LAPORAN PRATIKUM

KEAMANAN INFORMASI 2

Disusun Oleh :

NAMA : Riva Mahyuli

NIM :21/478709/SV/19365

KELAS :R1AA

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNOLOGI DAN INFORMATIKA
UNIVERSITAS GADJAH MADA
2022/2023

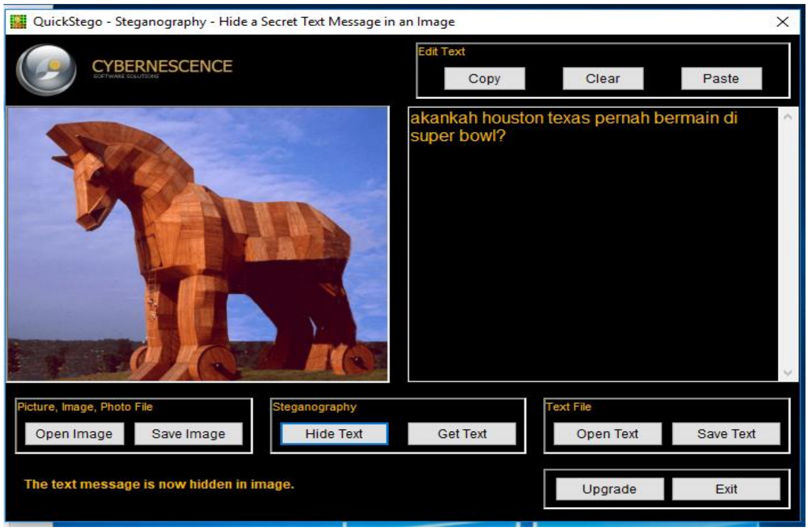
Tugas 1 STEGANOGRAFI

Alat dan bahan yang dibutuhkan:

1. Software QuickStego ,dowload file http://quickcrypto.com/free-steganography-software.html
2. Software MD5SUMS, dowload file http://www.pc-tools.net/win32/md5sums/
3. 2 buah gambar berformat jpg
4. Command prompt

Langkah Kerja

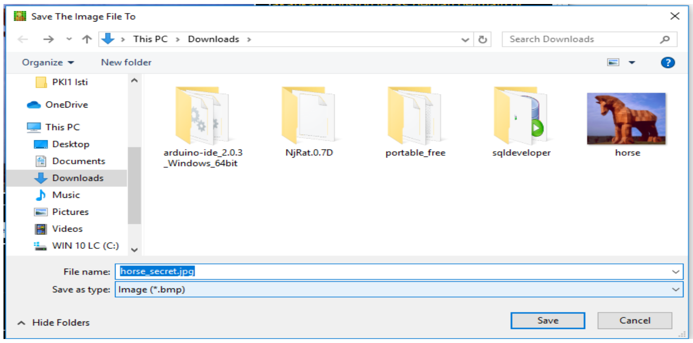
1. Buka software QuickStego dan masukan gambar yang ingin disembunyikan sebuah pesan.



akankah houston texas pernah bermain di super bowl?

The text message is now hidden in image.

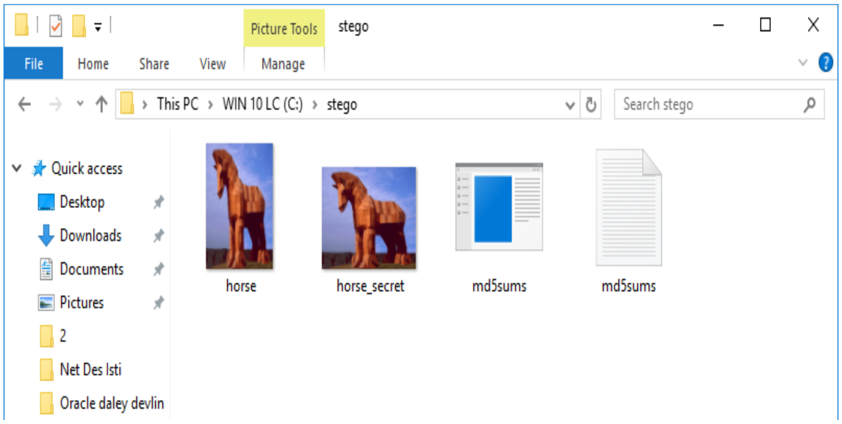
2. Simpan gambar yang telah disembunyikan sebuah pesan



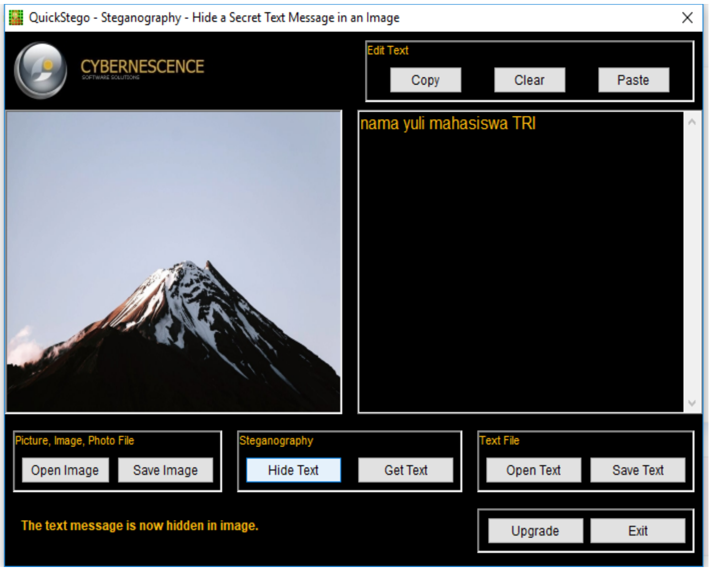
File name: horse_secret.jpg

Save as type: Image (*.bmp)

3. Jadikan gambar yang telah disembunyikan pesan, yang belum ,software MD5sum, dan ektraksnya dalam satu file.

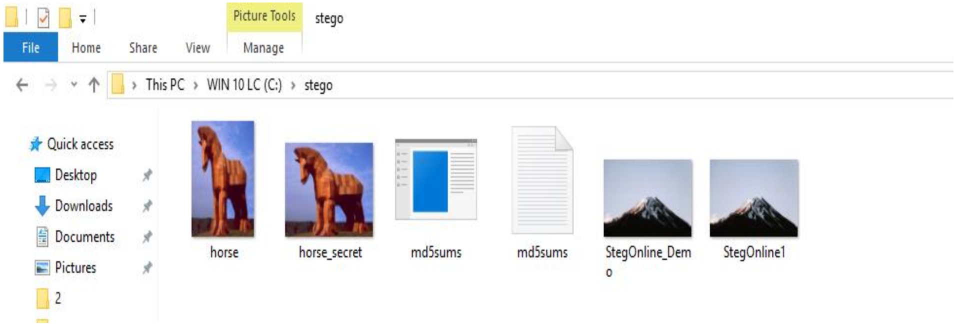


4. Ulangi setiap langkah untuk gambar 2.



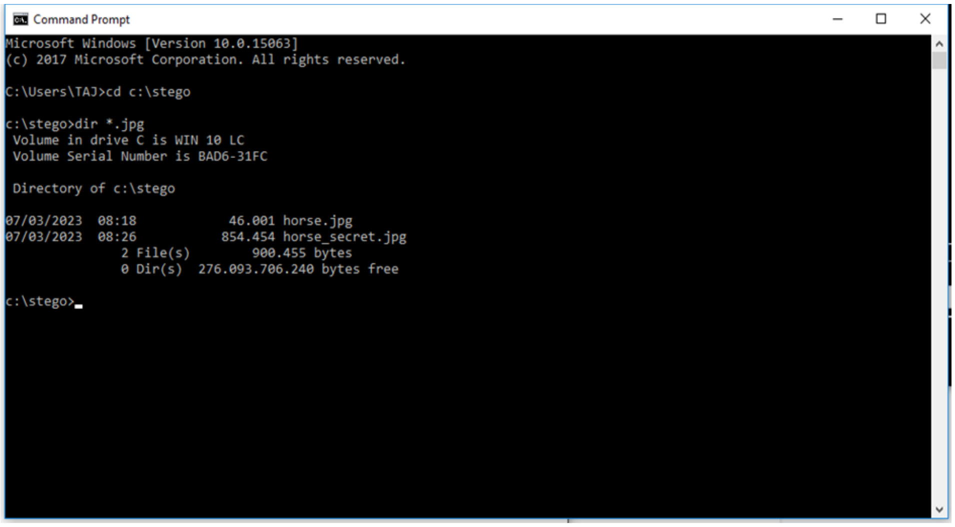
nama yuli mahasiswa TRI

The text message is now hidden in image.

