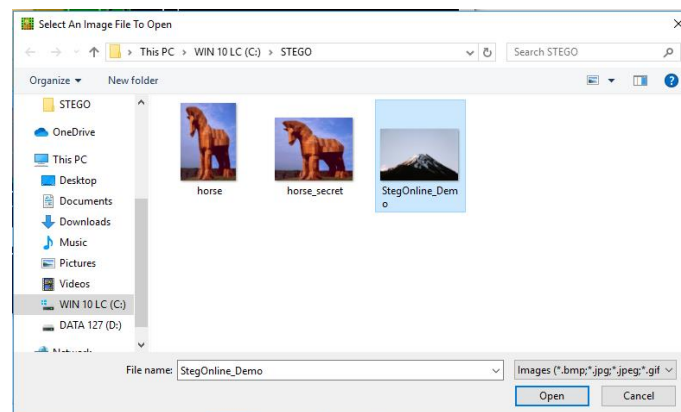
C:\STEGO>md5sums.exe *.jpg

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

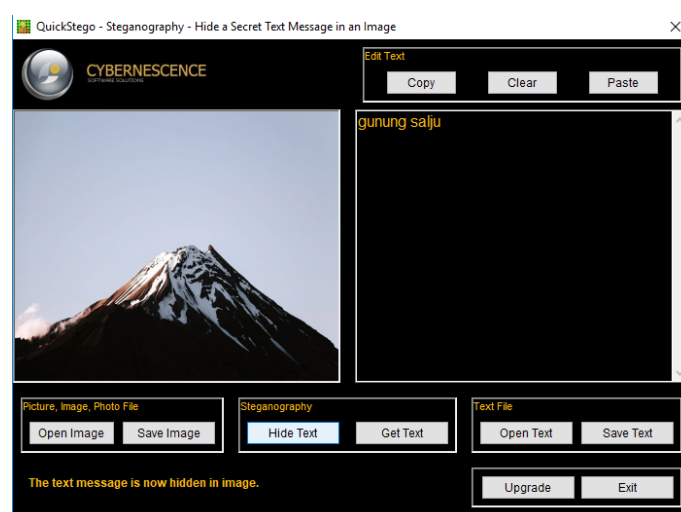
[Path] / filename                                MD5 sum
-----
[C:\STEGO\]
horse.jpg                                         fce8552170cced3dd545566309124097
horse_secret.jpg                               13eaf1ca6546fb37d4d2ee675451817b
C:\STEGO>
```

PADA GAMBAR 2

Ubah PNG to JPG terlebih dahulu, lalu pindahkan file ke STEGO



Masukkan hidden text



Buka 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                                         fce8552170cccd3dd545566309124097
horse_secret.jpg                                13eaf1ca6546fb37d4d2ee675451817b
StegOnline_Demo.jpg                             9f3b7b4b200da9fe48d4c38b9935a890
StegOnline_rhs.jpg                             e3ad125cea8f30b8d95653e9ac9ebe98

C:\STEGO>dir *.jpg
Volume in drive C is WIN 10 LC
Volume Serial Number is 23DA-BE09

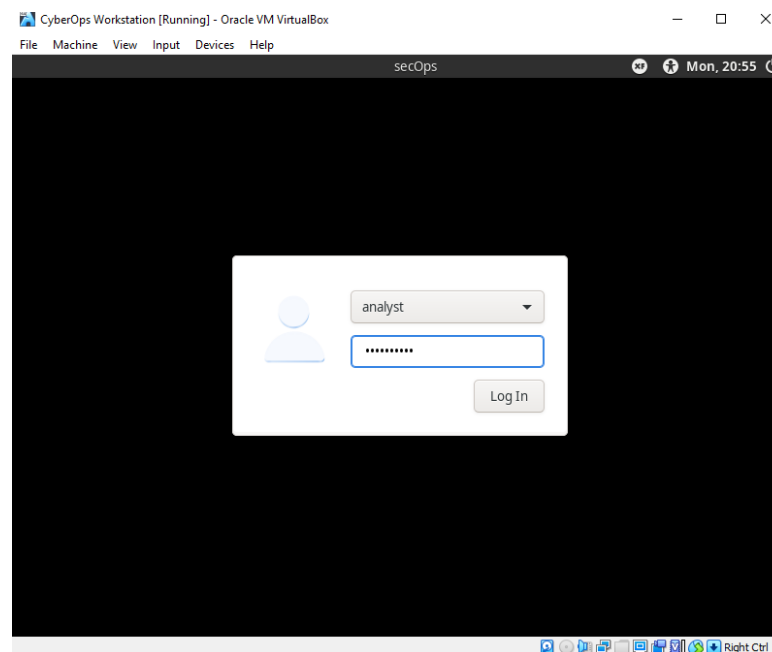
Directory of C:\STEGO

07/03/2023  08:33          46.001 horse.jpg
07/03/2023  08:39        854.454 horse_secret.jpg
07/03/2023  08:43         48.590 StegOnline_Demo.jpg
07/03/2023  08:52       1.998.054 StegOnline_rhs.jpg
               4 File(s)      2.947.099 bytes
               0 Dir(s)    277.291.880.448 bytes free

C:\STEGO>
```

