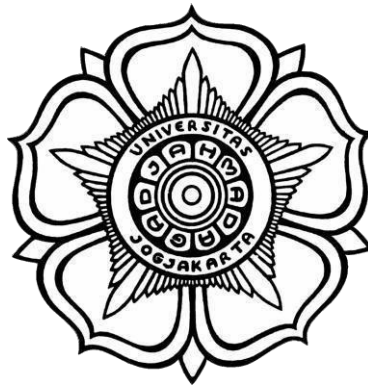


LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
UNIT 4

“Teknik Steganografi dan Analisis Log Server”



Disusun Oleh:

Nama	: Saadah Mardatillah
NIM	: 21/473000/SV/18792
Kelas	: Teknologi Rekayasa Internet A
Hari, Tanggal	: Senin, 13 Maret 2023
Dosen Pengampu	: Anni Karimatul Fauziyyah, S.Kom.,M.Eng.
Asisten Praktikum	: Gabriella Alvera Chaterine

PROGRAM STUDI DIPLOMA IV TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

A. Tujuan

1. Mahasiswa dapat memahami dan melakukan demonstrasi dari cara kerja steganografi
2. Mahasiswa dapat memahami bagaimana cara kerja pembacaan File Log dengan *Cat*, *More*, *Less*, dan *Tail*
3. Mahasiswa dapat memahami cara kerja File Log dan Syslog
4. Mahasiswa dapat memahami cara kerja File Log dan Jurnalctl

B. Alat dan Bahan

1. Pc
2. Jaringan Internet
3. *CyberOps Workstation VM*

C. Latar Belakang

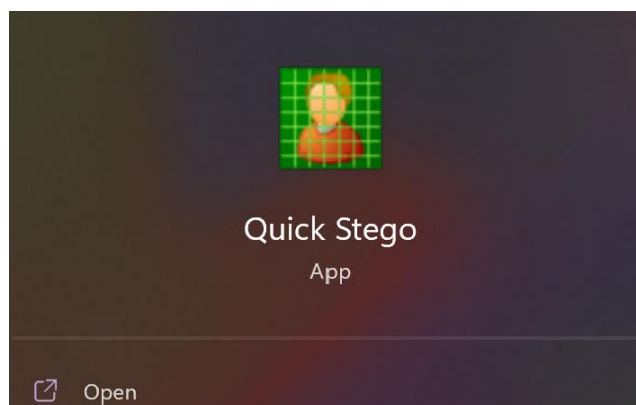
Steganografi merupakan teknik dalam menyembunyikan suatu pesan rahasia (*hiding message*) agar keberadaan atau makna pesan tidak dapat terdeteksi oleh orang lain kecuali oleh pengirim dan penerima pesan. Terdapat tujuh teknik steganografi yaitu : 1) *Injection* 2) *Substitution* 3) *Tranformasi Domain* 4) *Spread Spectrum* 5) *Statistical Method* 6) *Distortion* 7) *Cover Generation* (Ariyus, 2009). Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan yang tersembunyi atau sebuah informasi. Steganografi dapat digunakan untuk berbagai alasan, seperti alasan baik ataupun sebaliknya “alasan tidak baik”. Dalam tujuan legitimasi digunakan untuk pengamanan seperti citra dengan *watermarking* dengan alasan perlindungan *copyright*. Steganografi berbeda dengan Kriptografi perbedaan terletak pada visabilitas pesan. Pada kriptografi pihak ketiga dapat mendeteksi adanya data acak (*chipertext*), karena hasil dari kriptografi berupa data yang berbeda dari data asli dan data seolah – olah berantakan, akan tetapi dapat dikembalikan ke bentuk semula. Kriptografi menjaga kerahasiaan pesan dengan cara mengubah pesan untuk tidak dapat dipahami oleh orang lain. Sedangkan pada steganografi pesan tidak perlu diubah, tetapi pesan disembunyikan pada suatu medium agar pesan tidak dapat terlihat.

Log Server adalah *file log* yang dibuat dan dipelihara oleh server secara otomatis. Peringatan yang berisi daftar aktivitas yang dilakukan oleh server, seperti jumlah permintaan halaman, alamat IP klien, jenis permintaan dan lainnya. *File Log* merupakan alat penting dalam memecahkan masalah dan pemantauan. Aplikasi yang berbeda menghasilkan *file log* yang berbeda, masing – masing berisi kumpulan bidang dan informasi sendiri. Secara struktur bidang dapat berubah di antara *file log*, alat yang digunakan untuk membacanya Sebagian besar sama. *File Log* merupakan *file* digunakan untuk merekam peristiwa tertentu untuk dihasilkan oleh aplikasi, layanan, atau sistem operasi itu sendiri. Biasanya *File Log* disimpan sebagai teks biasa. *File Log* berisi informasi teks yang dapat terlihat oleh semua program yang dapat menangani teks. Namun, kemudahan, kegunaan dan kecepatan, beberapa alat lebih umum digunakan daripada lainnya. *File Log* penting karena menyediakan catatan informasi sistem yang terperinci dan mudah diakses, yang jika tidak, akan sulit untuk disusun. *File log* juga memberikan wawasan mengenai performa dan kepatuhan aplikasi serta sistem pada pengguna.

D. Data Instruksi Kerja

Steganografi:

1. Melakukan download file STEGO



2. Melakukan download file MD5SUMS

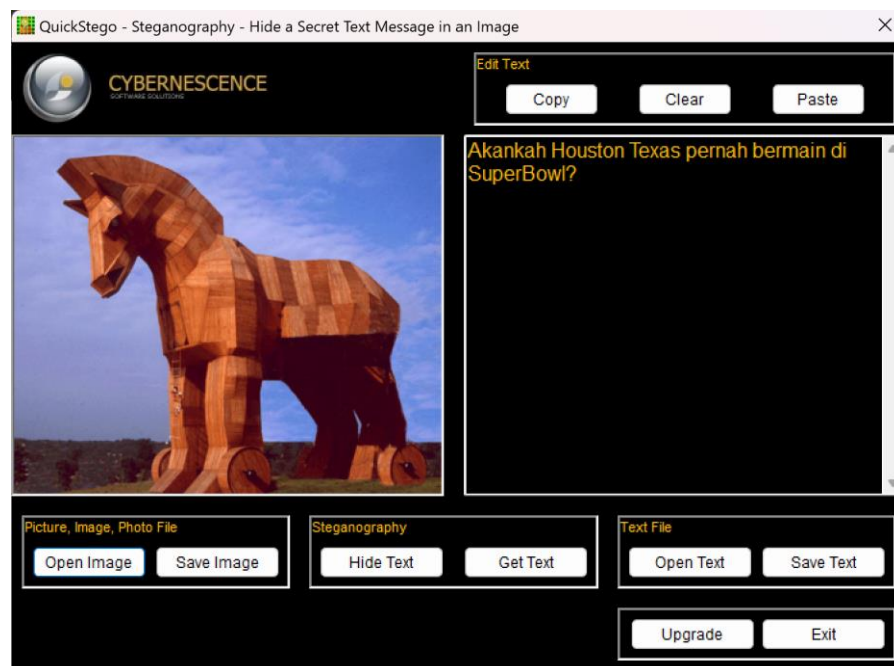


3. Membuat folder STEGO

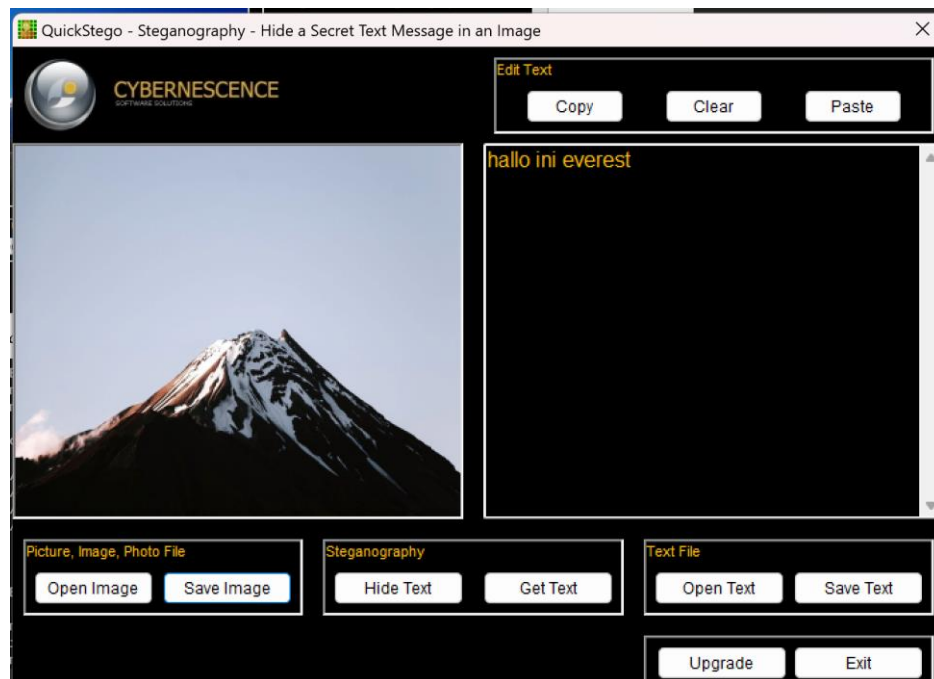
File Explorer view of the STEGO folder (C:\STEGO):