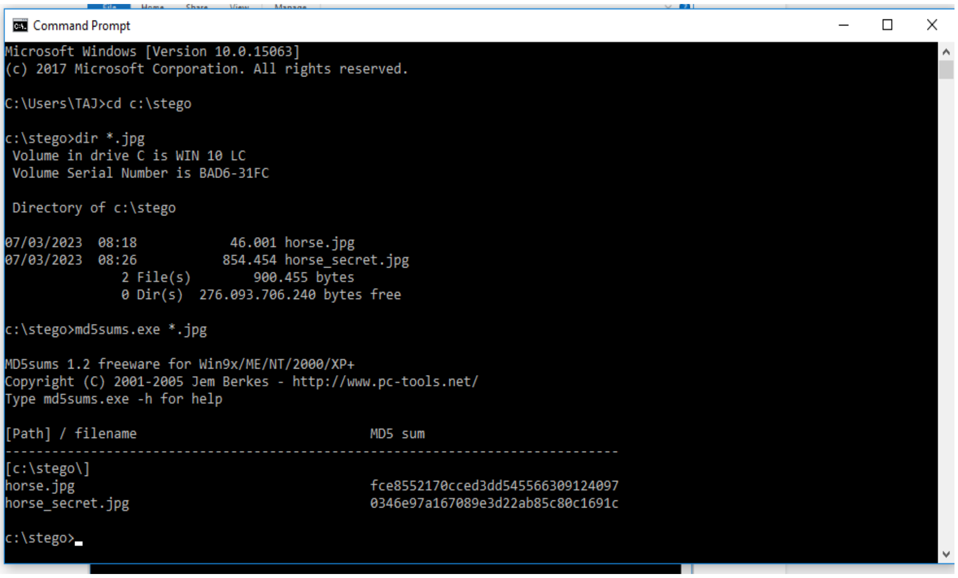


Hasil Pratikum

Gambar 1

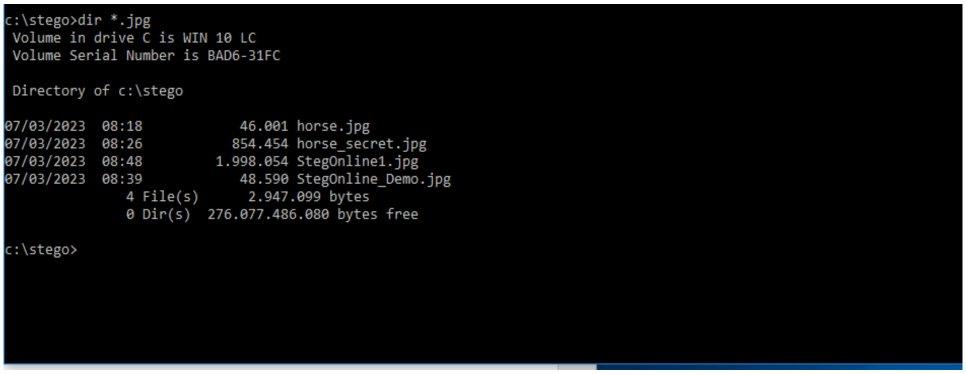


```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\TAJ>cd c:\stego

c:\stego>dir *.jpg
 Volume in drive C is WIN 10 LC
 Volume Serial Number is BAD6-31FC

 Directory of c:\stego

07/03/2023  08:18            46.001 horse.jpg
07/03/2023  08:26           854.454 horse_secret.jpg
               2 File(s)        900.455 bytes
               0 Dir(s)  276.093.706.240 bytes free

c:\stego>
```

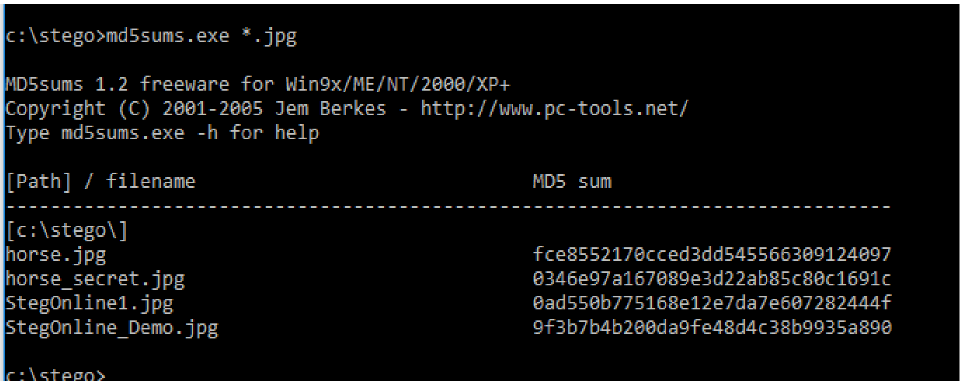


```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\TAJ>cd c:\stego

c:\stego>dir *.jpg
 Volume in drive C is WIN 10 LC
 Volume Serial Number is BAD6-31FC

 Directory of c:\stego

07/03/2023  08:18            46.001 horse.jpg
07/03/2023  08:26           854.454 horse_secret.jpg
               2 File(s)        900.455 bytes
               0 Dir(s)  276.093.706.240 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\]
horse.jpg                                      fce8552170cced3dd545566309124097
horse_secret.jpg                               0346e97a167089e3d22ab85c80c1691c

c:\stego>
```

Gambar 2



```
c:\stego>dir *.jpg
 Volume in drive C is WIN 10 LC
 Volume Serial Number is BAD6-31FC

 Directory of c:\stego

07/03/2023  08:18            46.001 horse.jpg
07/03/2023  08:26           854.454 horse_secret.jpg
07/03/2023  08:48         1.998.054 StegOnline1.jpg
07/03/2023  08:39            48.590 StegOnline_Demo.jpg
               4 File(s)      2.947.099 bytes
               0 Dir(s)  276.077.486.080 bytes free

c:\stego>
```



```
c:\stego>md5sums.exe *.jpg

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

[Path] / filename                           MD5 sum
---------------------------------------------------------------------------
[c:\stego\]
horse.jpg                                   fce8552170cced3dd545566309124097
horse_secret.jpg                            0346e97a167089e3d22ab85c80c1691c
StegOnline1.jpg                             0ad550b775168e12e7da7e607282444f
StegOnline_Demo.jpg                         9f3b7b4b200da9fe48d4c38b9935a890

c:\stego>
```

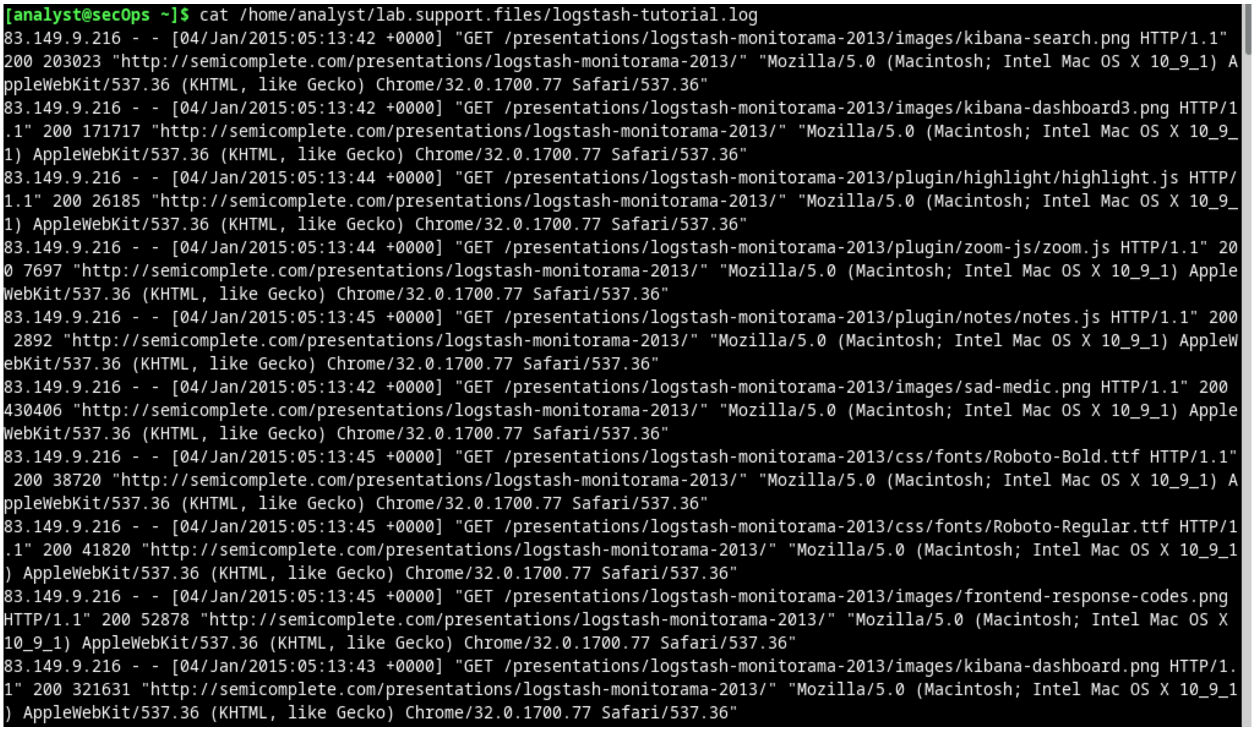
2. TUGAS 2 ANALISIS LOG SERVER

Alat dan bahan yang dibutuhkan :

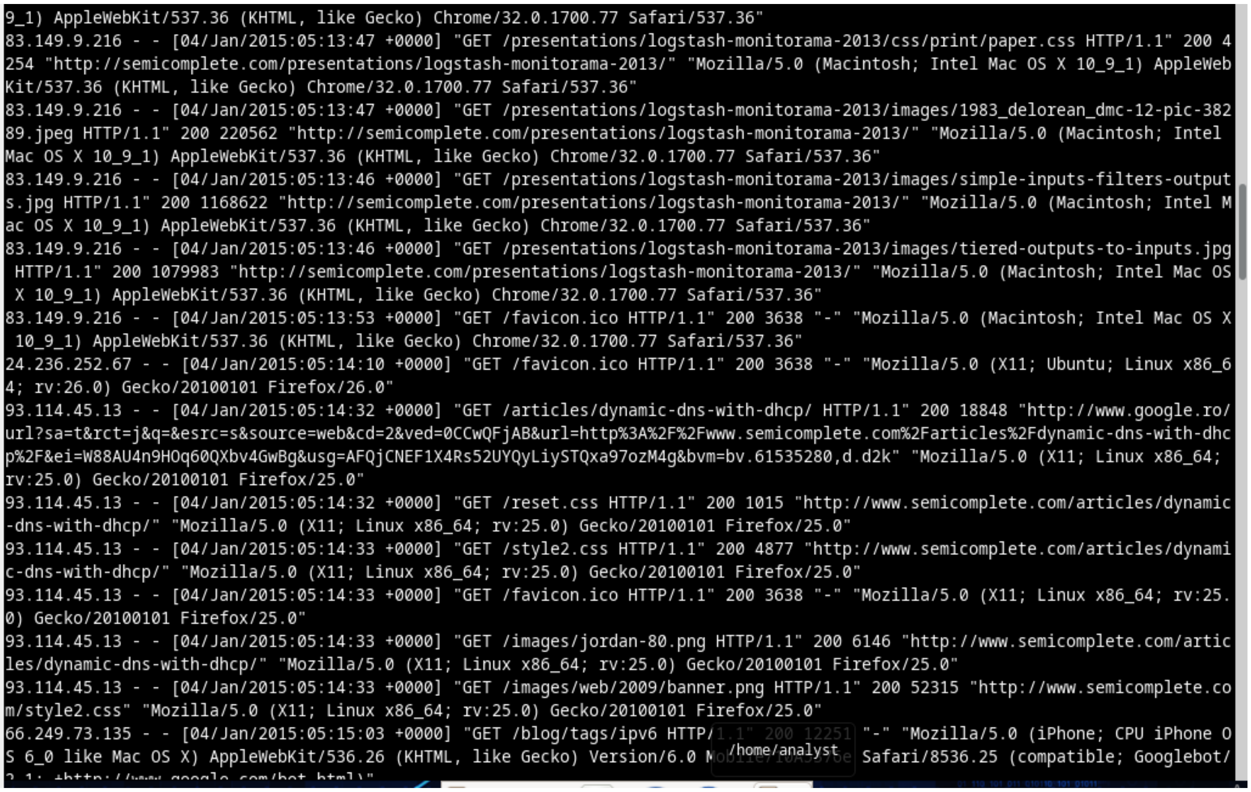
-CyberOps Workstation virtual machine

Hasil Pratikum

1. Membaca File Log dengan Cat, More, Less, dan Tail
2. Perintah di bawah ini untuk menampilkan konten filelogstash-tutorial.log, yang terletak di folder /home/analyst/lab.support.files/:

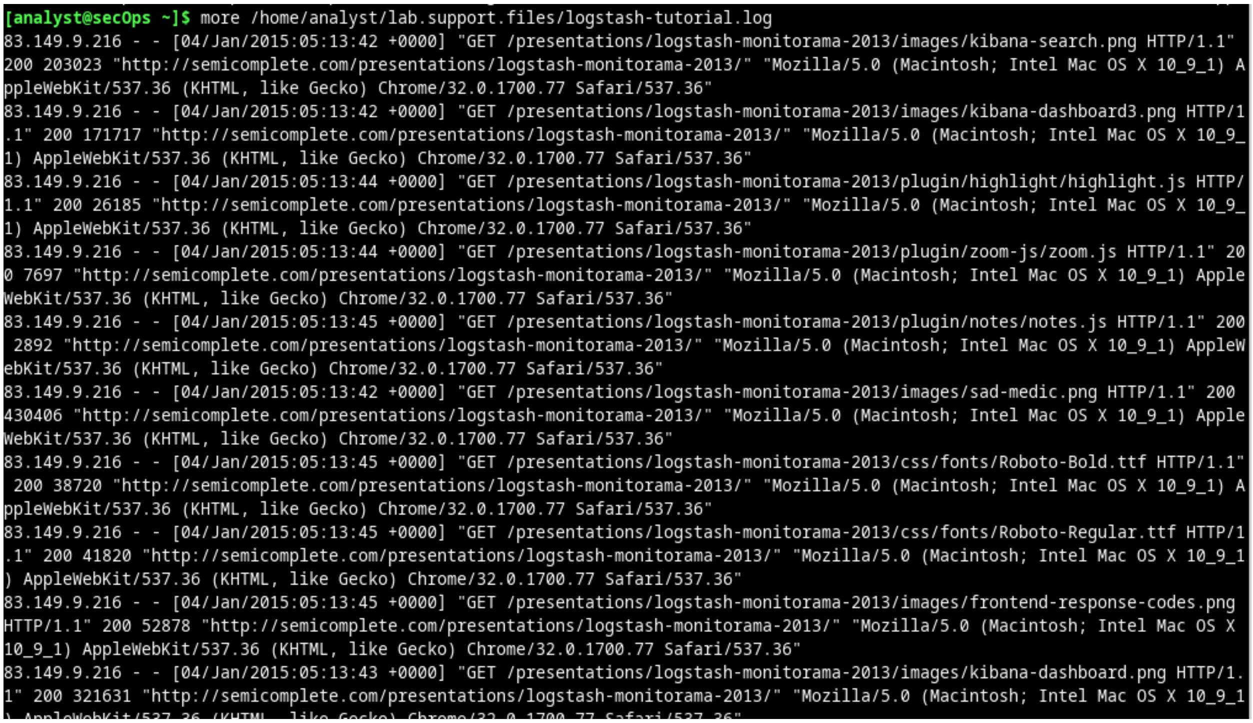


```
[analyst@secOps ~]$ cat /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1"
200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; 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"
```

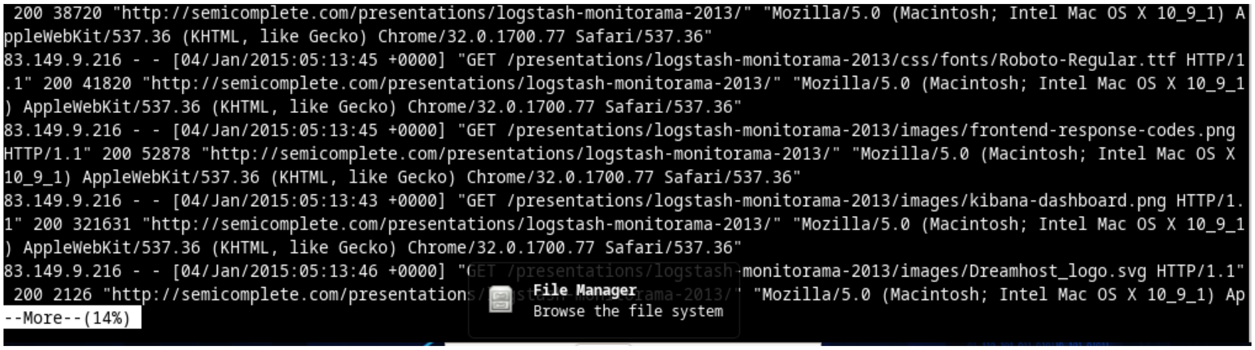


```
9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/css/print/paper.css HTTP/1.1" 200 4
254 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWeb
Kit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:47 +0000] "GET /presentations/logstash-monitorama-2013/images/1983_delorean_dmc-12-pic-382
89.jpeg HTTP/1.1" 200 220562 "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/simple-inputs-filters-output
s.jpg HTTP/1.1" 200 1168622 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel M
ac 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/tiered-outputs-to-inputs.jpg
 HTTP/1.1" 200 1079983 "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/2015:05:13:53 +0000] "GET /favicon.ico HTTP/1.1" 200 3638 "-" "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"
24.236.252.67 - - [04/Jan/2015:05:14:10 +0000] "GET /favicon.ico HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_6
4; rv:26.0) Gecko/20100101 Firefox/26.0"
93.114.45.13 - - [04/Jan/2015:05:14:32 +0000] "GET /articles/dynamic-dns-with-dhcp/ HTTP/1.1" 200 18848 "http://www.google.ro/
url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCwQFjAB&url=http%3A%2F%2Fwww.semicomplete.com%2Farticles%2Fdynamic-dns-with-dhc
p%2F&ei=W88AU4n9HOq60QXbv4GwBg&usg=AFQjCNEF1X4Rs52UYQyLiySTQxa97ozM4g&bvm=bv.61535280,d.d2k" "Mozilla/5.0 (X11; Linux x86_64;
rv:25.0) Gecko/20100101 Firefox/25.0"
93.114.45.13 - - [04/Jan/2015:05:14:32 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/articles/dynamic
-dns-with-dhcp/" "Mozilla/5.0 (X11; Linux x86_64; rv:25.0) Gecko/20100101 Firefox/25.0"
93.114.45.13 - - [04/Jan/2015:05:14:33 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/articles/dynami
c-dns-with-dhcp/" "Mozilla/5.0 (X11; Linux x86_64; rv:25.0) Gecko/20100101 Firefox/25.0"
93.114.45.13 - - [04/Jan/2015:05:14:33 +0000] "GET /favicon.ico HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:25.
0) Gecko/20100101 Firefox/25.0"
93.114.45.13 - - [04/Jan/2015:05:14:33 +0000] "GET /images/jordan-80.png HTTP/1.1" 200 6146 "http://www.semicomplete.com/artic
les/dynamic-dns-with-dhcp/" "Mozilla/5.0 (X11; Linux x86_64; rv:25.0) Gecko/20100101 Firefox/25.0"
93.114.45.13 - - [04/Jan/2015:05:14:33 +0000] "GET /images/web/2009/banner.png HTTP/1.1" 200 52315 "http://www.semicomplete.co
m/style2.css" "Mozilla/5.0 (X11; Linux x86_64; rv:25.0) Gecko/20100101 Firefox/25.0"
66.249.73.135 - - [04/Jan/2015:05:15:03 +0000] "GET /blog/tags/ipv6 HTTP/1.1" 200 12251 "-" "Mozilla/5.0 (iPhone; CPU iPhone O
S 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)"
```