UNIT 6

Pembacaan Log Server



```
Applications: Terminal - analyst@sec02 Mon 06 Mar, 21:02 analyst
Terminal - analyst@sec0ps~
File Edit View Terminal Tabs Help

[analyst@sec0ps ~]$ 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 203962 [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-dashboards.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.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 438406 [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-dashboards.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/0eamhost_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"
Application Finder: logstash-monitorama-2013/images/0eamhost_logo.svg HTTP/1.1"
Find and Launch applications installed on your system. Intel Mac OS X 10_9_1) AppleWebkit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
Application Finder: logstash-monitorama-2013/images/0eamhost_logo.svg HTTP/1.1"
Find and Launch applications installed on your system. Intel Mac OS X 10_9_1) AppleWebkit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
```

```

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

```

```
Applications - Terminal - analyst@sec0ps:~$
Terminal - analyst@sec0ps:~$
File Edit View Terminal Tabs Help

[analyst@sec0ps ~]$ more /home/analyst/lab.support.files/logstash-tutorial.log
6.140 9.216 - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1"
200 203802 "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"
63.149 9.216 - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboards3.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"
63.149 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"
63.149 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"
63.149 9.216 - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/plugin/note/note.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"
63.149 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"
63.149 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"
63.149 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"
63.149 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"
63.149 9.216 - [04/Jan/2015:05:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboards.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"
63.149 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) Ap
```

```

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

```

```

Applications - Terminal - analyst@sec0ps:~
Terminal - analyst@sec0ps:~
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 203923 "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-dashbaord3.png HTTP/1.1"
200 177177 "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-med.png HTTP/1.1"
200 438406 "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 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/2015:05:13:45 +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-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"
/home/analyst/lab.support.files/logstash-tutorial.log

```

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

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

```
[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%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html HTTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently_asked_questions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
[analyst@secOps ~]$
```

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

```
[analyst@secOps ~]$ tail -f /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny 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/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"

```

Pilihlah jendela terminal bawah dan masukkan perintah berikut:

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

The screenshot shows two terminal windows. The left window displays the command `echo "this is a new entry for the monitored log file" >> lab.support.files/logstash-tutorial.log` and the output `bash: lab.support.files/logstash-tutorial.log: No such file or directory`. The right window displays the command `echo "ini adalah entri baru yang dipantau" >> lab.support.files/logstash-tutorial.log` and the output `bash: lab.support.files/logstash-tutorial.log: No such file or directory`. Both windows show the file `lab.support.files/logstash-tutorial.log` with the following content:

```
this is a new entry for the monitored log file
ini adalah entri baru yang dipantau
ini adalah entri baru bintang
```

Memahami File Log dan Syslog

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

The screenshot shows a terminal window displaying the contents of `/var/log/syslog.1`. The output is a log of system events, including kernel messages and user actions. The log entries are as follows:

```
Apr 20 06:10:55 secOps kernel: [ 1.941729] fb: switching to vboxdmfb from VESA VGA
Apr 20 06:10:55 secOps kernel: [ 1.941746] Console: switching to colour dummy device 80x25
Apr 20 06:10:55 secOps kernel: [ 1.942421] fbcon: vboxdmfb (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: vboxdmfb 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] plix4_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 ppi-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 0800:00:03:0 enp0s3: renamed from eth0
Apr 20 06:10:55 secOps kernel: [ 2.953163] pcnet32 0800:00:03:0 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 ~]$ sudo cat /var/log/syslog.1
```