Name	Date modified	Type	Size
everest	13/03/2023 14:36	JPG File	98 KB
everest_secret	13/03/2023 14:43	JPG File	1.952 KB
horse	09/03/2023 20:05	JPG File	45 KB
horse_secret	13/03/2023 14:05	JPG File	834 KB
md5sums	09/03/2023 20:02	Application	28 KB
md5sums	09/03/2023 20:02	Text Document	5 KB
md5sums-1.2	12/03/2023 16:23	Compressed (zipped)...	29 KB
QS.lic	18/10/2009 14:42	LIC File	1 KB
quickstego	18/10/2009 14:41	Application	284 KB
QuickStego.exe.manifest	09/06/2009 13:51	MANIFEST File	1 KB
quickstego_license	11/09/2008 14:40	Text Document	2 KB
unins000.dat	09/03/2023 19:48	DAT File	2 KB
unins000	09/03/2023 19:47	Application	701 KB

4. Menjalankan STEGO gambar kuda



5. Menjalankan STEGO gambar gunung everest



6. Bukti *command prompt*

```
Command Prompt
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hp>cd C:\STEGO

C:\STEGO>dir *.jpg
Volume in drive C is Windows
Volume Serial Number is A81F-28AD

Directory of C:\STEGO

13/03/2023  14:36           100.145 everest.jpg
13/03/2023  14:43       1.998.054 everest_secret.jpg
09/03/2023  20:05           46.001 horse.jpg
13/03/2023  14:05       853.974 horse_secret.jpg
               4 File(s)      2.998.174 bytes
               0 Dir(s)  56.999.354.368 bytes free

C:\STEGO>md5sums.exe *.jpg

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

[Path] / filename                               MD5 sum
-----
[C:\STEGO\]
everest.jpg                                     166f7a0c1b733bd18b1dd48864bd8b5b
everest_secret.jpg                             45d648fdb1ab93568dbd4d0631bf2a7d
horse.jpg                                       fce8552170cccd3dd545566309124097
horse_secret.jpg                               adb2b90cf413b38ffb885ac2a0b62c0
```

Steganografi:

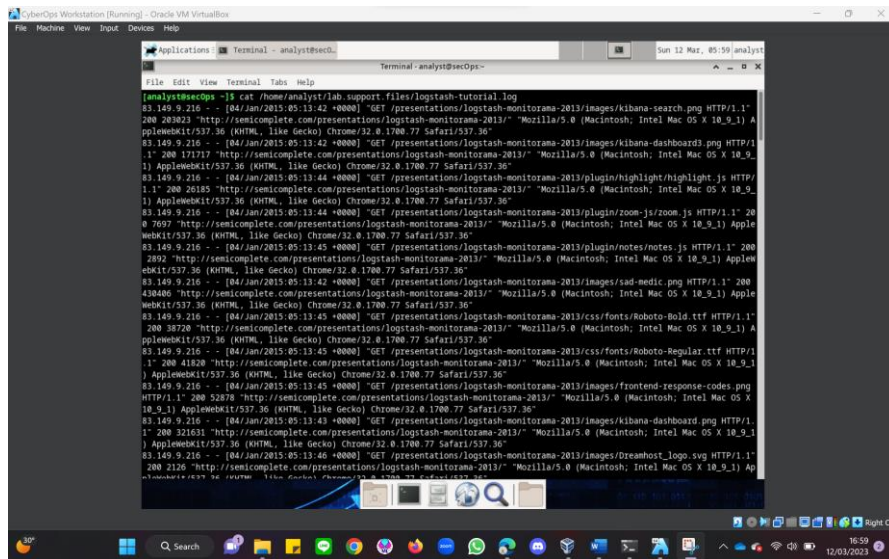
1. Membaca *file log cat*

Tugas = Dari jendela terminal, jalankan perintah di bawah ini untuk menampilkan konten file logstash-tutorial.log, yang terletak di folder /home/analyst/lab.support.files/:

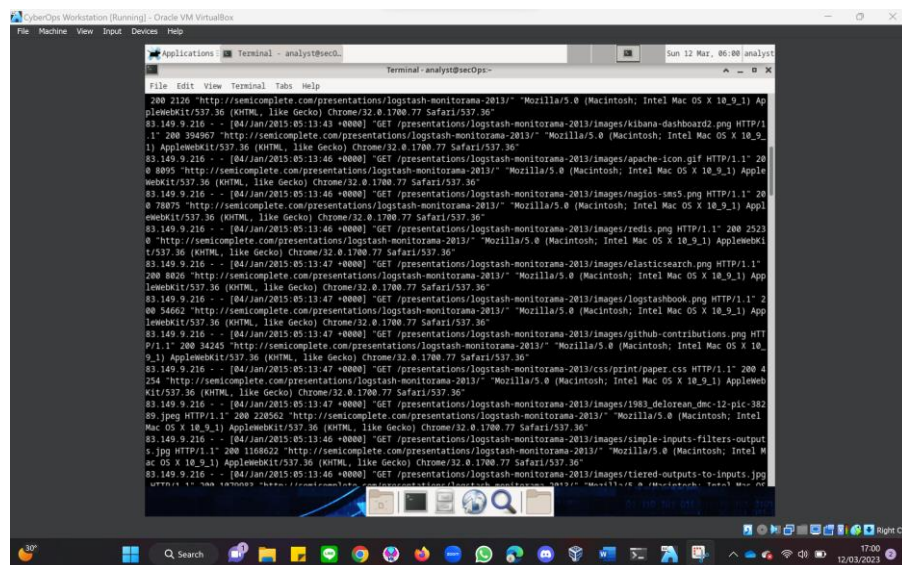
```
analis@secOps ~$ cat /home/analyst/lab.support.files/logstash-tutorial.log
```

Isi file harus ditampilkan melalui jendela terminal.

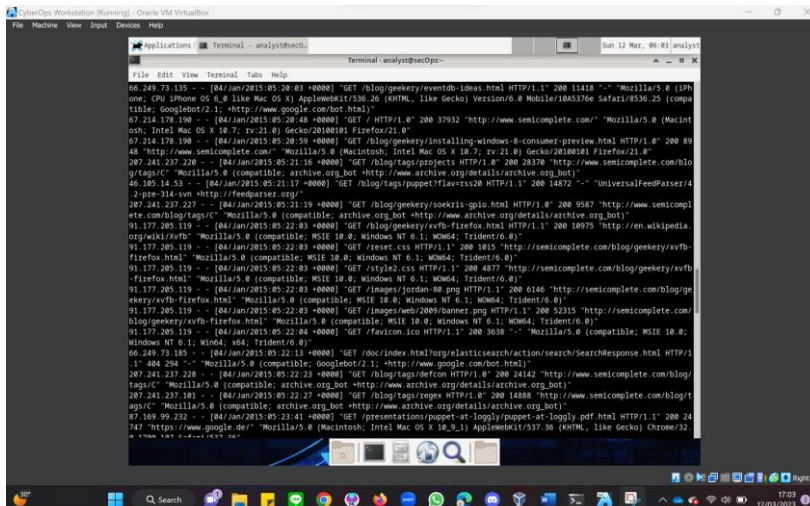
Pertanyaan: Apa kelemahan menggunakan cat dengan file teks besar?



```
[analyst@secOps ~]$ cat /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1"
200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/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 171117 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/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 208185 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/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) Apple
WebKit/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) AppleWe
bKit/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 430466 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) Apple
WebKit/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) A
ppleWebKit/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) A
ppleWebKit/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 52078 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/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) A
ppleWebKit/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) A
ppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
```



```
200 2126 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/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 394967 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/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/apache-iron.gif HTTP/1.1"
200 80095 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) Apple
WebKit/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/nagios-sm5.png HTTP/1.1"
200 78875 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWe
bKit/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/redis.png HTTP/1.1"
200 2523 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebsi
t/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/images/elasticsearch.png HTTP/1.1"
200 8820 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebsi
t/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/images/logstashbook.png HTTP/1.1"
200 54662 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) App
leWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/images/github-contributions.png HT
TP/1.1"
200 34245 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/css/print/paper.css HTTP/1.1"
200 4254 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebsi
t/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/images/1983_dolorum_dsc-12-pic-382
69.jpg HTTP/1.1"
200 116622 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/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/single-inputs-filters-output
s.jpg HTTP/1.1"
200 116622 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/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/tiered-outputs-to-inputs.jpg
HTTP/1.1"
200 116622 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
```



2. Membaca *file log more*

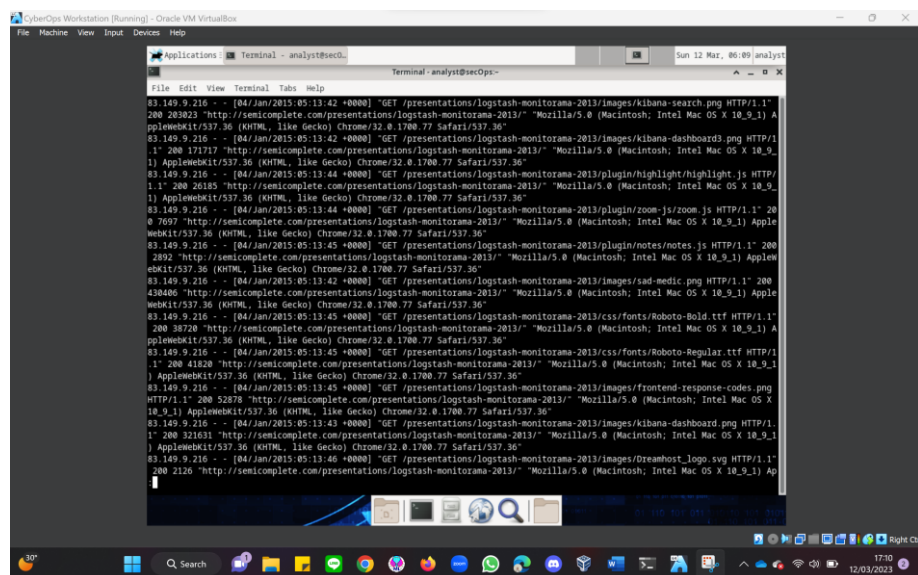
Tugas = Dari jendela terminal yang sama, gunakan perintah di bawah ini untuk menampilkan kembali isi file logstash-tutorial.log. Proses ini menggunakan more: analis@secOps ~\$ more /home/analyst/lab.support.files/logstash-tutorial.log Isi file harus ditampilkan melalui jendela terminal dan berhenti ketika satu halaman tersebut ditampilkan. Tekan spasi untuk berpindah ke halaman berikutnya. Tekan enter untuk menampilkan baris teks berikutnya.