3. Perintah di bawah ini untuk menampilkan kembali isi file logstash-tutorial.log. Proses ini menggunakan more

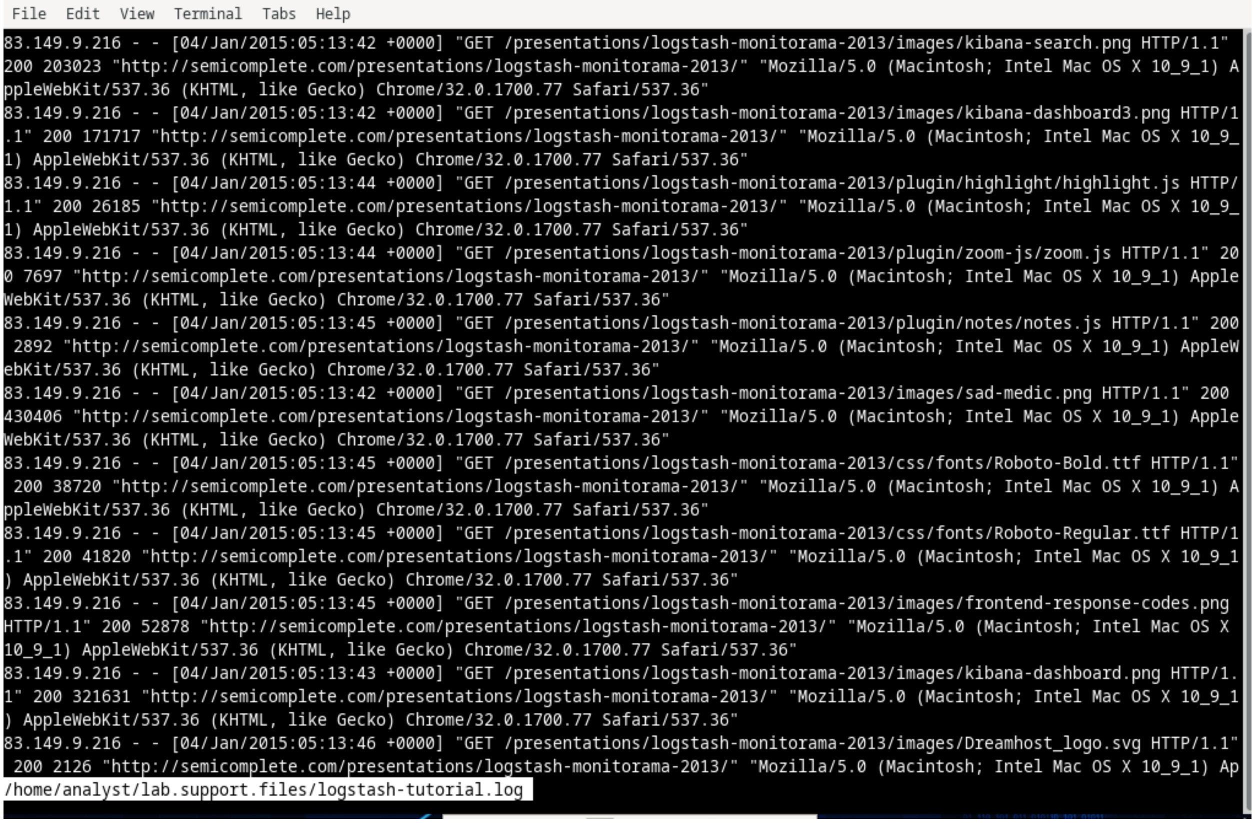


```
[analyst@secOps ~]$ more /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1"
200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) 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"
```

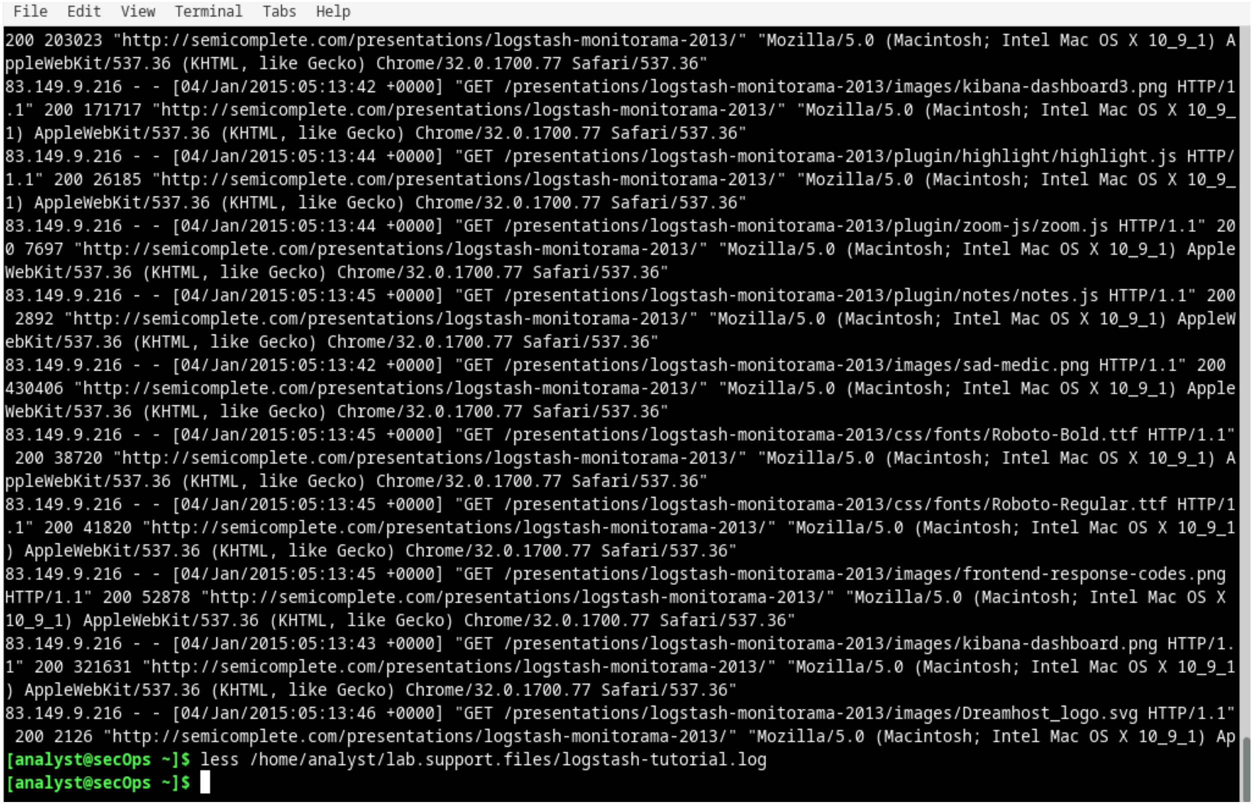


```
 200 38720 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf 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
--More--(14%)
```

4. Menggunakan less untuk menampilkan konten file logstash-tutorial.log lagi:

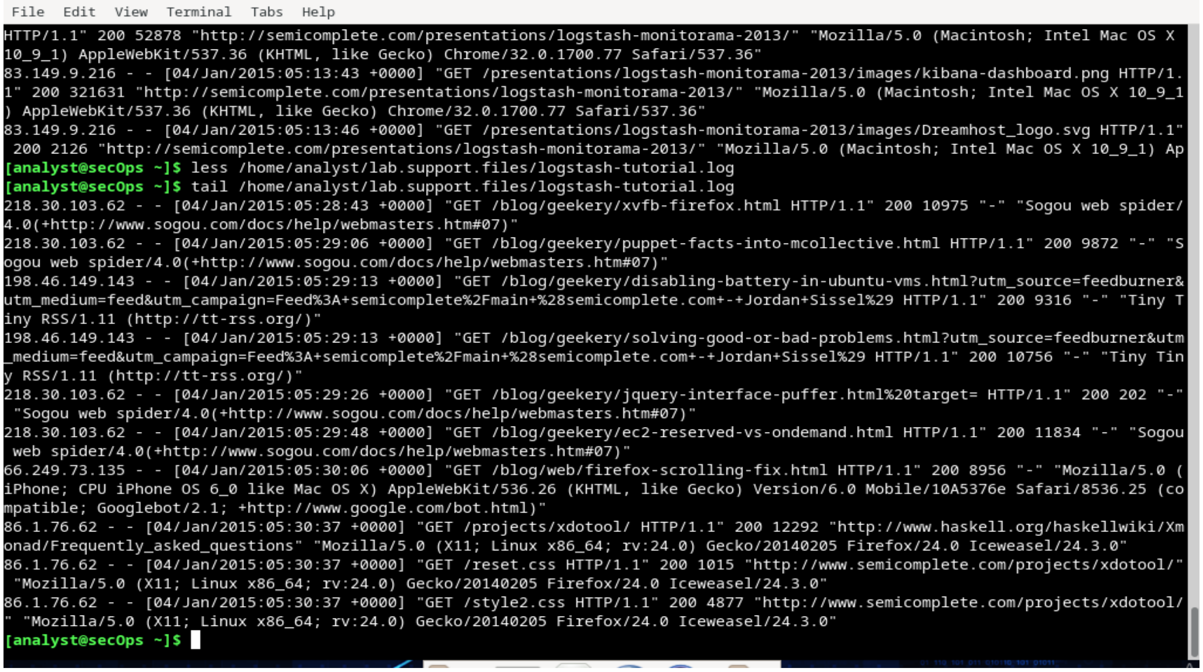


```
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1"
200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 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
```



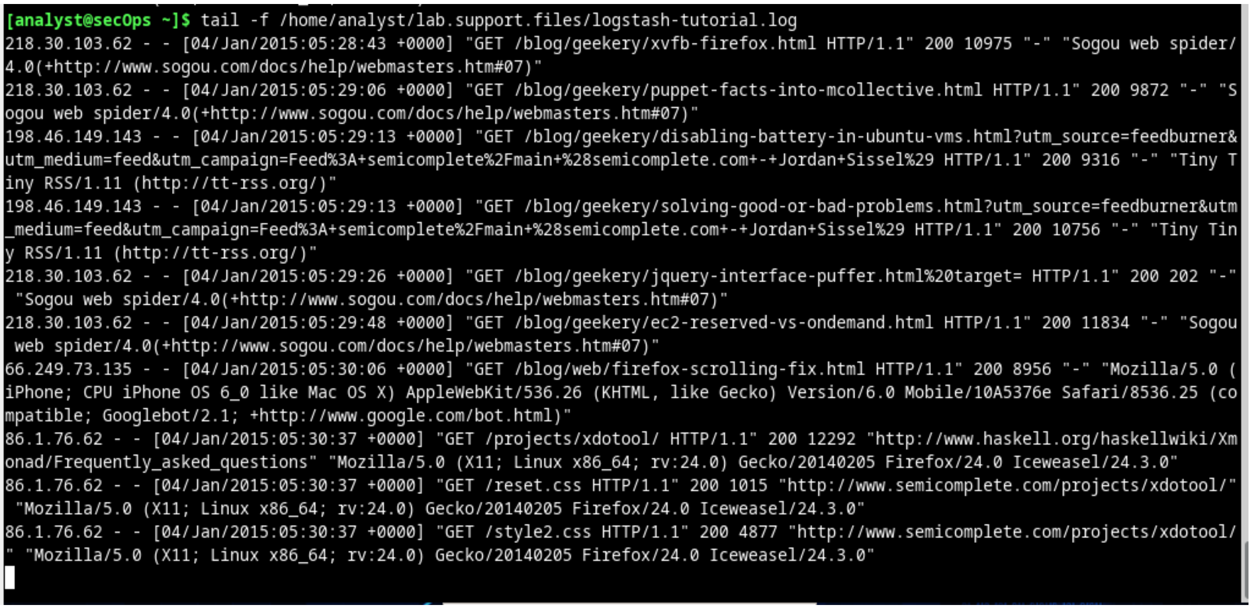
```
200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) A
ppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard3.png 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
[analyst@secOps ~]$ less /home/analyst/lab.support.files/logstash-tutorial.log
[analyst@secOps ~]$ 
```