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

```
Applications Terminal - analis@sec0. Mon 06 Mar, 21:26 analis
Terminal - analis@secOps~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo cat /var/log/syslog.3
Nov 29 11:30:40 secOps kernel: [ 6.668727] pppdev: user-space parallel port driver
Nov 29 11:30:40 secOps kernel: [ 6.681487] pcnet32 0000:00:03.0 enp0s3: renamed from eth0
Nov 29 11:30:40 secOps kernel: [ 6.757097] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Nov 29 11:30:40 secOps kernel: [ 7.084534] IPv6: enp0s3: IPv6 duplicate address fe80::a00:27ff:fe23:b231 detected!
Nov 29 11:30:42 secOps kernel: [ 9.118427] floppy0: no floppy controllers found
Nov 29 11:30:42 secOps kernel: [ 9.118544] 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_xsta
te+0x465/0x7b2
Nov 29 04:36:27 secOps kernel: [ 0.000000] XSAVE consistency problem, dumping leaves
Nov 29 04:36:27 secOps kernel: [ 0.000000] Modules linked in:
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPU: 0 PID: 0 Comm: swapper Not tainted 4.10.10-1-ARCH #1
Nov 29 04:36:27 secOps kernel: [ 0.000000] Call Trace:
Nov 29 04:36:27 secOps kernel: [ 0.000000] dump_stack+0x58/0x74
Nov 29 04:36:27 secOps kernel: [ 0.000000] __warn+0xea/0x110
Nov 29 04:36:27 secOps kernel: [ 0.000000] ? fpu__init_system_xstate+0x465/0x7b2
Nov 29 04:36:27 secOps kernel: [ 0.000000] warn_slowpath_fmt+0x46/0x60
Nov 29 04:36:27 secOps kernel: [ 0.000000] fpu__init_system_xstate+0x465/0x7b2
Nov 29 04:36:27 secOps kernel: [ 0.000000] fpu__init_system+0x18c/0x1b1
Nov 29 04:36:27 secOps kernel: [ 0.000000] early_cpu_init+0x110/0x113
Nov 29 04:36:27 secOps kernel: [ 0.000000] setup_arch+0xe4/0xbb6
Nov 29 04:36:27 secOps kernel: [ 0.000000] start_kernel+0x8f/0x3ce
Nov 29 04:36:27 secOps kernel: [ 0.000000] i386_start_kernel+0x91/0x95
Nov 29 04:36:27 secOps kernel: [ 0.000000] startup_32_smp+0x16b/0x16d
Nov 29 04:36:27 secOps kernel: [ 0.000000] ---[ end trace 3451dc0d6e69451e ]---
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPUID[0d, 00]: eax=00000007 ebx=00000440 ecx=00000440 edx=00000000
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPUID[0d, 01]: eax=00000000 ebx=000003c0 ecx=00000000 edx=00000000
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPUID[0d, 02]: eax=00000100 ebx=00000240 ecx=00000000 edx=00000000
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPUID[0d, 03]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPUID[0d, 04]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
```

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

```
File Edit View Terminal Tabs Help
Mar 6 11:58:56 secOps kernel: [ 6.016025] openvswitch: Open vSwitch switching datapath
[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
```

Memahami File Log dan Jurnaltctl

```
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache (access for web browsers).
[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 20:56:17 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 3ms.
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).
lines 1-23... skipping...
-- Logs begin at Tue 2018-03-20 16:10:08 EDT, end at Mon 2023-03-06 20:56:17 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.
```

analisis@secOps ~\$ sudo journalctl -utc

```
File Edit View Terminal Tabs Help
analisis@secOps:~$ sudo journalctl --utc
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Tue 2023-03-07 02:31:04 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 0x0000000000000000-0x000000000009f000] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000009f000-0x00000000000fffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000fffff-0x00000000001fffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000001fffff-0x00000000003fffff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000003fffff-0x00000000003fffff] ACPI data
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000003fffff-0x00000000003fffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000003fffff-0x00000000003fffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000003fffff-0x00000000003fffff] reserved
Mar 20 19:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 19:28:45 secOps kernel: random: fast init done
lines 1-23... skipping...
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Tue 2023-03-07 02:31:04 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'
```


