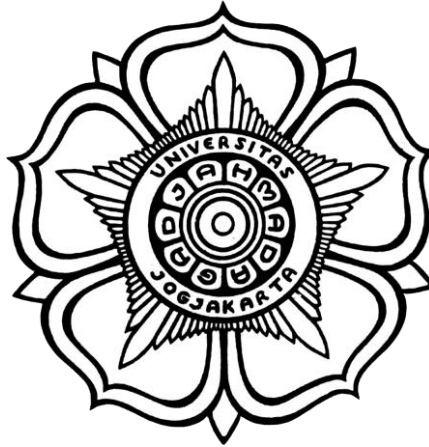


LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

“Steganografi dan log server”

Pertemuan 4



Disusun oleh :

Nama	:Nayaka Iman Wiraputra
NIM	: 21/482203/SV/19910
Kelas	: TRI A
Hari, Tanggal	: Selasa, 28 Febuary 2022
Dosen Pengampu S.Kom., M.Eng.	: Anni Karimatul Fauziyyah,
Asisten Dosen	: Gabriella Alvera Chaterine

LABORATORIUM KEAMANAN INFORMASI
SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPATEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
YOGYAKARTA

2022

1. TUJUAN

Tujuan dari praktikum pada pertemuan kali ini adalah memberikan pemahaman kepada mahasiswa terhadap konsep dan teknik penyembunyian pesan rahasia dalam sebuah media digital, seperti gambar, suara, video, dan text. Praktikum kali ini bertujuan memberikan pemahaman tentang dasar-dasar steganografi, algoritma dan Teknik yang digunakan untuk menyembunyikan pesan rahasia dalam media digital dengan cara yang aman dan efektif.

Tujuan dari praktikum log server kali ini adalah untuk memonitor dan menganalisis aktivitas yang terjadi pada server, seperti siapa yang mengakses server, kapan mereka mengakses server, kapan mengakses, dan apa yang mereka lakukan selama mengakses. Log server menyimpan catatan aktivitas dan informasi penting yang terjadi pada server, termasuk kejadian yang tak terduga atau kejadian yang tidak diinginkan seperti serangan siber atau kesalahan sistem.

2. ALAT DAN BAHAN

1. Koneksi internet
2. Cybercops workstation virtual machine
3. Stego

3. DASAR TEORI

Stego adalah singkatan dari steganografi, yang merupakan seni atau ilmu menyembunyikan pesan atau informasi di dalam objek atau media lain dengan cara yang tidak terlihat oleh orang yang tidak berkepentingan. Tujuan dari steganografi adalah untuk menjaga kerahasiaan dan keamanan pesan, serta menghindari deteksi oleh pihak yang tidak berwenang. Contoh penerapan steganografi adalah dalam penyembunyian pesan rahasia di dalam gambar, video, atau file suara.

Log server adalah catatan atau rekaman dari aktivitas dan peristiwa yang terjadi pada server. Log server mencakup informasi seperti waktu kejadian, jenis kejadian, IP address atau nama host yang terlibat, serta informasi detail tentang kejadian itu sendiri.

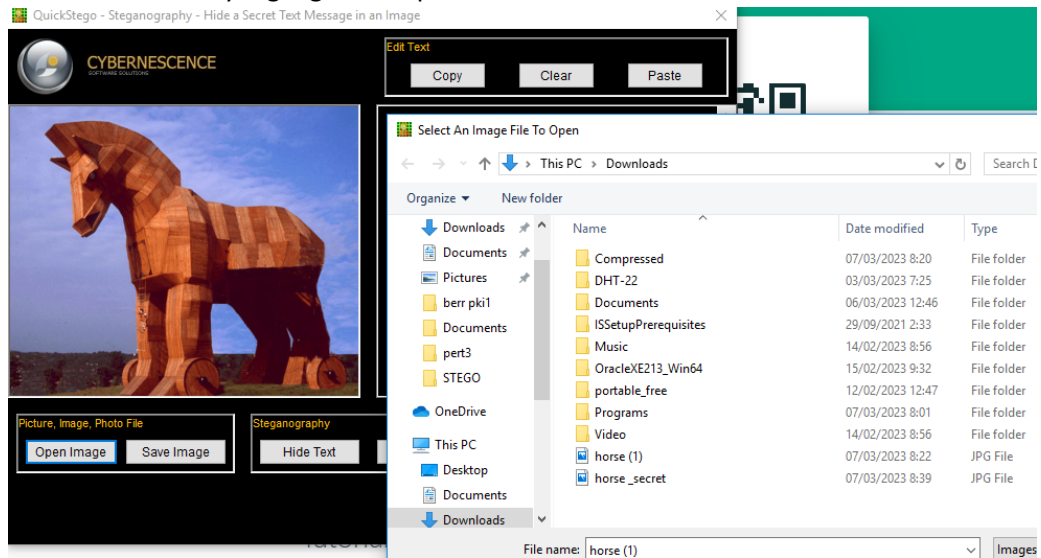
Log server biasanya digunakan untuk tujuan keamanan dan pemecahan masalah. Dengan memonitor log server, administrator sistem dapat melacak aktivitas dan peristiwa yang mencurigakan atau tidak diinginkan pada server, seperti serangan jaringan, akses yang tidak sah, atau kesalahan sistem. Informasi ini dapat membantu dalam memperkuat keamanan sistem dan mencegah serangan yang lebih serius.

Selain itu, log server juga digunakan untuk memecahkan masalah teknis dan operasional pada server. Dengan memeriksa log server, administrator sistem dapat mengidentifikasi masalah atau kesalahan pada server, seperti kegagalan server, kesalahan konfigurasi, atau permasalahan performa. Informasi ini dapat membantu dalam menemukan dan memperbaiki masalah pada sistem dengan cepat dan efektif.

4. LANGKAH KERJA

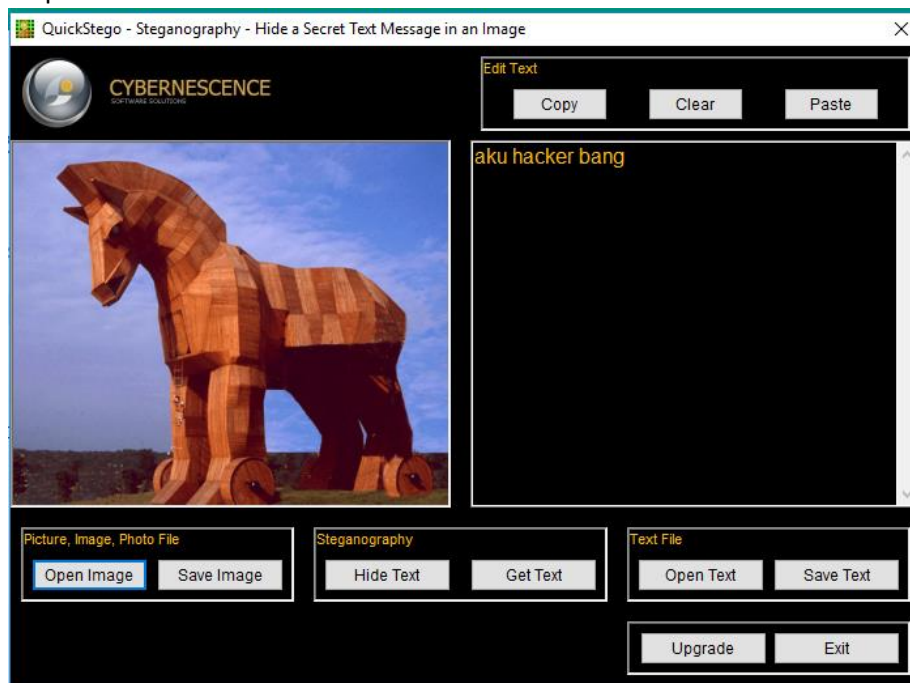
LAB 1 (STEGO)

1. INSTAL STEGO
2. Masukkan file foto yang ingin di sisipkan text




Pada gambar di atas saya menggunakan file foto horse (1)