Pertanyaan: Apa kelemahan menggunakan more?

```
[analyst@secOps ~]$ more /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-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 HTTP/1.1" 2
00 7697 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) App
leWebKit/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" 20
0 2892 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) Appl
eWebKit/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) App
leWebKit/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"
--More-- (10%)
```

3. Membaca *file log less*

Tugas = Dari tampilan terminal yang sama, gunakan less untuk menampilkan konten file logstashtutorial.log lagi: analis@secOps ~\$ lebih sedikit /home/analyst/lab.support.files/logstash-tutorial.log



4. Membaca *file log tail*

Tugas = 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`.

Pertanyaan: Apa yang berbeda dalam output `tail` dan `tail -f`? Jelaskan

```
[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"
```

5. Membaca *file log tail -f*

Tugas = Pada jendela terminal tersebut, jalankanlah `tail -f` untuk melihat file `/home/analyst/lab.support.files/logstash-tutorial.log`. Gunakan jendela terminal di bagian bawah untuk menambahkan informasi ke file yang dipantau. Untuk memudahkan visualisasi, pilih jendela terminal atas (yang menjalankan `tail -f`) dan tekan enter beberapa kali. Ini akan menambahkan beberapa baris antara konten file saat ini dan informasi baru yang akan ditambahkan

```
[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"
```

6. Melakukan pemantauan file pada *tail -f*

```
[analyst@secOps ~]$ echo "this is a new entry to the monitored log file" >>lab.support.files/logstash-tutorial.log

[analyst@secOps ~]$ tail -f /home/analyst/lab.support.files/logstash-tutorial.log
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 11834 "-" "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"
this is a new entry to the monitored log file
this is a new entry to the monitored log file
this is a new entry to the monitored log file
```

7. Memahami file log dan *syslog*

Tugas = Gunakan perintah **cat** sebagai **root** untuk membuat daftar isi file `/var/log/syslog.1`. File ini menyimpan entri log yang dihasilkan oleh sistem operasi CyberOps Workstation VM dan dikirim ke layanan syslog.

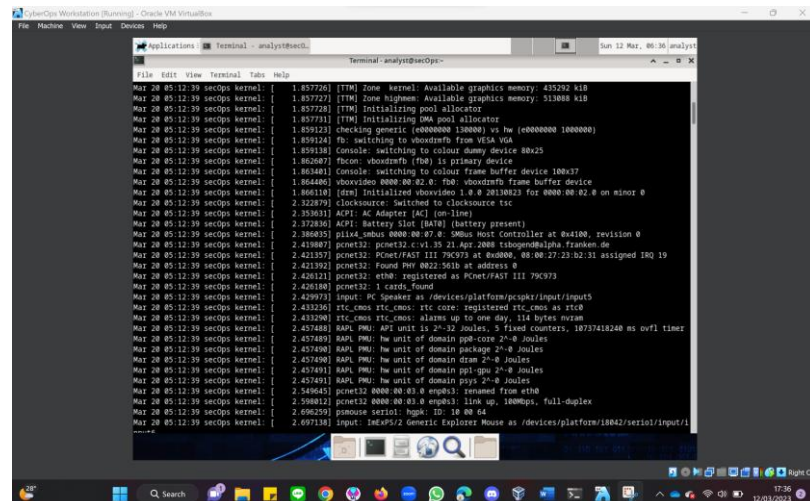
analis@secOps ~\$ sudo cat /var/log/syslog.1

[Sudo] kata sandi untuk analis:

Pertanyaan:

Mengapa perintah cat harus dijalankan sebagai root?

```
[analyst@secOps ~]$ sudo cat /var/log/syslog.1
[sudo] password for analyst:
```

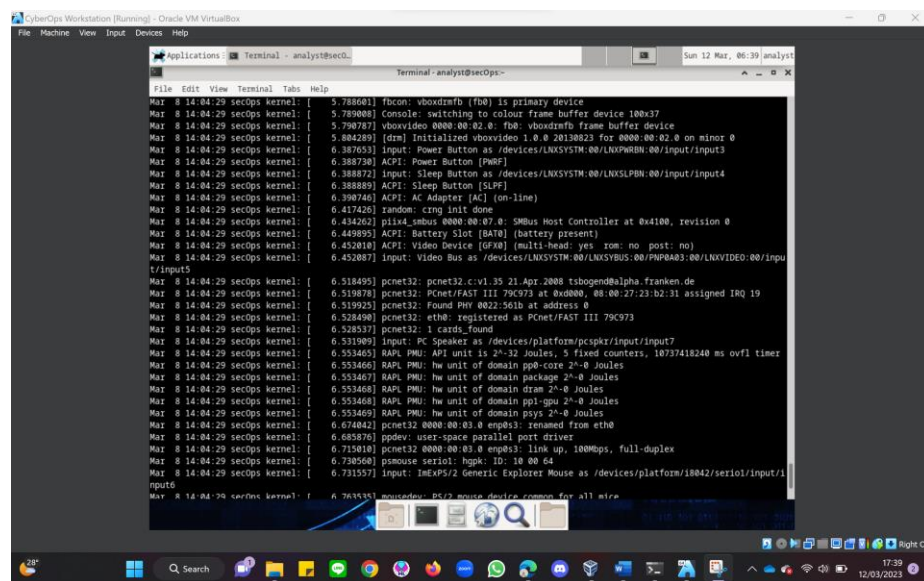


8. Perhatikan bahwa file `/var/log/syslog` hanya menyimpan entri log terbaru. Untuk menjaga agar file `syslog` tetap kecil, sistem operasi secara berkala merotasi file log, mengganti nama file log lama menjadi `syslog.1`, `syslog.2`, dan seterusnya.
9. Gunakan perintah `cat` untuk membuat daftar file `syslog` yang lebih lama:
`analis@secOps ~$ sudo cat /var/log/syslog.2`
`analis@secOps ~$ sudo cat /var/log/syslog.3`
`analis@secOps ~$ sudo cat /var/log/syslog.4`

Pertanyaan: Jelaskan kenapa harus mensinkronkan waktu dan tanggal komputer dengan benar?

Syslog2

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



Syslog3

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

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

Applications: Terminal - analyst@secOps-
Terminal - analyst@secOps-
Sun 12 Mar, 06:48 analyst

File Edit View Terminal Tabs Help

Mar 6 06:58:55 secOps kernel: [ 4.628315] Console: switching to colour dummy device 80x25
Mar 6 06:58:55 secOps kernel: [ 4.628447] fbcon: vboxdmfb (fb0) is primary device
Mar 6 06:58:55 secOps kernel: [ 4.630243] Console: switching to colour frame buffer device 100x37
Mar 6 06:58:55 secOps kernel: [ 4.637132] vboxdmfb 0000:00:02.0: fb0: vboxdmfb frame buffer device
Mar 6 06:58:55 secOps kernel: [ 4.646881] [drm] Initialized vboxdmfb 1.0.0 20130823 for 0000:00:02.0 on minor 0
Mar 6 06:58:55 secOps kernel: [ 4.713663] EXT4-fs (sda1): re-mounted. Opts: data=ordered
Mar 6 06:58:55 secOps kernel: [ 5.230999] ACPI: AC Adapter [AC] (on-line)
Mar 6 06:58:55 secOps kernel: [ 5.359785] input: Power Button as /devices/LNXSYSTM:00/LNXPWRBN:00/input/input3
Mar 6 06:58:55 secOps kernel: [ 5.361299] ACPI: Power Button [PWRB]
Mar 6 06:58:55 secOps kernel: [ 5.361417] input: Sleep Button as /devices/LNXSYSTM:00/LNKSLPBN:00/input/input4
Mar 6 06:58:55 secOps kernel: [ 5.361452] ACPI: Sleep Button [SLPF]
Mar 6 06:58:55 secOps kernel: [ 5.412866] ACPI: Video Device [GFXA] (multi-head: yes rom: no post: no)
Mar 6 06:58:55 secOps kernel: [ 5.412948] input: Video Bus as /devices/LNXSYSTM:00/LNKSYSBUS:00/PNP0A03:00/LNXXVIDEO:00/input/input5
Mar 6 06:58:55 secOps kernel: [ 5.446998] FUJITSU Extended Socket Network Device Driver - version 1.2 - Copyright (c) 2015 FUJITSU LIMITED
Mar 6 06:58:55 secOps kernel: [ 5.510986] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
Mar 6 06:58:55 secOps kernel: [ 5.517557] pcnet32: PCnet/FAST III 79C973 at 0x0000, 08:00:27:23:b2:31 assigned IRQ 19
Mar 6 06:58:55 secOps kernel: [ 5.517609] pcnet32: Found PHY 0022:561b at address 0
Mar 6 06:58:55 secOps kernel: [ 5.517956] pcnet32: eth0: registered as PCnet/FAST III 79C973
Mar 6 06:58:55 secOps kernel: [ 5.531118] ACPI: Battery Slot [BAT0] (battery present)
Mar 6 06:58:55 secOps kernel: [ 5.537141] piix4_smbus 0000:00:07.0: SMBus Host Controller at 0x4100, revision 0
Mar 6 06:58:55 secOps kernel: [ 5.552943] pcnet32: 1 cards found
Mar 6 06:58:55 secOps kernel: [ 5.587936] mousedev: PS/2 mouse device common for all mice
Mar 6 06:58:55 secOps kernel: [ 5.608268] input: PC Speaker as /devices/platform/pcspkr/input/input6
Mar 6 06:58:55 secOps kernel: [ 5.707891] RAPL PMU: API unit is 2^-32 Joules, 5 fixed counters, 10737418240 ms ovfl timer
Mar 6 06:58:55 secOps kernel: [ 5.707893] RAPL PMU: hw unit of domain pp0-core 2^-0 Joules
Mar 6 06:58:55 secOps kernel: [ 5.707894] RAPL PMU: hw unit of domain package 2^-0 Joules
Mar 6 06:58:55 secOps kernel: [ 5.707894] RAPL PMU: hw unit of domain dram 2^-0 Joules
Mar 6 06:58:55 secOps kernel: [ 5.707895] RAPL PMU: hw unit of domain ppi-gpu 2^-0 Joules
Mar 6 06:58:55 secOps kernel: [ 5.707895] RAPL PMU: hw unit of domain pssys 2^-0 Joules
Mar 6 06:58:55 secOps kernel: [ 5.776653] random: cng init done
Mar 6 06:58:55 secOps kernel: [ 5.788340] VBoxService 5.1.18 r114002 (verbosity: 0) linux.x86 (Mar 16 2017 20:50:16) relea
```

Syslog4

