

**LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1
TEKNIK STEGANOGRAFI & ANALISIS LOG SERVER**



DI SUSUN OLEH

Nama : M Abdul Aziz
NIM : 21/474516/SV/18951
Hari, Tanggal : Selasa, 07 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

Teknik Steganografi & Analisis Log Server

I. Tujuan

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

II. Landasan Teori

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 di pecahkan akan tetapi itu akan menimbulkan kecurigaan pesan tersebut.

File log adalah file yang berada di sebuah sistem yang merupakan file-file penting yang senantiasa mencatat semua kejadian(kegiatan) yang berlangsung pada sistem. File ini sangat penting pada sebuah sistem untuk memudahkan kita khususnya admin untuk memeriksa dan menelusuri berbagai masalah yang terjadi, dengan file log admin dengan mudah menemukan sebuah bug, sumber-sumber penyerangan, dan kerusakan-kerusakan yang terjadi pada sistem yang ditimbulkan, walaupun kita tidak mengetahui cara menanggulangi kerusakan tersebut.

File log kebanyakan ditulis dalam bentuk file text yang ditulis perbaris (*record*) oleh program-program sistem bawaan saat kita menginstall sebuah program ataupun sebuah SO (sistem operasi). Sebagai contoh misalkan pada saat kita menjalankan perintah **su**, maka program su akan memberikan laporannya dan

membubuhkan ke dalam file log sulog (file ini akan menjelaskan apakah usaha su dilakukan user tersebut sukses atau tidak).

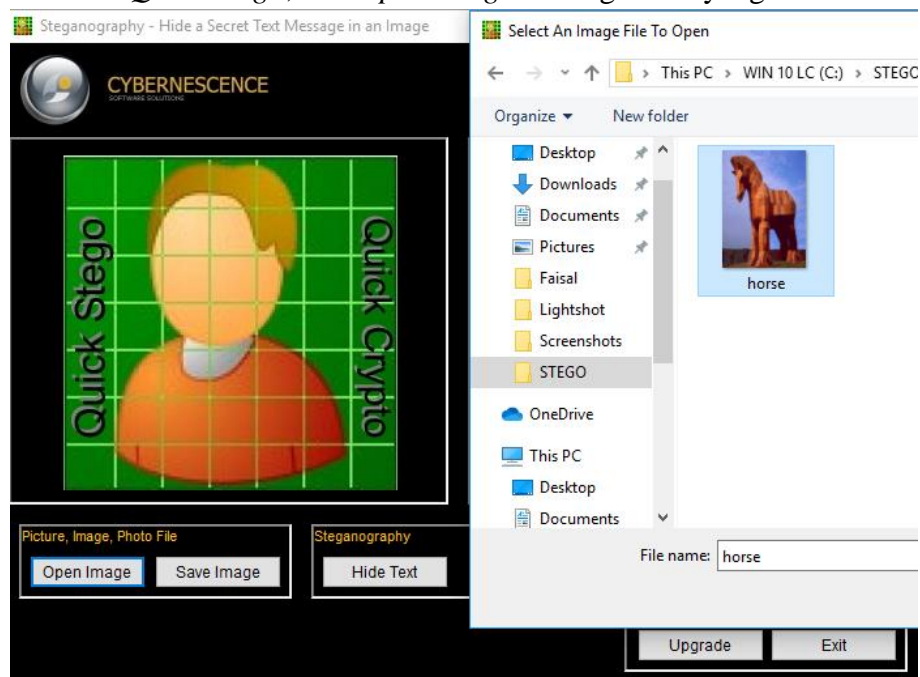
III. Alat & Bahan

- PC/Laptop
- CyberOps Workstation VM
- *Software Quick Stego*
- *Software MD5Sum*
- Koneksi internet

IV. Instruksi Kerja

1. TEKNIK STEGANOGRAFI

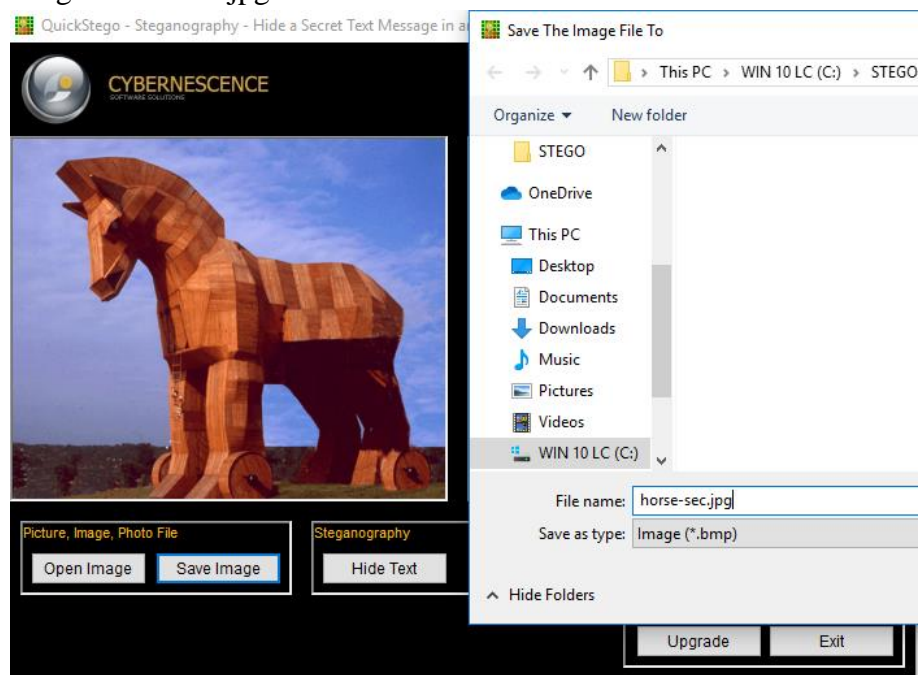
- Unduh *software Quick Stego* melalui link dibawah ini
<http://quickcrypto.com/products/QS12Setup.zip>
- Buka file hasil unduhan, lalu *Extract* file
- Install *Quick Stego*
- Buat folder khusus pada direktori C:\ dengan nama STEGO
- Unduh *tools MD5SUM* melalui link dibawah ini
<http://www.pc-tools.net/files/win32/freeware/md5sums-1.2.zip>
- Arahkan unduhan ke folder yang telah dibuat, lalu *Extract*
- Unduh gambar1 pada link yang telah disediakan
- Jalankan *Quick Stego*, lalu *Open Image*. Pilih gambar yang telah diunduh