3. Lalu setelah memilih gambar yang ingin di sisipin text kita masukan text yang ingin kita sisipkan

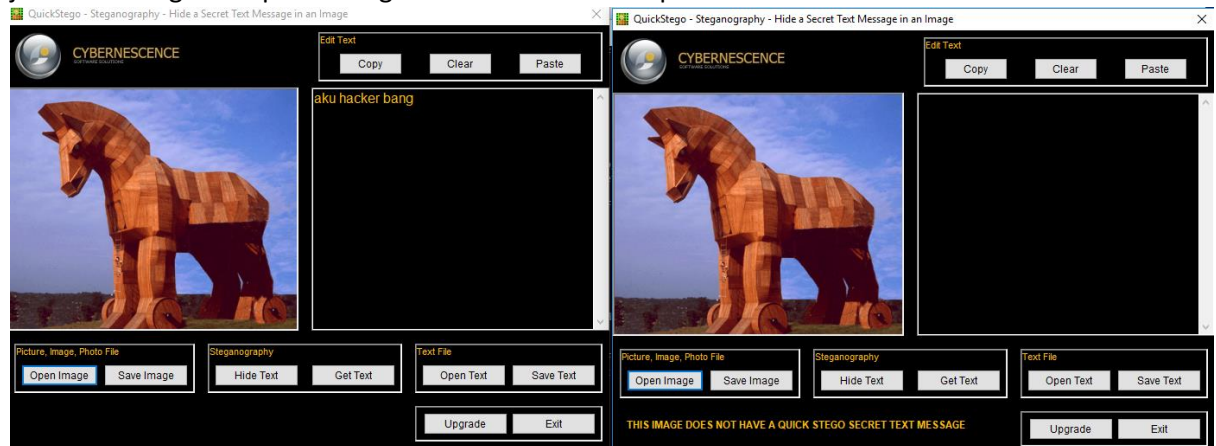


4. jika sudah selesai memasukan pesan tersembunyi klik hide text dan save image

 horse (1)	07/03/2023 8:22	JPG File	45 KB
 horse_secret	07/03/2023 8:39	JPG File	835 KB

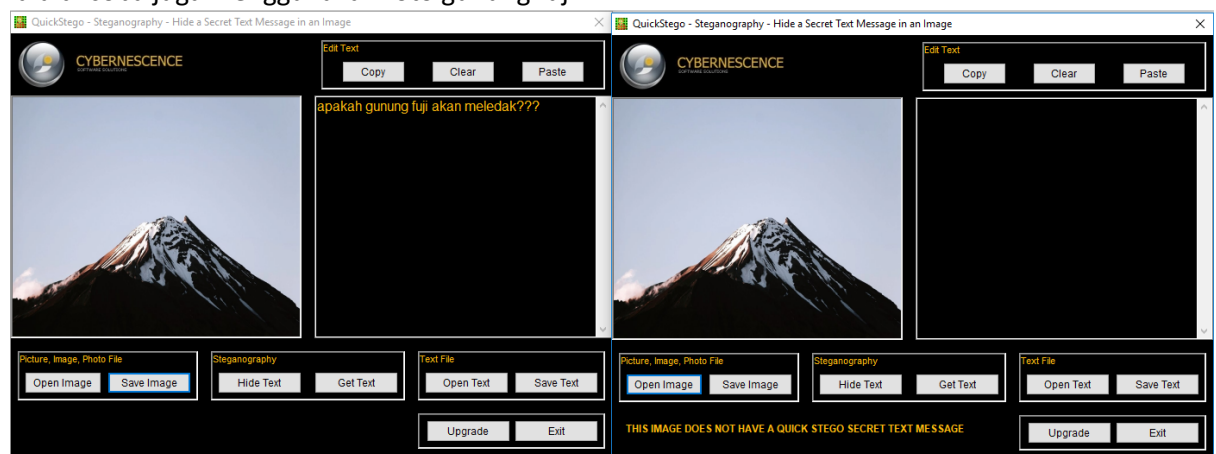
Ini adalah perbandingan besaran file nya, bisa di lihat file Bernama horse (1) lebih kecil di bandingkan Dengan horse_secret karena di file horse_secret sudah di sisipkan pesan tersembunyi

5. jika di bandingan di aplikasi stego maka akan terlihat seperti ini





di sebelah kiri adalah file horse_secret yang sudah di beri pesan tersembunyi dan di sebelah kanan adalah file horse (1) yang belum terdapat pesan

6. lalu di coba juga menggunakan foto gunung fuji



sama seperti sebelum nya file di sebeah kiri adalah file yang sudah di sisipkan pesan tersembunyi sedangkan file di sebelah kanan adalah file raw yang belum di sisipkan pesan

7. perbandingan besaran ke2 file

 gunung_fuji	07/03/2023 8:59	JPG File	48 KB
 gunung_fuji_secret	07/03/2023 9:00	JPG File	1.952 KB

terlihat kedua file memiliki besaran data yang berbeda karena salah satu gamba rya sudah di sisipkan pesan tersembunyi

8. bisa juga di bandingkan ke 4 foto melalui cmd

```
C:\STEGO>dir *.jpg
Volume in drive C is WIN 10 LC
Volume Serial Number is 74A6-B204

Directory of C:\STEGO

07/03/2023  08:59                48.590 gunung_fuji.jpg
07/03/2023  09:00             1.998.054 gunung_fuji_secret.jpg
07/03/2023  08:22                46.001 horse (1).jpg
07/03/2023  08:39             854.454 horse_secret.jpg
               4 File(s)          2.947.099 bytes
               0 Dir(s)  258.862.977.024 bytes free

C:\STEGO>md5sums.exe *.jpg

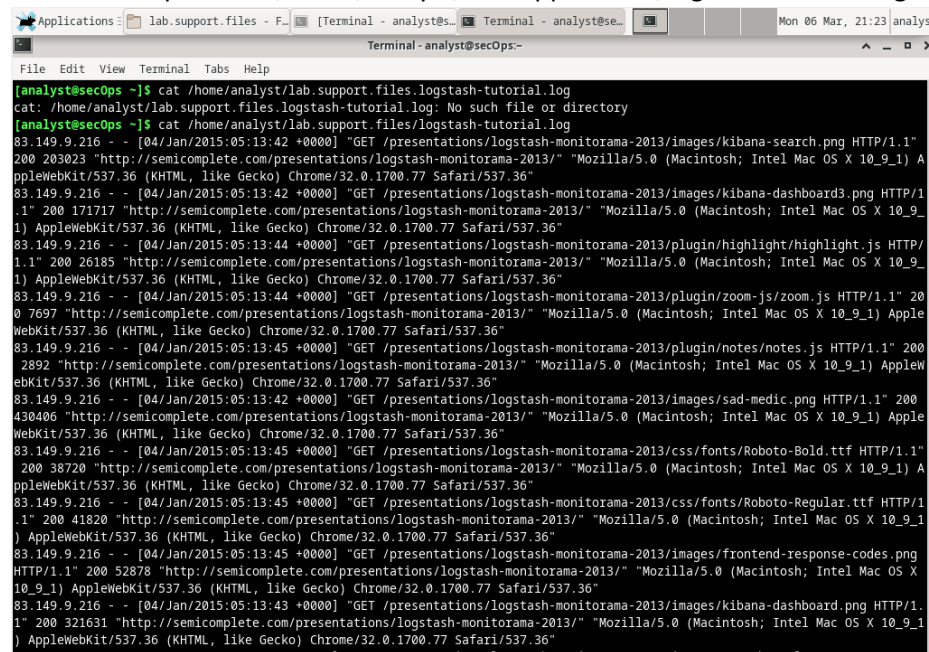
MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums.exe -h for help

[Path] / filename                                MD5 sum
-----
[C:\STEGO\]
gunung_fuji.jpg                                9f3b7b4b200da9fe48d4c38b9935a890
gunung_fuji_secret.jpg                        11a7968af509054b3623e78f77f064bc
horse (1).jpg                                fce8552170cccd3dd545566309124097
horse_secret.jpg                             c6aaaae67fa751cab8d594a7d8f3f0619
```

LAB 2 (LOG SERVER)