```
[analyst@secOps ~]$ sudo cat /var/log/syslog.4
```

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

Applications: Terminal - analyst@secOps-
Terminal - analyst@secOps-
Sun 12 Mar, 06:52 analyst

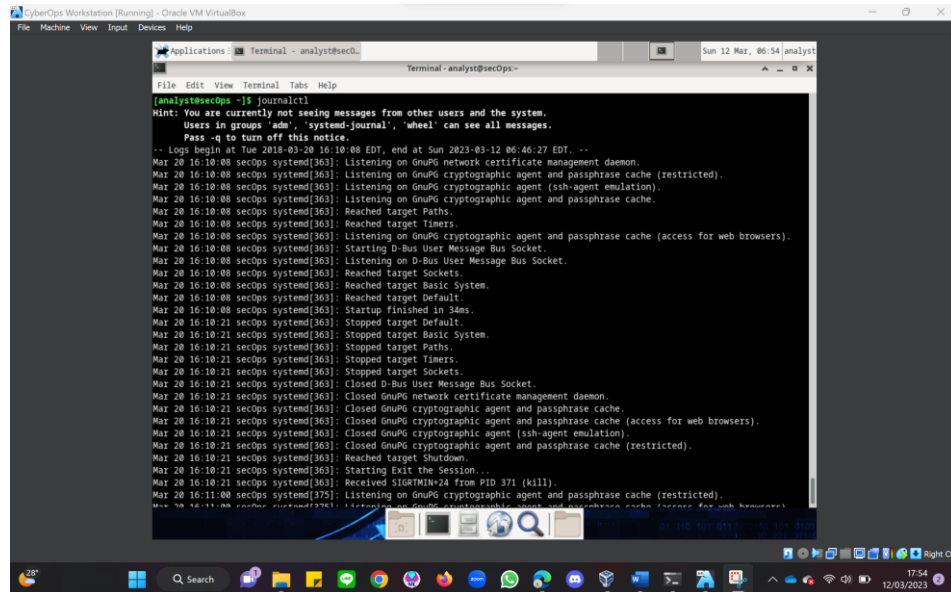
File Edit View Terminal Tabs Help

Nov 29 04:30:38 secOps kernel: [ 5.862607] input: Video Bus as /devices/LNXSYSTM:00/LNKSYSBUS:00/PNP0A03:00/LNXXVIDEO:00/input/input5
Nov 29 04:30:38 secOps kernel: [ 5.907769] nf_conntrack version 0.5.0 (16384 buckets, 65536 max)
Nov 29 04:30:38 secOps kernel: [ 5.925661] FUJITSU Extended Socket Network Device Driver - version 1.2 - Copyright (c) 2015 FUJITSU LIMITED
Nov 29 04:30:38 secOps kernel: [ 5.926186] piix4_smbus 0000:00:07.0: SMBus Host Controller at 0x4100, revision 0
Nov 29 04:30:38 secOps kernel: [ 5.947873] mousedev: PS/2 mouse device common for all mice
Nov 29 04:30:38 secOps kernel: [ 5.969873] ACPI: Battery Slot [BAT0] (battery present)
Nov 29 04:30:38 secOps kernel: [ 5.978844] input: Power Button as /devices/LNXSYSTM:00/LNXPWRBN:00/input/input4
Nov 29 04:30:38 secOps kernel: [ 5.979307] ACPI: Power Button [PWRB]
Nov 29 04:30:38 secOps kernel: [ 5.980814] input: Sleep Button as /devices/LNXSYSTM:00/LNKSLPBN:00/input/input5
Nov 29 04:30:38 secOps kernel: [ 5.985142] ACPI: Sleep Button [SLPF]
Nov 29 04:30:38 secOps kernel: [ 5.992292] openvswitch: Open vSwitch switching datapath
Nov 29 04:30:38 secOps kernel: [ 6.013723] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
Nov 29 04:30:38 secOps kernel: [ 6.014218] pcnet32: PCnet/FAST III 79C973 at 0x0000, 08:00:27:23:b2:31 assigned IRQ 19
Nov 29 04:30:38 secOps kernel: [ 6.014265] pcnet32: Found PHY 0022:561b at address 0
Nov 29 04:30:38 secOps kernel: [ 6.014587] pcnet32: eth0: registered as PCnet/FAST III 79C973
Nov 29 04:30:38 secOps kernel: [ 6.014605] pcnet32: 1 cards found
Nov 29 04:30:38 secOps kernel: [ 6.064002] input: PC Speaker as /devices/platform/pcspkr/input/input6
Nov 29 04:30:38 secOps kernel: [ 6.142925] RAPL PMU: API unit is 2^-32 Joules, 5 fixed counters, 10737418240 ms ovfl timer
Nov 29 04:30:38 secOps kernel: [ 6.142927] RAPL PMU: hw unit of domain pp0-core 2^-0 Joules
Nov 29 04:30:38 secOps kernel: [ 6.142927] RAPL PMU: hw unit of domain package 2^-0 Joules
Nov 29 04:30:38 secOps kernel: [ 6.142928] RAPL PMU: hw unit of domain dram 2^-0 Joules
Nov 29 04:30:38 secOps kernel: [ 6.142928] RAPL PMU: hw unit of domain ppi-gpu 2^-0 Joules
Nov 29 04:30:38 secOps kernel: [ 6.142929] RAPL PMU: hw unit of domain pssys 2^-0 Joules
Nov 29 04:30:38 secOps kernel: [ 6.180343] VBoxService 5.1.18 r114002 (verbosity: 0) linux.x86 (Mar 16 2017 20:50:16) relea
Nov 29 04:30:38 secOps kernel: [ 6.180343] se log
Nov 29 04:30:38 secOps kernel: [ 6.180343] 00:00:00.000124 main Log opened 2017-11-29T09:30:38.792377000Z
Nov 29 04:30:38 secOps kernel: [ 6.184374] 00:00:00.0004263 main OS Product: Linux
Nov 29 04:30:38 secOps kernel: [ 6.184681] 00:00:00.0004570 main OS Release: 4.10.10-1-ARCH
Nov 29 04:30:38 secOps kernel: [ 6.185021] 00:00:00.0004849 main OS Version: #1 SMP PREEMPT Wed Apr 12 19:10:40 CEST 2017
Nov 29 04:30:38 secOps kernel: [ 6.186194] 00:00:00.0006812 main Executable: /usr/bin/VBoxService
Nov 29 04:30:38 secOps kernel: [ 6.186194] 00:00:00.0006812 main
```


10. Memahami *file* log dan *journalctl*

Untuk melihat log *journald*, gunakan perintah *journalctl*. Alat *journalctl* menafsirkan dan menampilkan entri log yang sebelumnya disimpan dalam file log biner *jurnal*.