- i. Masukkan teks yang ingin disembunyikan, lalu klik *hide text*



- j. Setelah itu simpan gambar yang telah diberikan informasi tersembunyi dengan ekstensi .jpg



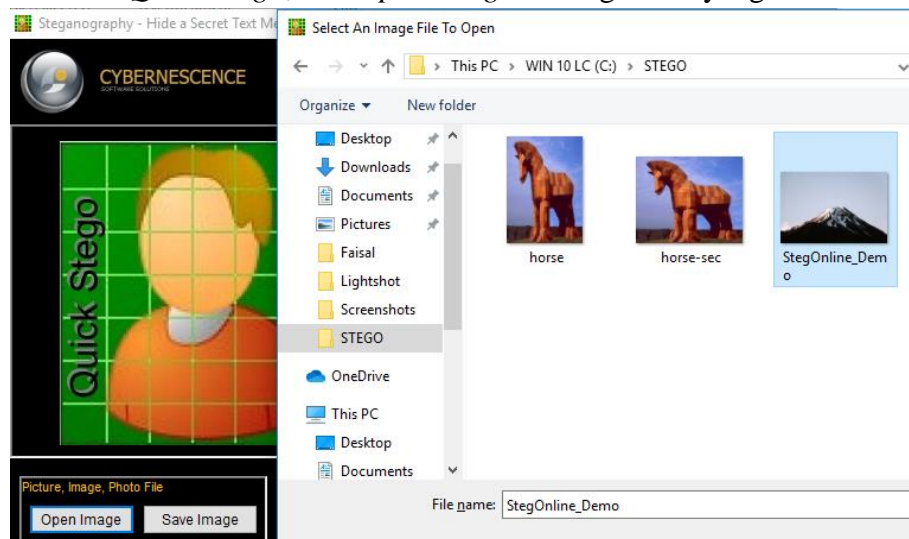
- k. Buka CMD, lalu arahkan ke direktori C:\STEGO. Lalu ketikkan *md5sums.exe* **.jpg* untuk menampilkan semua *hashing* file dengan ekstensi *.jpg*

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

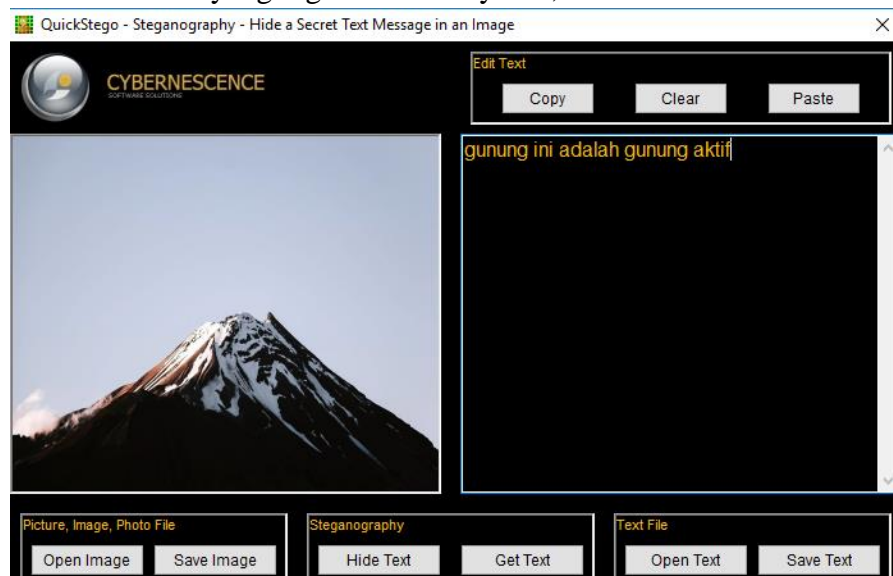
MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums.exe -h for help

