LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
UNIT 5 & 6

DI SUSUN OLEH:

Nama	: Bintang Nur K
NIM	: 21/481453/SV/19790
Kelas	: RI4AA
Hari, tanggal	: Selasa, 07 Maret 2023
Dosen Pengampu	: Anni Karimatul Fauziyyah, S.Kom., M.Eng
Asisten Praktikum	: Gabriella Alvera Chaterine

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

UNIT 5 & 6

TEKNIK STEGANOGRAFI DAN ANALISIS LOG SERVER

I. TUJUAN

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

II. LATAR BELAKANG

File Log adalah alat penting dalam pemecahan masalah dan pemantauan. Aplikasi yang berbeda menghasilkan file log yang berbeda, masing-masing berisi kumpulan bidang dan informasinya sendiri. Meskipun struktur bidang dapat berubah di antara file log, alat yang digunakan untuk membacanya sebagian besar sama. Di lab ini, Anda akan mempelajari tentang alat umum yang digunakan untuk membaca file log dan berlatih menggunakannya.

Steganografi adalah ilmu, teknik atau seni menyembunyikan pesan rahasia "*hiding message*" atau tulisan rahasia "*covered writing*" sehingga keberadaan pesan tidak terdeteksi orang lain kecuali pengirim dan penerima pesan tersebut. Steganografi berasal dari bahasa Yunani yaitu steganos "tersembunyi/ menyembunyikan" dan graphy "tulisan", sehingga secara lengkap bermakna tulisan yang disembunyikan.

III. ALAT DAN BAHAN

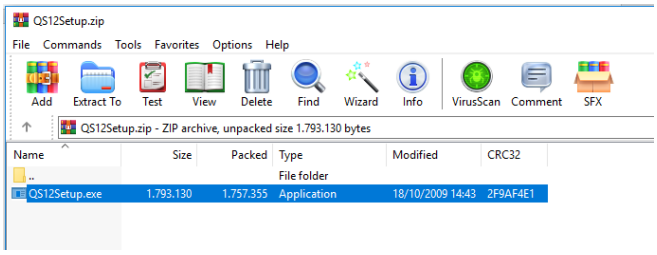
Alat dan Bahan yang dibutuhkan untuk melaksanakan praktikum adalah