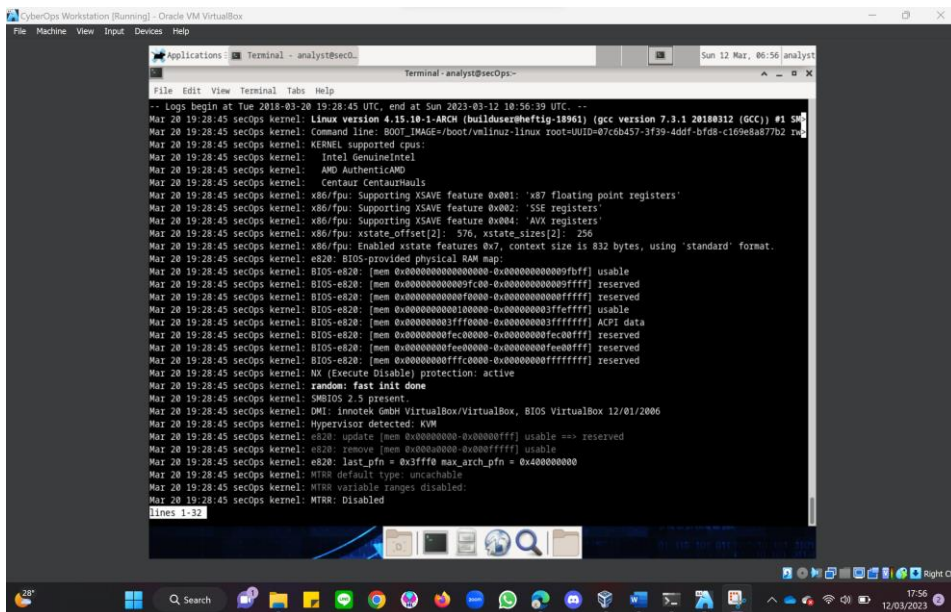
`analis@secOps ~$ journalctl`



```
analis@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 Sun 2023-03-12 06:46:27 EDT. --
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG network certificate management daemon.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache.
Mar 20 16:10:08 secOps systemd[363]: Reached target Paths.
Mar 20 16:10:08 secOps systemd[363]: Reached target Timers.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache (access for web browsers).
Mar 20 16:10:08 secOps systemd[363]: Starting D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Listening on D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Reached target Sockets.
Mar 20 16:10:08 secOps systemd[363]: Reached target Basic System.
Mar 20 16:10:08 secOps systemd[363]: Reached target Default.
Mar 20 16:10:08 secOps systemd[363]: Startup finished in 34ms.
Mar 20 16:10:21 secOps systemd[363]: Stopped target default.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Basic System.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Paths.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Timers.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Sockets.
Mar 20 16:10:21 secOps systemd[363]: Closed D-Bus User Message Bus Socket.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG network certificate management daemon.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache (access for web browsers).
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent (ssh-agent emulation).
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 16:10:21 secOps systemd[363]: Reached target Shutdown.
Mar 20 16:10:21 secOps systemd[363]: Starting Exit the Session...
Mar 20 16:10:21 secOps systemd[363]: Received SIGRMN=24 from PID 371 (kill).
Mar 20 16:11:00 secOps systemd[375]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 16:11:00 secOps systemd[375]: Listening on GnuPG cryptographic agent and passphrase cache (access for web browsers).
```

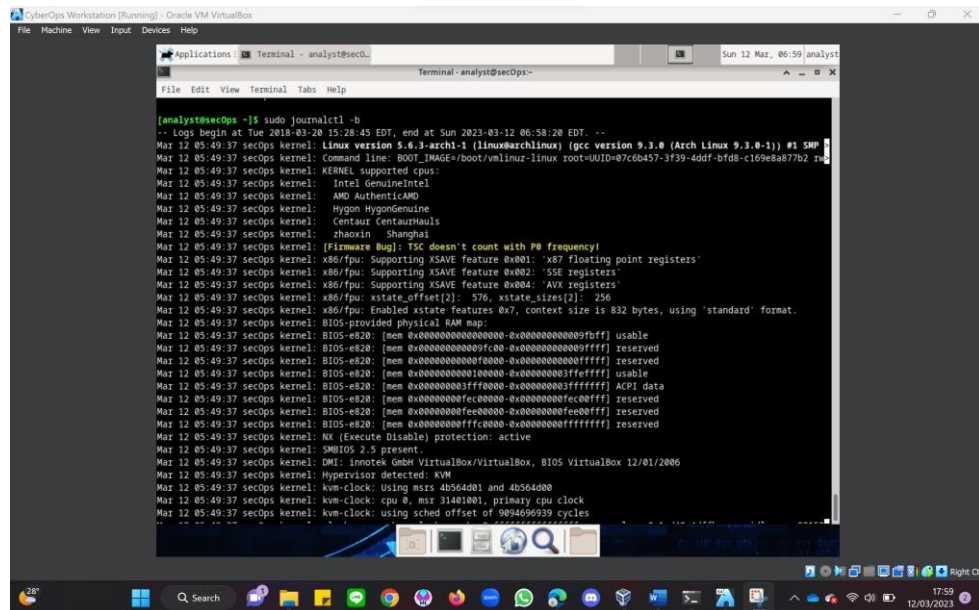
11. Menggunakan *journalctl --utc*

`analis@secOps ~$ sudo journalctl --utc`



```
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Sun 2023-03-12 10:56:39 UTC. --
Mar 20 19:28:45 secOps kernel: Linux version 4.19.1-ARCH (build@shftig-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=07c6d457-3f59-4d6f-bf88-c169e8a877b2 ro
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 CentaurIO
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 0x0000000000000000-0x00000000000009f0] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000009f0-0x0000000000000fff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000000fff-0x0000000000001fff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000001fff-0x0000000000003fff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000003fff-0x0000000000005fff] ACPI data
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000005fff-0x0000000000007fff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000007fff-0x0000000000009fff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000009fff-0x000000000000bfff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000000bfff-0x000000000000dfff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000000dfff-0x000000000000ffff] reserved
Mar 20 19:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 19:28:45 secOps kernel: random: fast init done
Mar 20 19:28:45 secOps kernel: SMBIOS 2.5 present.
Mar 20 19:28:45 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 20 19:28:45 secOps kernel: Hypervisor detected: KVM
Mar 20 19:28:45 secOps kernel: e820: update [mem 0x00000000-0x00000000] usable ==> reserved
Mar 20 19:28:45 secOps kernel: e820: remove [mem 0x00000000-0x00000000] usable
Mar 20 19:28:45 secOps kernel: e820: last_pfn = 0x3fff0 max_arch_pfn = 0x400000000
Mar 20 19:28:45 secOps kernel: MTRR default type: uncachable
Mar 20 19:28:45 secOps kernel: MTRR variable ranges disabled:
Mar 20 19:28:45 secOps kernel: MTRR: Disabled
lines 1-32
```

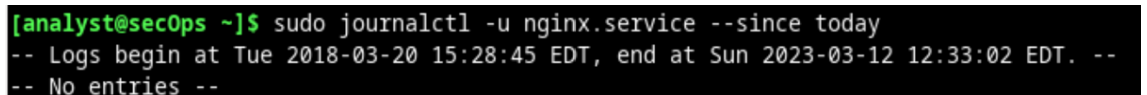
12. Menggunakan journalctl -b



```
[analyst@secOps ~]$ sudo journalctl -b
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Sun 2023-03-12 06:58:20 EDT. --
Mar 12 05:49:37 secOps kernel: Linux version 5.6.3-arch1-1 (linum@archlinux) (gcc version 9.3.0 (Arch Linux 9.3.0-1)) #1 SMP
Mar 12 05:49:37 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c1698a877b2 2
Mar 12 05:49:37 secOps kernel: KERNEL supported cpus:
Mar 12 05:49:37 secOps kernel: Intel GenuineIntel
Mar 12 05:49:37 secOps kernel: AMD AuthenticAMD
Mar 12 05:49:37 secOps kernel: Hygon HygonDenuine
Mar 12 05:49:37 secOps kernel: Centaur CentaurHauls
Mar 12 05:49:37 secOps kernel: zhaoxin Shanghai
Mar 12 05:49:37 secOps kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Mar 12 05:49:37 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 12 05:49:37 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 12 05:49:37 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 12 05:49:37 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Mar 12 05:49:37 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Mar 12 05:49:37 secOps kernel: BIOS-provided physical RAM map:
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009f0] usable
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x00000000000009f0-0x0000000000000fff] reserved
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000000fff-0x0000000000001fff] reserved
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000001fff-0x0000000000003fff] usable
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000003fff-0x0000000000007fff] ACPI data
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000007fff-0x000000000000ffff] reserved
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x000000000000ffff-0x0000000000010fff] reserved
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000010fff-0x000000000001ffff] reserved
Mar 12 05:49:37 secOps kernel: NX (Execute Disable) protection: active
Mar 12 05:49:37 secOps kernel: SMPTOS 2.5 present
Mar 12 05:49:37 secOps kernel: DMI: Innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 12 05:49:37 secOps kernel: Hypervisor detected: KVM
Mar 12 05:49:37 secOps kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
Mar 12 05:49:37 secOps kernel: kvm-clock: cpu 0, msrc 31a01001, primary cpu clock
Mar 12 05:49:37 secOps kernel: kvm-clock: using sched offset of 9094696939 cycles
Mar 12 05:49:37 secOps kernel: clocksource: kvm-clock: mask 0xfffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881510
```

13. Gunakan journalctl untuk menentukan layanan dan kerangka waktu untuk entri log. Perintah di bawah ini menunjukkan semua log layanan nginx yang direkam hari ini

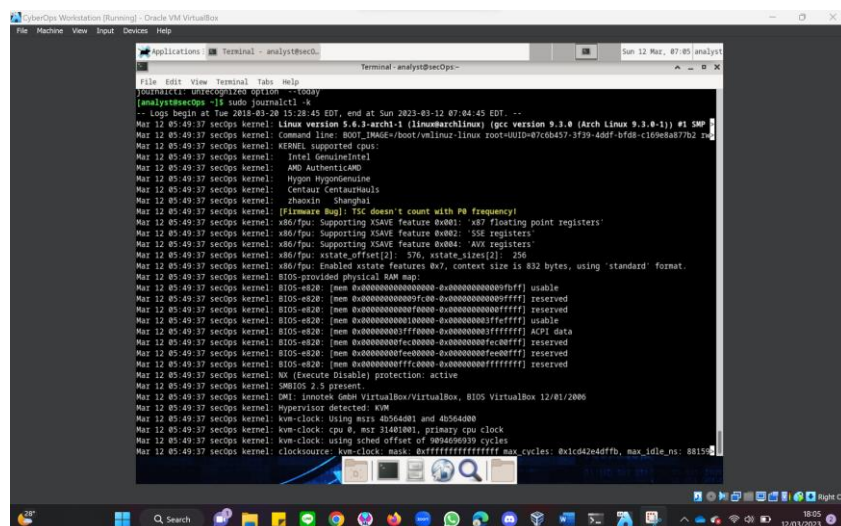
analis@secOps ~\$ sudo journalctl -u nginx.service --sejak hari ini



```
[analyst@secOps ~]$ sudo journalctl -u nginx.service --since today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Sun 2023-03-12 12:33:02 EDT. --
-- No entries --
```