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



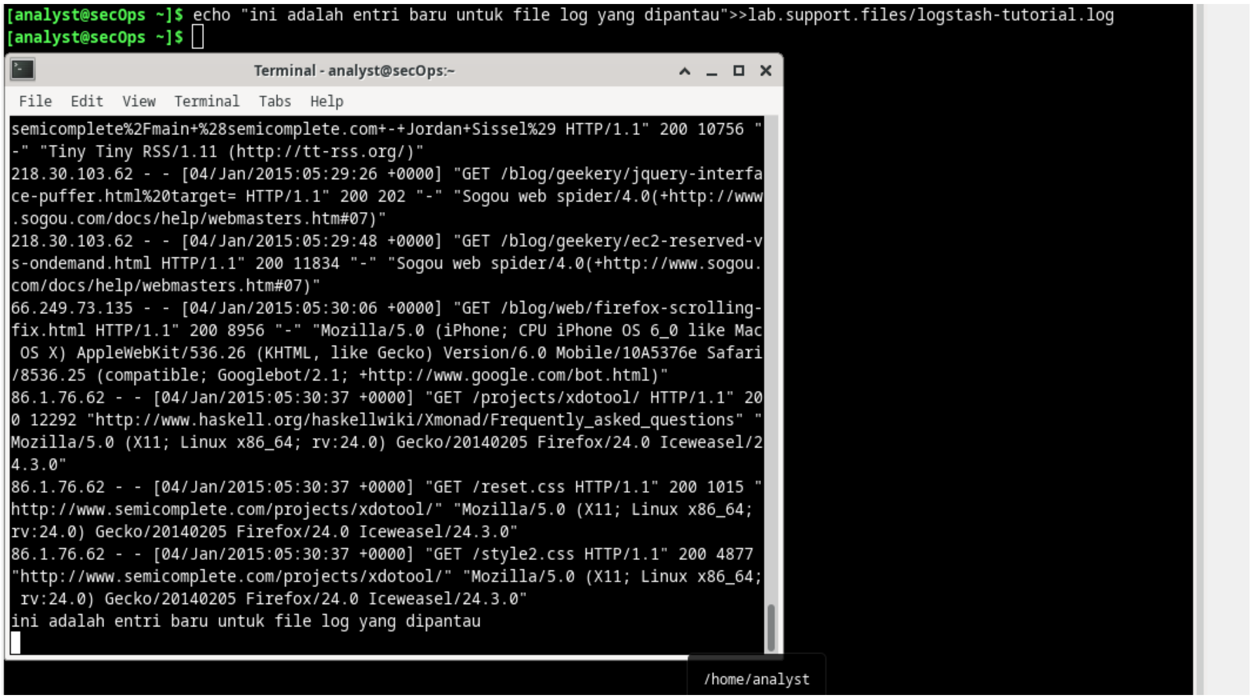
```
HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X
10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard.png 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
[analyst@secOps ~]$ less /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"
[analyst@secOps ~]$ 
```

6. Pada jendela terminal tersebut, jalankanlah tail -f Menggunakan tail-f



```
[analyst@secOps ~]$ tail -f /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/
4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 9872 "-" "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. Perintah echo 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.

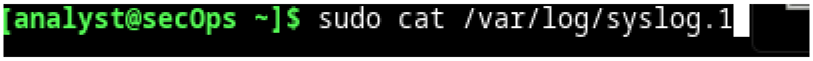


```
[analyst@secOps ~]$ echo "ini adalah entri baru untuk file log yang dipantau">>lab.support.files/logstash-tutorial.log
[analyst@secOps ~]$
```

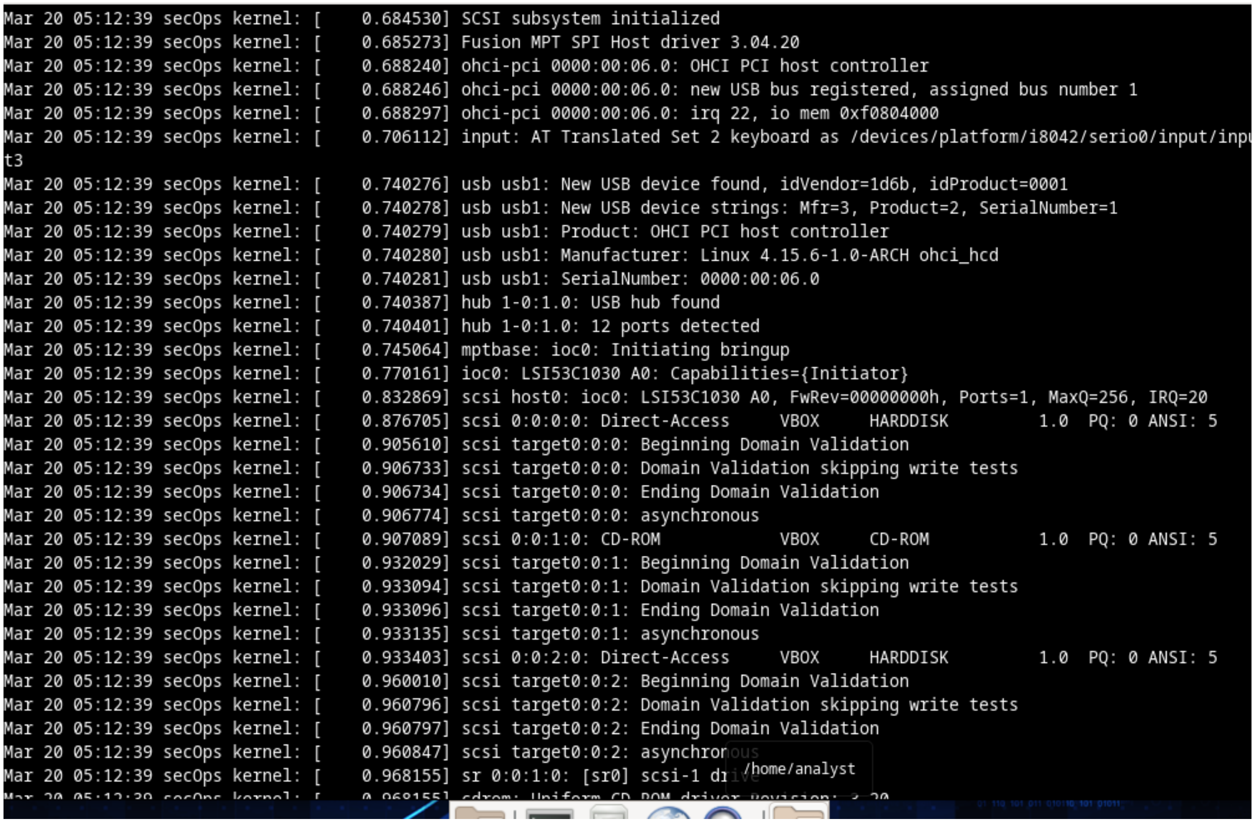
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
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-interfa
ce-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-v
s-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" 20
0 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/2
4.3.0"
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
```

8. Memahami file log dan syslog

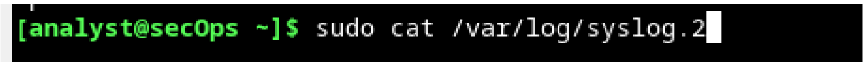


```
[analyst@secOps ~]$ sudo cat /var/log/syslog.1
```