1. Membaca file Log dengan Cat, More, Less, Tail
2. 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



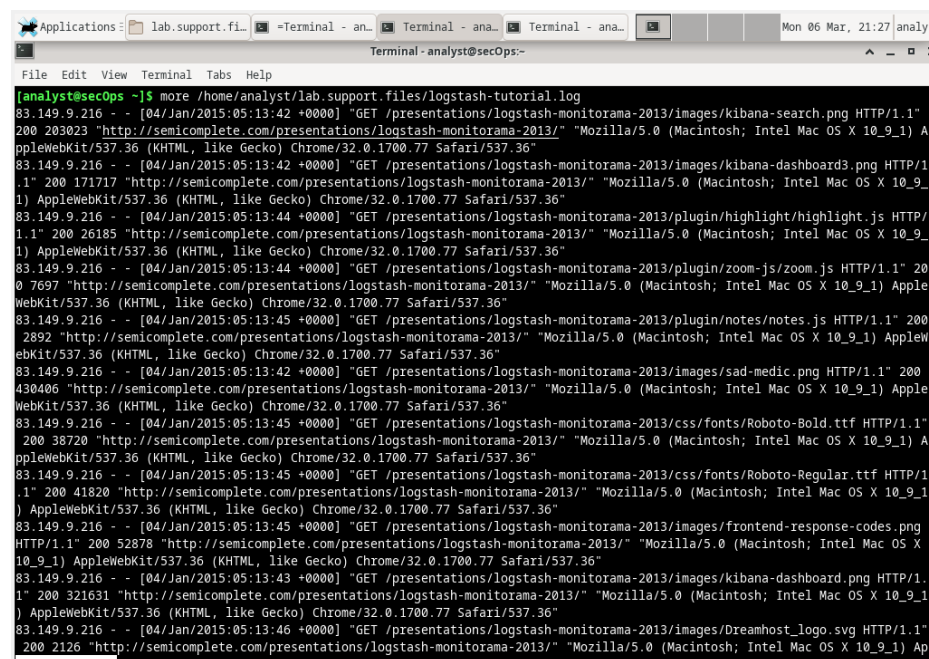
```
analyst@secOps ~$ cat /home/analyst/lab.support.files/logstash-tutorial.log
cat: /home/analyst/lab.support.files/logstash-tutorial.log: No such file or directory
[analyst@secOps ~]$ cat /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png 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-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" 20
0 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) AppleW
ebKit/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) 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
) 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/2015:05:13:45 +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"
```

pertanyaan: Apa kelemahan menggunakan cat dengan file teks besar?

Cat (concatenate) adalah perintah pada sistem operasi Unix/Linux yang digunakan untuk menggabungkan dan menampilkan isi dari satu atau beberapa file ke layar terminal atau ke file lain. Namun, ada beberapa kelemahan jika menggunakan cat untuk file teks besar, yaitu:

1. Performa yang lambat: Jika file teks sangat besar, penggunaan cat akan memakan waktu yang cukup lama untuk menampilkan seluruh isi file. Ini akan memperlambat proses dan membebani sistem.
 2. Konsumsi sumber daya yang tinggi: Ketika cat digunakan untuk file teks besar, ia memakan banyak memori dan sumber daya CPU, terutama jika file memiliki banyak baris atau karakter.
 3. Tidak efisien dalam mengolah data: Jika file memiliki banyak data terstruktur seperti file CSV atau JSON, menggunakan cat tidak efisien karena hanya menampilkan data mentah tanpa mengolahnya menjadi format yang lebih mudah dibaca atau digunakan.
 4. Tidak tahan terhadap kesalahan: Ketika menggunakan cat untuk file teks besar, kesalahan seperti kegagalan baca/write atau kegagalan sistem dapat menyebabkan hilangnya data atau rusaknya file.
3. Dari jendela terminal yang sama, gunakan perintah di bawah ini untuk menampilkan kembali isi file logstash-tutorial.log. Proses ini menggunakan more:

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



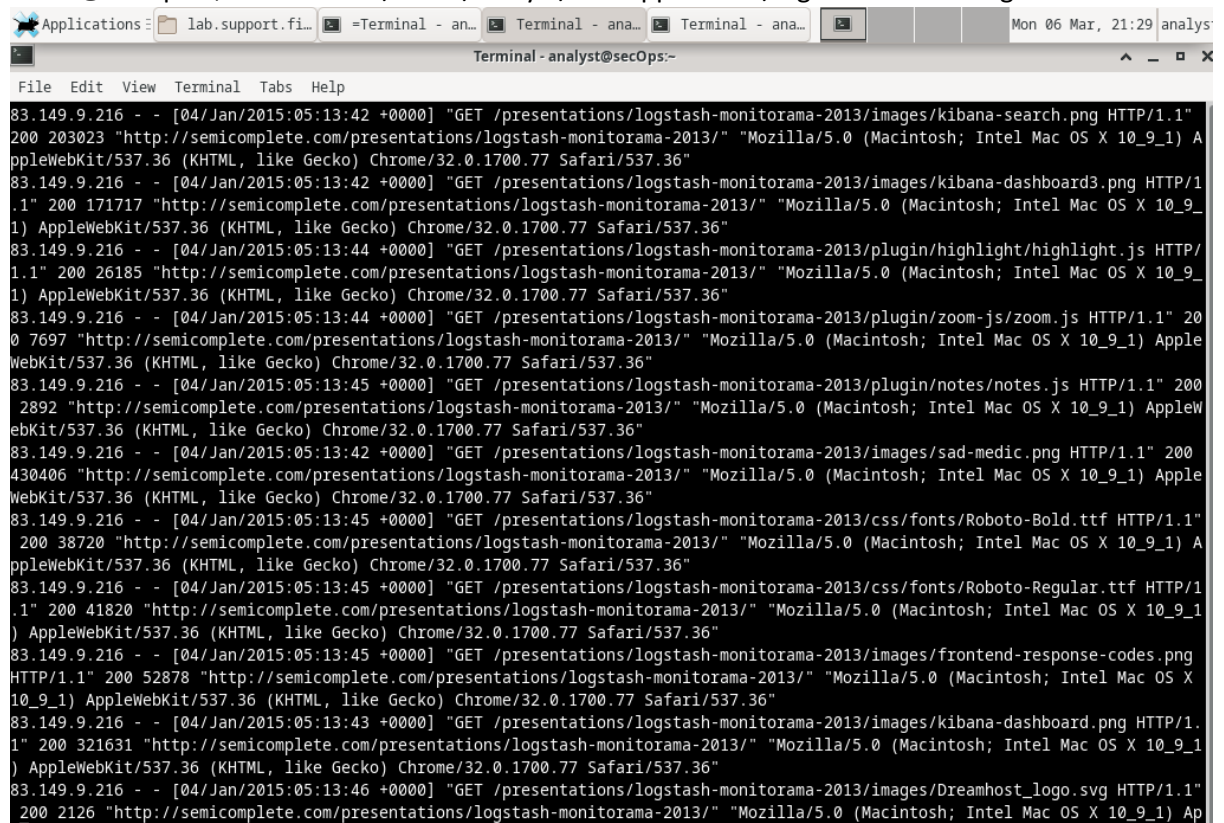
```
Applications: lab.support.fi... Terminal - ana... Terminal - ana... Terminal - ana... Mon 06 Mar, 21:27 analy
Terminal - analyst@secOps:
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ more /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /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) 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-dashboar3.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" 20
0 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) AppleW
ebKit/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) 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
) 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-dashboar3.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) Ap
pleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
More (149)
```


Pertanyaan: Apa kelemahan menggunakan more?

- Tidak bisa mengedit isi file: "more" hanya digunakan untuk menampilkan isi file teks saja, tidak bisa digunakan untuk mengedit isi file. Oleh karena itu, jika ingin mengedit isi file, harus menggunakan editor teks seperti "vi" atau "nano".
- Tidak efektif untuk file teks yang sangat besar: Perintah "more" bisa menjadi lambat dan kurang efektif jika digunakan untuk file teks yang sangat besar, karena memerlukan waktu yang lama untuk menampilkan halaman berikutnya, dan halaman tersebut tidak bisa langsung dicari. Untuk file teks yang sangat besar, lebih disarankan menggunakan perintah "less", yang lebih efektif dalam menampilkan isi file dan mencari data.
- Tidak bisa melakukan pencarian yang spesifik: Perintah "more" tidak memungkinkan pengguna untuk melakukan pencarian yang spesifik dalam isi file. Jika ingin melakukan pencarian, harus menggunakan perintah "grep" atau "sed".
- Tidak bisa menampilkan informasi metadata file: "more" hanya menampilkan isi dari file teks, tidak bisa menampilkan informasi metadata file seperti ukuran, tipe file, atau tanggal modifikasi.