- PC
- Koneksi internet
- *Software* Steganografi
- CyberOps Workstation VM

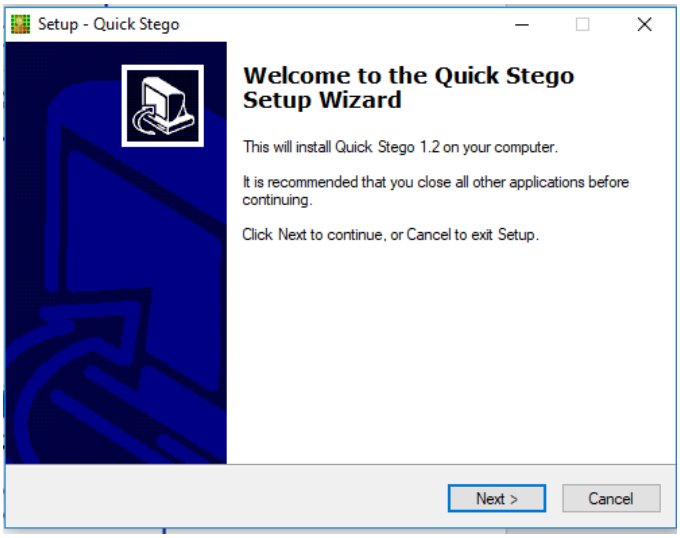
IV. LANGKAH KERJA DAN HASIL

Langkah kerja steganografi

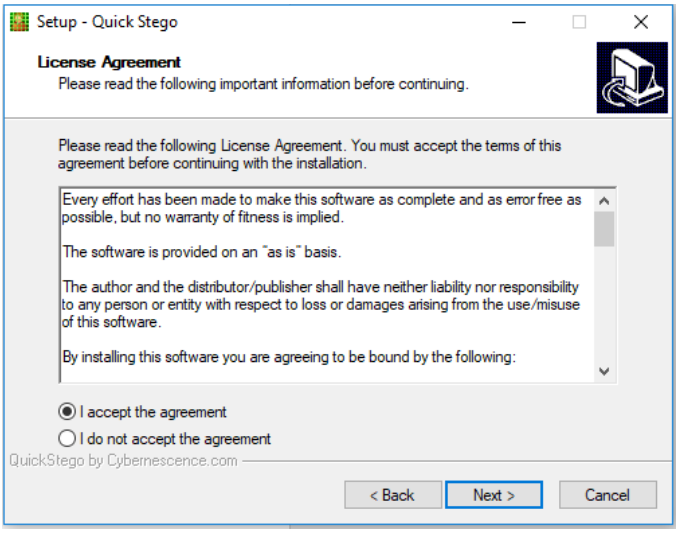
1. Buka windows



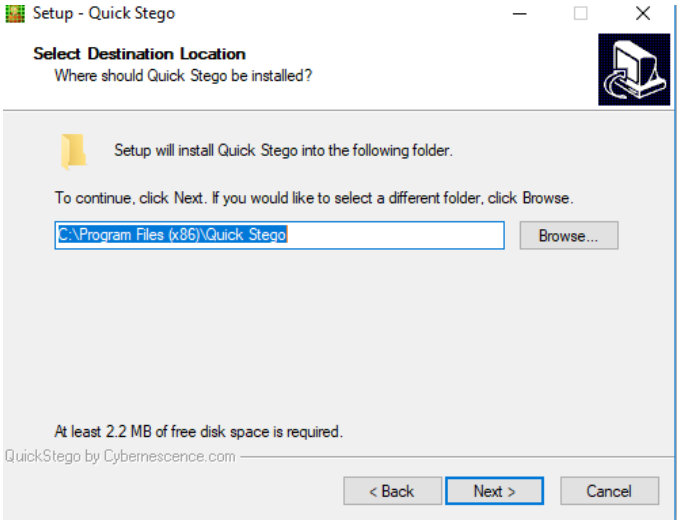
2. Instal quick stego



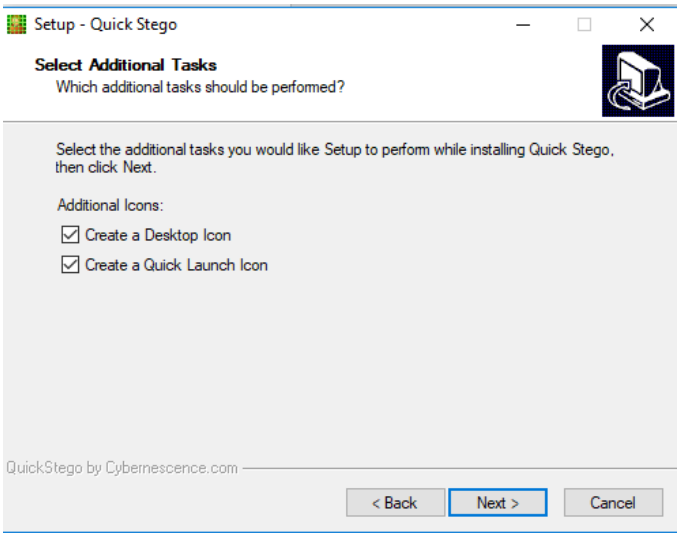
Pengaturan lisensi

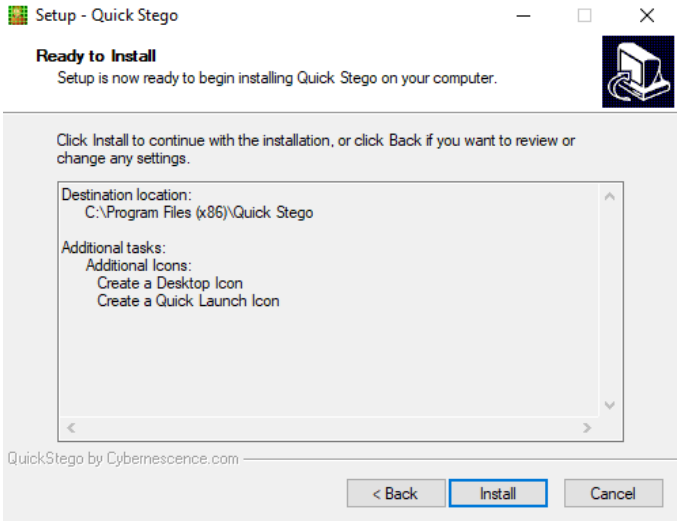


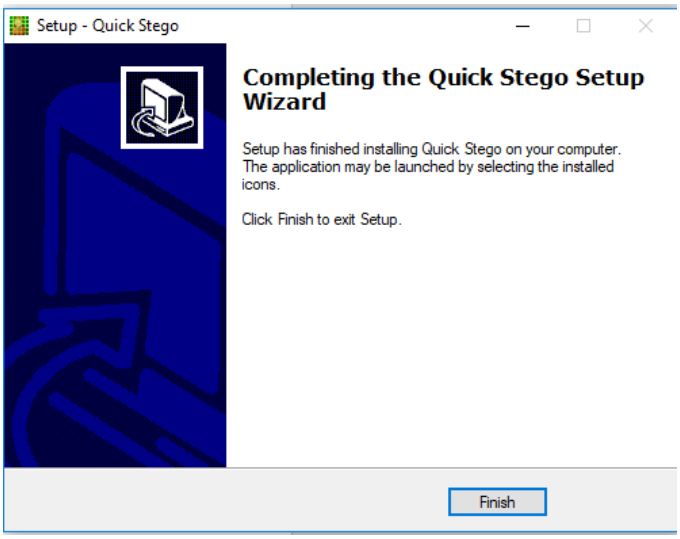
Pilih tujuan



Pilih tugas tambahan, lalu klik siap instal







Buka Command Prompt

Buat Direktori STEGO

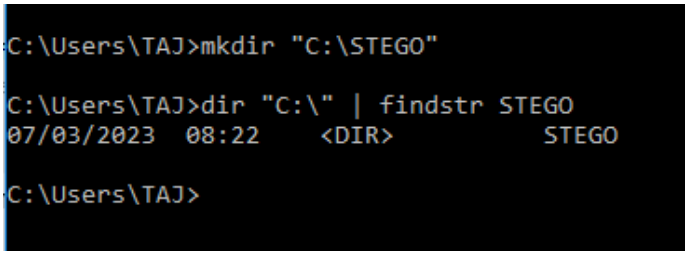
mkdir "C:\STEGO"

dir "C:\" | temukanstr STEGO

catatan

mkdir, buat direktori. Dalam hal ini, buat direktori STEGO langsung di bawah Drive C.

dir "C:\", daftar semua direktori dan file langsung di bawah Drive C. Kemudian gunakan findstr untuk mencantumkan hanya file dan/atau direktori yang berisi string STEGO.



