LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
UNIT 5
TEKNIK STEGANOGRAFI

DISUSUN OLEH:

Nama : Yana Dayinta Nesthi
Kelas : RI4AA
NIM : 21/478358/SV/19272
Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

TEKNIK STEGANOGRAFI

A. TUJUAN

- Mempelajari cara melakukan steganografi dan mengamati hasilnya

B. DASAR TEORI

- **Steganografi**

  Steganografi, yang berasal dari kata Yunani "Stegano" yang berarti "tersembunyi atau menyembunyikan" dan "graphy" yang berarti "tulisan", merupakan seni atau teknik untuk menyembunyikan pesan rahasia sehingga hanya pengirim dan penerima yang dapat mengetahuinya. Dalam steganografi, pesan tersebut disembunyikan dengan cara tertentu, sehingga tidak menarik perhatian atau menimbulkan kecurigaan. Hal ini berbeda dengan kriptografi, yang hanya menyamarkan arti pesan rahasia tanpa menyembunyikan kenyataan bahwa pesan tersebut ada. Meskipun pesan dalam kriptografi sulit untuk dipecahkan, namun pesan tersebut tetap menimbulkan kecurigaan. Oleh karena itu, kelebihan steganografi dibandingkan dengan kriptografi adalah bahwa pesan-pesan yang disampaikan melalui steganografi tidak menimbulkan kecurigaan dan tidak terlihat mencurigakan.

  Untuk menyimpan pesan rahasia secara tersembunyi, pesan tersebut akan dimasukkan ke dalam media seperti citra, suara, atau video, yang tampak tidak mencurigakan. Agar hanya pihak yang berwenang yang dapat membuka atau mengambil pesan rahasia, pesan tersebut akan dilindungi oleh suatu kunci rahasia yang dikenal sebagai stego-key.

C. ALAT DAN BAHAN

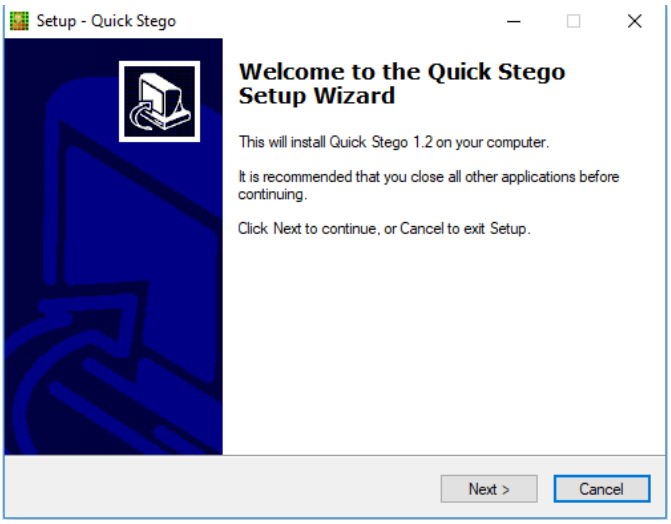
- *Software* QuickStego
- File MD5SUMS
- OS Windows
- PC / Laptop

D. HASIL DAN ANALISIS

1. Pengaturan - Stego

   Petunjuk:

   Klik tombol Next

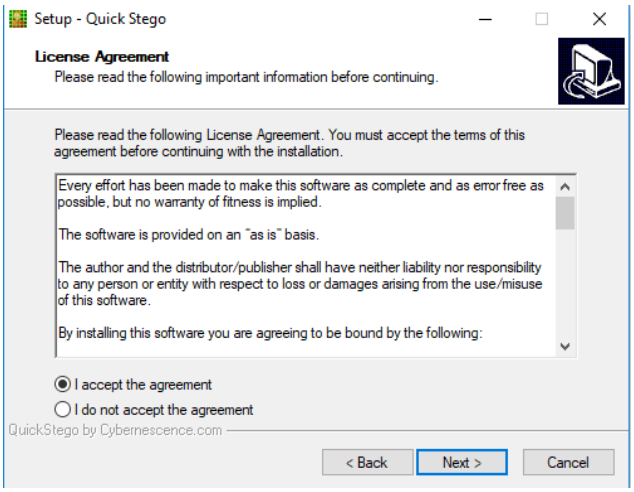


2. Perjanjian Lisensi

   Petunjuk:

   Pilih tombol radio **I accept the agreement**

   Klik tombol **Next**

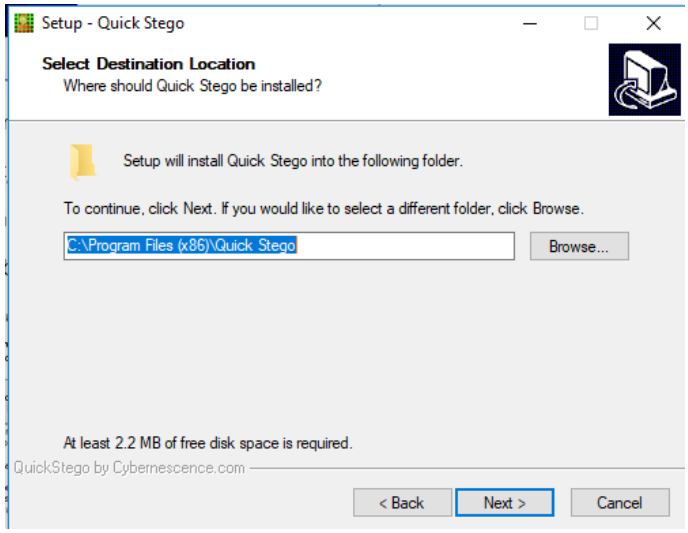


3. Pilih Tujuan

   Petunjuk:

   Terima Lokasi Tujuan Default

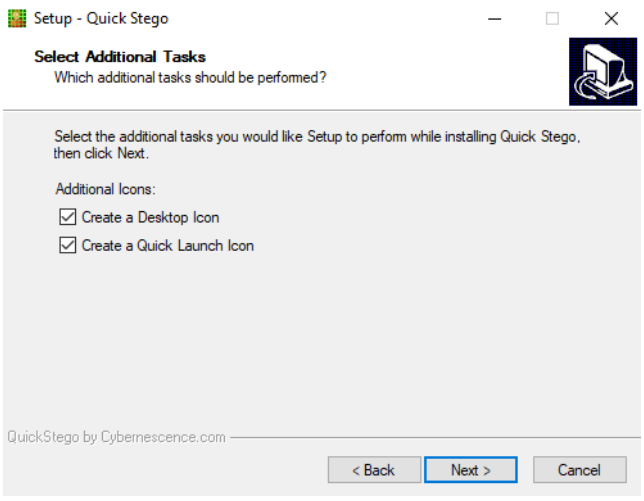
   Klik tombol **Next**



4. Pilih Tugas Tambahan

   Petunjuk:

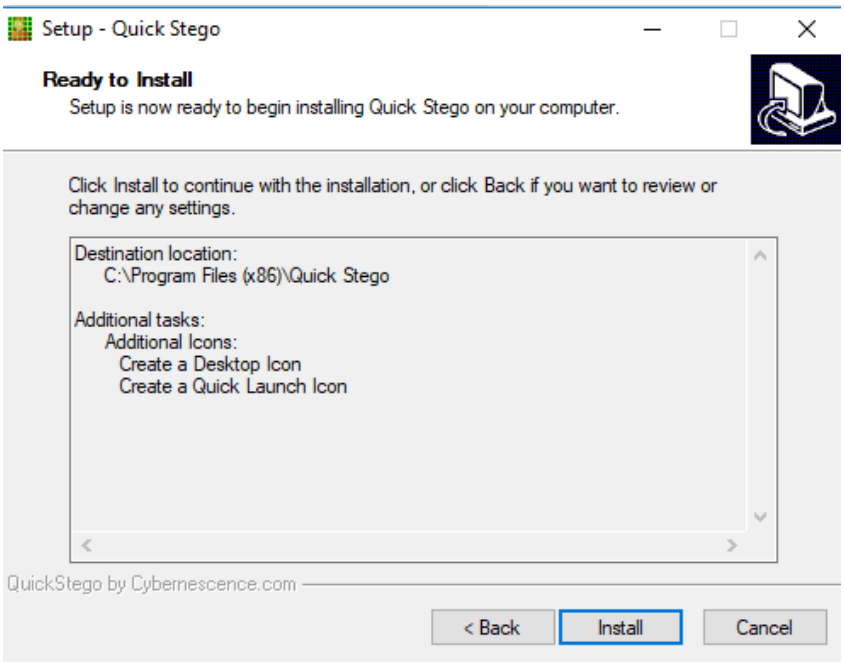
   Centang kotak **Create a Desktop Icon,** Centang kotak **Create a Quick Launch Icon,** Klik pada tombol **Next**

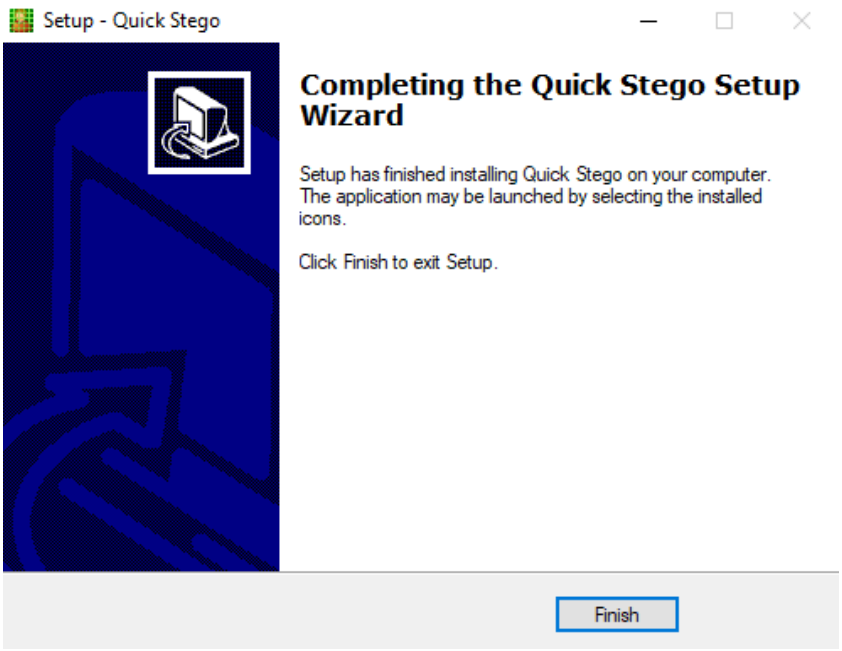


5. Siap dipasang

Petunjuk:

Klik tombol **Install**





6. Masuk Command Prompt

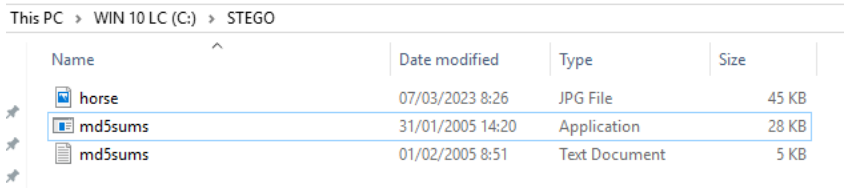
   Buat Direktori STEGO

   Peraturan:

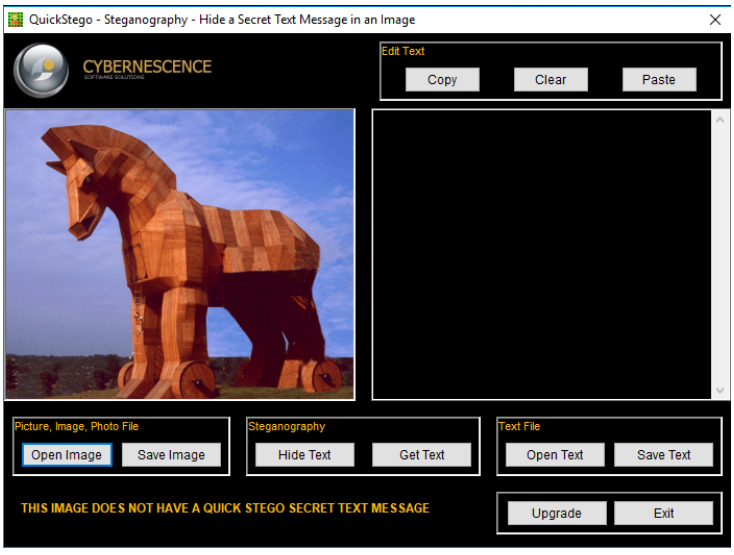
   a. mkdir "C:\STEGO"
   b. dir "C:\" | findstr STEGO

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\TAJ>mkdir "C:\STEGO"
A subdirectory or file C:\STEGO already exists.