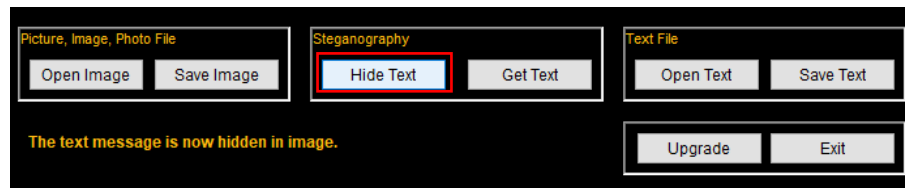
[Path] / filename                                MD5 sum
-----
[C:\STEGO\]
horse-sec.jpg                                     aa3cc2dde8f49318f7ad908093e9b6ec
horse.jpg                                         fce8552170cccd3dd545566309124097
```

- l. Lakukan hal yang sama pada gambar 2
m. Unduh gambar2 pada link yang telah disediakan
n. Karena gambar2 berekstensi *.png*, maka *convert* terlebih dahulu ke *.jpg*
o. Jalankan *Quick Stego*, lalu *Open Image*. Pilih gambar yang telah diunduh

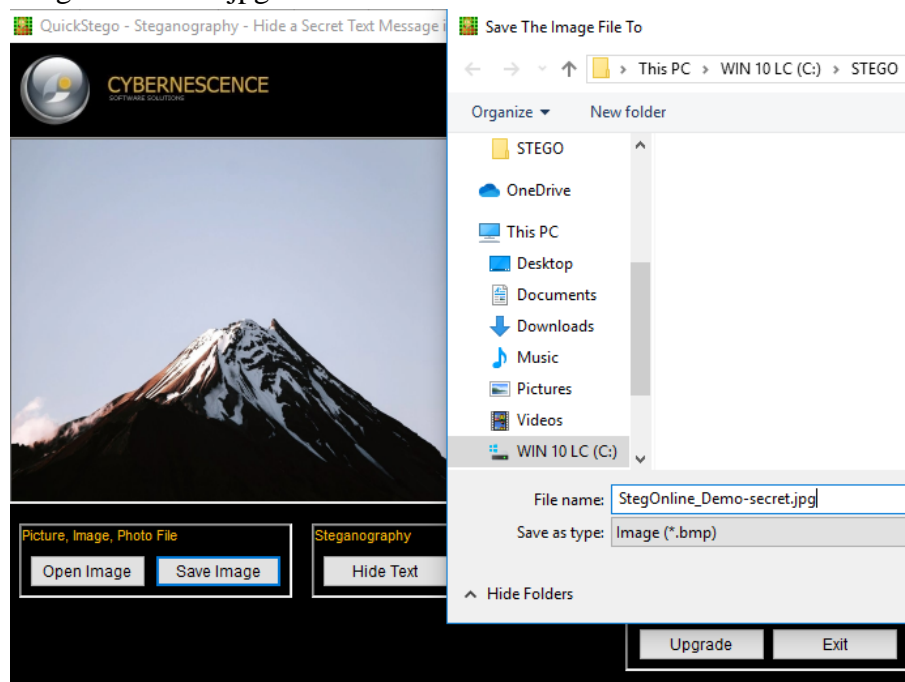


- p. Masukkan teks yang ingin disembunyikan, lalu klik *hide text*





- q. Setelah itu simpan gambar yang telah diberikan informasi tersembunyi dengan ekstensi .jpg



- r. Buka CMD, lalu arahkan ke direktori C:\STEGO. Lalu ketikkan *md5sums.exe* *.jpg untuk menampilkan semua *hashing* 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-sec.jpg                                     aa3cc2dde8f49318f7ad908093e9b6ec
horse.jpg                                         fce8552170cccd3dd545566309124097
StegOnline_Demo-secret.jpg                       a4ce88b2db0cb7552b1fc33ff65238c2
StegOnline_Demo.jpg                             9f3b7b4b200da9fe48d4c38b9935a890

C:\STEGO>

```

2. Log Server

- Buka VM *CyberOps Workstation*
- Lakukan pengujian pembacaan file *log* dengan CAT

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

```
File Edit View Terminal Tabs Help
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/sad-medic.png HTTP/1.1" 200 430406 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Bold.ttf HTTP/1.1" 200 38720 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf HTTP/1.1" 200 41820 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard.png HTTP/1.1" 200 321631 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:46 +0000] "GET /presentations/logstash-monitorama-2013/images/Dreamhost_logo.svg HTTP/1.1" 200 2126 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
/home/analyst/lab.support.files/logstash-tutorial.log
```

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

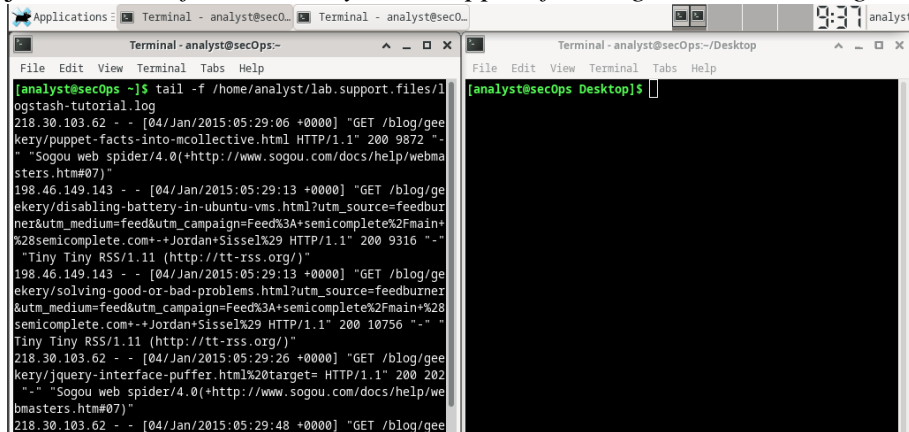
```
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ tail /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
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 Icwaeasel/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 Icwaeasel/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 Icwaeasel/24.3.0"
[analyst@secOps Desktop]$
```

Tail -f

```
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ sudo tail -f /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-problems.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/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 Icwaeasel/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 Icwaeasel/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 Icwaeasel/24.3.0"

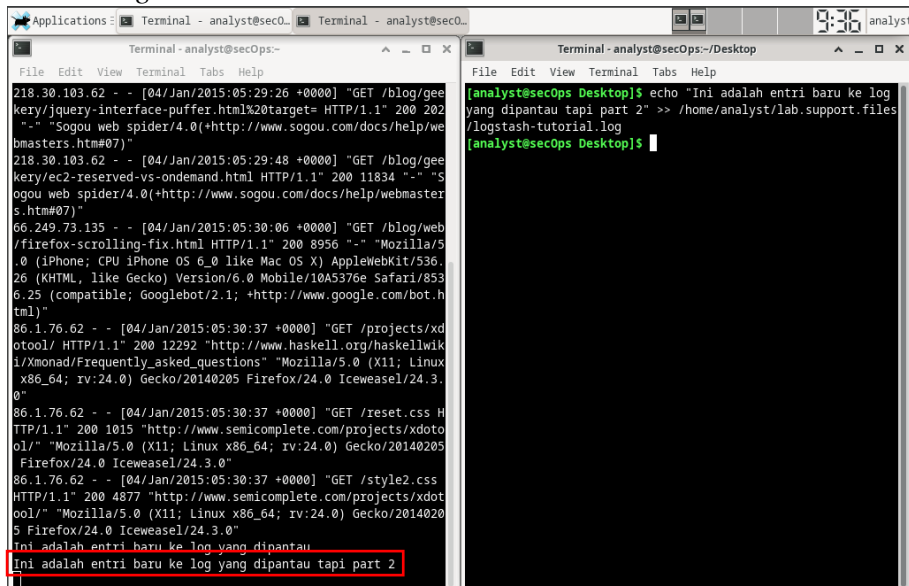
```