3. Install MD5SUMS

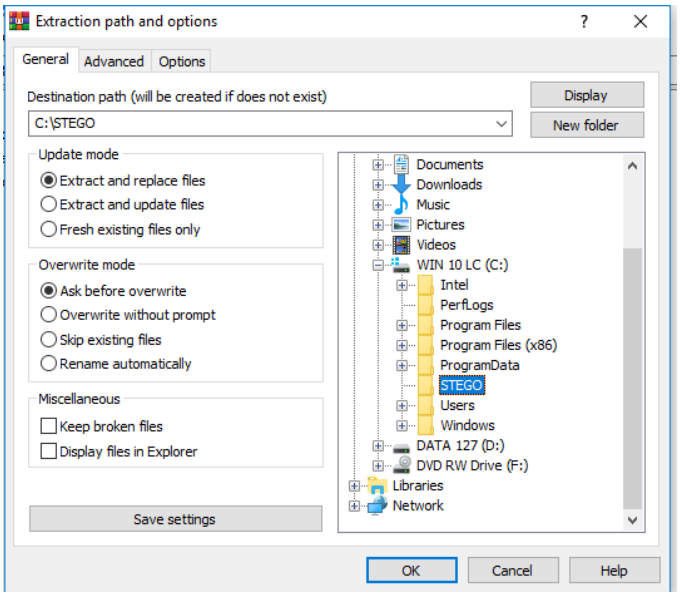
   Unduh md5sums-1.2

   Arahkan ke URL berikut

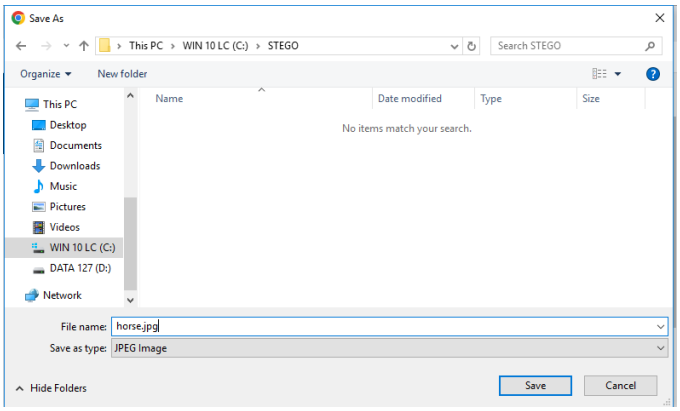
   http://www.pc-tools.net/files/win32/freeware/md5sums-1.2.zip