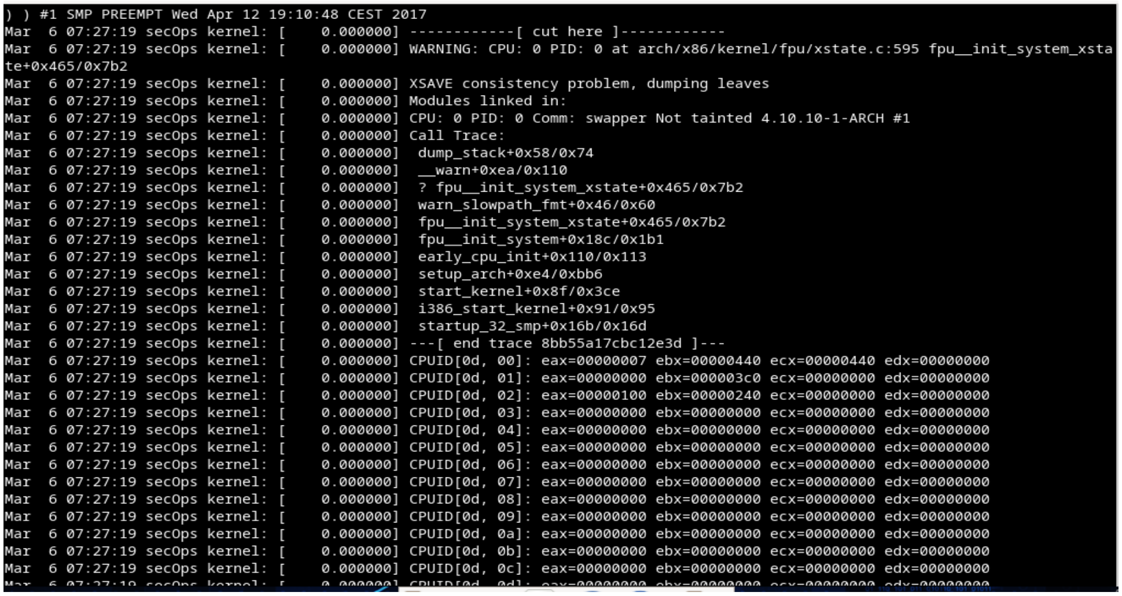


```
Mar 20 05:12:39 secOps kernel: [    0.684530] SCSI subsystem initialized
Mar 20 05:12:39 secOps kernel: [    0.685273] Fusion MPT SPI Host driver 3.04.20
Mar 20 05:12:39 secOps kernel: [    0.688240] ohci-pci 0000:00:06.0: OHCI PCI host controller
Mar 20 05:12:39 secOps kernel: [    0.688246] ohci-pci 0000:00:06.0: new USB bus registered, assigned bus number 1
Mar 20 05:12:39 secOps kernel: [    0.688297] ohci-pci 0000:00:06.0: irq 22, io mem 0xf0804000
Mar 20 05:12:39 secOps kernel: [    0.706112] input: AT Translated Set 2 keyboard as /devices/platform/i8042/serio0/input/inpu
t3
Mar 20 05:12:39 secOps kernel: [    0.740276] usb usb1: New USB device found, idVendor=1d6b, idProduct=0001
Mar 20 05:12:39 secOps kernel: [    0.740278] usb usb1: New USB device strings: Mfr=3, Product=2, SerialNumber=1
Mar 20 05:12:39 secOps kernel: [    0.740279] usb usb1: Product: OHCI PCI host controller
Mar 20 05:12:39 secOps kernel: [    0.740280] usb usb1: Manufacturer: Linux 4.15.6-1.0-ARCH ohci_hcd
Mar 20 05:12:39 secOps kernel: [    0.740281] usb usb1: SerialNumber: 0000:00:06.0
Mar 20 05:12:39 secOps kernel: [    0.740387] hub 1-0:1.0: USB hub found
Mar 20 05:12:39 secOps kernel: [    0.740401] hub 1-0:1.0: 12 ports detected
Mar 20 05:12:39 secOps kernel: [    0.745064] mptbase: ioc0: Initiating bringup
Mar 20 05:12:39 secOps kernel: [    0.770161] ioc0: LSI53C1030 A0: Capabilities={Initiator}
Mar 20 05:12:39 secOps kernel: [    0.832869] scsi host0: ioc0: LSI53C1030 A0, FwRev=00000000h, Ports=1, MaxQ=256, IRQ=20
Mar 20 05:12:39 secOps kernel: [    0.876705] scsi 0:0:0:0: Direct-Access     VBOX     HARDDISK         1.0  PQ: 0 ANSI: 5
Mar 20 05:12:39 secOps kernel: [    0.905610] scsi target0:0:0: Beginning Domain Validation
Mar 20 05:12:39 secOps kernel: [    0.906733] scsi target0:0:0: Domain Validation skipping write tests
Mar 20 05:12:39 secOps kernel: [    0.906734] scsi target0:0:0: Ending Domain Validation
Mar 20 05:12:39 secOps kernel: [    0.906774] scsi target0:0:0: asynchronous
Mar 20 05:12:39 secOps kernel: [    0.907089] scsi 0:0:1:0: CD-ROM            VBOX     CD-ROM           1.0  PQ: 0 ANSI: 5
Mar 20 05:12:39 secOps kernel: [    0.932029] scsi target0:0:1: Beginning Domain Validation
Mar 20 05:12:39 secOps kernel: [    0.933094] scsi target0:0:1: Domain Validation skipping write tests
Mar 20 05:12:39 secOps kernel: [    0.933096] scsi target0:0:1: Ending Domain Validation
Mar 20 05:12:39 secOps kernel: [    0.933135] scsi target0:0:1: asynchronous
Mar 20 05:12:39 secOps kernel: [    0.933403] scsi 0:0:2:0: Direct-Access     VBOX     HARDDISK         1.0  PQ: 0 ANSI: 5
Mar 20 05:12:39 secOps kernel: [    0.960010] scsi target0:0:2: Beginning Domain Validation
Mar 20 05:12:39 secOps kernel: [    0.960796] scsi target0:0:2: Domain Validation skipping write tests
Mar 20 05:12:39 secOps kernel: [    0.960797] scsi target0:0:2: Ending Domain Validation
Mar 20 05:12:39 secOps kernel: [    0.960847] scsi target0:0:2: asynchronous
Mar 20 05:12:39 secOps kernel: [    0.968155] sr 0:0:1:0: [sr0] scsi-1 drive
Mar 20 05:12:39 secOps kernel: [    0.968155] cdrom: Uniform CD-ROM driver Revision: 3.20
```

9. Perhatikan bahwa file /var/log/syslog hanya menyimpan entri log terbaru

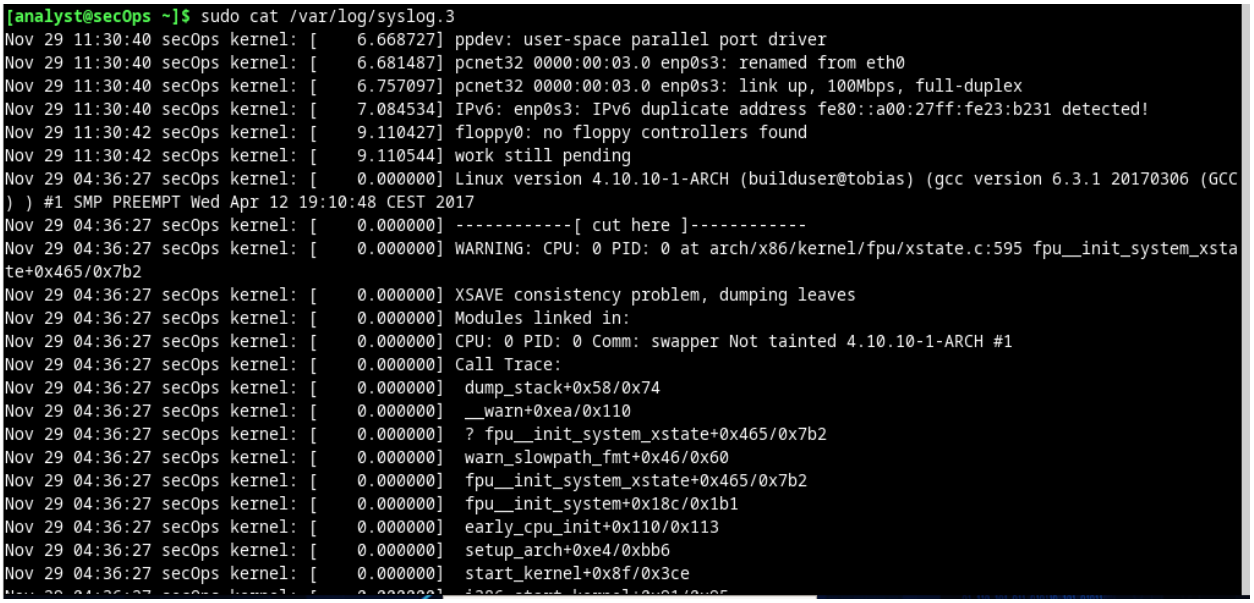


```
[analyst@secOps ~]$ sudo cat /var/log/syslog.2
```



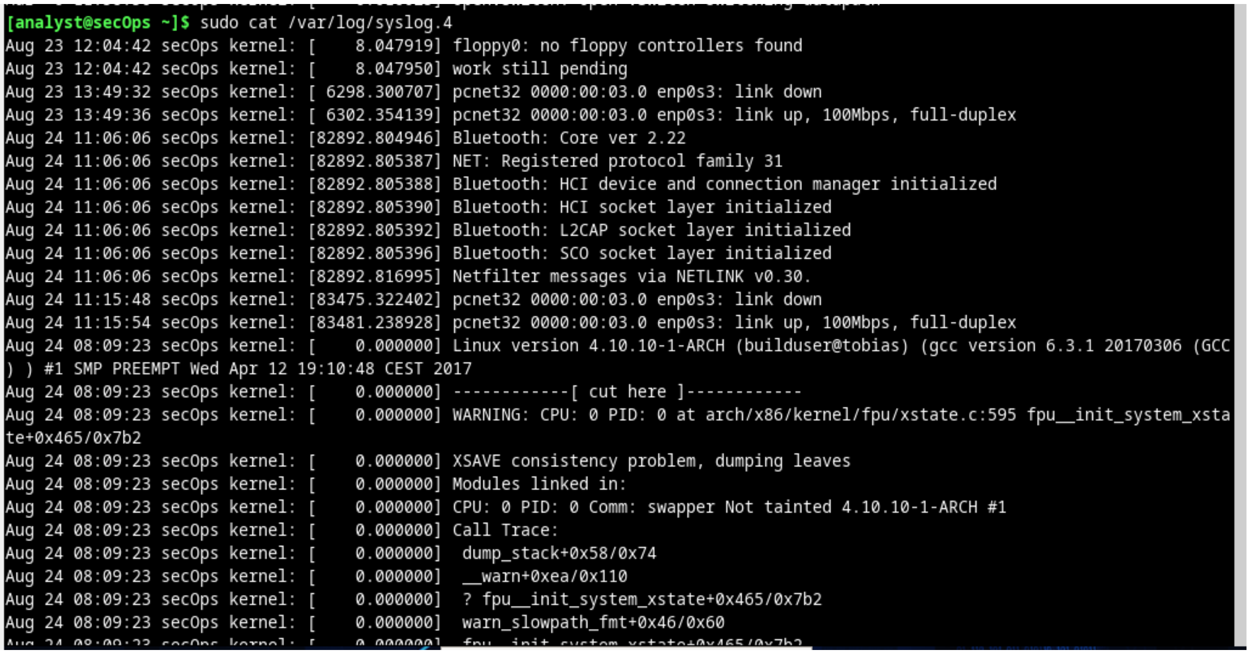
```
) ) #1 SMP PREEMPT Wed Apr 12 19:10:48 CEST 2017
Mar  6 07:27:19 secOps kernel: [    0.000000] ------------[ cut here ]------------
Mar  6 07:27:19 secOps kernel: [    0.000000] WARNING: CPU: 0 PID: 0 at arch/x86/kernel/fpu/xstate.c:595 fpu__init_system_xsta
te+0x465/0x7b2
Mar  6 07:27:19 secOps 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 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
Mar  6 07:27:19 secOps kernel: [    0.000000] CPUID[0d, 0d]: eax=00000000 ebx=00000000 ecx=00000000 edx=00000000
```