- 4 Dari tampilan terminal yang sama, gunakan less untuk menampilkan konten file logstash tutorial.log lagi:

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



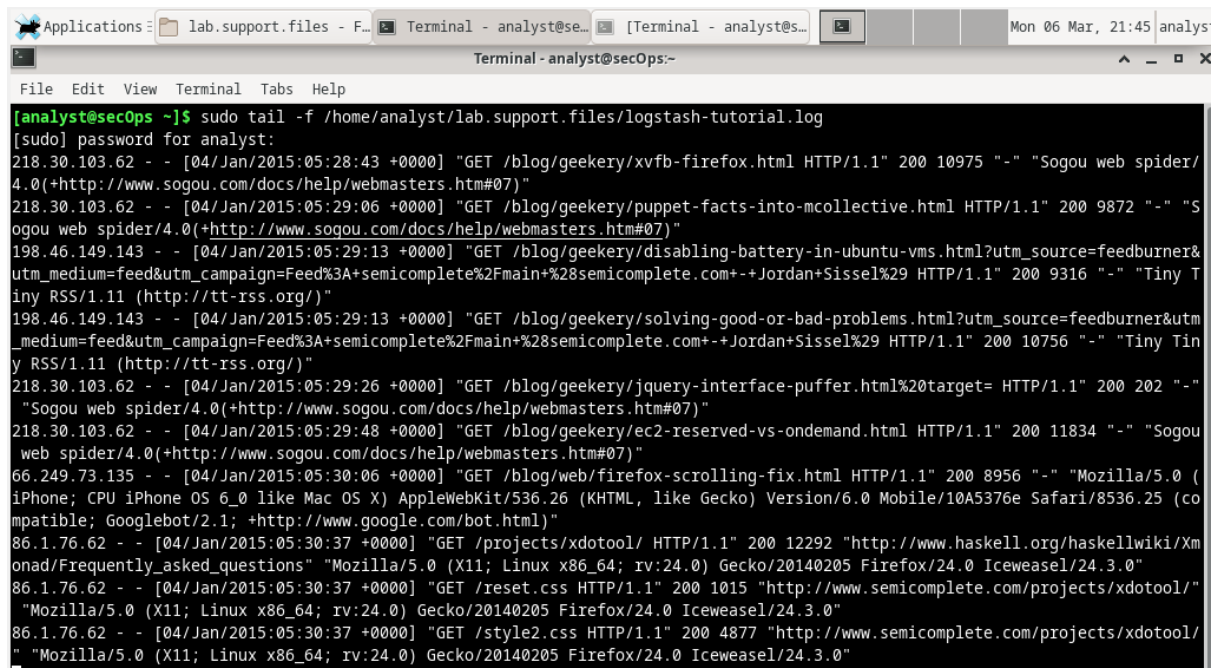
```
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77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

Isi file harus menggulir melalui jendela terminal dan berhenti ketika satu halaman ditampilkan. Tekan spasi untuk maju ke halaman berikutnya. Tekan enter untuk menampilkan baris teks berikutnya. Gunakan tombol panah atas dan bawah untuk bergerak maju mundur melalui file teks. Gunakan tombol q pada keyboard untuk keluar

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

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

```
[analyst@secOps ~]$ tail /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-problems.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html HTTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently_asked_questions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Icedragon/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 Icedragon/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 Icedragon/24.3.0"
```



Pertanyaan:

Apa yang berbeda dalam output **tail** dan **tail -f**? Jelaskan

Perintah **tail** dan **tail -f** digunakan untuk melihat isi file pada bagian akhir atau "tail" dari file.

Perbedaan antara **tail** dan **tail -f** adalah:

tail: secara default, **tail** akan menampilkan 10 baris terakhir dari file dan kemudian keluar. Setelah keluar, Anda harus mengetik perintah lagi untuk melihat isi file terbaru.

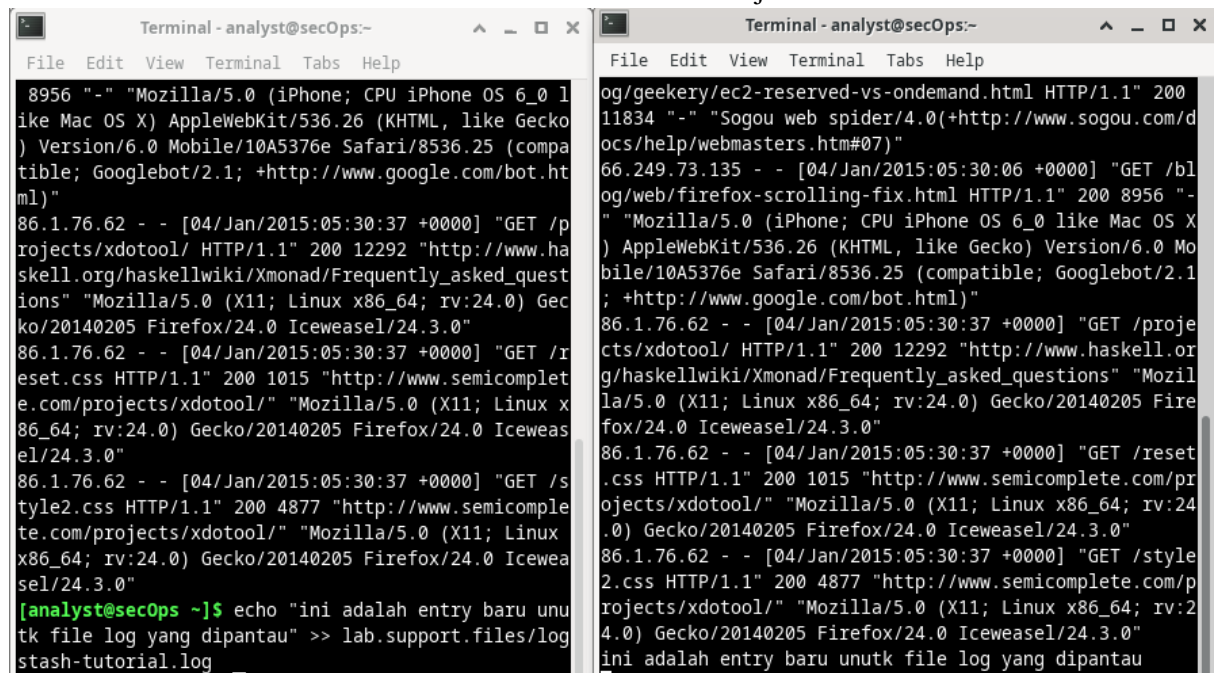
tail -f: **tail -f** akan menampilkan isi file secara real-time dan terus-menerus. Artinya, ketika file terus diperbarui dengan data baru, **tail -f** akan terus menampilkan isi file terbaru. Ini sangat berguna ketika Anda ingin memantau log file yang sedang diperbarui secara dinamis

6. Pilihlah jendela terminal bawah dan masukkan perintah berikut:

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

Perintah di atas menambahkan pesan "ini adalah entri baru ke file log yang dipantau" ke file /home/analyst/lab.support.files/logstash-tutorial.log. Karena **tail -f** sedang memantau file pada saat sebuah baris ditambahkan ke file. Jendela atas akan menampilkan baris baru secara real-time.

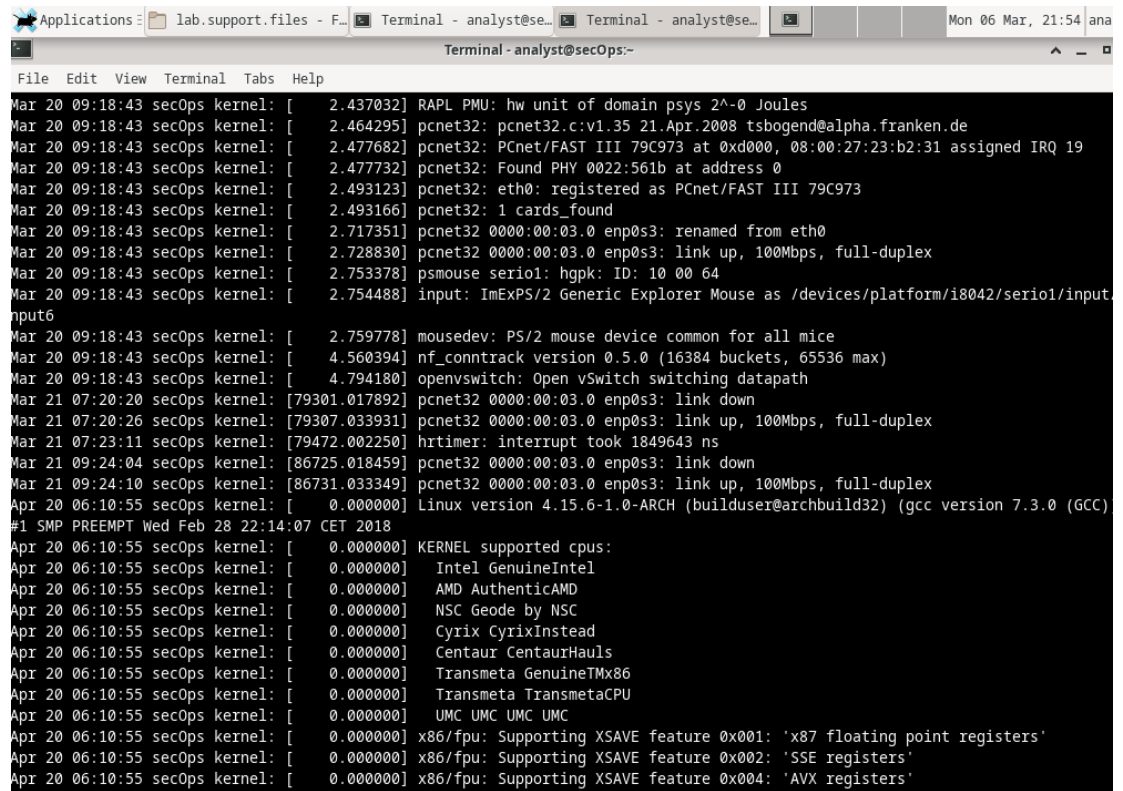
Tekan **CTRL + C** untuk menghentikan eksekusi **tail -f** dan kembali ke prompt shell. Tutup salah satu dari dua jendela terminal.



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"  
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently_asked_questions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"  
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"  
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"  
[analyst@secOps ~]$ echo "ini adalah entri baru untuk file log yang dipantau" >> lab.support.files/logstash-tutorial.log  
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
og/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"  
ini adalah entri baru untuk file log yang dipantau
```