C:\Users\TAJ>dir "C:\" | temukanstr STEGO
'temukanstr' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\TAJ>dir "C:\" | findstr STEGO
07/03/2023  08:20    <DIR>          STEGO
```

7. Md5sum dan gambar yang sudah diunduh, disimpan di folder stego



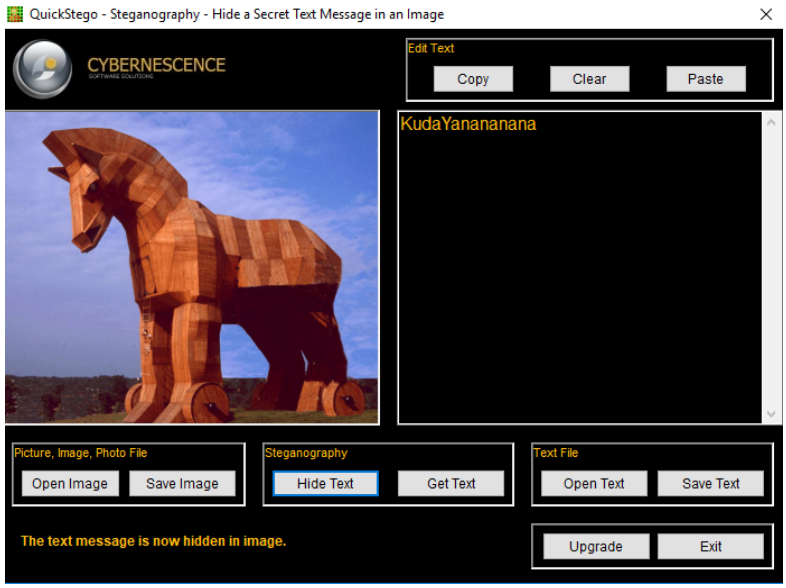
8. Buka QuickStego, lalu masukkan gambar (gambar harus dengan format .jpg)



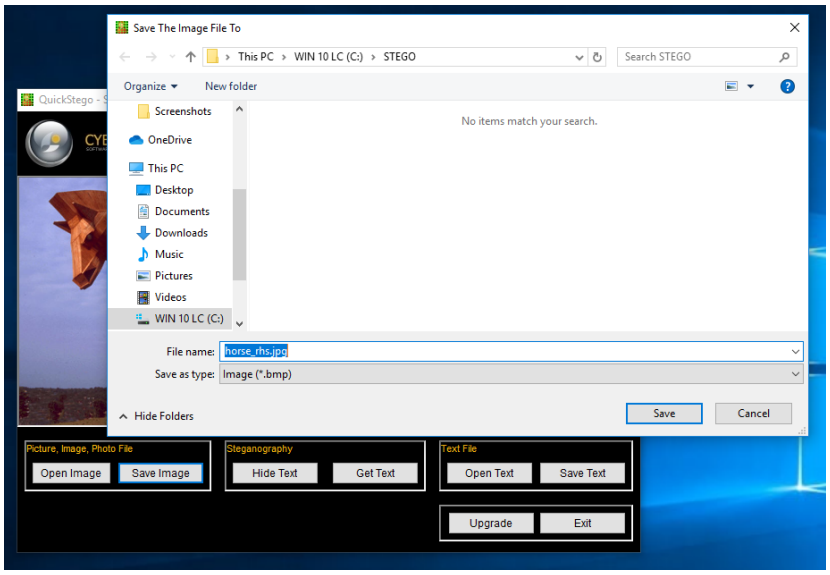
9. Sembunyikan text.

   Petunjuk:

   a. Berikan Pesan Tersembunyi Anda. Pesan tersembunyi saya ada di bawah. (Lihat Gambar)
   b. Klik tombol Sembunyikan Teks
   c. Perhatikan pesan yang menyatakan "This text message is now hidden in image".



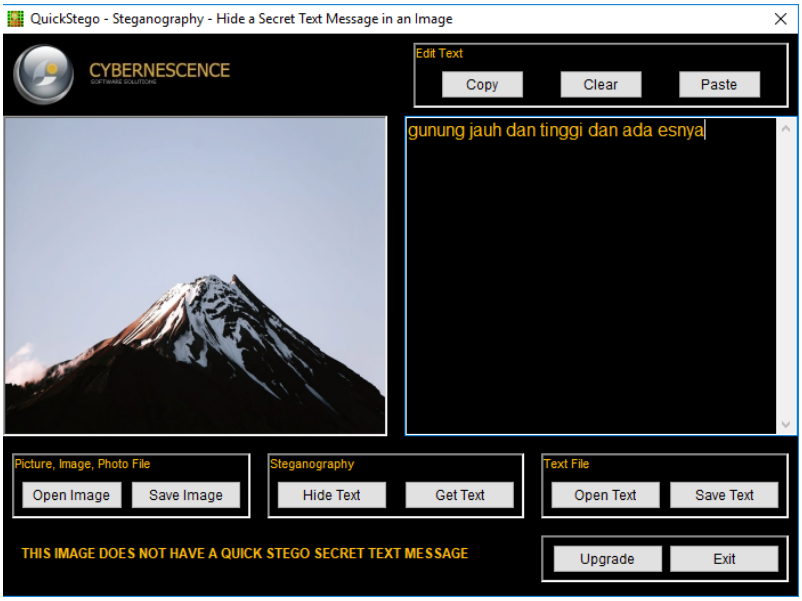
10. Simpan gambar, nama file bebas namun beri nama yang berbeda dengan yang awal.



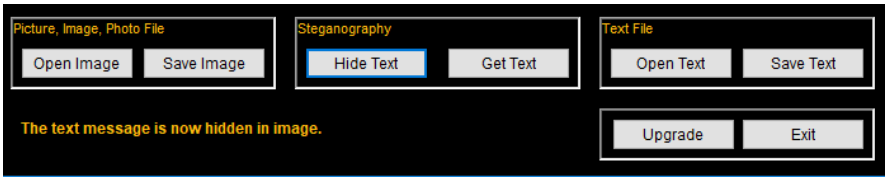
11. Pembuktian bahwa kedua file memiliki isi yang berbeda

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

C:\STEGO>md5sums.exe *.jpg

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

[Path] / filename                                MD5 sum
-------------------------------------------------------------------------------
[C:\STEGO\]
horse.jpg                                        fce8552170cced3dd545566309124097
horse_rhs.jpg                                    a3913a573f44a0d4c66ccb80f050a131

C:\STEGO>dir *.jpg
 Volume in drive C is WIN 10 LC
 Volume Serial Number is 2493-2E86

 Directory of C:\STEGO

07/03/2023  08:26            46.001 horse.jpg
07/03/2023  08:36           854.454 horse_rhs.jpg
               2 File(s)        900.455 bytes
               0 Dir(s)  279.418.818.560 bytes free
```