   Klik tombol Simpan File Radio

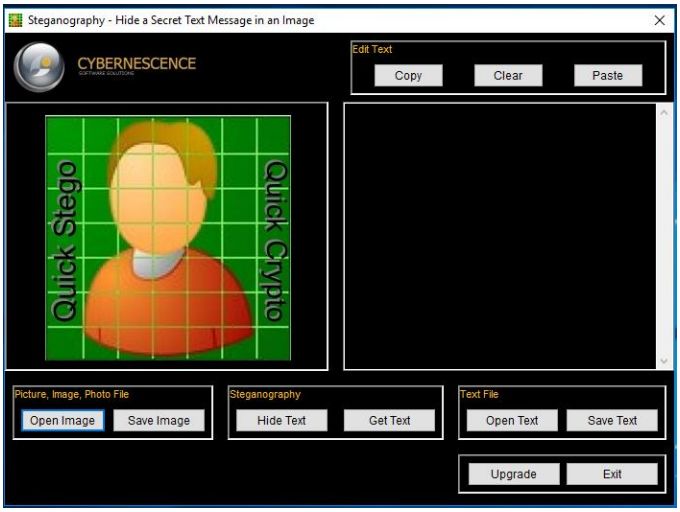
Klik tombol **OK**



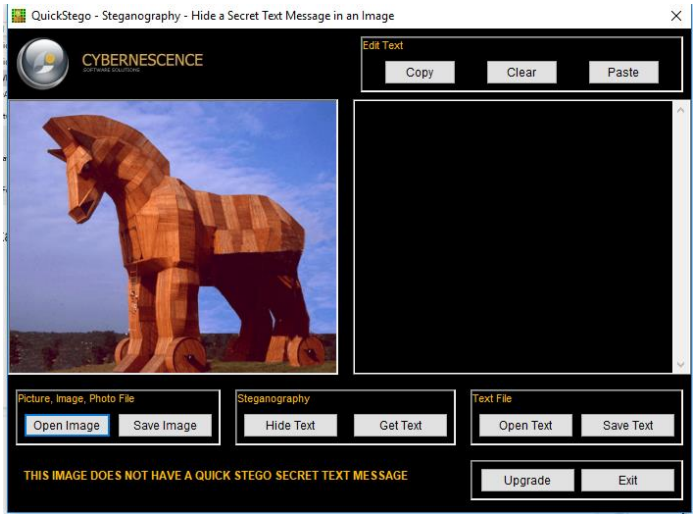
Beri nama dengan jenis file jpg



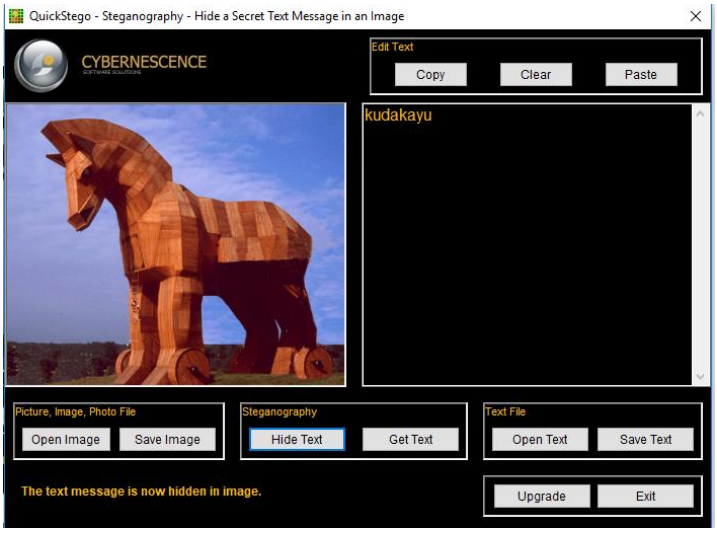
Jalankan Stego Cepat



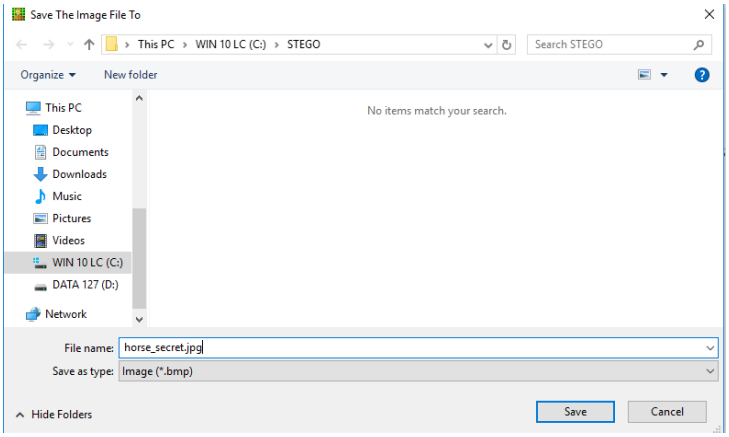
Masukkan gambar yang ingin diberi kata tersembunyi



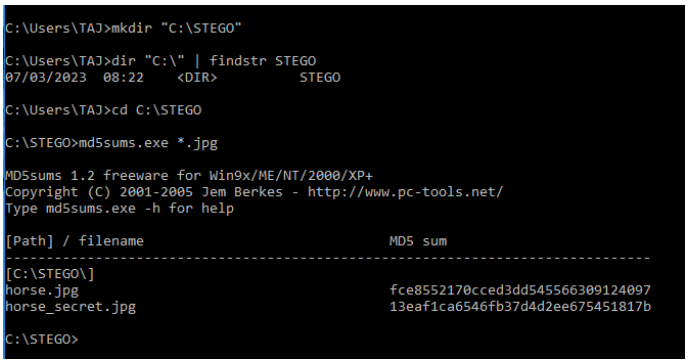
Sembunyikan Teks



Simpan gambar dengan nama file “horse_secret.jpg”