7. Memahami File Log dan Syslog

File log dapat dijadikan dalam satu server agar lebih mudah dalam pemantauannya. Syslog adalah sistem yang dirancang agar perangkat dapat mengirim file log ke server, yang dikenal sebagai server syslog. Klien berkomunikasi ke server syslog menggunakan protokol syslog. Syslog umumnya digunakan dan mendukung hampir semua platform komputer. VM CyberOps Workstation menghasilkan file log dan mengirimkannya ke syslog.



```
Applications: lab.support.files - F... Terminal - analyst@se... Terminal - analyst@se... Mon 06 Mar, 21:54 ana
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
Mar 20 09:18:43 secOps kernel: [ 2.437032] RAPL PMU: hw unit of domain psys 2^-0 Joules
Mar 20 09:18:43 secOps kernel: [ 2.464295] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
Mar 20 09:18:43 secOps kernel: [ 2.477682] pcnet32: PCnet/FAST III 79C973 at 0xd000, 08:00:27:23:b2:31 assigned IRQ 19
Mar 20 09:18:43 secOps kernel: [ 2.477732] pcnet32: Found PHY 0022:561b at address 0
Mar 20 09:18:43 secOps kernel: [ 2.493123] pcnet32: eth0: registered as PCnet/FAST III 79C973
Mar 20 09:18:43 secOps kernel: [ 2.493166] pcnet32: 1 cards_found
Mar 20 09:18:43 secOps kernel: [ 2.717351] pcnet32 0000:00:03.0 enp0s3: renamed from eth0
Mar 20 09:18:43 secOps kernel: [ 2.728830] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Mar 20 09:18:43 secOps kernel: [ 2.753378] psmouse serio1: hgpk: ID: 10 00 64
Mar 20 09:18:43 secOps kernel: [ 2.754488] input: ImExPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input
input6
Mar 20 09:18:43 secOps kernel: [ 2.759778] mousedev: PS/2 mouse device common for all mice
Mar 20 09:18:43 secOps kernel: [ 4.560394] nf_conntrack version 0.5.0 (16384 buckets, 65536 max)
Mar 20 09:18:43 secOps kernel: [ 4.794180] openvswitch: Open vSwitch switching datapath
Mar 21 07:20:20 secOps kernel: [79301.017892] pcnet32 0000:00:03.0 enp0s3: link down
Mar 21 07:20:26 secOps kernel: [79307.033931] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Mar 21 07:23:11 secOps kernel: [79472.002250] hrtimer: interrupt took 1849643 ns
Mar 21 09:24:04 secOps kernel: [86725.018459] pcnet32 0000:00:03.0 enp0s3: link down
Mar 21 09:24:10 secOps kernel: [86731.033349] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Apr 20 06:10:55 secOps kernel: [ 0.000000] Linux version 4.15.6-1.0-ARCH (builduser@archbuild32) (gcc version 7.3.0 (GCC)
#1 SMP PREEMPT Wed Feb 28 22:14:07 CET 2018
Apr 20 06:10:55 secOps kernel: [ 0.000000] KERNEL supported cpus:
Apr 20 06:10:55 secOps kernel: [ 0.000000] Intel GenuineIntel
Apr 20 06:10:55 secOps kernel: [ 0.000000] AMD AuthenticAMD
Apr 20 06:10:55 secOps kernel: [ 0.000000] NSC Geode by NSC
Apr 20 06:10:55 secOps kernel: [ 0.000000] Cyrix CyrixInstead
Apr 20 06:10:55 secOps kernel: [ 0.000000] Centaur CentaurHauls
Apr 20 06:10:55 secOps kernel: [ 0.000000] Transmeta GenuineTMx86
Apr 20 06:10:55 secOps kernel: [ 0.000000] Transmeta TransmetaCPU
Apr 20 06:10:55 secOps kernel: [ 0.000000] UMC UMC UMC UMC
Apr 20 06:10:55 secOps kernel: [ 0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Apr 20 06:10:55 secOps kernel: [ 0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Apr 20 06:10:55 secOps kernel: [ 0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
```

Pertanyaan:

Mengapa perintah **cat** harus dijalankan sebagai **root**?

Secara umum, perintah cat tidak perlu dijalankan sebagai root. Namun, dalam beberapa situasi, pengguna harus menjalankan cat sebagai root, terutama ketika ingin membaca atau menyalin isi file yang hanya dapat diakses oleh pengguna root. Beberapa contoh situasi ini antara lain:

- File yang hanya dapat diakses oleh root: Jika file yang ingin dibaca atau disalin hanya dapat diakses oleh pengguna root, maka pengguna harus menjalankan cat sebagai root untuk dapat membaca atau menyalin isi file tersebut.
- Perubahan hak akses: Jika pengguna ingin mengubah hak akses file, seperti mengubah kepemilikan atau hak akses file, maka pengguna harus menjalankan cat sebagai root agar dapat melakukan perubahan tersebut.
- Pemasangan file system: Jika pengguna ingin membaca atau menyalin isi file system yang di-mount sebagai read-only, maka pengguna harus menjalankan cat sebagai root agar dapat membaca atau menyalin isi file tersebut

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.

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

```
Applications: lab.support.files - F... Terminal - analis@se... Terminal - analis@se... Mon 06 Mar, 21:56 analis
Terminal - analis@secOps:~
File Edit View Terminal Tabs Help
) #1 SMP PREEMPT Wed Apr 12 19:10:48 CEST 2017
Mar 6 07:27:19 secOps kernel: [ 0.000000] -----[ cut here ]-----
Mar 6 07:27:19 secOps kernel: [ 0.000000] WARNING: CPU: 0 PID: 0 at arch/x86/kernel/fpu/xstate.c:595 fpu__init_system_xsta
te+0x465/0x7b2
Mar 6 07:27:19 secOps kernel: [ 0.000000] XSAVE consistency problem, dumping leaves
Mar 6 07:27:19 secOps kernel: [ 0.000000] Modules linked in:
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPU: 0 PID: 0 Comm: swapper Not tainted 4.10.10-1-ARCH #1
Mar 6 07:27:19 secOps kernel: [ 0.000000] Call Trace:
Mar 6 07:27:19 secOps kernel: [ 0.000000] dump_stack+0x58/0x74
Mar 6 07:27:19 secOps kernel: [ 0.000000] __warn+0xea/0x110
Mar 6 07:27:19 secOps kernel: [ 0.000000] ? fpu__init_system_xstate+0x465/0x7b2
Mar 6 07:27:19 secOps kernel: [ 0.000000] warn_slowpath_fmt+0x46/0x60
Mar 6 07:27:19 secOps kernel: [ 0.000000] fpu__init_system_xstate+0x465/0x7b2
Mar 6 07:27:19 secOps kernel: [ 0.000000] fpu__init_system+0x18c/0x1b1
Mar 6 07:27:19 secOps kernel: [ 0.000000] early_cpu_init+0x110/0x113
Mar 6 07:27:19 secOps kernel: [ 0.000000] setup_arch+0xe4/0xbb6
Mar 6 07:27:19 secOps kernel: [ 0.000000] start_kernel+0x8f/0x3ce
Mar 6 07:27:19 secOps kernel: [ 0.000000] i386_start_kernel+0x91/0x95
Mar 6 07:27:19 secOps kernel: [ 0.000000] startup_32_smp+0x16b/0x16d
Mar 6 07:27:19 secOps kernel: [ 0.000000] ---[ end trace 8bb55a17c12e3d ]---
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 00]: eax=00000007 ebx=00000440 ecx=00000440 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 01]: eax=00000000 ebx=000003c0 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 02]: eax=00000100 ebx=00000240 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 03]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 04]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 05]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 06]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 07]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 08]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 09]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 0a]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 0b]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar 6 07:27:19 secOps kernel: [ 0.000000] CPUID[0d, 0c]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
```