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



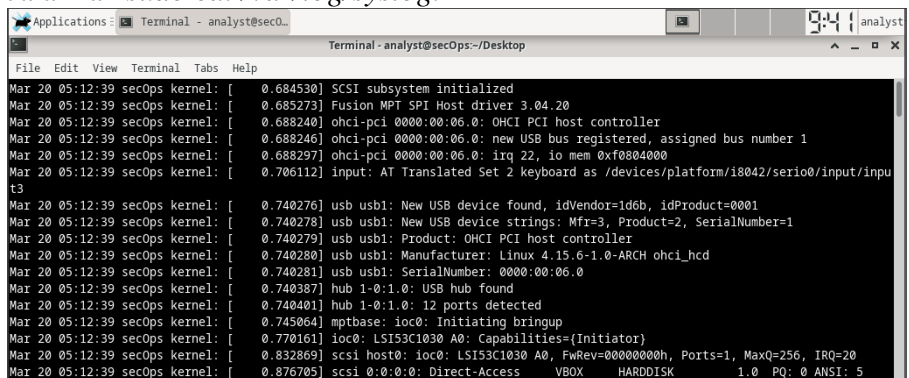
```
[analyst@secOps ~]$ tail -f /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
198.46.149.143 -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

- g. 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`



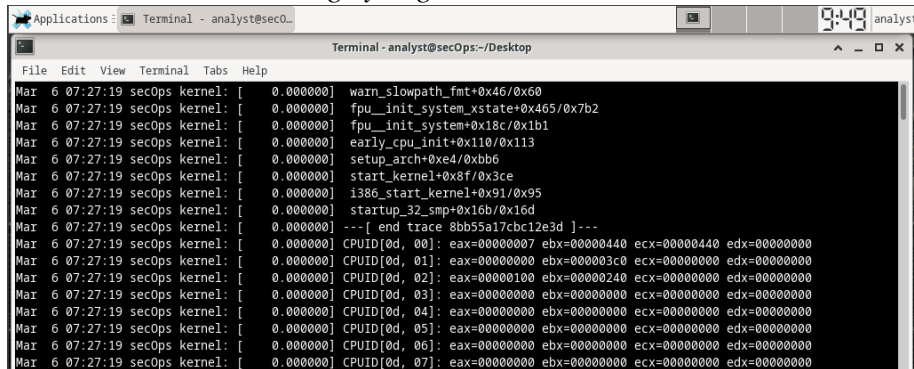
```
[analyst@secOps Desktop]$ echo "ini adalah entri baru untuk file log yang dipantau tapi part 2" >> /home/analyst/lab.support.files/logstash-tutorial.log
[analyst@secOps Desktop]$
```

- h. Jalankan `sudo cat /var/log/syslog.1`



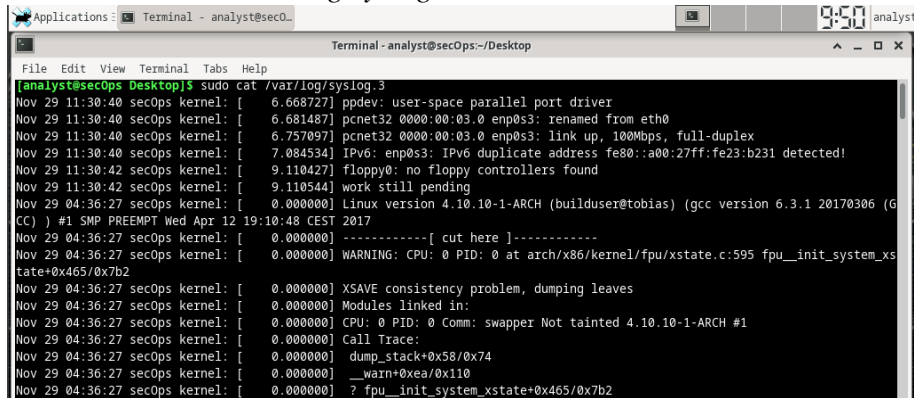
```
Mar 20 05:12:39 secOps kernel: [ 0.684530] SCSI subsystem initialized
Mar 20 05:12:39 secOps kernel: [ 0.685273] Fusion MPT SPI Host driver 3.04.20
Mar 20 05:12:39 secOps kernel: [ 0.688240] ohci-pci 0000:00:06.0: OHCI PCI host controller
Mar 20 05:12:39 secOps kernel: [ 0.688246] ohci-pci 0000:00:06.0: new USB bus registered, assigned bus number 1
Mar 20 05:12:39 secOps kernel: [ 0.688297] ohci-pci 0000:00:06.0: irq 22, io mem 0xf0804000
Mar 20 05:12:39 secOps kernel: [ 0.706112] input: AT Translated Set 2 keyboard as /devices/platform/i8042/serio0/input/input3
Mar 20 05:12:39 secOps kernel: [ 0.740276] usb 1-0:1.0: New USB device found, idVendor=1d6b, idProduct=0001
Mar 20 05:12:39 secOps kernel: [ 0.740278] usb 1-0:1.0: New USB device strings: Mfr=3, Product=2, SerialNumber=1
Mar 20 05:12:39 secOps kernel: [ 0.740279] usb 1-0:1.0: Product: OHCI PCI host controller
Mar 20 05:12:39 secOps kernel: [ 0.740280] usb 1-0:1.0: Manufacturer: Linux 4.15.6-1.0-ARCH ohci_hcd
Mar 20 05:12:39 secOps kernel: [ 0.740281] usb 1-0:1.0: SerialNumber: 0000:00:06.0
Mar 20 05:12:39 secOps kernel: [ 0.740387] hub 1-0:1.0: USB hub found
Mar 20 05:12:39 secOps kernel: [ 0.740401] hub 1-0:1.0: 12 ports detected
Mar 20 05:12:39 secOps kernel: [ 0.745064] mptbase: ioc0: Initiating bringup
Mar 20 05:12:39 secOps kernel: [ 0.770161] ioc0: LSI53C1030 A0: Capabilities={Initiator}
Mar 20 05:12:39 secOps kernel: [ 0.832869] scsi host0: ioc0: LSI53C1030 A0, FwRev=00000000h, Ports=1, MaxQ=256, IRQ=20
Mar 20 05:12:39 secOps kernel: [ 0.876705] scsi 0:0:0:0: Direct-Access VBOX HARDISK 1.0 PQ: 0 ANSI: 5
```

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



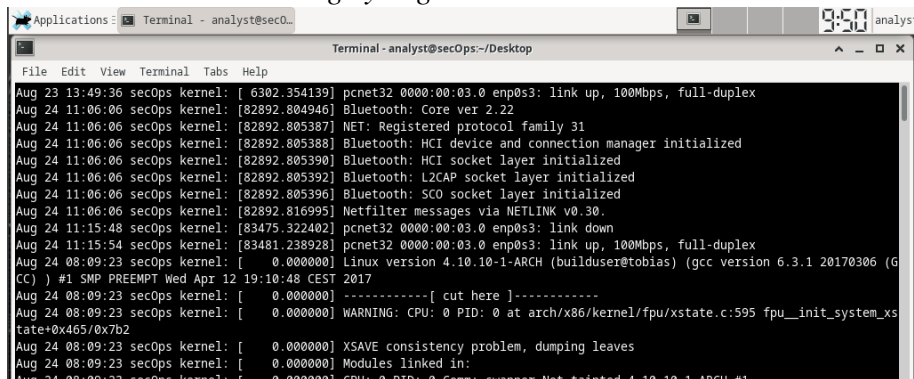
```
File Edit View Terminal Tabs Help
Mar 6 07:27:19 secOps kernel: [ 0.000000] warn_slowpath_fmt+0x46/0x60
Mar 6 07:27:19 secOps kernel: [ 0.000000] fpu_init_system_xstate+0x465/0x7b2
Mar 6 07:27:19 secOps kernel: [ 0.000000] fpu_init_system+0x18c/0x1b1
Mar 6 07:27:19 secOps kernel: [ 0.000000] early_cpu_init+0x110/0x113
Mar 6 07:27:19 secOps kernel: [ 0.000000] setup_arch+0xe4/0xbb6
Mar 6 07:27:19 secOps kernel: [ 0.000000] start_kernel+0x8f/0x3ce
Mar 6 07:27:19 secOps kernel: [ 0.000000] i386_start_kernel+0x91/0x95