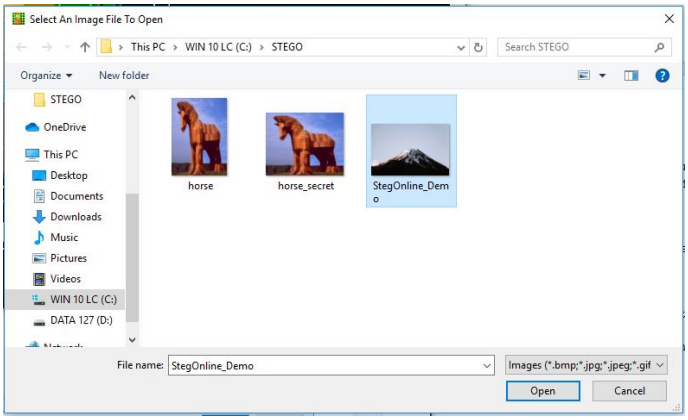


Buka Command Prompt

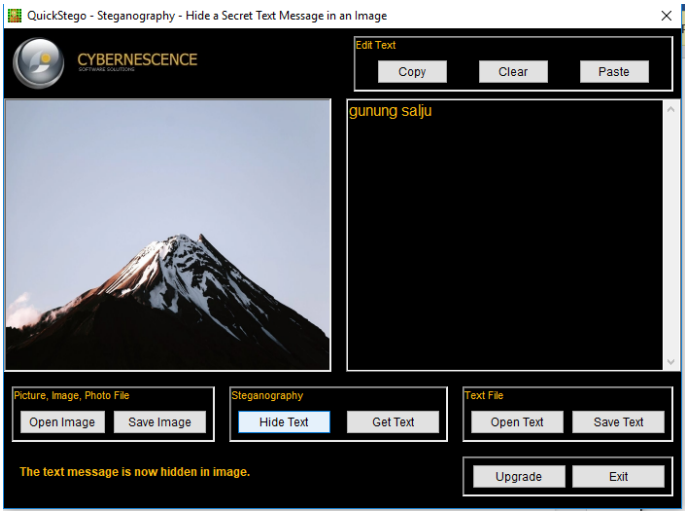


PADA GAMBAR 2

Ubah PNG to JPG terlebih dahulu, lalu pindahkan file ke STEGO



Masukkan hidden text

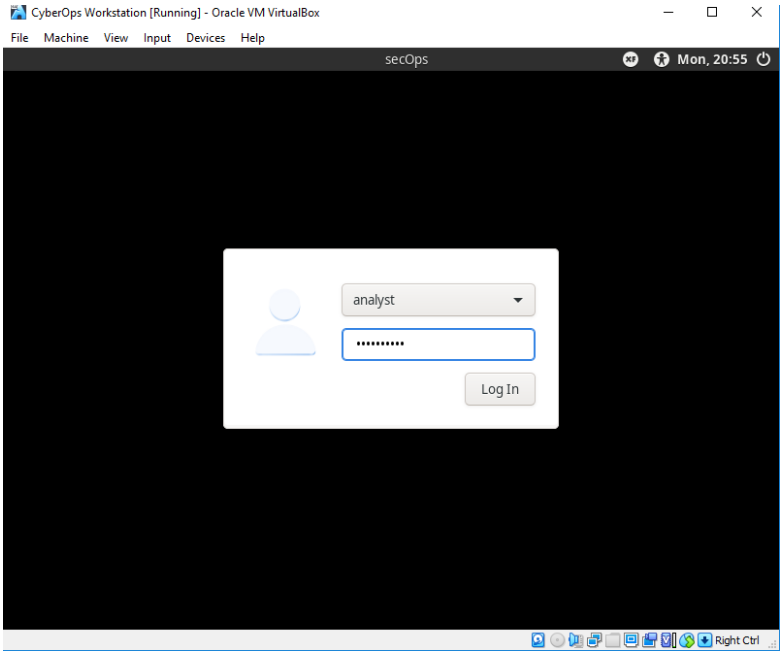


Buka command prompt

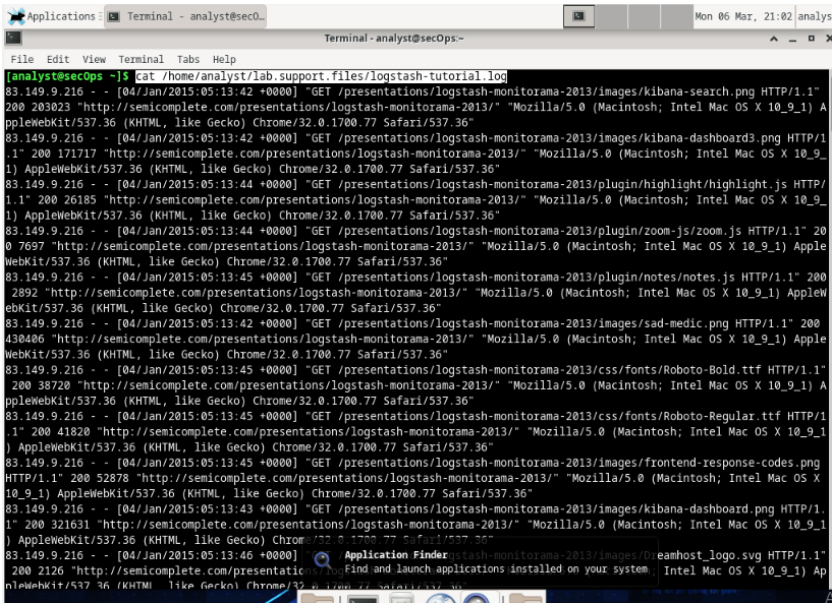
```
C:\STEGO>md5sums.exe *.jpg

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                               13eaf1ca6546fb37d4d2ee675451817b
StegOnline_Demo.jpg                            9f3b7b4b200da9fe48d4c38b9935a890
StegOnline_rhs.jpg                             e3ad125cea8f30b8d95653e9ac9ebe98

C:\STEGO>dir *.jpg
 Volume in drive C is WIN 10 LC
 Volume Serial Number is 23DA-BE09

 Directory of C:\STEGO

07/03/2023  08:33            46.001 horse.jpg
07/03/2023  08:39           854.454 horse_secret.jpg
07/03/2023  08:43            48.590 StegOnline_Demo.jpg
07/03/2023  08:52         1.998.054 StegOnline_rhs.jpg
               4 File(s)      2.947.099 bytes
               0 Dir(s)  277.291.880.448 bytes free

C:\STEGO>_
```