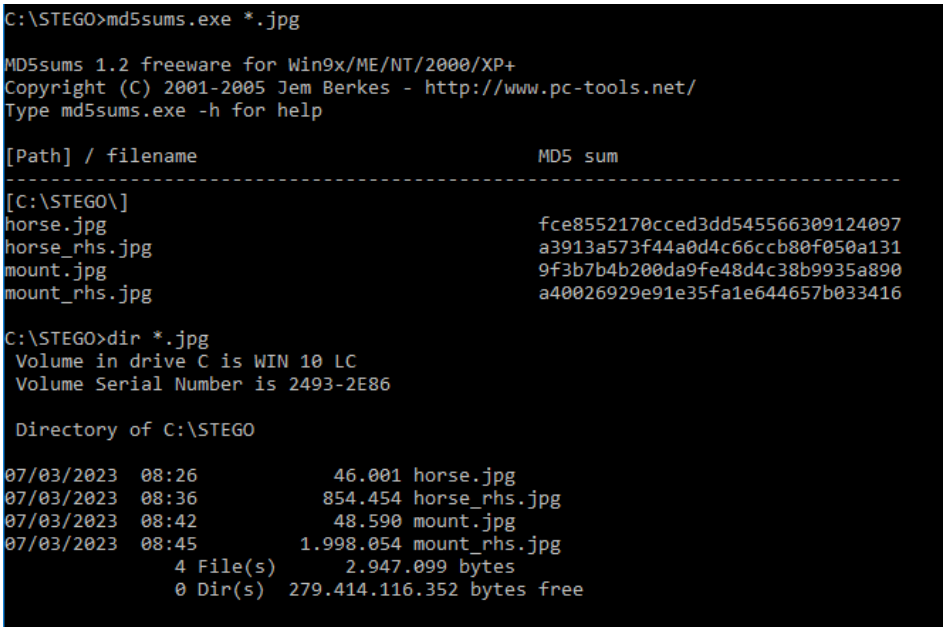
12. Masukkan gambar kedua, dan tuliskan pesannya



13. Sembunyikan text, lalu simpan gambar



14. Pembuktian



PEMBAHASAN:

Steganografi ini sering digunakan untuk menyembunyikan pesan dalam format digital. Bermacam-macam bisa digunakan, contohnya gambar dengan format jpg. Pada praktikum kali ini teknik steganografi yang digunakan adalah *injection*. *Injection* atau *Embedding* yaitu cara langsung menanamkan pesan rahasia ke dalam suatu media, memiliki kelemahan di mana media yang telah diinjeksi akan menjadi lebih besar dari ukuran aslinya, sehingga dapat mudah terdeteksi.

Software pendukung yang digunakan kali ini adalah QuickStego. QuickStego adalah sebuah program yang memungkinkan pengguna untuk menyembunyikan teks dalam sebuah gambar agar hanya pengguna QuickStego lain yang dapat mengambil dan membaca pesan rahasia yang tersembunyi. Setelah teks disembunyikan dalam gambar, gambar tersebut masih akan berfungsi seperti gambar biasa dan dapat dimuat seperti biasa. Gambar yang mengandung pesan tersembunyi dapat disimpan, dikirim melalui email, atau diunggah ke web tanpa menimbulkan kecurigaan, karena tidak ada perbedaan yang mencolok pada tampilannya.

Dapat dilihat pada hasil tampilan gambarnya. Kedua gambar ini sekilas tidak memiliki perbedaan. Namun apabila dibandingkan ukuran filenya, maka akan tampak perbedaannya. File asli memiliki ukuran file lebih kecil dibanding file gambar yang sudah disisipkan pesan rahasia.

E. KESIMPULAN

- Kata steganografi (steganography) berasal dari bahasa Yunani steganos yang artinya “tersembunyi/terselubung” dan graphein “menulis” sehingga kurang lebih artinya “menulis (tulisan) terselubung”.
- QuickStego adalah sebuah program yang memungkinkan pengguna untuk menyembunyikan teks dalam sebuah gambar agar hanya pengguna QuickStego lain yang dapat mengambil dan membaca pesan rahasia yang tersembunyi.
- Kelemahan teknik *injection* adalah, media yang telah diinjeksi akan menjadi lebih besar dari ukuran aslinya, sehingga dapat mudah terdeteksi.

F. DAFTAR PUSTAKA

Pengertian Steganografi, Jenis-Jenis, dan Prinsip Kerja. (2018, Februari 14). Immersa Lab. Diakses pada Maret 9, 2023, dari https://www.immersa-lab.com/pengertian-steganografi-jenis-jenis-dan-prinsip-kerja.htm

Wijaya, E. S., & Prayudi, Y. (2004). KONSEP HIDDEN MESSAGE MENGGUNAKAN TEKNIK STEGANOGRAFI DYNAMIC CELL SPREADING. *Media Informatika*, *Vol. 2, No. 1*, 35-37.

LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
UNIT 6
PEMBACAAN LOG SERVER

DISUSUN OLEH:

Nama : Yana Dayinta Nesthi
Kelas : RI4AA
NIM : 21/478358/SV/19272
Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

PEMBACAAN LOG SERVER

A. TUJUAN

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

B. DASAR TEORI

a. File Log

File log merupakan file yang dihasilkan oleh software yang berisi informasi mengenai operasi, aktivitas, dan pola penggunaan sistem IT, server, atau aplikasi. File log ini mencakup catatan historis dari semua proses, peristiwa, dan pesan yang terjadi, beserta data deskriptif lainnya seperti stempel waktu untuk memberikan konteks pada informasi tersebut. Stempel waktu tersebut memberikan informasi tentang apa yang terjadi pada sistem dan kapan peristiwa tersebut terjadi. Dengan adanya file log, jika terjadi kesalahan pada sistem, kita dapat melihat catatan terperinci dari setiap tindakan sebelum peristiwa tersebut terjadi.

File log menyediakan catatan informasi yang terperinci dan mudah diakses mengenai sistem, yang jika tidak ada file log, akan sulit untuk disusun. File log memberikan pemahaman mengenai kinerja dan kepatuhan dari aplikasi dan sistem. Terutama untuk aplikasi cloud yang memiliki fitur dinamis dan terdistribusi, file log sangat penting. Beberapa manfaat dari file log meliputi kemampuan untuk memperoleh pemahaman yang berarti mengenai kesehatan dan fungsionalitas sistem secara keseluruhan, kemampuan untuk mendapatkan garis waktu insiden dan mempercepat pemecahan masalah, kemampuan untuk mengidentifikasi bug keamanan dan meminimalkan risiko keamanan, serta kemampuan untuk mengoptimalkan kinerja aplikasi dari waktu ke waktu.

Salah satu tipe file log adalah log server. Log server sendiri merupakan sebuah file log yang dibuat secara otomatis dan dijaga oleh server. File log tersebut berisi daftar aktivitas yang telah dilakukan oleh server, seperti jumlah permintaan halaman, alamat IP klien, jenis permintaan, dan lain-lain.

C. ALAT DAN BAHAN

- PC / Laptop
- Virtual Box
- CyberOps Workstation virtual machine

D. HASIL DAN ANALISIS

1. Buka vm cyberops workstation

2. Buka terminal, lalu ketikkan perintah

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

   Isi file harus ditampilkan melalui jendela terminal.