Mar 6 07:27:19 secOps kernel: [ 0.000000] startup_32_smp+0x16b/0x16d
Mar 6 07:27:19 secOps kernel: [ 0.000000] ---[ end trace 8bb55a17cbc12e3d ]---
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 00]: eax=00000007 ebx=00000440 ecx=00000440 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 01]: eax=00000000 ebx=000003c0 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 02]: eax=00000100 ebx=00000240 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 03]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 04]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 05]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 06]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 07]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
```

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



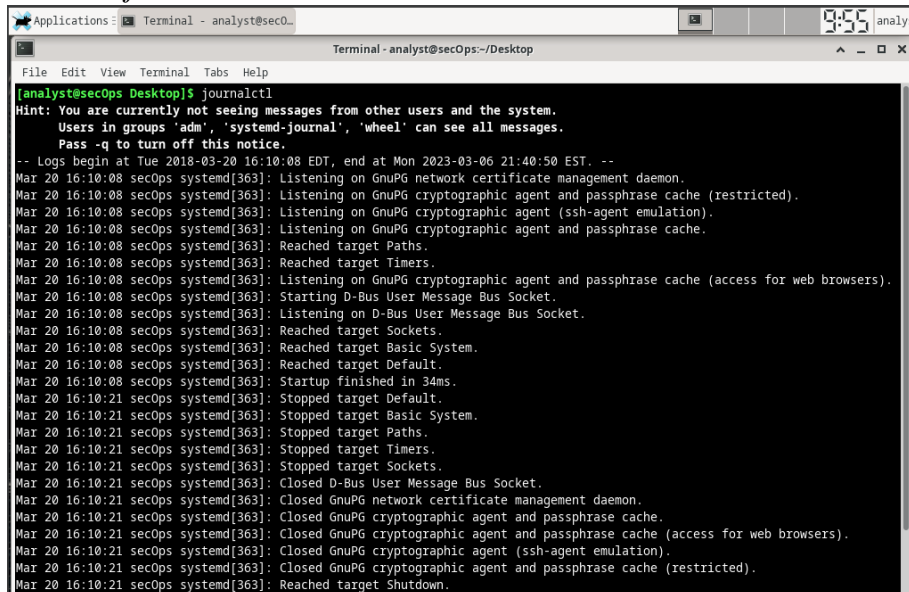
```
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ sudo cat /var/log/syslog.3
Nov 29 11:30:40 secOps kernel: [ 6.668727] ppdev: user-space parallel port driver
Nov 29 11:30:40 secOps kernel: [ 6.681487] pcnet32 0000:00:03.0 enp0s3: renamed from eth0
Nov 29 11:30:40 secOps kernel: [ 6.757097] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Nov 29 11:30:40 secOps kernel: [ 7.084534] IPv6: enp0s3: IPv6 duplicate address fe80::a00:27ff:fe23:b231 detected!
Nov 29 11:30:42 secOps kernel: [ 9.110427] floppy0: no floppy controllers found
Nov 29 11:30:42 secOps kernel: [ 9.110544] work still pending
Nov 29 04:36:27 secOps kernel: [ 0.000000] Linux version 4.10.10-1-ARCH (builduser@tobias) (gcc version 6.3.1 20170306 (G
CC) ) #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_x
tate+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
```

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



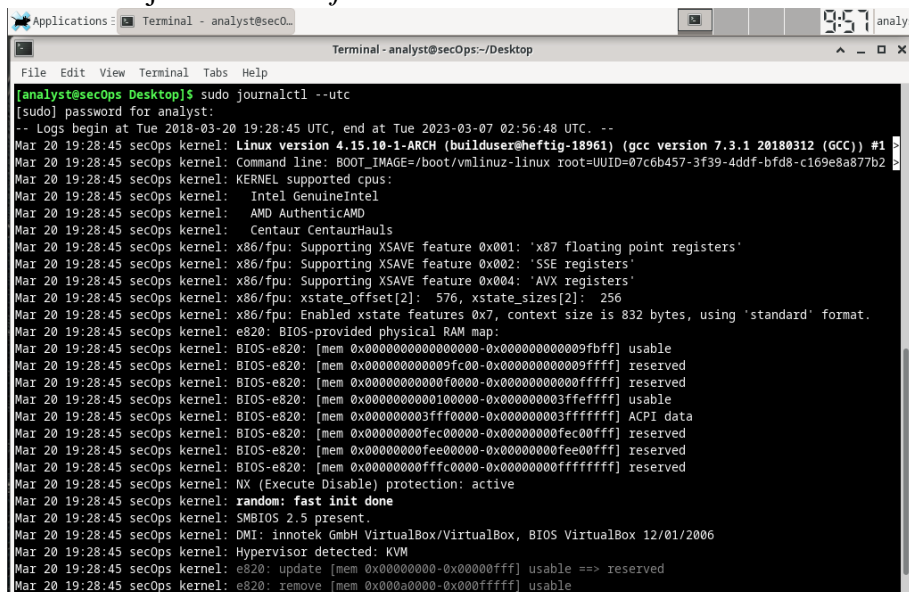
```
File Edit View Terminal Tabs Help
Aug 23 13:49:36 secOps kernel: [ 6302.354139] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Aug 24 11:06:06 secOps kernel: [82892.804946] Bluetooth: Core ver 2.22
Aug 24 11:06:06 secOps kernel: [82892.805387] NET: Registered protocol family 31
Aug 24 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 (G
CC) ) #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_x
tate+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
```

i. Jalankan *journalctl*.



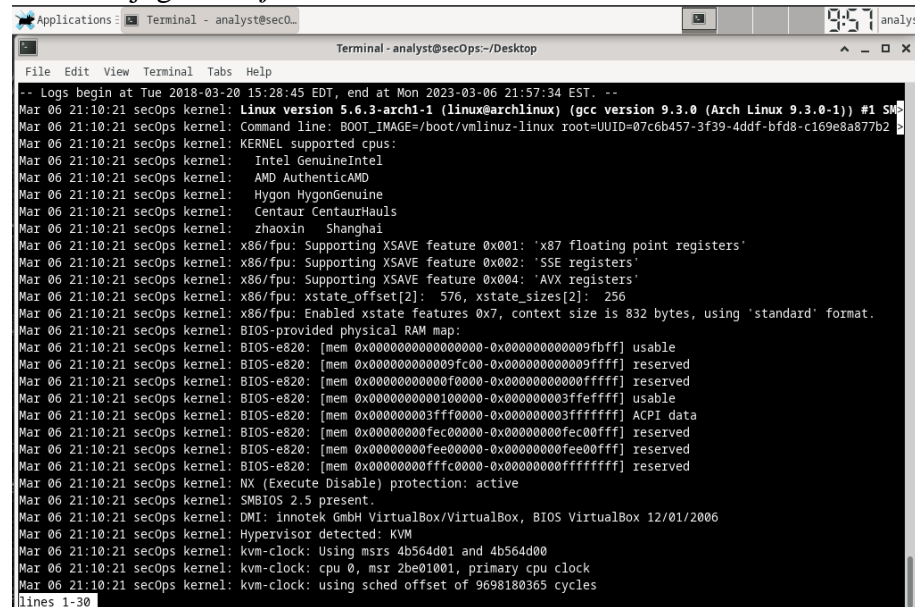
```
Applications: Terminal - analyst@sec0... 9:55 analys
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ journalctl
Hint: You are currently not seeing messages from other users and the system.
Users in groups 'adm', 'systemd-journal', 'wheel' can see all messages.
Pass -q to turn off this notice.
-- Logs begin at Tue 2018-03-20 16:10:08 EDT, end at Mon 2023-03-06 21:40:50 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.
```

Kemudian jalankan *sudo journalctl -utc*