analis@secOps ~\$ sudo journalctl -b

```
analis@secOps ~$ sudo journalctl -b
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:32:00 EST. --
Mar 06 20:55:23 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 20:55:23 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 06 20:55:23 secOps kernel: KERNEL supported cpus:
Mar 06 20:55:23 secOps kernel: Intel GenuineIntel
Mar 06 20:55:23 secOps kernel: AMD AuthenticAMD
Mar 06 20:55:23 secOps kernel: Hygon HygonGenuine
Mar 06 20:55:23 secOps kernel: Centaur CentaurHauls
Mar 06 20:55:23 secOps kernel: zhaoxin Shanghai
Mar 06 20:55:23 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 20:55:23 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 20:55:23 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 20:55:23 secOps kernel: BIOS-provided physical RAM map:
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x00000000000a0000-0x00000000000fffff] reserved
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000003fffff] usable
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x00000000003ff000-0x00000000003fffff] ACPI data
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x0000000000fc0000-0x0000000000fc0fff] reserved
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x0000000000fee0000-0x0000000000fee0fff] reserved
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x0000000000fffc000-0x0000000000ffffff] reserved
Mar 06 20:55:23 secOps kernel: NX (Execute Disable) protection: active
Mar 06 20:55:23 secOps kernel: SMBIOS 2.5 present.
Mar 06 20:55:23 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 20:55:23 secOps kernel: Hypervisor detected: KVM
Mar 06 20:55:23 secOps kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
Mar 06 20:55:23 secOps kernel: kvm-clock: cpu 0, msrc 13801001, primary cpu clock
Mar 06 20:55:23 secOps kernel: kvm-clock: using sched offset of 8827868016 cycles
Mar 06 20:55:23 secOps kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 88151
Mar 06 20:55:23 secOps kernel: tsc: Detected 2993.208 MHz processor
Mar 06 20:55:23 secOps kernel: e820: update [mem 0x00000000-0x0000ffff] usable ==> reserved
Mar 06 20:55:23 secOps kernel: e820: remove [mem 0x00000000-0x0000ffff] usable
```

analis@secOps ~\$ sudo journalctl -u nginx.service --sejak hari ini

```
analis@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 21:35:54 EST. --
-- No entries --
analis@secOps ~$
```

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

```
analis@secOps ~$ sudo journalctl -k
-- No entries --
analis@secOps ~$ sudo journalctl -k
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:36:59 EST. --
Mar 06 20:55:23 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 20:55:23 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 06 20:55:23 secOps kernel: KERNEL supported cpus:
Mar 06 20:55:23 secOps kernel: Intel GenuineIntel
Mar 06 20:55:23 secOps kernel: AMD AuthenticAMD
Mar 06 20:55:23 secOps kernel: Hygon HygonGenuine
Mar 06 20:55:23 secOps kernel: Centaur CentaurHauls
Mar 06 20:55:23 secOps kernel: zhaoxin Shanghai
Mar 06 20:55:23 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 20:55:23 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 20:55:23 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 20:55:23 secOps kernel: BIOS-provided physical RAM map:
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x00000000000a0000-0x00000000000fffff] reserved
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000003fffff] usable
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x00000000003ff000-0x00000000003fffff] ACPI data
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x0000000000fc0000-0x0000000000fc0fff] reserved
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x0000000000fee0000-0x0000000000fee0fff] reserved
Mar 06 20:55:23 secOps kernel: BIOS-e820: [mem 0x0000000000fffc000-0x0000000000ffffff] reserved
Mar 06 20:55:23 secOps kernel: NX (Execute Disable) protection: active
Mar 06 20:55:23 secOps kernel: SMBIOS 2.5 present.
lines 1-23... skipping...
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:36:59 EST. --
Mar 06 20:55:23 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 20:55:23 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 06 20:55:23 secOps kernel: KERNEL supported cpus:
Mar 06 20:55:23 secOps kernel: Intel GenuineIntel
Mar 06 20:55:23 secOps kernel: AMD AuthenticAMD
Mar 06 20:55:23 secOps kernel: Hygon HygonGenuine
Mar 06 20:55:23 secOps kernel: Centaur CentaurHauls
```