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

```
Applications: lab.support.files - F... Terminal - analis@se... Terminal - analis@se... Mon 06 Mar, 21:57 analis
Terminal - analis@secOps:~
File Edit View Terminal Tabs Help
Mar 8 15:04:50 secOps kernel: [ 3630.532445] 01:00:21.083765 main Closing all guest files ...
[analisis@secOps ~]$ sudo cat /var/log/syslog.3
Nov 29 11:30:40 secOps kernel: [ 6.668727] ppdev: user-space parallel port driver
Nov 29 11:30:40 secOps kernel: [ 6.681487] pcnet32 0000:00:03:0 enp0s3: renamed from eth0
Nov 29 11:30:40 secOps kernel: [ 6.757097] pcnet32 0000:00:03:0 enp0s3: link up, 100Mbps, full-duplex
Nov 29 11:30:40 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 (GCC
) ) #1 SMP PREEMPT Wed Apr 12 19:10:48 CEST 2017
Nov 29 04:36:27 secOps kernel: [ 0.000000] -----[ cut here ]-----
Nov 29 04:36:27 secOps kernel: [ 0.000000] WARNING: CPU: 0 PID: 0 at arch/x86/kernel/fpu/xstate.c:595 fpu__init_system_xsta
te+0x465/0x7b2
Nov 29 04:36:27 secOps kernel: [ 0.000000] XSAVE consistency problem, dumping leaves
Nov 29 04:36:27 secOps kernel: [ 0.000000] Modules linked in:
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPU: 0 PID: 0 Comm: swapper Not tainted 4.10.10-1-ARCH #1
Nov 29 04:36:27 secOps kernel: [ 0.000000] Call Trace:
Nov 29 04:36:27 secOps kernel: [ 0.000000] dump_stack+0x58/0x74
Nov 29 04:36:27 secOps kernel: [ 0.000000] __warn+0xea/0x110
Nov 29 04:36:27 secOps kernel: [ 0.000000] ? fpu__init_system_xstate+0x465/0x7b2
Nov 29 04:36:27 secOps kernel: [ 0.000000] warn_slowpath_fmt+0x46/0x60
Nov 29 04:36:27 secOps kernel: [ 0.000000] fpu__init_system_xstate+0x465/0x7b2
Nov 29 04:36:27 secOps kernel: [ 0.000000] fpu__init_system+0x18c/0x1b1
Nov 29 04:36:27 secOps kernel: [ 0.000000] early_cpu_init+0x110/0x113
Nov 29 04:36:27 secOps kernel: [ 0.000000] setup_arch+0xe4/0xbb6
Nov 29 04:36:27 secOps kernel: [ 0.000000] start_kernel+0x8f/0x3ce
Nov 29 04:36:27 secOps kernel: [ 0.000000] i386_start_kernel+0x91/0x95
Nov 29 04:36:27 secOps kernel: [ 0.000000] startup_32_smp+0x16b/0x16d
Nov 29 04:36:27 secOps kernel: [ 0.000000] ---[ end trace 3451dc0d6e69451e ]---
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPUID[0d, 00]: eax=00000007 ebx=00000440 ecx=00000440 edx=00000000
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPUID[0d, 01]: eax=00000000 ebx=000003c0 ecx=00000000 edx=00000000
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPUID[0d, 02]: eax=00000100 ebx=00000240 ecx=00000000 edx=00000000
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPUID[0d, 03]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Nov 29 04:36:27 secOps kernel: [ 0.000000] CPUID[0d, 04]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
```

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

```
Applications: lab.support.files - F... Terminal - analyst@se... Terminal - analyst@se... Mon 06 Mar, 21:58 | analis
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
nput/
Mar 6 11:58:56 secOps kernel: [ 6.016025] openvswitch: Open vSwitch switching datapath
[analyst@secOps ~]$ sudo cat /var/log/syslog.4
Aug 23 12:04:42 secOps kernel: [ 8.047919] floppy0: no floppy controllers found
Aug 23 12:04:42 secOps kernel: [ 8.047950] work still pending
Aug 23 13:49:32 secOps kernel: [ 6298.300707] pcnet32 0000:00:03.0 enp0s3: link down
Aug 23 13:49:36 secOps kernel: [ 6302.354139] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Aug 24 11:06:06 secOps kernel: [82892.804946] Bluetooth: Core ver 2.22
Aug 24 11:06:06 secOps kernel: [82892.805387] NET: Registered protocol family 31
Aug 24 11:06:06 secOps kernel: [82892.805388] Bluetooth: HCI device and connection manager initialized
Aug 24 11:06:06 secOps kernel: [82892.805390] Bluetooth: HCI socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.805392] Bluetooth: L2CAP socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.805396] Bluetooth: SCO socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.816995] Netfilter messages via NETLINK v0.30.
Aug 24 11:15:48 secOps kernel: [83475.322402] pcnet32 0000:00:03.0 enp0s3: link down
Aug 24 11:15:54 secOps kernel: [83481.238928] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Aug 24 08:09:23 secOps kernel: [ 0.000000] Linux version 4.10.10-1-ARCH (builduser@tobias) (gcc version 6.3.1 20170306 (GCC
) ) #1 SMP PREEMPT Wed Apr 12 19:10:48 CEST 2017
Aug 24 08:09:23 secOps kernel: [ 0.000000] -----[ cut here ]-----
Aug 24 08:09:23 secOps kernel: [ 0.000000] WARNING: CPU: 0 PID: 0 at arch/x86/kernel/fpu/xstate.c:595 fpu__init_system_xsta
te+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [ 0.000000] XSAVE consistency problem, dumping leaves
Aug 24 08:09:23 secOps kernel: [ 0.000000] Modules linked in:
Aug 24 08:09:23 secOps kernel: [ 0.000000] CPU: 0 PID: 0 Comm: swapper Not tainted 4.10.10-1-ARCH #1
Aug 24 08:09:23 secOps kernel: [ 0.000000] Call Trace:
Aug 24 08:09:23 secOps kernel: [ 0.000000] dump_stack+0x58/0x74
Aug 24 08:09:23 secOps kernel: [ 0.000000] __warn+0xea/0x110
Aug 24 08:09:23 secOps kernel: [ 0.000000] ? fpu__init_system_xstate+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [ 0.000000] warn_slowpath_fmt+0x46/0x60
Aug 24 08:09:23 secOps kernel: [ 0.000000] fpu__init_system_xstate+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [ 0.000000] fpu__init_system_xstate+0x18c/0x1b1
```

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

Mensinkronkan waktu dan tanggal komputer dengan benar sangat penting karena:

Menjaga konsistensi data: Waktu yang akurat dan terkini sangat penting dalam mengelola data dan informasi. Jika waktu dan tanggal pada komputer tidak sinkron dengan benar, maka dapat menyebabkan data yang dihasilkan menjadi tidak konsisten atau tidak akurat, yang pada akhirnya dapat menyebabkan kesalahan dalam pengambilan keputusan.

Menghindari kesalahan dalam transaksi: Dalam transaksi yang dilakukan melalui komputer, waktu yang akurat sangat penting. Jika waktu pada komputer tidak sinkron dengan benar, maka dapat menyebabkan kesalahan dalam transaksi, seperti kesalahan dalam penjadwalan atau pembayaran tagihan.

Mencegah masalah dalam audit: Audit sistem memerlukan informasi yang akurat tentang waktu dan tanggal suatu transaksi atau kejadian. Jika waktu pada komputer tidak sinkron dengan benar, maka audit tidak akan dapat mengidentifikasi masalah atau melacak jejak kejadian yang terjadi di sistem.

Memperbaiki masalah jaringan: Jika komputer tidak memiliki waktu yang sinkron dengan benar, maka dapat menyebabkan masalah dalam jaringan, seperti pengiriman email yang salah waktu atau sinkronisasi data yang tidak berfungsi dengan baik.