```
Applications: Terminal - analyst@sec0... 9:57 analys
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ sudo journalctl --utc
[sudo] password for analyst:
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Tue 2023-03-07 02:56:48 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
Mar 20 19:28:45 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2
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 0x0000000000000000-0x0000000000009fbfff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009fffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000fffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000100000-0x0000000000003fffff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000003ffff0000-0x00000000003fffffff] ACPI data
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00fff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000fee00000-0x000000000fee00fff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000fffc0000-0x000000000fffffff] reserved
Mar 20 19:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 19:28:45 secOps kernel: random: fast init done
Mar 20 19:28:45 secOps kernel: SMBIOS 2.5 present.
Mar 20 19:28:45 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 20 19:28:45 secOps kernel: Hypervisor detected: KVM
Mar 20 19:28:45 secOps kernel: e820: update [mem 0x000000000-0x00000fff] usable ==> reserved
Mar 20 19:28:45 secOps kernel: e820: remove [mem 0x000000000-0x00000fff] usable
```

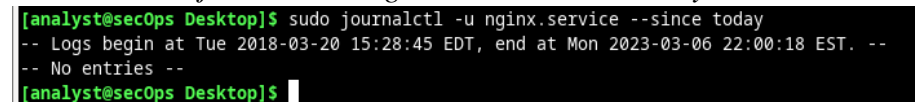
Jalankan juga *sudo journalctl -b*



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

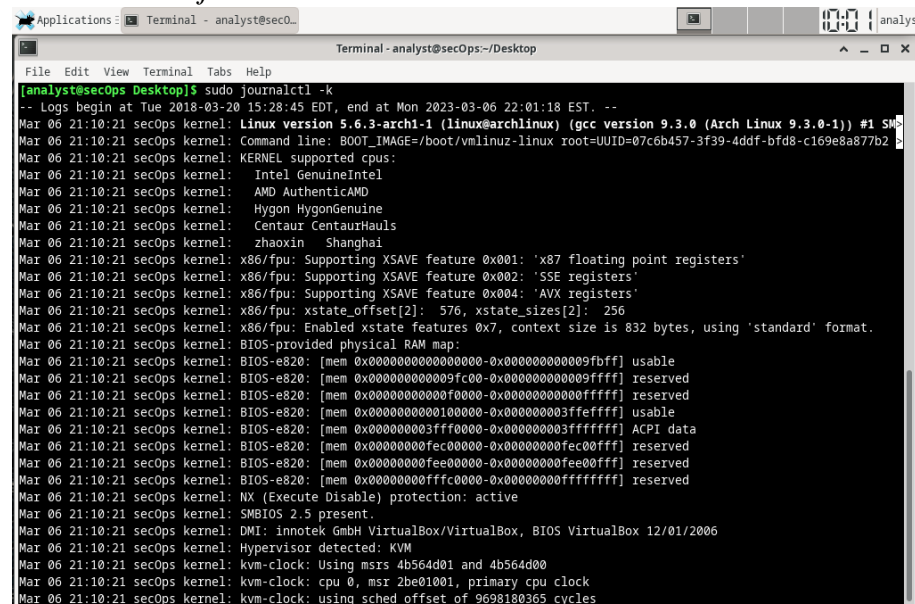
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:57:34 EST. --
Mar 06 21:10:21 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (gcc version 9.3.0 (Arch Linux 9.3.0-1)) #1 SMP
Mar 06 21:10:21 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2
Mar 06 21:10:21 secOps kernel: KERNEL supported cpus:
Mar 06 21:10:21 secOps kernel: Intel GenuineIntel
Mar 06 21:10:21 secOps kernel: AMD AuthenticAMD
Mar 06 21:10:21 secOps kernel: Hygon HygonGenuine
Mar 06 21:10:21 secOps kernel: Centaur CentaurHauls
Mar 06 21:10:21 secOps kernel: zhaoxin Shanghai
Mar 06 21:10:21 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 21:10:21 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 21:10:21 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 06 21:10:21 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Mar 06 21:10:21 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Mar 06 21:10:21 secOps kernel: BIOS-provided physical RAM map:
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbfff] usable
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x00000000000100000-0x0000000000003ffffff] usable
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x000000000003ffff000-0x000000000003ffffff] ACPI data
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 06 21:10:21 secOps kernel: NX (Execute Disable) protection: active
Mar 06 21:10:21 secOps kernel: SMBIOS 2.5 present.
Mar 06 21:10:21 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 21:10:21 secOps kernel: Hypervisor detected: KVM
Mar 06 21:10:21 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 21:10:21 secOps kernel: kvm-clock: cpu 0, msr 2be01001, primary cpu clock
Mar 06 21:10:21 secOps kernel: kvm-clock: using sched offset of 9698180365 cycles
lines 1-30
```