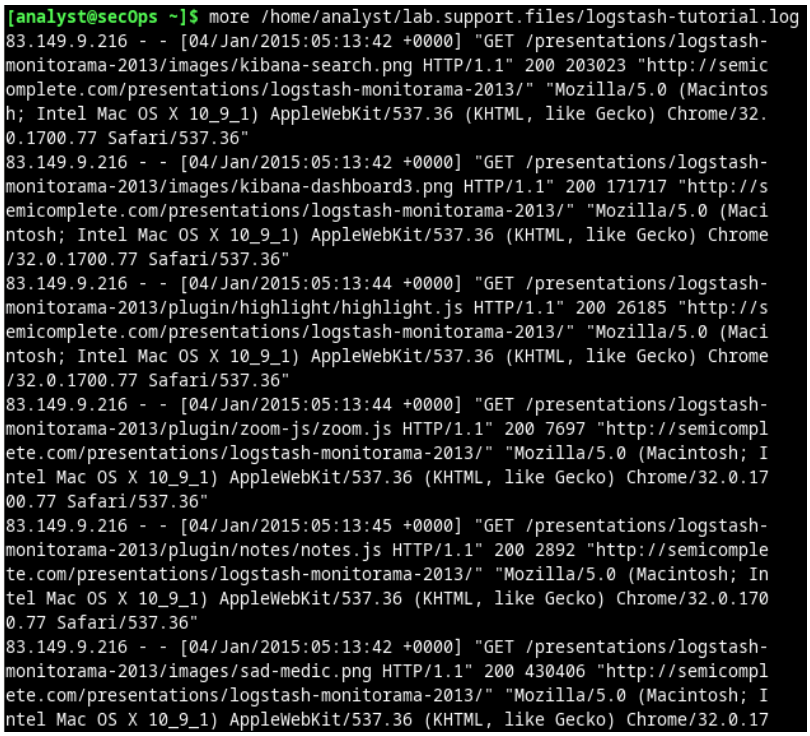
   Pertanyaan: Apa kelemahan menggunakan cat dengan file teks besar?

```
[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)
 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" 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"
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
```

3. 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

   Pertanyaan : Apa kelemahan menggunakan more?



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

   analis@secOps ~$ less /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/2015:05:13:46 +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
/home/analyst/lab.support.files/logstash-tutorial.log
```

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

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

```
[analyst@secOps ~]$ tail /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/
4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 9872 "-" "S
ogou 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 T
iny 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 Tin
y 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 (co
mpatible; 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/Xm
onad/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. Atur tampilan Anda sehingga Anda dapat melihat kedua jendela terminal. Ubah ukuran jendela sehingga Anda dapat melihat keduanya secara bersamaan. Pada jendela terminal tersebut, jalankanlah tail -f untuk melihat file /home/analyst/lab.support.files/logstash-tutorial.log. Gunakan jendela terminal di bagian bawah untuk menambahkan informasi ke file yang dipantau

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

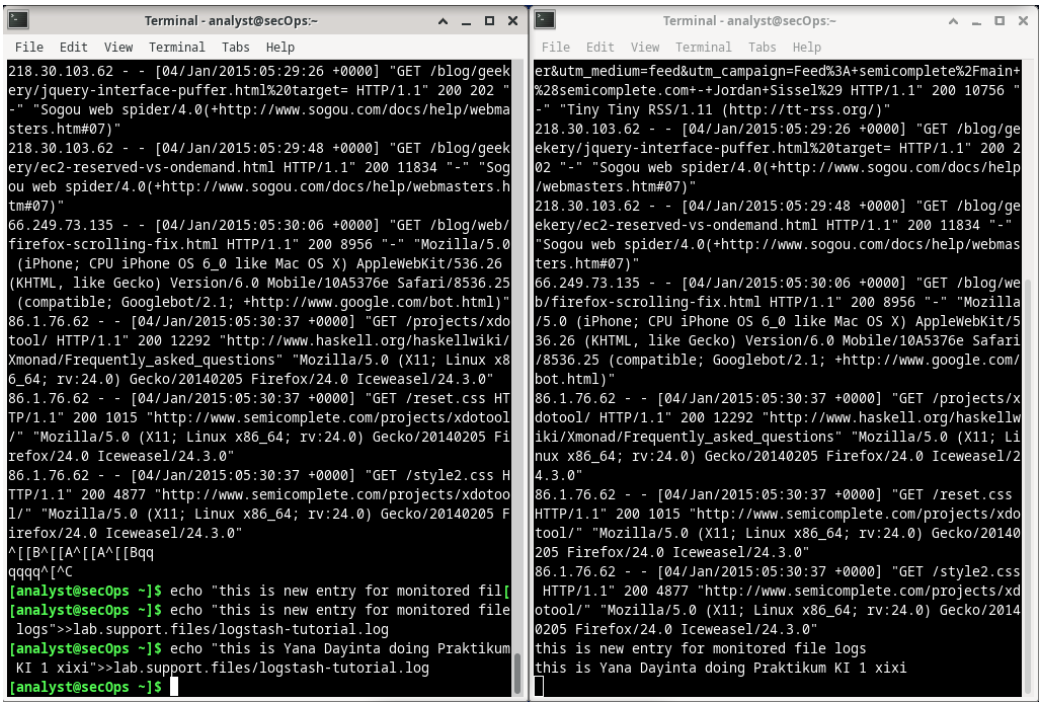
Pertanyaan: Apa yang berbeda dalam output tail dan tail -f? Jelaskan

```
[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 "-" "S
ogou 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 T
iny 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 Tin
y 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 (co
mpatible; 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/Xm
onad/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"
```

7. Pilihlah jendela terminal bawah dan masukkan perintah berikut:

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

   Saya juga menambahkan satu entry lain, yaitu “this is Yana Dayinta doing Praktikum KI 1 xixi”