14. Gunakan sakelar -k untuk hanya menampilkan pesan yang dihasilkan oleh kernel:

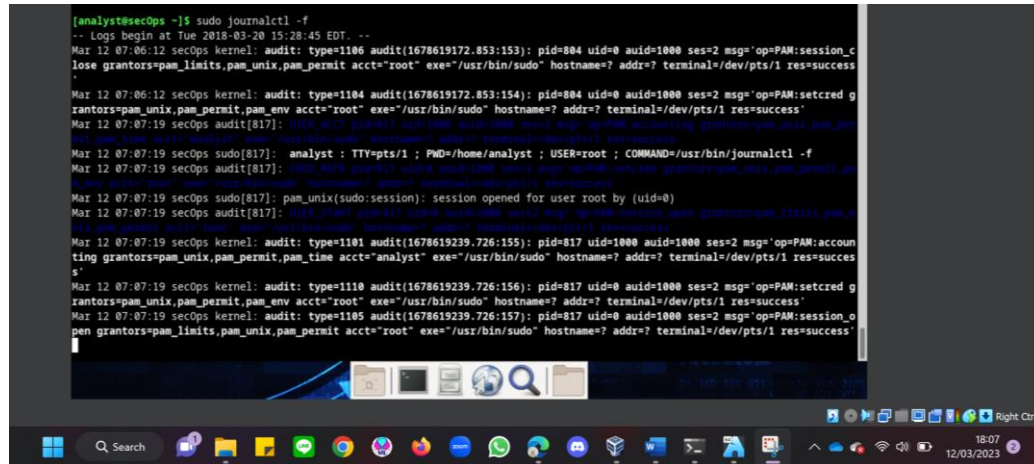
analis@secOps ~\$ sudo journalctl -k



```
[analyst@secOps ~]$ sudo journalctl -k
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Sun 2023-03-12 07:04:43 EDT. --
Mar 12 05:49:37 secOps kernel: Linux version 5.6.3-arch1-1 (linum@archlinux) (gcc version 9.3.0 (Arch Linux 9.3.0-1)) #1 SMP
Mar 12 05:49:37 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c1698a877b2 2
Mar 12 05:49:37 secOps kernel: KERNEL supported cpus:
Mar 12 05:49:37 secOps kernel: Intel GenuineIntel
Mar 12 05:49:37 secOps kernel: AMD AuthenticAMD
Mar 12 05:49:37 secOps kernel: Hygon HygonDenuine
Mar 12 05:49:37 secOps kernel: Centaur CentaurHauls
Mar 12 05:49:37 secOps kernel: zhaoxin Shanghai
Mar 12 05:49:37 secOps kernel: [Firmware Bug]: TSC doesn't count with P0 frequency!
Mar 12 05:49:37 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 12 05:49:37 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 12 05:49:37 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 12 05:49:37 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Mar 12 05:49:37 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Mar 12 05:49:37 secOps kernel: BIOS-provided physical RAM map:
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x00000000000009f0] usable
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x00000000000009f0-0x0000000000000fff] reserved
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000000fff-0x0000000000001fff] reserved
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000001fff-0x0000000000003fff] usable
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000003fff-0x0000000000007fff] ACPI data
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000007fff-0x000000000000ffff] reserved
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x000000000000ffff-0x0000000000010fff] reserved
Mar 12 05:49:37 secOps kernel: BIOS-e820: [mem 0x0000000000010fff-0x000000000001ffff] reserved
Mar 12 05:49:37 secOps kernel: NX (Execute Disable) protection: active
Mar 12 05:49:37 secOps kernel: SMPTOS 2.5 present
Mar 12 05:49:37 secOps kernel: DMI: Innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 12 05:49:37 secOps kernel: Hypervisor detected: KVM
Mar 12 05:49:37 secOps kernel: kvm-clock: Using msrc 4b564d01 and 4b564d00
Mar 12 05:49:37 secOps kernel: kvm-clock: cpu 0, msrc 31a01001, primary cpu clock
Mar 12 05:49:37 secOps kernel: kvm-clock: using sched offset of 9094696939 cycles
Mar 12 05:49:37 secOps kernel: clocksource: kvm-clock: mask 0xfffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881510
```

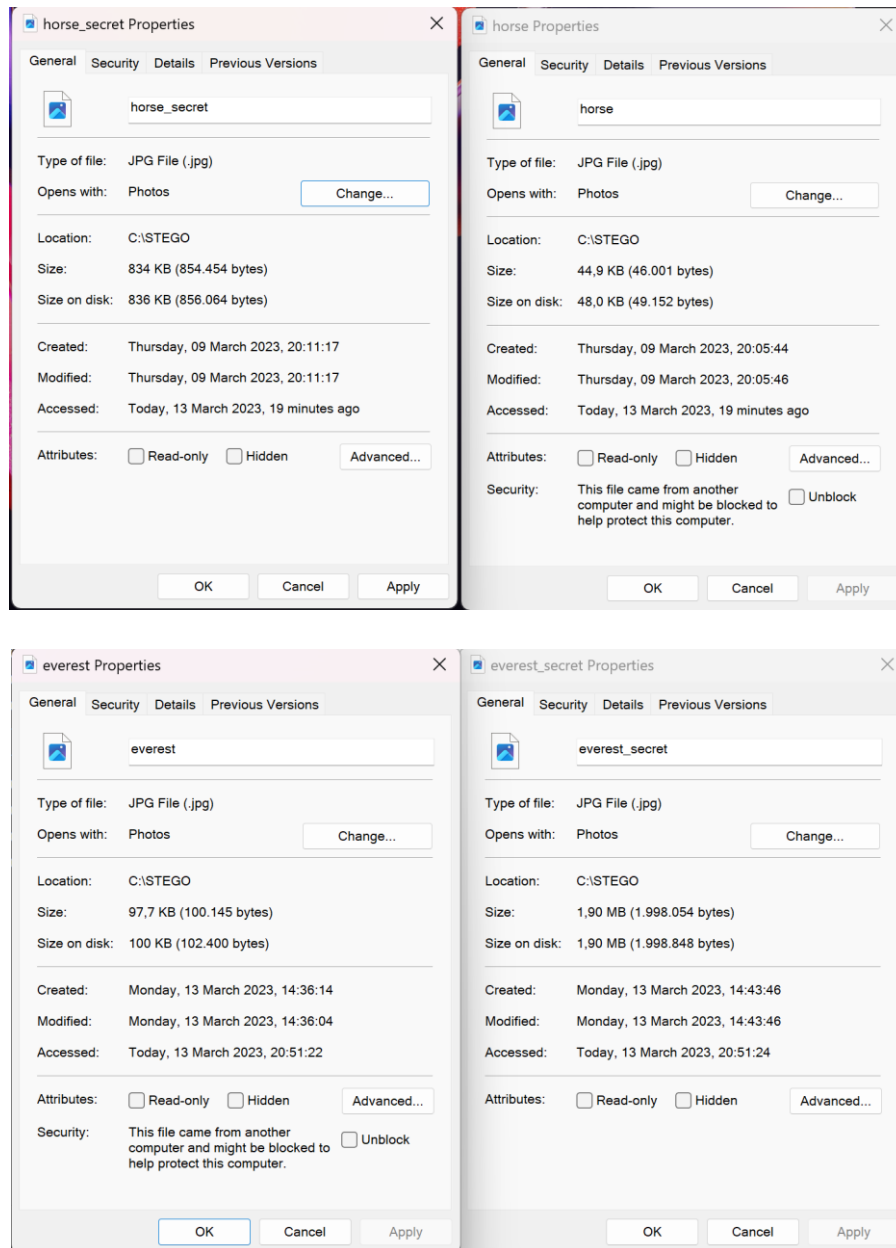

15. Mirip dengan tail -f yang dijelaskan di atas, gunakan -f untuk secara aktif mengikuti log saat sedang ditulis:

analis@secOps ~\$ sudo journalctl -f



E. Analisis Instruksi Kerja

Pada praktikum kali ini membahas 2 topik yaitu, steganografi dan analisis log server. Sesuai dengan instruksi praktikum, yang akan saya bahas terlebih dahulu adalah steganografi, dimana pada topik ini mahasiswa diharapkan dapat menganalisis perbandingan *hash value* dan *size* dari gambar. Pada steganografi saya menggunakan gambar kuda dan gunung Everest yang saya *download* melalui platform elok. Pada proses *download* gambar kedua sedikit mengalami kendala, yaitu gambar kedua tidak dapat di *embed* melalui STEGO, namun kendala ini dapat diselesaikan dengan mengubah format file dari PNG menjadi JPG secara manual tidak bisa langsung dengan mengubah ekstensi *file* pada laptop. Sesuai dengan instruksi kerja analisis STEGO adalah dengan membandingkan *hash value* dan *size* dari setiap gambar. Pada kedua gambar terlihat *size* mengalami perubahan, ketika di *download* dari elok dan se sudah di *embed* melalui STEGO. Terjadi perubahan yang signifikan pada ukuran hasil keluaran JPG, hal ini dapat terjadi setelah melalui proses steganografi yang disebabkan adanya penyusutan *bit* dan struktur JPG yang tinggi pada tingkat *error* nya. Besarnya *file* JPG dikarenakan memanfaatkan metode kompresi dalam menjaga kualitas gambar dengan teknik redundansi data yang lebih sedikit.



Terlihat pada kedua gambar diatas merupakan hasil perbandingan ukuran kedua gambar yang menjadi bukti *file* menjadi lebih besar.