j. Jalankan *sudo journalctl -u nginx.service --since today*



```
[analyst@secOps Desktop]$ sudo journalctl -u nginx.service --since today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 22:00:18 EST. --
-- No entries --
[analyst@secOps Desktop]$
```

k. Jalankan *sudo journalctl -k*



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

[analyst@secOps Desktop]$ sudo journalctl -k
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 22:01:18 EST. --
Mar 06 21:10:21 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 21:10:21 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2
Mar 06 21:10:21 secOps kernel: KERNEL supported cpus:
Mar 06 21:10:21 secOps kernel: Intel GenuineIntel
Mar 06 21:10:21 secOps kernel: AMD AuthenticAMD
Mar 06 21:10:21 secOps kernel: Hygon HygonGenuine
Mar 06 21:10:21 secOps kernel: Centaur CentaurHauls
Mar 06 21:10:21 secOps kernel: zhaoxin Shanghai
Mar 06 21:10:21 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 21:10:21 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 21:10:21 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 06 21:10:21 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Mar 06 21:10:21 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Mar 06 21:10:21 secOps kernel: BIOS-provided physical RAM map:
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbfff] usable
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x00000000000100000-0x0000000000003ffffff] usable
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x000000000003ffff000-0x000000000003ffffff] ACPI data
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 21:10:21 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 06 21:10:21 secOps kernel: NX (Execute Disable) protection: active
Mar 06 21:10:21 secOps kernel: SMBIOS 2.5 present.
Mar 06 21:10:21 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 21:10:21 secOps kernel: Hypervisor detected: KVM
Mar 06 21:10:21 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 21:10:21 secOps kernel: kvm-clock: cpu 0, msr 2be01001, primary cpu clock
Mar 06 21:10:21 secOps kernel: kvm-clock: using sched offset of 9698180365 cycles
```


Dari pengujian diatas dapat dilihat bahwa ketika hanya melakukan *copy-paste* pada suatu file, maka *hashing file* tidak akan berubah, karena tidak ada informasi dari file yang berubah.

Kemudian praktikum yang kedua adalah menjalankan file log server dengan beberapa perintah seperti *cat*, *more*, *less*, atau *tail*. Pengujian pertama adalah menggunakan *cat*. *Cat* sendiri merupakan akronim dari *concatenate* yang berfungsi untuk mencantumkan, menggabungkan, dan menulis konten atau isi file dalam *output* standar. Kelemahan perintah *cat* ini adalah ketika digunakan untuk preview file dengan ukuran besar, karena *cat* akan melakukan review semua isi file hingga teks atau karakter paling terakhir. Sehingga akan mengalami kesulitan ketika digunakan untuk mengoreksi hasil tulisan dalam memeriksa teks awal.

Perintah yang kedua adalah *more*, memiliki fungsi yang hampir sama seperti *cat* yaitu untuk menampilkan isi suatu file. Perbedaannya adalah pada perintah *more* ini akan menampilkan isi file dengan batasan 1 halaman. Untuk melihat teks berikutnya dapat menggunakan enter untuk 1 baris berikutnya atau menggunakan spasi untuk menampilkan 1 halaman berikutnya. Kelemahan dari perintah *more* ini adalah tidak dapat menampilkan teks pada halaman sebelumnya.

Perintah selanjutnya adalah *less*, yang memiliki fungsi sama seperti perintah sebelumnya, yaitu untuk menampilkan isi dari suatu file. Perintah *less* ini memiliki keunggulan dari *cat* maupun *more*, yaitu dapat menampilkan teks dengan batasan 1 halaman dan dapat melihat teks pada halaman sebelum maupun setelahnya.

Kemudian perintah berikutnya adalah *tail*, yang berfungsi untuk menampilkan 10 baris terakhir isi file secara default. Perintah ini sangat cocok untuk melihat log server, karena dapat digunakan untuk memantau perubahan isi file secara *realtime* dengan menambahkan opsi *-f* setelah perintah *tail*. Berikut merupakan hasil ketika mengetikkan perintah **man tail**.