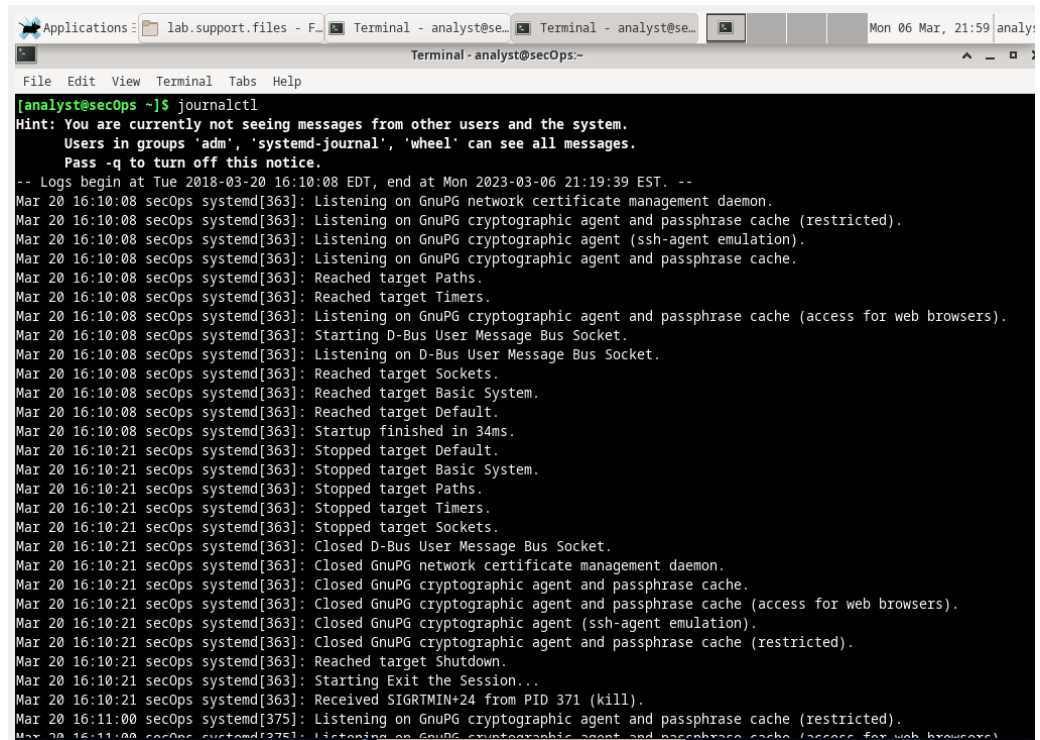
9. Memahami File Log dan Jurnalcti

Sistem manajemen log populer lainnya dikenal sebagai jurnal. Dikelola oleh **daemon journald**, sistem ini dirancang untuk memusatkan pengelolaan log terlepas dari mana pesan berasal. Dalam konteks lab ini, fitur

yang paling jelas dari daemon sistem jurnal adalah penggunaan file biner khusus tambahan yang berfungsi sebagai file lognya.

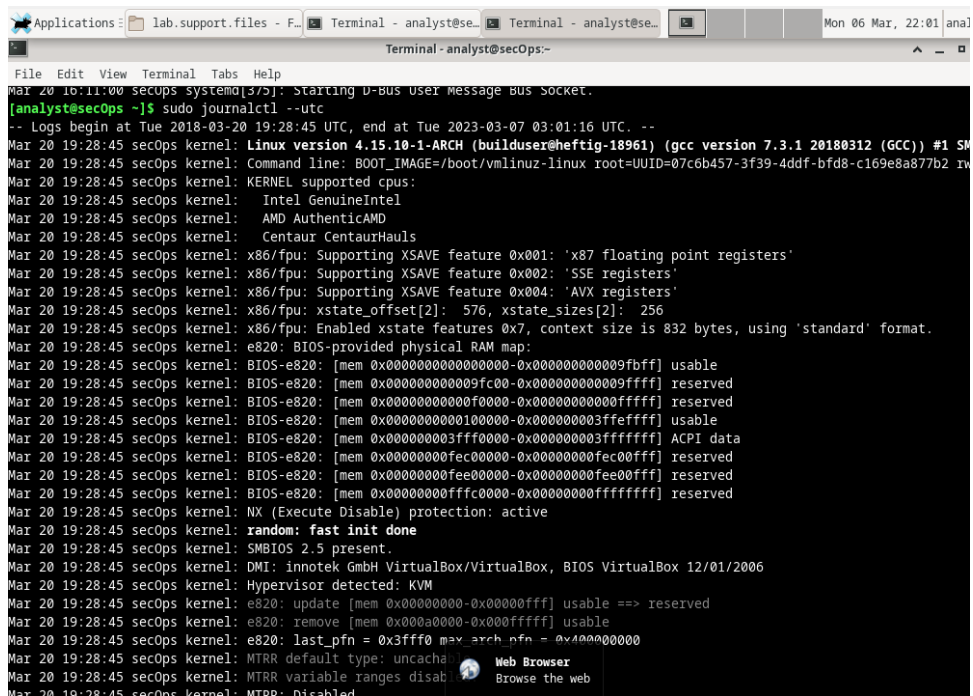
Untuk melihat log journald, gunakan perintah **journalctl**. Alat journalctl menafsirkan dan menampilkan entri log yang sebelumnya disimpan dalam file log biner jurnal.

analis@secOps ~\$ journalctl



```
[analyst@secOps ~]$ journalctl
Hint: You are currently not seeing messages from other users and the system.
Users in groups 'adm', 'systemd-journal', 'wheel' can see all messages.
Pass -q to turn off this notice.
-- Logs begin at Tue 2018-03-20 16:10:08 EDT, end at Mon 2023-03-06 21:19:39 EST. --
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG network certificate management daemon.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache.
Mar 20 16:10:08 secOps systemd[363]: Reached target Paths.
Mar 20 16:10:08 secOps systemd[363]: Reached target Timers.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphrase cache (access for web browsers).
Mar 20 16:10:08 secOps systemd[363]: Starting D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Listening on D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Reached target Sockets.
Mar 20 16:10:08 secOps systemd[363]: Reached target Basic System.
Mar 20 16:10:08 secOps systemd[363]: Reached target Default.
Mar 20 16:10:08 secOps systemd[363]: Startup finished in 34ms.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Default.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Basic System.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Paths.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Timers.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Sockets.
Mar 20 16:10:21 secOps systemd[363]: Closed D-Bus User Message Bus Socket.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG network certificate management daemon.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache (access for web browsers).
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent (ssh-agent emulation).
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 16:10:21 secOps systemd[363]: Reached target Shutdown.
Mar 20 16:10:21 secOps systemd[363]: Starting Exit the Session...
Mar 20 16:10:21 secOps systemd[363]: Received SIGRTMIN+24 from PID 371 (kill).
Mar 20 16:11:00 secOps systemd[375]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Mar 20 16:11:00 secOps systemd[375]: Listening on GnuPG cryptographic agent and passphrase cache (access for web browsers).
```

analis@secOps ~\$ sudo journalctl -utc



```
Mar 20 16:11:00 secOps systemd[375]: Starting D-Bus User Message Bus Socket.
[analyst@secOps ~]$ sudo journalctl -utc
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Tue 2023-03-07 03:01:16 UTC. --
Mar 20 19:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builduser@heftig-18961) (gcc version 7.3.1 20180312 (GCC)) #1 SMP
Mar 20 19:28:45 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 20 19:28:45 secOps kernel: KERNEL supported cpus:
Mar 20 19:28:45 secOps kernel: Intel GenuineIntel
Mar 20 19:28:45 secOps kernel: AMD AuthenticAMD
Mar 20 19:28:45 secOps kernel: Centaur CentaurHauls
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 20 19:28:45 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Mar 20 19:28:45 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
Mar 20 19:28:45 secOps kernel: e820: BIOS-provided physical RAM map:
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000009f000-0x000000000000ffffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000003ffffff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000003ff0000-0x000000000003ffffff] ACPI data
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffff] 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 0x00000000-0x000000ff] usable ==> reserved
Mar 20 19:28:45 secOps kernel: e820: remove [mem 0x000a0000-0x000ffffff] 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: uncached
Mar 20 19:28:45 secOps kernel: MTRR variable ranges disabled
Mar 20 19:28:45 secOps kernel: MTRR: Disabled
```