Berikut saya tabel kompresi gambar:

Nama <i>file</i>	Ukuran Awal	Ukuran STEGO	Selisih
Horses.jpg	45 Kb	834 Kb	789 Kb
Everest.jpg	98 Kb	1.952 Kb	1.854 Kb

Dari data hasil Analisa diatas terlihat nilai faktor kompresi horses dan Everest memiliki nilai faktor kompresi yang tinggi, karena nilai horses dan Everest yang kecil berubah jauh lebih besar ketika terjadinya penyisipan pesan atau *text*.

Pada analisis pembacaan log server mahasiswa menggunakan empat program, yaitu *cat*, *more*, *less* dan *tail* dan terdapat pertanyaan dari setiap masing-masing soal. Uji coba pertama adalah menggunakan perintah *cat*. Disini saya berhasil menjalankan perintah *cat* pada terminal. Perintah *cat* sendiri digunakan untuk membuat, menggabungkan, atau menampilkan file di layar output standar atau ke file lain, dan banyak lagi. Menjawab pertanyaan dari uji coba pertama adalah sebagai berikut: **Menggunakan cat dengan file teks besar memiliki beberapa kelemahan, di antaranya:**

1. **Memakan banyak memori:** Cat akan membaca seluruh file ke dalam memori sebelum mencetaknya ke layar. Hal ini dapat menyebabkan penggunaan memori yang berlebihan jika file terlalu besar, dan bahkan dapat mengakibatkan kegagalan karena kekurangan memori.
2. **Tidak efisien untuk file besar:** Ketika menggunakan cat untuk file teks yang sangat besar, waktu untuk membaca dan mencetak isi file akan menjadi sangat lama. Ini karena cat mencetak isi file secara sekuensial dan tidak dapat memproses bagian file yang lebih kecil secara efektif.
3. **Tidak dapat mengedit isi file:** Ketika menggunakan cat, Anda hanya dapat melihat isi file dan tidak dapat mengeditnya. Ini dapat menyulitkan jika Anda perlu mengubah isi file dengan cepat.
4. **Output terlalu banyak:** Jika file teks sangat besar, output yang dihasilkan oleh cat akan sangat banyak dan sulit untuk dibaca atau dianalisis. Hal ini dapat menyebabkan kesulitan dalam menemukan informasi yang relevan dalam file tersebut.
5. **Tidak fleksibel:** Cat hanya bisa mencetak isi file secara sekuensial dan tidak bisa melakukan manipulasi atau transformasi pada isi file, seperti mencari kata kunci tertentu atau mengubah format file.

Uji coba kedua adalah menggunakan perintah *more*. Dilihat dari fungsinya *more* digunakan untuk melihat isi suatu file dengan fasilitas melihat isi file dari atas. Dalam menjalankan perintah ini saya berhasil menjalankan pada terminal. Terdapat pertanyaan pada uji coba kedua ini, berikut pembahasan dari pertanyaannya: **Meskipun *more* sangat berguna untuk membaca dan menampilkan isi file teks yang panjang, tetapi ada beberapa kelemahan penggunaan *more*, di antaranya:**

1. **Tidak efisien untuk navigasi mundur:** Ketika menggunakan *more*, Anda dapat menggulir ke bawah untuk membaca lebih lanjut, tetapi sulit untuk kembali ke atas. Ini karena *more* tidak menyimpan isi file yang telah Anda lewati, sehingga Anda harus membaca ulang file dari awal jika ingin kembali ke bagian sebelumnya.
2. **Tidak fleksibel:** *More* tidak dapat melakukan manipulasi atau transformasi pada isi file, seperti mencari kata kunci tertentu atau mengubah format file.
3. **Output terlalu banyak:** Jika file teks sangat besar, output yang dihasilkan oleh *more* akan sangat banyak dan sulit untuk dibaca atau dianalisis. Hal ini dapat menyebabkan kesulitan dalam menemukan informasi yang relevan dalam file tersebut.
4. **Tidak dapat mengedit isi file:** Ketika menggunakan *more*, Anda hanya dapat melihat isi file dan tidak dapat mengeditnya. Ini dapat menyulitkan jika Anda perlu mengubah isi file dengan cepat.

Uji coba yang ketiga adalah menggunakan perintah *less*, disini tidak terdapat pertanyaan. Namun disini saya berhasil menjalankan perintah *less* dengan menampilkan *output* dari file sesuai dengan teori *less* adalah utilitas baris perintah yang menampilkan konten file atau output dari suatu perintah dalam satu halaman. Ini mirip dengan perintah *more*, tetapi memiliki fitur yang lebih maju dan memungkinkan Anda menavigasi maju dan mundur melalui file. Ketika dihubungkan dengan pertanyaan perintah *cat* tadi, perintah *less* yang banyak digunakan untuk membuka *file* yang lebih besar.

Uji coba keempat adalah dengan menggunakan perintah *tail* dan *tail -f*. disini saya berhasil menjalankan perintah pada terminal. Pada analisis perbedaan *output* dari *tal* dan *tail -f* sebagai berikut:

1. **Output *tail*:** digunakan untuk menampilkan beberapa baris terakhir dari sebuah file teks. Ketika Anda menjalankan perintah *tail*, kita akan melihat isi file yang terakhir dibaca pada saat itu. Hal ini sesuai dengan data yang saya ambil pada terminal.
2. **Output *tail -f*:** Perintah *tail -f* memiliki arti yaitu: "follow" atau "mengikuti" digunakan untuk menampilkan isi file teks secara *real-time*. Ketika saya menjalankan perintah *tail -f*, saya akan melihat isi file yang sedang terus bertambah seiring dengan penambahan isi file tersebut. Perintah *tail -f* sangat berguna dalam memantau file log atau file yang terus diperbarui oleh aplikasi.

Dalam output *tail -f*, ketika ada perubahan pada file, maka perintah akan terus berjalan secara *real-time* dan akan menambahkan baris baru ke layar. Sedangkan pada output *tail*, saya harus menjalankan perintah kembali setiap kali ingin melihat isi file yang terbaru.

Uji coba kelima adalah memahami *file* log dan *syslog*. Dimana saya akan menggunakan perintah *cat* sebagai *root* dalam membuat daftar ini *file/var/log/syslog*. **Analisis mengenai mengapa perintah *cat* harus dijalankan sebagai *root*, hal ini dikarenakan:** Perintah *cat* tidak harus dijalankan sebagai *root*, karena perintah ini biasanya hanya digunakan untuk membaca isi file teks dan tidak memerlukan akses ke hak istimewa *root*. Namun, dalam beberapa kasus, *cat* harus dijalankan sebagai *root*, seperti:

1. **Membaca file dengan hak akses terbatas:** Jika file yang ingin dibaca hanya dapat diakses oleh pengguna dengan hak akses tertentu, maka perintah *cat* harus dijalankan sebagai pengguna dengan hak akses tersebut. Dalam hal ini, jika pengguna tidak memiliki hak akses yang cukup, perintah *cat* tidak akan dapat membaca isi file.

2. **Mengakses file yang terletak di direktori sistem:** Beberapa file yang terletak di direktori sistem hanya dapat dibaca oleh pengguna root. Dalam hal ini, perintah `cat` harus dijalankan sebagai root untuk membaca isi file.

Namun, dalam kondisi umum, sebaiknya perintah `cat` dijalankan dengan hak akses pengguna biasa, kecuali jika ada kebutuhan tertentu untuk menggunakan hak akses root. Hal ini untuk menjaga keamanan sistem dan mencegah penggunaan hak akses root yang tidak perlu.

Uji coba keenam sama dengan sebelumnya perbedaannya hanya pada penggunaan perintah `cat` dalam membuat daftar file `syslog` yang lebih lama. Disini saya berhasil menjalankan perintah pada terminal dan mendapatkan *output* sesuai instruksi kerja. **Analisis dari pertanyaan mengapa kita harus mensinkronisasikan waktu dan tanggal komputer dengan benar adalah sebagai berikut:**

1. **Menjaga akurasi waktu:** Ketika waktu dan tanggal pada komputer tidak sinkron dengan waktu sebenarnya, maka waktu yang tercatat pada file, catatan, dan aplikasi pada komputer tidak akurat. Ini dapat menyebabkan kesalahan dalam log aplikasi, pengolahan data, dan sinkronisasi antara komputer dan server lainnya.
2. **Memudahkan manajemen jaringan:** Banyak jaringan dan protokol yang mengandalkan waktu yang tepat untuk berfungsi dengan benar. Misalnya, protokol pengaturan waktu (NTP) digunakan untuk menyinkronkan waktu di seluruh jaringan dan memastikan bahwa semua komputer memiliki waktu yang sama. Jika waktu pada komputer tidak sinkron, ini dapat menyebabkan masalah dalam manajemen jaringan.
3. **Mencegah kegagalan sertifikat:** Sertifikat digital pada situs web dan aplikasi juga bergantung pada waktu yang tepat untuk berfungsi dengan benar. Jika waktu pada komputer tidak sinkron dengan waktu yang diatur pada sertifikat, maka sertifikat tersebut dapat dianggap tidak valid, dan situs web atau aplikasi mungkin tidak dapat diakses.

4. Mencegah kerentanan keamanan: Beberapa serangan keamanan mengandalkan waktu yang tidak sinkron untuk berhasil. Sebagai contoh, serangan pengalihan waktu (*time drift attack*) dapat memanipulasi waktu pada komputer untuk mengakses sistem dan data yang seharusnya terbatas. **Mengatur waktu dengan benar dapat mencegah serangan semacam ini.**

Dengan demikian, mensinkronkan waktu dan tanggal pada komputer dengan benar sangat penting untuk memastikan akurasi waktu, kelancaran jaringan, keamanan, dan fungsi aplikasi.