Mirip dengan tail -f yang dijelaskan di atas, gunakan -f untuk secara aktif mengikuti log saat sedang ditulis: analis@secOps ~\$ sudo journalctl -f

```
[analis@secOps ~]$ sudo journalctl -f
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Mar 06 21:37:51 secOps kernel: audit: type=1106 audit(1678156671.429:123): pid=661 uid=0 auid=1000 ses=2 msg='op=PAM:session_c
lose grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 21:37:51 secOps kernel: audit: type=1104 audit(1678156671.429:124): pid=661 uid=0 auid=1000 ses=2 msg='op=PAM:setcred g
rantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 21:37:58 secOps audit[671]: USER_ACCT pid=671 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 21:37:58 secOps sudo[671]: analyst : TTY=pts/0 ; PWD=/home/analyst ; USER=root ; COMMAND=/usr/bin/journalctl -f
Mar 06 21:37:58 secOps kernel: audit: type=1101 audit(1678156678.543:125): pid=671 uid=1000 auid=1000 ses=2 msg='op=PAM:accoun
ting grantors=pam_unix,pam_permit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succes
s'
Mar 06 21:37:58 secOps audit[671]: CRED_REFR pid=671 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 21:37:58 secOps sudo[671]: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 06 21:37:58 secOps audit[671]: USER_START pid=671 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 21:37:58 secOps kernel: audit: type=1110 audit(1678156678.546:126): pid=671 uid=0 auid=1000 ses=2 msg='op=PAM:setcred g
rantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 21:37:58 secOps kernel: audit: type=1105 audit(1678156678.546:127): pid=671 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'
```

File yang tersimpan:

<https://simpan.ugm.ac.id/apps/files/>

V. ANALISIS

Pada praktikum kali ini melakukan praktik steganografi dan pembacaan log server/ file log.

Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.

Cara Kerja Steganografi antara lain dengan menyisipkan data yang ingin disembunyikan membutuhkan dua unsur. Unsur pertama ialah media penampung seperti citra, suara, video dan sebagainya yang terlihat tidak mencurigakan untuk menyimpan pesan rahasia. Unsur kedua adalah pesan yang ingin disembunyikan yaitu media penampungnya berupa citra yang disebut *cover-object* dan citra yang telah disisipi pesan disebut *stego-object*.

Secara umum, terdapat dua proses didalam steganografi yaitu proses embedding untuk menyisipkan pesan kedalam cover-object dan proses decoding untuk ekstraksi pesan dari stego-object. Kedua proses ini mungkin memerlukan kunci rahasia yang dinamakan stego-key agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

Pada lab stegano ini mengunduh gambar yang sudah diberikan di modul elok lalu disimpan pada folder yang Bernama “STEGO” kemudian buka cmd dan ketik perintah `dir *.jpg` untuk menampilkan informasi file berupa gambar yang ada pada folder STEGO. Terlihat sebelum dan sesudah gambar tersebut disispi pesan hidden text dimana terjadi perbedaan ukuran file. Untuk dari segi visual hamper tidak terjadi perbedaan dan hanya bisa diketahui melalui perintah pada CMD. Ditampilkan juga total ukuran 4 files gambar yang ada. Lanjut untuk mengecek keaslian/integritas pda gambar yang ada pada folder STEGO menggunakan MD5SUMS.

Pesan yang ditampilkan berupa pesan acak untuk menjaga keamanan dan bernilai 32 karakter

File-file log adalah file yang berada di sebuah sistem yang merupakan file-file penting yang senantiasa mencatat semua kejadian-kejadian(kegiatan) yang berlangsung pada system. File -file log kebanyakan ditulis dalam bentuk file text yang ditulis perbaris (istilah untuk namanya adalah record) oleh program-program sistem bawaan saat kita menginstall sebuah program ataupun sebuah SO (sistem operasi).

Pada perintah ini dilakukan di CyberOps Workstation virtual machine.

Perintah echo untuk menambahkan data baru berupa tulisan yang terdapat pada baris akhir. Setelah perintah echo dijalankan lalu membuka text menggunakan tail -f, maka akan muncul text yang kita tulis tadi pada baris akhir. Perintah syslog untuk mengirim/mengeksport pesan log ke dalam satu server. Untuk pembuatan syslog yang lain berguna agar ukuran file yang dihasilkan tidak terlalu besar dan membebani satu server. Perintah journalctl untuk membaca dan berkomunikasi dengan jurnal log, serta menampilkan

pesan log oleh jurnal log. Perintah `-utc` pada `journalctl` berfungsi untuk menampilkan waktu log in UTC dengan menampilkan waktu yang sesungguhnya. Perintah `-b` pada `journalctl` berfungsi untuk menampilkan rekaman log terakhir selama boot berakhir. Perintah `sudo journalctl -u nginx.service--day` untuk menampilkan catatan seluruh log.