analis@secOps ~\$ sudo journalctl -b

```
Applications: lab.support.files - F... Terminal - analyst@se... Terminal - analyst@se... Mon 06 Mar, 22:03 | analys...
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
Mar 20 19:28:45 secOps kernel: MTRR: Disabled
[analyst@secOps ~]$ sudo journalctl -b
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 22:03:15 EST. --
Mar 06 21:06:38 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 21:06:38 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 06 21:06:38 secOps kernel: KERNEL supported cpus:
Mar 06 21:06:38 secOps kernel: Intel GenuineIntel
Mar 06 21:06:38 secOps kernel: AMD AuthenticAMD
Mar 06 21:06:38 secOps kernel: Hygon HygonGenuine
Mar 06 21:06:38 secOps kernel: Centaur CentaurHauls
Mar 06 21:06:38 secOps kernel: zhaoxin Shanghai
Mar 06 21:06:38 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 21:06:38 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 21:06:38 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 21:06:38 secOps kernel: BIOS-provided physical RAM map:
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbfff] usable
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009fffff] reserved
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x00000000000100000-0x0000000000003fffff] usable
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x000000000003ffff000-0x000000000003ffffff] ACPI data
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffff] reserved
Mar 06 21:06:38 secOps kernel: NX (Execute Disable) protection: active
Mar 06 21:06:38 secOps kernel: SMBIOS 2.5 present.
Mar 06 21:06:38 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 21:06:38 secOps kernel: Hypervisor detected: KVM
Mar 06 21:06:38 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 21:06:38 secOps kernel: kvm-clock: cpu 0, msr 3ca01001, primary cpu clock
Mar 06 21:06:38 secOps kernel: kvm-clock: using sched offset of 11333723690 cycles
Mar 06 21:06:38 secOps kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 88159
Mar 06 21:06:38 secOps kernel: tsc: Detected 2993.210 MHz processor
Mar 06 21:06:38 secOps kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Mar 06 21:06:38 secOps kernel: e820: remove [mem 0x00000000-0x00000fff] usable
```

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

```
[analyst@secOps ~]$ sudo journalctl -u nginx.service --until today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 22:05:29 EST. --
-- No entries --
```

analis@secOps ~\$ sudo journalctl -k

```
Applications: lab.support.files - F... Terminal - analyst@se... Terminal - analyst@se... Mon 06 Mar, 22:08 | analys...
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
-- No entries --
[analyst@secOps ~]$ sudo journalctl -k
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 22:07:47 EST. --
Mar 06 21:06:38 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 21:06:38 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw
Mar 06 21:06:38 secOps kernel: KERNEL supported cpus:
Mar 06 21:06:38 secOps kernel: Intel GenuineIntel
Mar 06 21:06:38 secOps kernel: AMD AuthenticAMD
Mar 06 21:06:38 secOps kernel: Hygon HygonGenuine
Mar 06 21:06:38 secOps kernel: Centaur CentaurHauls
Mar 06 21:06:38 secOps kernel: zhaoxin Shanghai
Mar 06 21:06:38 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 21:06:38 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 21:06:38 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 21:06:38 secOps kernel: BIOS-provided physical RAM map:
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbfff] usable
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009fffff] reserved
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x00000000000100000-0x0000000000003fffff] usable
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x000000000003ffff000-0x000000000003ffffff] ACPI data
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 21:06:38 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffff] reserved
Mar 06 21:06:38 secOps kernel: NX (Execute Disable) protection: active
Mar 06 21:06:38 secOps kernel: SMBIOS 2.5 present.
Mar 06 21:06:38 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 21:06:38 secOps kernel: Hypervisor detected: KVM
Mar 06 21:06:38 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 21:06:38 secOps kernel: kvm-clock: cpu 0, msr 3ca01001, primary cpu clock
Mar 06 21:06:38 secOps kernel: kvm-clock: using sched offset of 11333723690 cycles
Mar 06 21:06:38 secOps kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 88159
Mar 06 21:06:38 secOps kernel: tsc: Detected 2993.210 MHz processor
Mar 06 21:06:38 secOps kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
```


analisis@secOps ~\$ sudo journalctl -f

```
[analisis@secOps ~]$ sudo journalctl -f
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Mar 06 22:08:37 secOps kernel: audit: type=1106 audit(1678158517.040:181): pid=820 uid=0 auid=1000 ses=2 msg='op=PAM:session_c
lose grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 22:08:37 secOps kernel: audit: type=1104 audit(1678158517.040:182): pid=820 uid=0 auid=1000 ses=2 msg='op=PAM:setcred g
rantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 22:08:39 secOps audit[829]: USER_ACCT pid=829 uid=0 auid=1000 ses=2 msg='op=PAM:accounting grantors=pam_unix,pam_per
mit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 22:08:39 secOps kernel: audit: type=1101 audit(1678158519.840:183): pid=829 uid=0 auid=1000 ses=2 msg='op=PAM:accoun
ting grantors=pam_unix,pam_permit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=succes
s'
Mar 06 22:08:39 secOps sudo[829]: analyst : TTY=pts/2 ; PWD=/home/analyst ; USER=root ; COMMAND=/usr/bin/journalctl -f
Mar 06 22:08:39 secOps audit[829]: CRED_REFR pid=829 uid=0 auid=1000 ses=2 msg='op=PAM:setcred grantors=pam_unix,pam_permit,p
am_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 22:08:39 secOps sudo[829]: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 06 22:08:39 secOps audit[829]: USER_START pid=829 uid=0 auid=1000 ses=2 msg='op=PAM:session_open grantors=pam_limits,pam_u
nix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 22:08:39 secOps kernel: audit: type=1110 audit(1678158519.846:184): pid=829 uid=0 auid=1000 ses=2 msg='op=PAM:setcred g
rantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 22:08:39 secOps kernel: audit: type=1105 audit(1678158519.846:185): pid=829 uid=0 auid=1000 ses=2 msg='op=PAM:session_o
pen grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
```

5. PEMBAHASAN

Steganografi atau stego adalah teknik menyembunyikan pesan atau data dalam objek yang tidak mencurigakan atau objek yang biasa-biasa saja. Objek tersebut dapat berupa gambar, audio, video, teks, atau jenis file lainnya. Tujuan dari steganografi adalah untuk menyembunyikan pesan atau data secara rahasia tanpa menimbulkan kecurigaan dari pihak lain yang tidak berhak mengaksesnya.

Ada beberapa metode atau teknik yang digunakan dalam steganografi, di antaranya adalah:

Least Significant Bit (LSB): Teknik ini adalah salah satu teknik steganografi yang paling populer. Pada teknik LSB, pesan atau data disisipkan ke dalam bit terakhir dari piksel gambar. Dalam gambar digital, setiap piksel terdiri dari tiga komponen warna yaitu merah, hijau, dan biru (RGB). LSB memanfaatkan fakta bahwa perubahan nilai pada bit terakhir warna tersebut tidak akan terlihat secara signifikan pada gambar, sehingga pesan atau data yang disisipkan tidak akan terdeteksi.

Spread Spectrum: Teknik ini menggunakan frekuensi atau bandwidth yang luas untuk menyebarkan data atau pesan secara acak dalam spektrum frekuensi. Dalam teknik spread spectrum, pesan atau data diubah menjadi sinyal digital dan kemudian ditambahkan ke dalam sinyal frekuensi lain yang memiliki bandwidth yang lebih besar. Pesan atau data dapat dipulihkan dengan menggunakan kunci rahasia yang sama dengan kunci yang digunakan saat penyisipan.

Transformasi Wavelet: Teknik ini menggunakan transformasi wavelet untuk menyisipkan pesan atau data ke dalam gambar digital. Transformasi wavelet memungkinkan informasi pada gambar digital untuk dikompresi dan dikodekan ke dalam ruang frekuensi yang lebih rendah. Pesan atau data kemudian disisipkan ke dalam komponen frekuensi yang lebih rendah tersebut.

Modulasi Frekuensi: Teknik modulasi frekuensi ini menggunakan frekuensi sinyal untuk menyisipkan pesan atau data. Dalam teknik ini, pesan atau data diubah menjadi sinyal digital dan kemudian dimodulasi ke dalam sinyal frekuensi yang berbeda dengan frekuensi sinyal

asli. Pesan atau data kemudian dapat dipulihkan dengan menggunakan kunci rahasia yang sama.

6. KESIMPULAN

Kesimpulan dari teknik steganografi atau stego adalah bahwa teknik ini dapat digunakan untuk menyembunyikan pesan atau data secara rahasia dalam objek yang tidak mencurigakan atau objek yang biasa-biasa saja, seperti gambar, audio, video, teks, atau jenis file lainnya. Dalam steganografi, pesan atau data disisipkan ke dalam objek dengan cara yang tidak dapat terdeteksi oleh pihak lain yang tidak berhak mengaksesnya.

DAFTAR PUSTAKA

KUNCORO, A. A. (2022, desember 21). *Universitas stekom*. Retrieved from <http://teknik-informatika-s1.stekom.ac.id/informasi/baca/Seni-dan-Ilmu-Menulis-Pesan-Tersembunyi-Steganografi/ff7dc125afd07f6dd43da9fa8a09809e96d41789>