Uji coba ketujuh adalah pemahaman mengenai *file* log dan *journalctl*, **Perintah *journalctl* adalah utilitas yang digunakan untuk membaca log sistem di sistem operasi Linux yang menggunakan sistem logging *journald*. Dengan perintah ini, kita dapat membaca, menampilkan, dan menganalisis log sistem yang disimpan oleh *journald*. Beberapa penggunaan dari perintah *journalctl* adalah sebagai berikut:**

1. Melihat log sistem secara keseluruhan
2. Mencari log berdasarkan kriteria tertentu
3. Menampilkan log dengan format yang berbeda
4. Melihat log pada unit service tertentu
5. Membaca log pada waktu tertentu

Perintah *journalctl* sangat berguna untuk menganalisis masalah sistem dan mencari tahu penyebab terjadinya masalah. Dengan perintah ini, kita dapat melihat log sistem dengan cara yang lebih terstruktur dan mudah dibaca. Namun, perintah ini hanya dapat digunakan pada sistem operasi Linux yang menggunakan *journald* sebagai sistem logging.

Uji coba kedelapan adalah dengan menjalankan perintah *journalctl -utc*. Saya berhasil menjalankan perintah pada terminal. Penggunaan perintah *journalctl -utc* adalah untuk menampilkan log sistem dalam waktu UTC (*Coordinated Universal Time*). UTC adalah standar waktu internasional yang digunakan sebagai referensi

untuk mengukur waktu di seluruh dunia. Dengan menggunakan perintah `journalctl --utc`, waktu yang ditampilkan dalam log sistem akan disesuaikan dengan waktu UTC, sehingga memudahkan analisis log sistem dalam konteks waktu global. Selain itu, penggunaan waktu UTC juga mempermudah sinkronisasi log sistem antara sistem yang berbeda dengan waktu lokal yang berbeda.

Uji coba kesembilan adalah menggunakan perintah `journalctl -b`. Perintah `journalctl -b` digunakan untuk menampilkan entri log dari sesi boot terakhir pada sistem Linux. Argumen `-b` menunjukkan bahwa kita ingin menampilkan log sesi boot terakhir, dan jika argumen tersebut tidak ditentukan, secara default akan menampilkan log untuk sesi saat ini. Ketika sistem Linux boot, jurnal sistem menyimpan semua entri log dalam sesi boot tersebut. Dengan menggunakan perintah `journalctl -b`, kita dapat menampilkan semua entri log yang dihasilkan selama sesi boot terakhir. Ini dapat sangat berguna untuk mendiagnosis masalah sistem yang terjadi selama sesi boot terakhir, seperti masalah kinerja, crash, atau masalah dengan layanan yang tidak berjalan dengan benar.

Uji coba kesepuluh adalah penggunaan `journalctl` untuk menentukan layanan dan kerangka waktu entri log. **Analisis dari uji coba ini adalah Perintah `journalctl` dapat digunakan untuk menentukan layanan dan kerangka waktu entri log dengan menggunakan beberapa argumen atau opsi. Berikut ini beberapa argumen atau opsi yang dapat digunakan:**

1. `-u <unit>`: Opsi ini digunakan untuk menampilkan entri log untuk unit (layanan) tertentu. Contoh penggunaan: `journalctl -u nginx.service`
2. `-k`: Opsi ini digunakan untuk menampilkan entri log kernel.
3. `--since <time>`: Opsi ini digunakan untuk menampilkan entri log yang terjadi setelah waktu tertentu
4. `--until <time>`: Opsi ini digunakan untuk menampilkan entri log yang terjadi sebelum waktu tertentu.
5. `--since today`: Opsi ini digunakan untuk menampilkan entri log yang terjadi hari ini.

6. `--since yesterday`: Opsi ini digunakan untuk menampilkan entri log yang terjadi kemarin.
7. `--since "1 hour ago"`: Opsi ini digunakan untuk menampilkan entri log yang terjadi satu jam yang lalu.
8. `--since "2 days 12 hours ago"`: Opsi ini digunakan untuk menampilkan entri log yang terjadi dua hari dan 12 jam yang lalu.
9. `--since <date> --until <date>`: Opsi ini digunakan untuk menampilkan entri log yang terjadi dalam rentang waktu tertentu.

Dengan menggunakan argumen atau opsi ini, pengguna dapat menentukan layanan (dengan argumen `-u`) dan kerangka waktu (dengan opsi `--since`, `--until`, `--since today`, `--since yesterday`, atau `--since "x time ago"`) untuk menampilkan entri log yang dibutuhkan. Disini saya menggunakan perintah **`analis@secOps ~$ sudo journalctl -u nginx.service --since today`**, yang berarti saya ingin menampilkan entri log untuk layanan tertentu dan menampilkan entri log yang terjadi hari ini.

Uji coba kesebelas adalah menjalankan perintah `journalctl -k`. Perintah `journalctl -k` digunakan untuk menampilkan entri log dari kernel. Argumen `-k` menunjukkan bahwa kita ingin menampilkan log kernel, dan jika argumen tersebut tidak ditentukan, secara default akan menampilkan log untuk jurnal sistem. Ketika sistem Linux berjalan, kernel menghasilkan entri log yang sangat penting untuk memantau kinerja dan keamanan sistem. Dengan menggunakan perintah `journalctl -k`, kita dapat menampilkan semua entri log yang dihasilkan oleh kernel sejak sistem dimulai. Ini dapat sangat berguna untuk mendiagnosis masalah sistem yang terkait dengan kernel seperti kernel panic, crash, atau masalah driver perangkat keras.

Uji coba terakhir adalah menjalankan perintah `journalctl -f`. Perintah `journalctl -f` digunakan untuk memantau secara langsung entri log yang baru dibuat pada sistem Linux. Argumen `-f` menunjukkan bahwa kita ingin memantau entri log secara langsung (real-time), dan jika argumen tersebut tidak ditentukan, secara default akan menampilkan seluruh entri log dalam jurnal sistem.

Ketika kita menjalankan perintah `journalctl -f`, terminal akan menampilkan entri log baru yang muncul pada jurnal sistem secara langsung. Ini dapat sangat berguna untuk memantau aktivitas sistem secara real-time, seperti memantau layanan sistem yang baru berjalan atau memeriksa masalah sistem yang terjadi saat ini.

F. Kesimpulan

1. Dalam steganografi, **ukuran file stego (file yang berisi pesan tersembunyi) biasanya akan lebih besar daripada ukuran file cover (file yang digunakan untuk menyembunyikan pesan) karena pesan yang tersembunyi akan menambah ukuran file tersebut.** Namun, ketika file stego dikompresi, ukurannya dapat menjadi lebih kecil daripada ukuran file stego tanpa dikompresi. Hal ini terjadi karena kompresi data dapat memanfaatkan redundansi dalam data untuk mengurangi ukuran file. Dalam konteks steganografi, pesan tersembunyi dalam file stego mungkin memiliki pola atau struktur tertentu yang dapat dieksploitasi oleh algoritma kompresi untuk mengurangi ukuran file.
2. Log server sangat penting untuk memantau kinerja dan keamanan sistem, serta untuk mendiagnosis masalah yang terjadi pada sistem. Dengan menganalisis log server secara teratur, kita dapat memperoleh wawasan yang lebih dalam tentang aktivitas sistem dan memperbaiki masalah yang terjadi.
3. `journalctl` memungkinkan kita untuk menampilkan dan memfilter entri log dalam jurnal sistem.
4. Dalam menganalisis log server, penting untuk memahami format log yang digunakan oleh sistem dan mengenali pola atau tanda-tanda yang menunjukkan masalah yang terjadi. Misalnya, log server dapat menunjukkan pesan kesalahan, status layanan, atau informasi tentang pengguna dan aktivitasnya.

5. Kita dapat menggunakan beberapa teknik untuk menganalisis log server, seperti mencari kata kunci tertentu, memfilter entri log dengan menggunakan waktu atau unit tertentu.

DAFTAR PUSTAKA

- [1] Amazon Web Services. (n.d.). What is a Log File?.
<https://aws.amazon.com/id/what-is/log-files/#:~:text=Log%20server%20adalah%20file%20log,%2C%20jenis%20permintaan%2C%20dan%20sebagainya>.
- [2] Dosen Pendidikan. (n.d.). Steganografi adalah.
<https://www.dosenpendidikan.co.id/steganografi-adalah/>
- [3] Fadloli, A. (2020). Cara Melihat Log di Linux CentOS.
<https://www.fadloli.web.id/2020/06/cara-melihat-log-linux-centos.html>
- [4] Hostinger Indonesia. (n.d.). 50+ Perintah Dasar Linux yang Wajib Anda Ketahui. <https://www.hostinger.co.id/tutorial/perintah-dasar-linux>
- [5] Hostinger Indonesia. (n.d.). Cat Command Linux: Panduan Lengkap. <https://www.hostinger.co.id/tutorial/cat-command-linux>
- [7] Immersa Lab. (n.d.). Pengertian Steganografi: Jenis-Jenis dan Prinsip Kerja. <https://www.immersa-lab.com/pengertian-steganografi-jenis-jenis-dan-prinsip-kerja.html>
- [8] Kajian Pustaka. (2017). Sejarah & Prinsip Kerja Teknik Steganografi. <https://www.kajianpustaka.com/2017/09/sejarah-prinsip-kerja-teknik-steganografi.html>
- [9] LinuxID. (2018). Tutorial Perintah Less dan Contoh Penggunaan Less di Linux. <https://www.linuxid.net/30452/tutorial-perintah-less-dan-contoh-penggunaan-less-di-linux/>
- [10] Nur, S. A. (2010). Analisis Logging dan Monitoring Pada Sistem Operasi Linux. (Bachelor's thesis). Institut Teknologi Sepuluh Nopember.

LINK GITHUB

https://github.com/saadahmardatillah/Unit4.1_KeamananInformasi