Versi-versi Unix menyimpan file-file log-nya pada direktory berbeda-beda.

Umumnya file ini berada pada:

`/usr/adm` ---> Digunakan oleh Unix Versi lama

`/var/adm` ---> Digunakan oleh kebanyakan Versi Unix/Linux terbaru.
dimana partisi `/usr` di-mount read only

`/var/log` ---> Digunakan oleh beberapa versi Solaris, Linux, BSD, dan FreeBSD

Di dalam *directory* - *directory* diatas terdapat *subdirectory* didalamnya terdapat file-file sebagai berikut:

`suolog` ---> Melakukan log penggunaan perintah `su`

`utmp` ---> Merekam setiap user yang tengah login

`utmpx` ---> Extended `utmp`

`wtmp` ---> Memberikan record permanen untuk setiap kali user login dan logout, juga merekam shutdown dan star up system

`acct` atau `pacct` ---> Merekam perintah-perintah yang dijalankan oleh setiap user

`aculog` ---> Merekam dial-out modem-modem (automatic call units)

`lastlog` ---> Melakukan log setiap login user, baik yang sukses maupun tidak

`loginlog` ---> Merekam usaha-usaha pada saat login yang gagal

`messages` ---> Merekam output ke "console" sistem atau pesan-pesan lain yang menghasilkan dari fasilitas `syslog`

`wtmpx` ---> Extended `wtmp`

`vold.log` ---> Melakukan log error-error yang dialami atas penggunaan external media seperti, disk-disk floppy atau CDROM.

`xferlog` ---> Melakukan log akses-akses ftp

aculog ---> Melakukan log pada setiap terjadi panggilan telepon yang di-dial

uucp ---> Melakukan log saat terjadi pelanggaran-pelanggaran restriksi atau penggunaan UUCP system (biasanya untuk aktivitas seorang user dan log-log file transfer).

access_log ---> Melakukan log pada saat menjalankan HTTPD untuk keperluan World Wide Web.

syslog ---> Melakukan log proses-proses system

dmesg ---> Melakukan log pada saat server reboot

www/access.log ---> file log access web server

www/error.log ---> file log error web server

.bash_history ---> Melakukan log hasil ketikan kita di console dan lain lain..

VI. KESIMPULAN

Setelah melaksanakan praktikum yang saya dapatkan adalah

- Rotasi file log, dilakukan berdasarkan ukuran file
- File log akan di-rotasi setelah mencapai ukuran tertentu
- Log adalah catatan dalam bentuk file yang berisi rekaman aktifitas dari sebuah aplikasi. Catatan ini dapat berupa pesan peringatan, pesan kesalahan atau pesan lainnya. Salah satu contoh file log yang sering ditemui adalah file “error_log”. File “error_log” ini bisa di temukan pada directory file website yang di buat.
- Steganografi adalah tulisan atau pesan yang disembunyikan

VII. DAFTAR PUSTAKA

Priyambodo, D. (2022, December 29). *Apa itu Log dan Setting Rotasi Log di VPS cPanel*. Rumahweb Journal – News, Article, and Tutorial of Web Dev.
<https://www.rumahweb.com/journal/apa-itu-log-adalah/>

Knowledge, S. S.-. S. I. A. (n.d.). *Mengenal berbagai jenis file log di server linux / Explore your Mind*.
<https://suryadisyamsu.blogspot.com/2009/05/mengenal-berbagai-jenis-file-log-di.html>

Komputer, U. S. &. T. (n.d.). *Seni dan Ilmu Menulis Pesan Tersembunyi (Steganografi)/SI Teknik Informatika S.Kom*. <http://teknik-informatika-s1.stekom.ac.id/informasi/baca/Seni-dan-Ilmu-Menulis-Pesan-Tersembunyi-Steganografi/ff7dc125afd07f6dd43da9fa8a09809e96d41789>