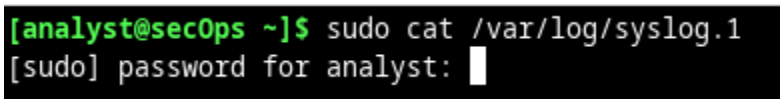


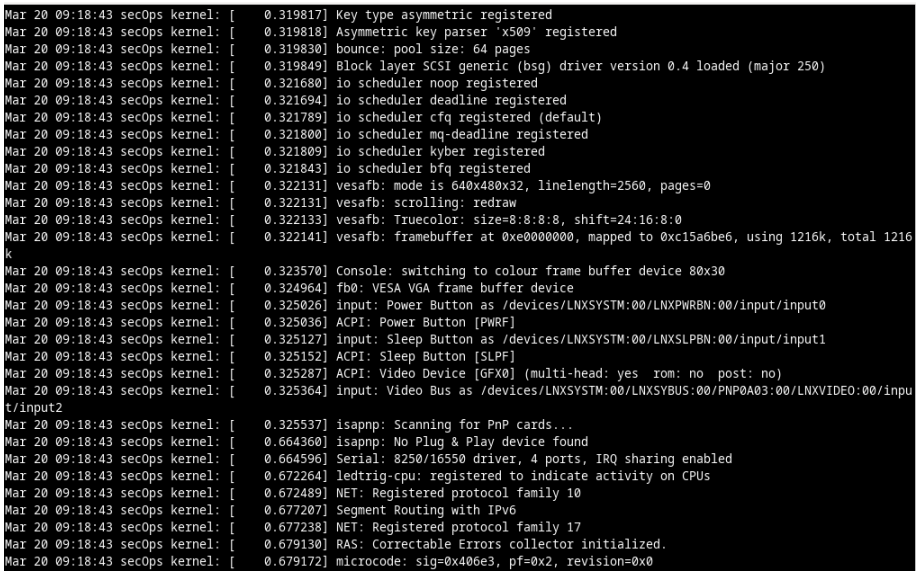
8. Memahami File Log dan Syslog, Gunakan perintah cat sebagai root untuk membuat daftar isi file /var/log/syslog.1. File ini menyimpan entri log yang dihasilkan oleh sistem operasi CyberOps Workstation VM dan dikirim ke layanan syslog.

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

   Pertanyaan:

   Mengapa perintah cat harus dijalankan sebagai root?





9. Gunakan perintah cat untuk membuat daftar file syslog yang lebih lama:

   analis@secOps ~$ sudo cat /var/log/syslog.2

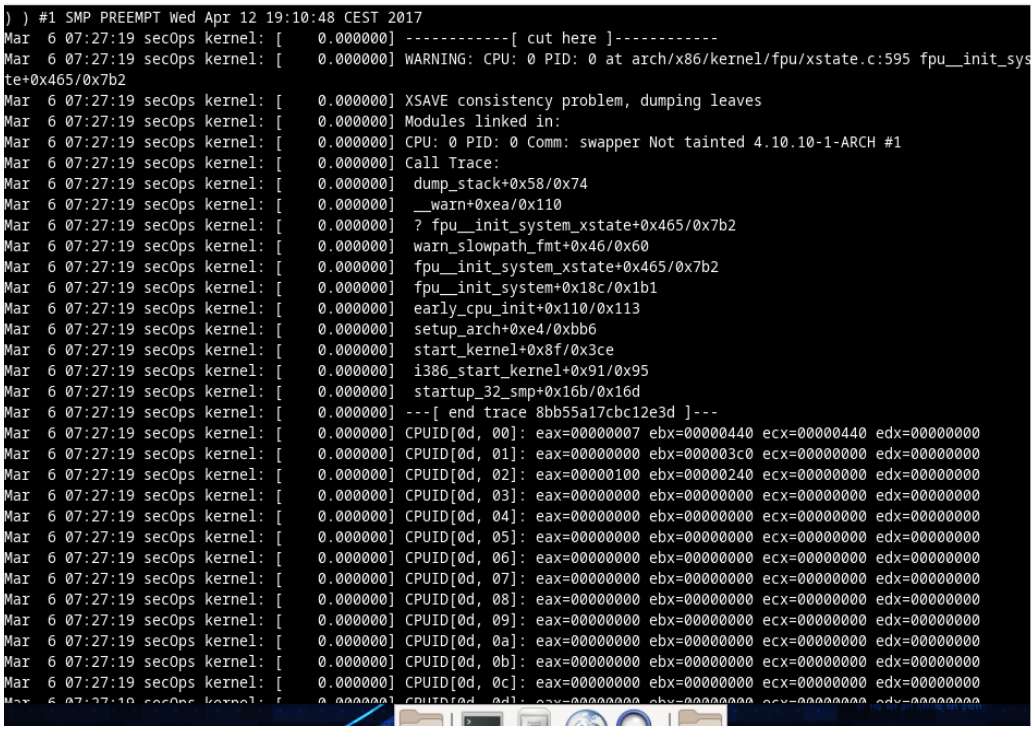
   analis@secOps ~$ sudo cat /var/log/syslog.3

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

   Pertanyaan:

   Jelaskan kenapa harus mensinkronkan waktu dan tanggal komputer dengan benar?

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



```
) ) #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_sys
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 8bb55a17cbc12e3d ]---
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 00]: eax=00000007 ebx=00000440 ecx=00000440 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 01]: eax=00000000 ebx=000003c0 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 02]: eax=00000100 ebx=00000240 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 03]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 04]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 05]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 06]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 07]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
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
```

```
[analyst@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
```

```
[analyst@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
```

```
[analyst@secOps ~]$ sudo cat /var/log/syslog.4
Aug 23 12:04:42 secOps kernel: [    8.047919] floppy0: no floppy controllers found
Aug 23 12:04:42 secOps kernel: [    8.047950] work still pending
Aug 23 13:49:32 secOps kernel: [ 6298.300707] pcnet32 0000:00:03.0 enp0s3: link down
Aug 23 13:49:36 secOps kernel: [ 6302.354139] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Aug 24 11:06:06 secOps kernel: [82892.804946] Bluetooth: Core ver 2.22
Aug 24 11:06:06 secOps kernel: [82892.805387] NET: Registered protocol family 31
Aug 24 11:06:06 secOps kernel: [82892.805388] Bluetooth: HCI device and connection manager initialized
Aug 24 11:06:06 secOps kernel: [82892.805390] Bluetooth: HCI socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.805392] Bluetooth: L2CAP socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.805396] Bluetooth: SCO socket layer initialized
Aug 24 11:06:06 secOps kernel: [82892.816995] Netfilter messages via NETLINK v0.30.
Aug 24 11:15:48 secOps kernel: [83475.322402] pcnet32 0000:00:03.0 enp0s3: link down
Aug 24 11:15:54 secOps kernel: [83481.238928] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Aug 24 08:09:23 secOps kernel: [    0.000000] Linux version 4.10.10-1-ARCH (builduser@tobias) (gcc version 6.3.1 20170306 (GCC
) ) #1 SMP PREEMPT Wed Apr 12 19:10:48 CEST 2017
Aug 24 08:09:23 secOps kernel: [    0.000000] ------------[ cut here ]------------
Aug 24 08:09:23 secOps kernel: [    0.000000] WARNING: CPU: 0 PID: 0 at arch/x86/kernel/fpu/xstate.c:595 fpu__init_system_xsta
te+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [    0.000000] XSAVE consistency problem, dumping leaves
Aug 24 08:09:23 secOps kernel: [    0.000000] Modules linked in:
Aug 24 08:09:23 secOps kernel: [    0.000000] CPU: 0 PID: 0 Comm: swapper Not tainted 4.10.10-1-ARCH #1
Aug 24 08:09:23 secOps kernel: [    0.000000] Call Trace:
Aug 24 08:09:23 secOps kernel: [    0.000000]  dump_stack+0x58/0x74
Aug 24 08:09:23 secOps kernel: [    0.000000]  __warn+0xea/0x110
Aug 24 08:09:23 secOps kernel: [    0.000000]  ? fpu__init_system_xstate+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [    0.000000]  warn_slowpath_fmt+0x46/0x60
Aug 24 08:09:23 secOps kernel: [    0.000000]  fpu__init_system_xstate+0x465/0x7b2
Aug 24 08:09:23 secOps kernel: [    0.000000]  fpu__init_system+0x18c/0x1b1
Aug 24 08:09:23 secOps kernel: [    0.000000]  early_cpu_init+0x110/0x113
Aug 24 08:09:23 secOps kernel: [    0.000000]  setup_arch+0xe4/0xbb6
Aug 24 08:09:23 secOps kernel: [    0.000000]  start_kernel+0x8f/0x3ce
Aug 24 08:09:23 secOps kernel: [    0.000000]  i386_start_kernel+0x91/0x95
Aug 24 08:09:23 secOps kernel: [    0.000000]  startup_32_smp+0x16b/0x16d
```