```
-f, --follow[={name|descriptor}]
    output appended data as the file grows;

    an absent option argument means 'descriptor'
```

Setelah itu, terdapat juga *syslog*, yang mana *syslog* adalah *system logging* protocol standar yang digunakan untuk merekam semua kegiatan yang dilakukan

dalam sebuah sistem dari suatu server. Untuk menampilkan isi file *syslog* harus dijalankan sebagai root karena direktori */var/log/syslog* berada dalam direktori root. Maka dalam perintah *cat* perlu ditambahkan *sudo* agar dapat dijalankan sebagai root. Untuk menghindari file yang terlalu besar, biasanya OS secara berkala akan mengganti nama file *syslog*. Agar dapat diketahui waktu aktivitas dari suatu file *syslog*, maka kita perlu melakukan sinkronisasi waktu dan tanggal dengan benar.

Terdapat juga *tools journald* dengan perintah dasarnya yaitu *journalctl* yang memiliki fungsi untuk menganalisis log. Pada perintah ini dapat juga digunakan untuk menampilkan hasil analisis log yang telah disimpan sebelumnya. Dalam *journalctl* ini memiliki kelebihan bahwa terdapat cukup banyak pilihan (*option*) untuk menjalankan perintah tersebut, seperti opsi *-utc* untuk menampilkan cap waktu sesuai dengan zona waktu UTC. Kemudian terdapat juga opsi *-b* yang berfungsi untuk menampilkan entri log yang direkam selama *boot* terakhir.

Tools journald dapat dikombinasikan dengan suatu opsi *filtering* agar hanya menampilkan pesan tertentu. Contohnya adalah *-k* yang merupakan opsi hanya menampilkan pesan yang dihasilkan oleh kernel. Kemudian dapat juga *filtering* untuk menampilkan suatu layanan tertentu dan kerangka waktu untuk entri log seperti *-u nginx.service --since today*. *Journalctl* dapat juga dipantau secara *realtime* seperti halnya *tail*, yaitu dengan menggunakan opsi *-f*.

VI. Kesimpulan

Pada praktikum kali ini dapat disimpulkan bahwa :

1. Kita dapat menyembunyikan informasi pada sebuah file dengan menggunakan teknik *steganography*.
2. File asli dengan file yang telah diisi suatu informasi tersembunyi memiliki kode hash yang berbeda.
3. Terdapat beberapa perintah untuk menampilkan isi file *log*
4. *Syslog* harus dijalankan sebagai *root* karena *syslog* disimpan pada direktori yang ada pada sistem *root*.
5. Terdapat *tools* untuk menganalisis suatu file log yang biasa disebut sebagai *journald*.
6. Kita dapat melakukan pemantauan file log maupun *journalctl* dengan menambahkan opsi *-f*

VII. Daftar Pustaka

- Gemilang, R. (February 14, 2018). PENGERTIAN STEGANOGRAFI, JENIS-JENIS, DAN PRINSIP KERJA. Retrieved March 10, 2023, from <https://www.immersa-lab.com/pengertian-steganografi-jenis-jenis-dan-prinsip-kerja.htm>
- Syamsu, S. (May 06, 2009). Mengenal berbagai jenis file log di server linux. Retrieved March 10, 2023, from <https://suryadisamsu.blogspot.com/2009/05/mengenal-berbagai-jenis-file-log-di.html>
- Gupta, A. (May 06, 2022). Lakukan sulap dengan log Linux Anda dengan Manajemen Log. Retrieved March 10, 2023, from <https://www.motadata.com/id/blog/do-magic-with-your-linux-logs-with-log-management/#:~:text=Amartya%20Gupta&text=Data%20log%20adalah%20file%20yang,aplikasi%20yang%20berjalan%20di%20server>.
- Motadata. (February 15, 2023). Pemantauan Syslog. Retrieved March 10, 2023, from <https://www.motadata.com/id/syslog-monitoring/>
- Ariata, C. (February, 17 2023). 40 Perintah Dasar Linux yang Perlu Anda Tahu. Retrieved March 10, 2023, from [https://www.hostinger.co.id/tutorial/perintah-dasar-linux#:~:text=cat%20\(akronim%20dari%20concatenate\)%20adalah,diikuti%20nama%20dan%20ekstensi%20file](https://www.hostinger.co.id/tutorial/perintah-dasar-linux#:~:text=cat%20(akronim%20dari%20concatenate)%20adalah,diikuti%20nama%20dan%20ekstensi%20file).
- Xsand. (October 26, 2022). Memahami Perintah Tail Pada Linux Terminal. Retrieved March 10, 2023, from <https://www.linuxid.net/24803/memahami-perintah-tail-pada-linux-terminal/>
- Putra, C. A. (December 19, 2012). Perintah Menampilkan file teks di Linux. Retrieved March 10, 2023, from <https://www.candra.web.id/perintah-menampilkan-file-teks-di-linux/>
- Menggunakan journalctl untuk melihat dan menganalisis log: panduan terperinci. Geek, C. (*Unknown*). Menggunakan journalctl untuk melihat dan menganalisis log: panduan terperinci. Retrieved March 10, 2023, from <https://tech-id.netlify.app/articles/id533918/index.html>