UNIT 6

Pembacaan Log Server

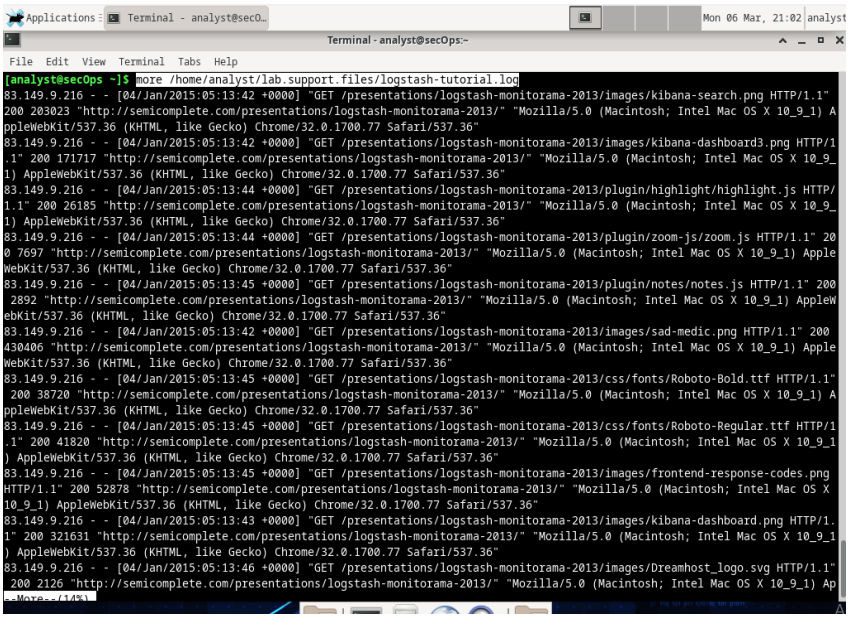


analis@secOps ~$ cat /home/analyst/lab.support.files/logstash-tutorial.log



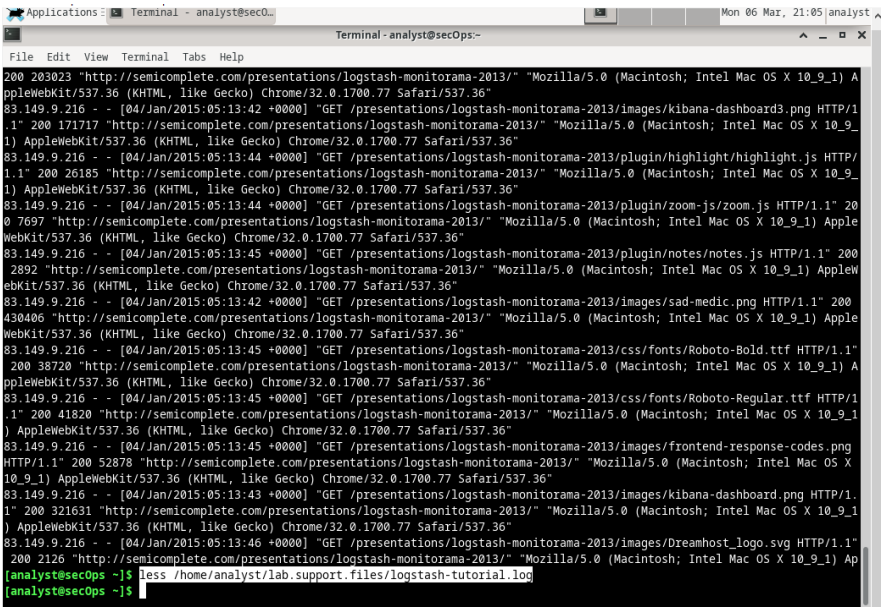
Dari jendela terminal yang sama, gunakan perintah di bawah ini untuk menampilkan kembali isi file logstash-tutorial.log. Proses ini menggunakan more:

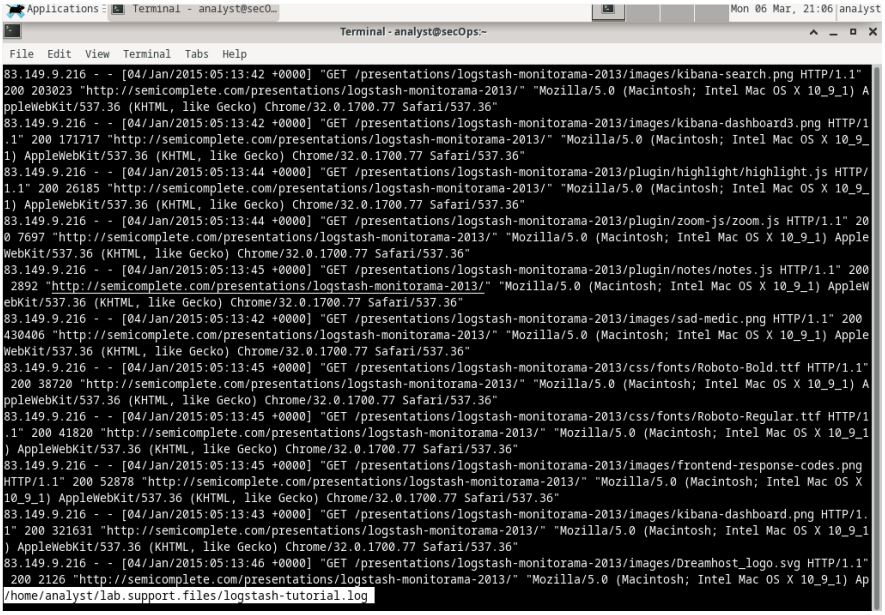
analis@secOps ~$ more /home/analyst/lab.support.files/logstash-tutorial.log



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

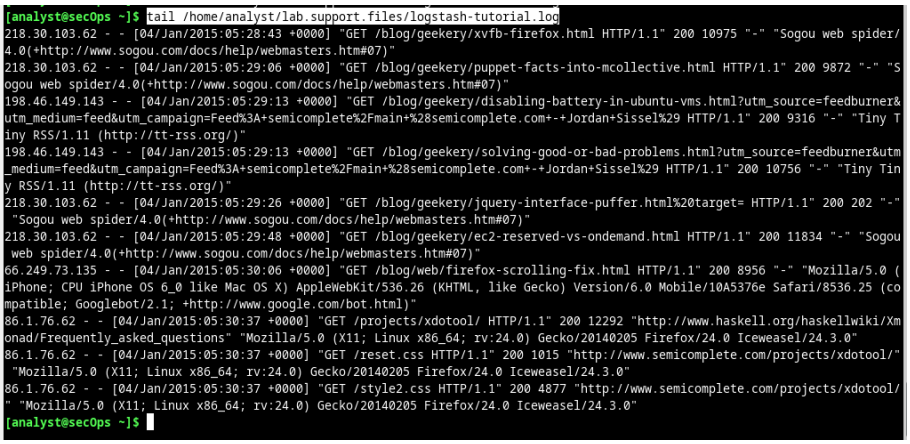
analis@secOps ~$ lebih sedikit /home/analyst/lab.support.files/logstash-tutorial.log



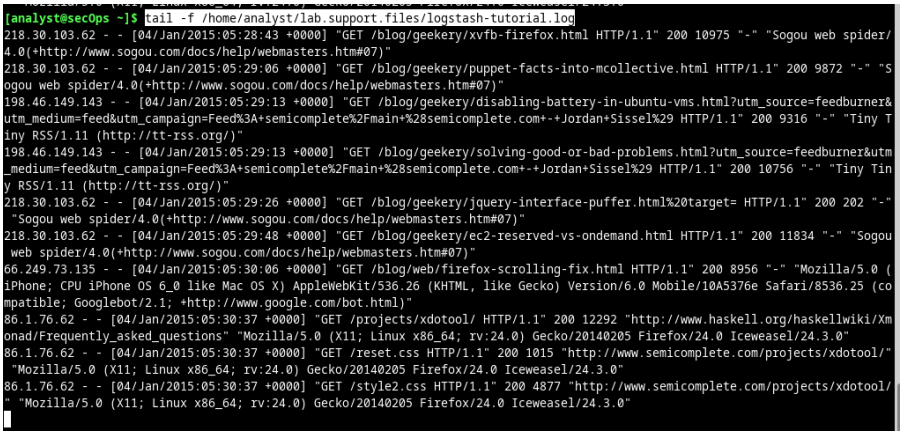


Perintah tail menampilkan akhir file teks. Secara default, tail menampilkan sepuluh baris terakhir file. Gunakan tail untuk menampilkan sepuluh baris terakhir dari file /home/analyst/lab.support.files/logstash-tutorial.log.