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

analyst@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 20:51:33 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).
```

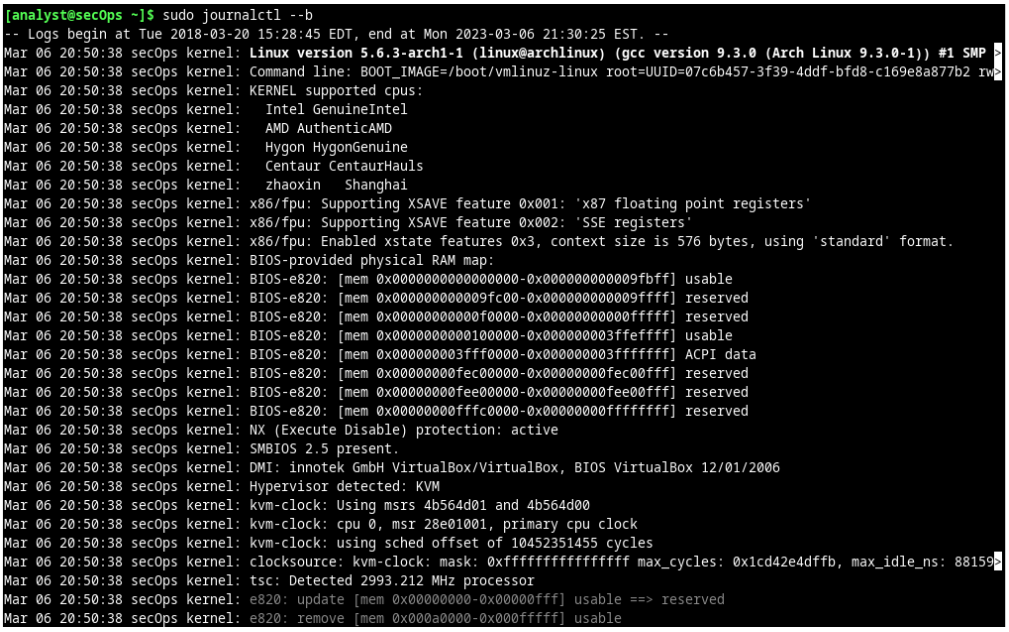
Kelebihan menggunakan journalctl terletak pada banyaknya pilihan. Gunakan journalctl --utc untuk menampilkan semua cap waktu dalam waktu UTC:

analyst@secOps ~$ sudo journalctl --utc

```
[analyst@secOps ~]$ sudo journalctl --utc
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Tue 2023-03-07 02:27:23 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 SM>
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 0x00000000000f0000-0x00000000000fffff] reserved
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x00000003ffefffff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000003fff0000-0x00000003ffffffff] 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 0x00000000fffc0000-0x00000000ffffffff] 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 0x00000000-0x00000fff] usable ==> reserved
Mar 20 19:28:45 secOps kernel: e820: remove [mem 0x000a0000-0x000fffff] 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
```

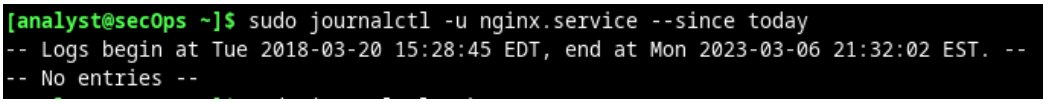
Gunakan journalctl -b untuk menampilkan entri log yang direkam selama boot terakhir:

analyst@secOps ~$ sudo journalctl –b



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

    analyst@secOps ~$ sudo journalctl -u nginx.service --since today



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

    analyst@secOps ~$ sudo journalctl –k

```
[analyst@secOps ~]$ sudo journalctl -k
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:32:29 EST. --
Mar 06 20:50:38 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 20:50:38 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw>
Mar 06 20:50:38 secOps kernel: KERNEL supported cpus:
Mar 06 20:50:38 secOps kernel:   Intel GenuineIntel
Mar 06 20:50:38 secOps kernel:   AMD AuthenticAMD
Mar 06 20:50:38 secOps kernel:   Hygon HygonGenuine
Mar 06 20:50:38 secOps kernel:   Centaur CentaurHauls
Mar 06 20:50:38 secOps kernel:   zhaoxin   Shanghai
Mar 06 20:50:38 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 20:50:38 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 20:50:38 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 20:50:38 secOps kernel: BIOS-provided physical RAM map:
Mar 06 20:50:38 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 06 20:50:38 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 06 20:50:38 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Mar 06 20:50:38 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usable
Mar 06 20:50:38 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACPI data
Mar 06 20:50:38 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 20:50:38 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 20:50:38 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 06 20:50:38 secOps kernel: NX (Execute Disable) protection: active
Mar 06 20:50:38 secOps kernel: SMBIOS 2.5 present.
Mar 06 20:50:38 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 20:50:38 secOps kernel: Hypervisor detected: KVM
Mar 06 20:50:38 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 20:50:38 secOps kernel: kvm-clock: cpu 0, msr 28e01001, primary cpu clock
Mar 06 20:50:38 secOps kernel: kvm-clock: using sched offset of 10452351455 cycles
Mar 06 20:50:38 secOps kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 88159>
Mar 06 20:50:38 secOps kernel: tsc: Detected 2993.212 MHz processor
Mar 06 20:50:38 secOps kernel: e820: update [mem 0x00000000-0x0000fff] usable ==> reserved
```

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

    analyst@secOps ~$ sudo journalctl –f