sudo cat /var/log/syslog.3



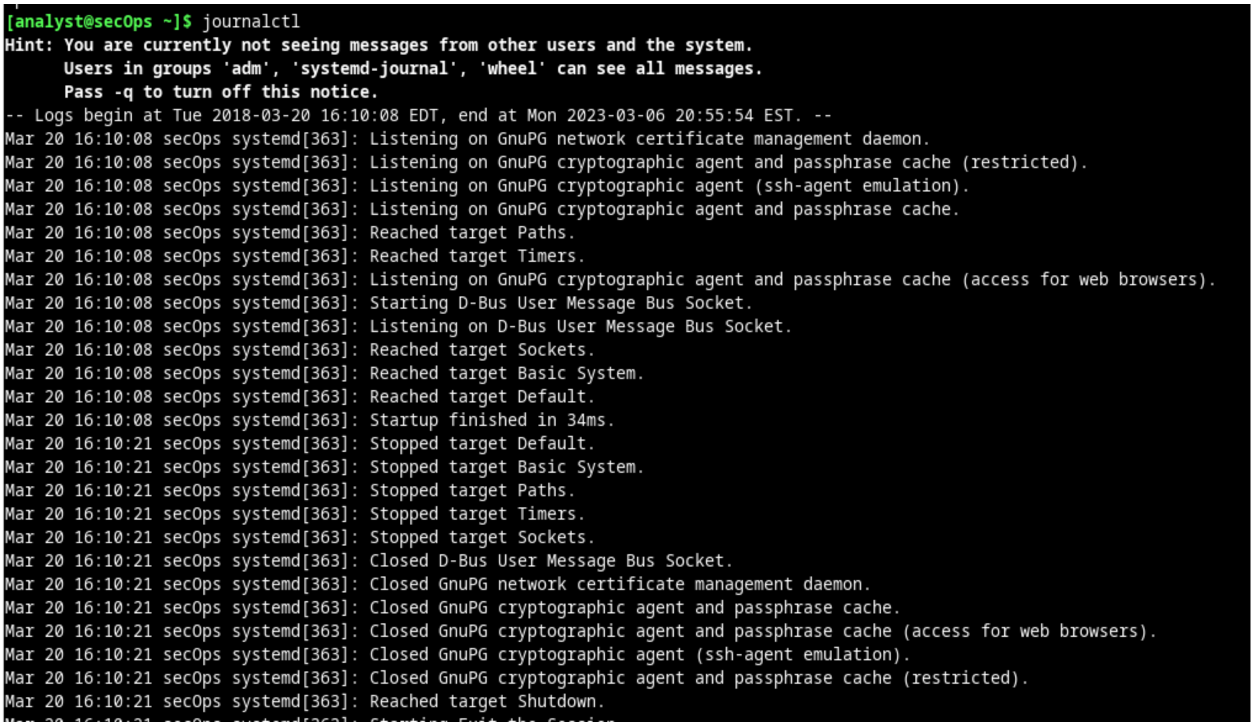
```
[analyst@secOps ~]$ sudo cat /var/log/syslog.3
Nov 29 11:30:40 secOps kernel: [    6.668727] ppdev: user-space parallel port driver
Nov 29 11:30:40 secOps kernel: [    6.681487] pcnet32 0000:00:03.0 enp0s3: renamed from eth0
Nov 29 11:30:40 secOps kernel: [    6.757097] pcnet32 0000:00:03.0 enp0s3: 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
```

sudo cat /var/log/syslog.4



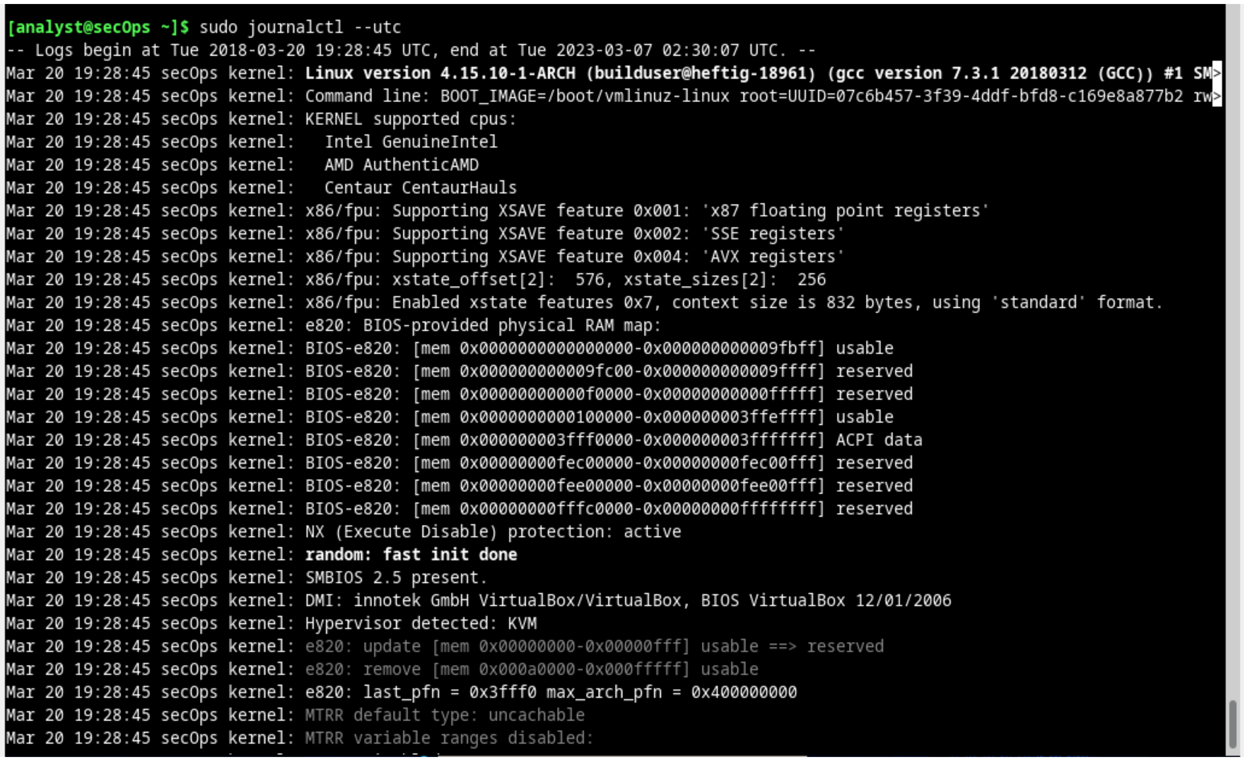
```
[analyst@secOps ~]$ sudo cat /var/log/syslog.4
Aug 23 12:04:42 secOps kernel: [    8.047919] floppy0: no floppy controllers found
Aug 23 12:04:42 secOps kernel: [    8.047950] work still pending
Aug 23 13:49:32 secOps kernel: [ 6298.300707] pcnet32 0000:00:03.0 enp0s3: link down
Aug 23 13:49:36 secOps 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
```

10. Memahami File Log dan Jurnalctl



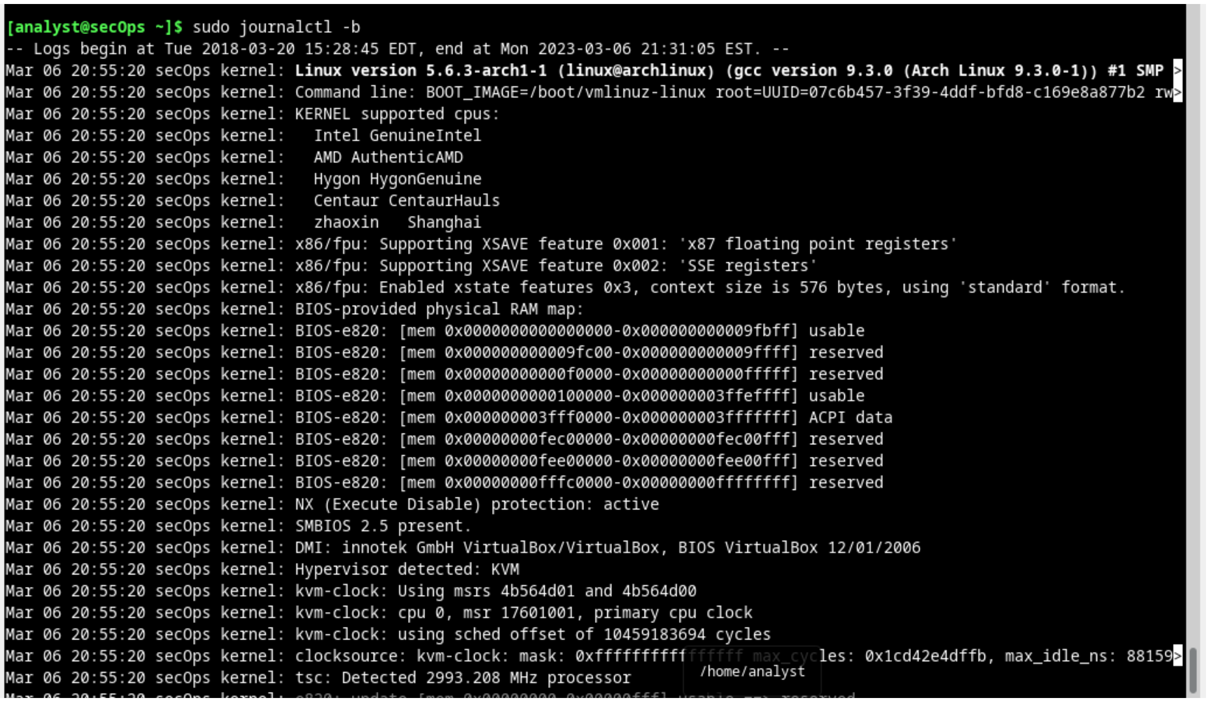
```
[analyst@secOps ~]$ journalctl
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal', 'wheel' can see all messages.
      Pass -q to turn off this notice.
-- Logs begin at Tue 2018-03-20 16:10:08 EDT, end at Mon 2023-03-06 20:55:54 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.
```