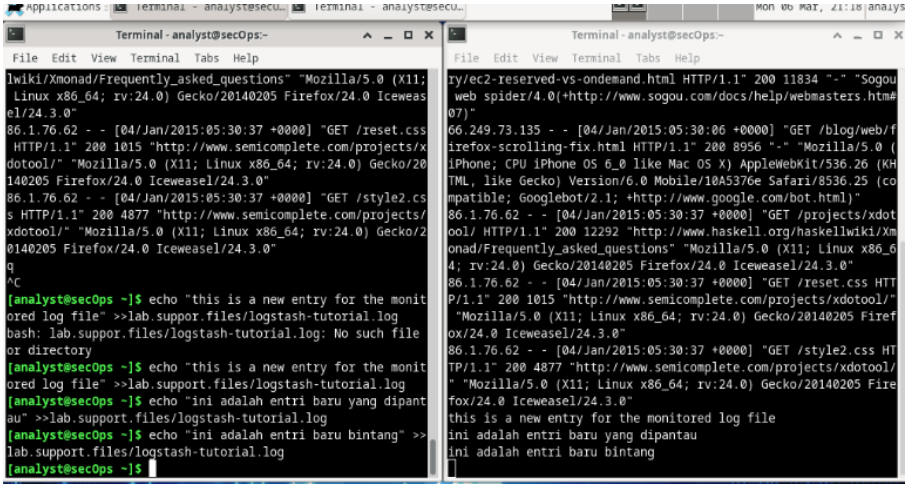
analis@secOps ~$ tail /home/analyst/lab.support.files/logstash-tutorial.log



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

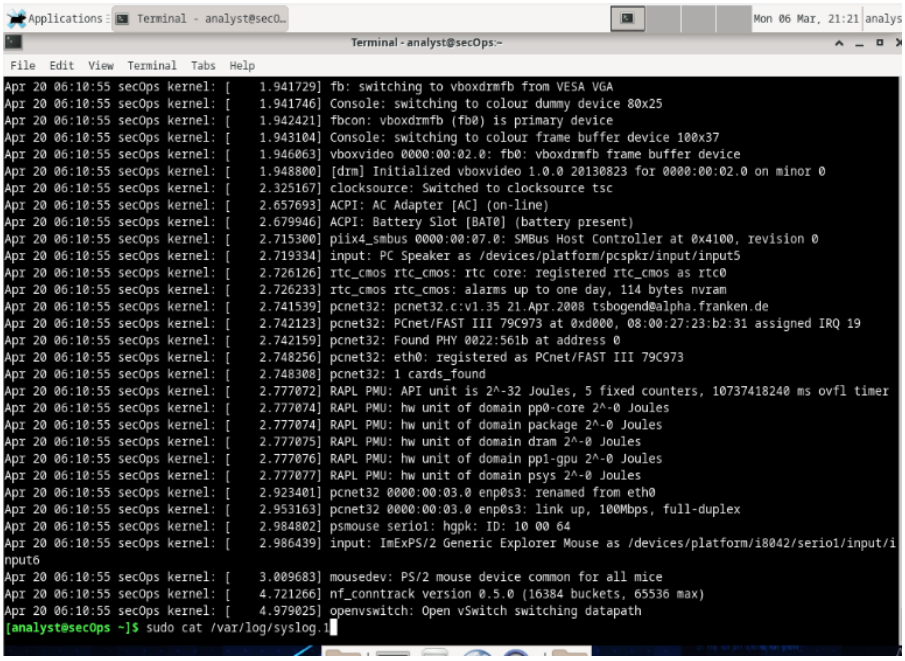


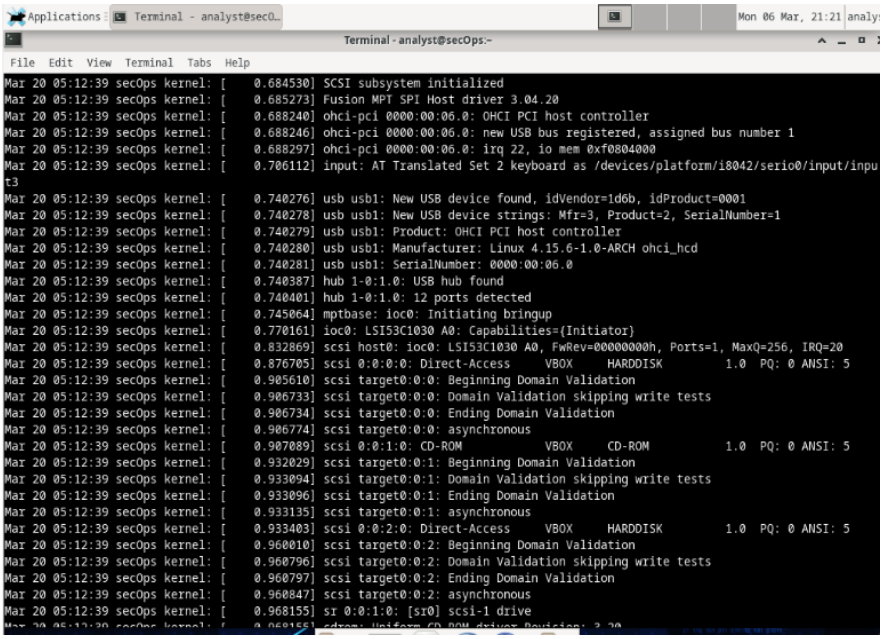
Pilihlah jendela terminal bawah dan masukkan perintah berikut: [analyst@secOps ~]$ echo "ini adalah entri baru untuk file log yang dipantau" >> lab.support.files/logstash-tutorial.log