```
[analyst@secOps ~]$ sudo journalctl -f
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Mar 06 21:34:13 secOps kernel: audit: type=1106 audit(1678156453.440:131): pid=719 uid=0 auid=1000 ses=2 msg='op=PAM:session_c
lose grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success
'
Mar 06 21:34:13 secOps kernel: audit: type=1104 audit(1678156453.440:132): pid=719 uid=0 auid=1000 ses=2 msg='op=PAM:setcred g
rantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 21:34:19 secOps audit[728]: USER_ACCT pid=728 uid=1000 auid=1000 ses=2 msg='op=PAM:accounting grantors=pam_unix,pam_per
mit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 21:34:19 secOps sudo[728]:  analyst : TTY=pts/0 ; PWD=/home/analyst ; USER=root ; COMMAND=/usr/bin/journalctl -f
Mar 06 21:34:19 secOps audit[728]: CRED_REFR pid=728 uid=0 auid=1000 ses=2 msg='op=PAM:setcred grantors=pam_unix,pam_permit,pa
m_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 21:34:19 secOps sudo[728]: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 06 21:34:19 secOps audit[728]: USER_START pid=728 uid=0 auid=1000 ses=2 msg='op=PAM:session_open grantors=pam_limits,pam_u
nix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 21:34:19 secOps kernel: audit: type=1101 audit(1678156459.763:133): pid=728 uid=1000 auid=1000 ses=2 msg='op=PAM:accoun
ting grantors=pam_unix,pam_permit,pam_time acct="analyst" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succes
s'
Mar 06 21:34:19 secOps kernel: audit: type=1110 audit(1678156459.763:134): pid=728 uid=0 auid=1000 ses=2 msg='op=PAM:setcred g
rantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
Mar 06 21:34:19 secOps kernel: audit: type=1105 audit(1678156459.763:135): pid=728 uid=0 auid=1000 ses=2 msg='op=PAM:session_o
pen grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
```

PEMBAHASAN:

1. Apa kelemahan menggunakan cat dengan file teks besar?
   Perintah "cat" untuk Data Besar akan menampilkan seluruh isi file ke terminal secara terus-menerus hingga proses selesai, kecuali jika dihentikan dengan CTRL+C. Jika ukuran file sangat besar, maka proses ini mungkin memakan waktu yang lama dan mengunci terminal dalam proses tersebut.
2. Apa kelemahan menggunakan more?

"More" memungkinkan kita untuk melihatnya sebagai satu file yang dipisahkan oleh garis. Kekurangan dari more adalah tidak bisa menampilkan teks di halaman layar sebelumnya.

3. Apa yang berbeda dalam output tail dan tail -f? Jelaskan
   Tail mendefinisikan sebuah data pada file menurut barisnya.Tail secara default ditampilkan 10 baris terakhir dari isi file. Tail -f untuk memantau file untuk perubahan. Opsi ini sangat berguna untuk memonitor file log. Misalnya, untuk menampilkan 10 baris terakhir file dan pantau file untuk pembaruan yang akan digunakan
4. Mengapa perintah cat harus dijalankan sebagai root?
   Karena, perintah cat (akronim dari concatenate) berfungsi untuk membuat daftar konten atau isi file pada standard output (sdout) dan karena diawali dengan sudo, dimana sudo adalah root yang berarti awalan dari sistem file Linux.
5. Jelaskan kenapa harus mensinkronkan waktu dan tanggal komputer dengan benar?
   Dengan waktu yang tersinkronisasi untuk semua komputer maka akan terjamin keakuratan dan konsistensi dari data date-time dari file, data base dan sistem yang menggunakan aplikasi jaringan yang melibatkan penjadwalan proses dan komunikasi data secara Time Division Multiple Access (TDMA).

   Penjelasan singkat dari perintah yang ada akan dijabarkan pada tabel dibawah ini:

Perintah	Fungsi
cat	Digunakan untuk melihat logs secara utuh
tail	Digunakan untuk menampilkan 10 baris logs terakhir
tail -f	Dapat digunakan untuk membaca logs paling baru (paling bawah di file log)
more	untuk menampilkan logs lebih banyak
less	mampuannya melihat halaman di layar sebelumnya dan melihat layar sesudahnya.
sudo	digunakan jika suatu operasi membutuhkan hak akses root untuk digunakan, atau jika akses administratif membutuhkan akses.
Tool journalctl	menafsirkan dan menampilkan entri log yang sebelumnya disimpan dalam file log biner jurnal
journalctl --utc	untuk menampilkan semua cap waktu dalam waktu UTC

journalctl -b	untuk menampilkan entri log yang direkam selama boot terakhir
journalctl -u nginx.service	untuk menentukan layanan dan kerangka waktu untuk entri log
journalctl -k	untuk hanya menampilkan pesan yang dihasilkan oleh kernel
journalctl -f	untuk secara aktif mengikuti log saat sedang ditulis

E. KESIMPULAN

- File log merupakan file yang dihasilkan oleh software yang berisi informasi mengenai operasi, aktivitas, dan pola penggunaan sistem IT, server, atau aplikasi.
- Log server sendiri merupakan sebuah file log yang dibuat secara otomatis dan dijaga oleh server

F. DAFTAR PUSTAKA

Amazon Web Service. (n.d.). *What are Log Files? - Log Files Explained - AWS*. Amazon AWS. Diakses pada Maret 11, 2023, dari https://aws.amazon.com/id/what-is/log-files/

Dewaweb Team. (2023, Februari 16). *18 Perintah Dasar Linux yang Wajib Kamu Ketahui*. Dewaweb. Diakses pada Maret 11, 2023, dari https://www.dewaweb.com/blog/perintah-dasar-linux/#4_cat

Iswanto. (2019, Mei). PENTINGNYA SINKRONISASI WAKTU PADA JARINGAN KOMPUTER. *Jurnal Teknologi Informasi dan Komunikasi*, *Volume IX, No. 1*, 5.

Jawaban Cepat Apa Kelemahan Menggunakan Lebih Banyak Di Linux – Belajarbacaandoa.com. (2023, Februari 12). Belajarbacaandoa.com. Diakses pada Maret 11, 2023, dari https://belajarbacaandoa.com/jawaban-cepat-apa-kelemahan-menggunakan-lebih-banyak-di-linux.html

Latief, A. (2020, October 14). *Cara membaca logs pada linux server debian / ubuntu server – Materi Pembelajaran Online*. Materi Pembelajaran Online. Diakses pada Maret 11, 2023, dari http://materi.smkn43jkt.sch.id/?p=3513

Memahami Perintah Tail Pada Linux Terminal. (n.d.). LinuxID. Diakses pada Maret 11, 2023, dari https://www.linuxid.net/24803/memahami-perintah-tail-pada-linux-terminal/

Putra, C. A. (2012, Desember 19). *Perintah Menampilkan file teks di Linux – CandraLab Studio*. CandraLab Studio. Diakses pada Maret 11, 2023, dari https://www.candra.web.id/perintah-menampilkan-file-teks-di-linux/