analis@secOps ~$ sudo journalctl --utc



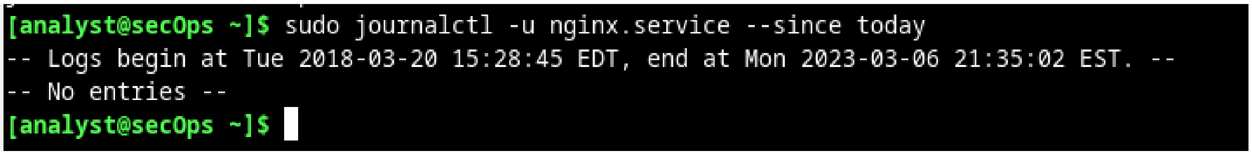
```
[analyst@secOps ~]$ sudo journalctl --utc
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Tue 2023-03-07 02:30:07 UTC. --
Mar 20 19:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builduser@heftig-18961) (gcc version 7.3.1 20180312 (GCC)) #1 SM>
Mar 20 19:28:45 secOps kernel: Command line: 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 0x0000000000100000-0x000000003ffeffff] usable
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] 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:
```

analis@secOps ~$ sudo journalctl -b



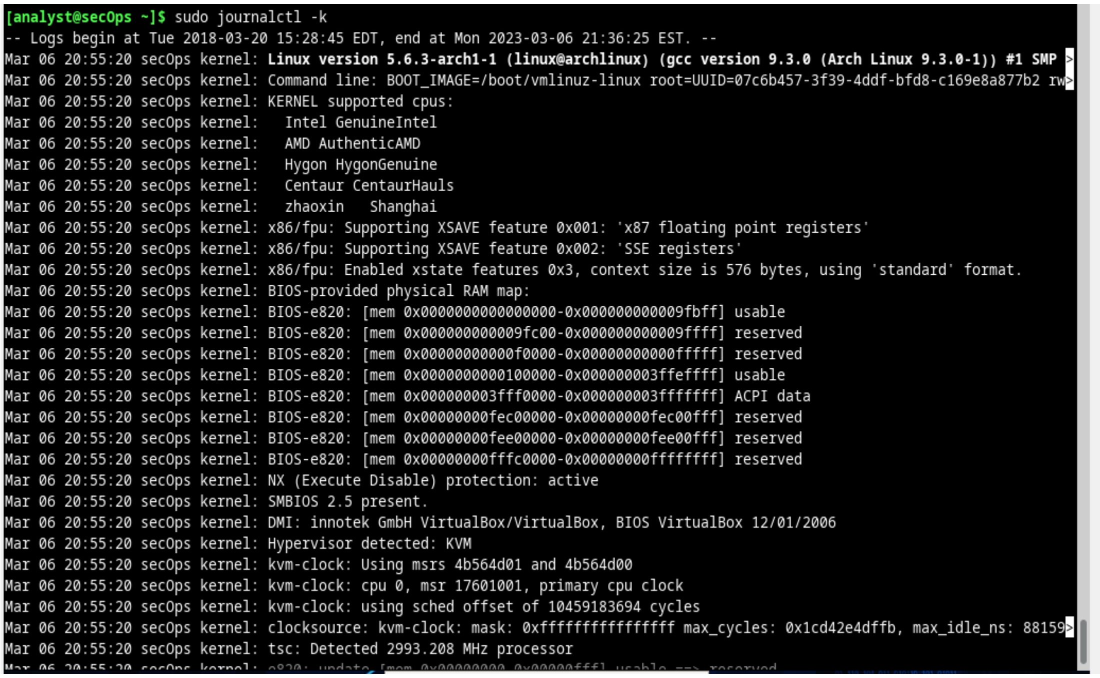
```
[analyst@secOps ~]$ sudo journalctl -b
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:31:05 EST. --
Mar 06 20:55:20 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (gcc version 9.3.0 (Arch Linux 9.3.0-1)) #1 SMP >
Mar 06 20:55:20 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw>
Mar 06 20:55:20 secOps kernel: KERNEL supported cpus:
Mar 06 20:55:20 secOps kernel:   Intel GenuineIntel
Mar 06 20:55:20 secOps kernel:   AMD AuthenticAMD
Mar 06 20:55:20 secOps kernel:   Hygon HygonGenuine
Mar 06 20:55:20 secOps kernel:   Centaur CentaurHauls
Mar 06 20:55:20 secOps kernel:   zhaoxin   Shanghai
Mar 06 20:55:20 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 20:55:20 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 20:55:20 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 20:55:20 secOps kernel: BIOS-provided physical RAM map:
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usable
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACPI data
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 06 20:55:20 secOps kernel: NX (Execute Disable) protection: active
Mar 06 20:55:20 secOps kernel: SMBIOS 2.5 present.
Mar 06 20:55:20 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 20:55:20 secOps kernel: Hypervisor detected: KVM
Mar 06 20:55:20 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 20:55:20 secOps kernel: kvm-clock: cpu 0, msr 17601001, primary cpu clock
Mar 06 20:55:20 secOps kernel: kvm-clock: using sched offset of 10459183694 cycles
Mar 06 20:55:20 secOps kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 88159>
Mar 06 20:55:20 secOps kernel: tsc: Detected 2993.208 MHz processor
Mar 06 20:55:20 secOps kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
```

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:



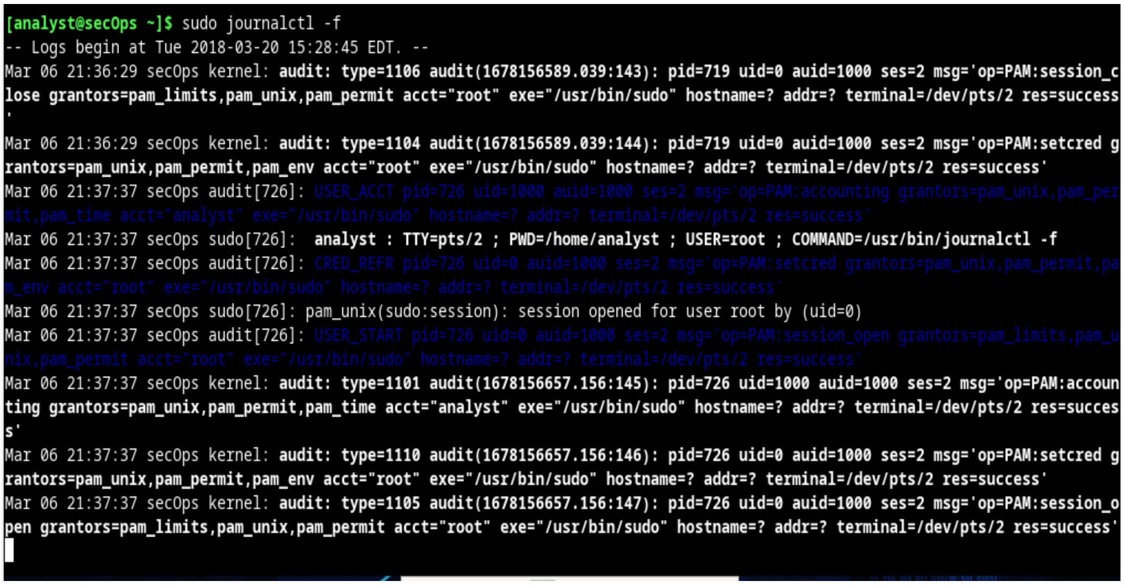
```
[analyst@secOps ~]$ sudo journalctl -u nginx.service --since today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:35:02 EST. --
-- No entries --
[analyst@secOps ~]$ 
```

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



```
[analyst@secOps ~]$ sudo journalctl -k
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:36:25 EST. --
Mar 06 20:55:20 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (gcc version 9.3.0 (Arch Linux 9.3.0-1)) #1 SMP >
Mar 06 20:55:20 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-4ddf-bfd8-c169e8a877b2 rw>
Mar 06 20:55:20 secOps kernel: KERNEL supported cpus:
Mar 06 20:55:20 secOps kernel:   Intel GenuineIntel
Mar 06 20:55:20 secOps kernel:   AMD AuthenticAMD
Mar 06 20:55:20 secOps kernel:   Hygon HygonGenuine
Mar 06 20:55:20 secOps kernel:   Centaur CentaurHauls
Mar 06 20:55:20 secOps kernel:   zhaoxin   Shanghai
Mar 06 20:55:20 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 06 20:55:20 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 20:55:20 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 bytes, using 'standard' format.
Mar 06 20:55:20 secOps kernel: BIOS-provided physical RAM map:
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usable
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACPI data
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 06 20:55:20 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 06 20:55:20 secOps kernel: NX (Execute Disable) protection: active
Mar 06 20:55:20 secOps kernel: SMBIOS 2.5 present.
Mar 06 20:55:20 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 06 20:55:20 secOps kernel: Hypervisor detected: KVM
Mar 06 20:55:20 secOps kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Mar 06 20:55:20 secOps kernel: kvm-clock: cpu 0, msr 17601001, primary cpu clock
Mar 06 20:55:20 secOps kernel: kvm-clock: using sched offset of 10459183694 cycles
Mar 06 20:55:20 secOps kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 88159>
Mar 06 20:55:20 secOps kernel: tsc: Detected 2993.208 MHz processor
Mar 06 20:55:20 secOps kernel: e820: update [mem 0x00000000-0x00000fff] 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
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Mar 06 21:36:29 secOps kernel: audit: type=1106 audit(1678156589.039:143): 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/2 res=success
'
Mar 06 21:36:29 secOps kernel: audit: type=1104 audit(1678156589.039:144): 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/2 res=success'
Mar 06 21:37:37 secOps audit[726]: USER_ACCT pid=726 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/2 res=success'
Mar 06 21:37:37 secOps sudo[726]:  analyst : TTY=pts/2 ; PWD=/home/analyst ; USER=root ; COMMAND=/usr/bin/journalctl -f
Mar 06 21:37:37 secOps audit[726]: CRED_REFR pid=726 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/2 res=success'
Mar 06 21:37:37 secOps sudo[726]: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 06 21:37:37 secOps audit[726]: USER_START pid=726 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 21:37:37 secOps kernel: audit: type=1101 audit(1678156657.156:145): pid=726 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/2 res=succes
s'
Mar 06 21:37:37 secOps kernel: audit: type=1110 audit(1678156657.156:146): pid=726 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 21:37:37 secOps kernel: audit: type=1105 audit(1678156657.156:147): pid=726 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'
█
```