Memahami File Log dan Syslog

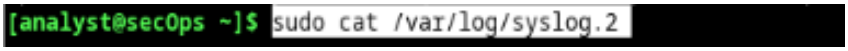
analis@secOps ~$ sudo cat /var/log/syslog.1

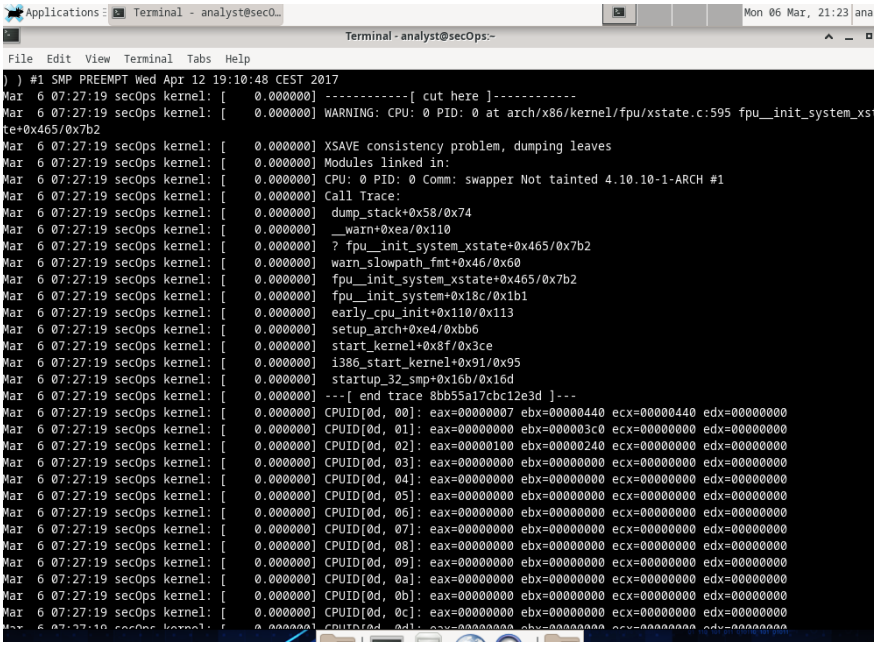




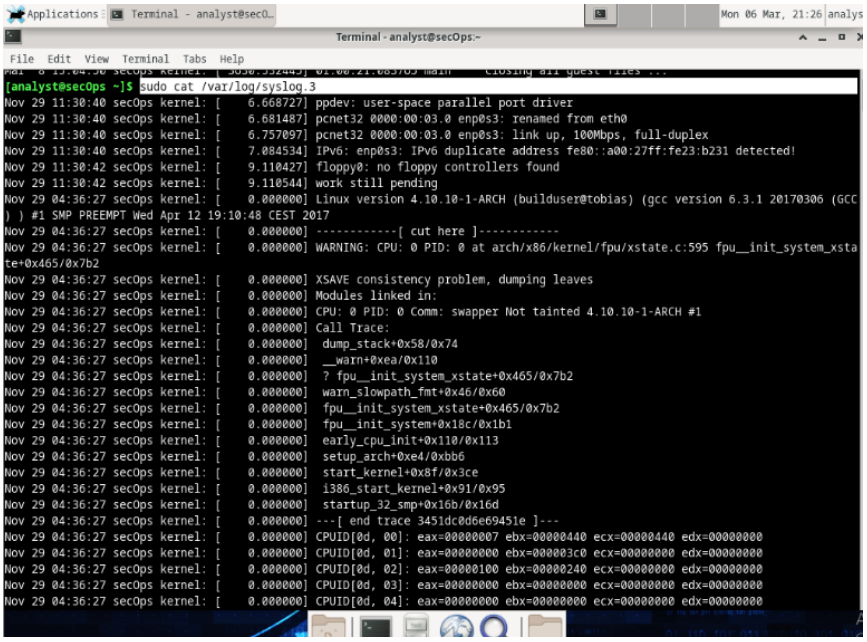
Untuk menjaga agar file syslog tetap kecil, sistem operasi secara berkala merotasi file log, mengganti nama file log lama menjadi syslog.1, syslog.2, dan seterusnya.

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

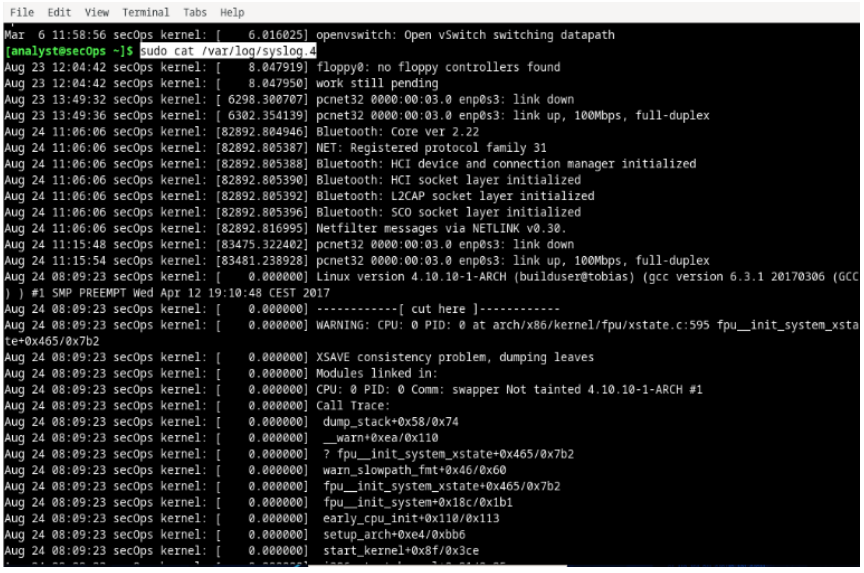




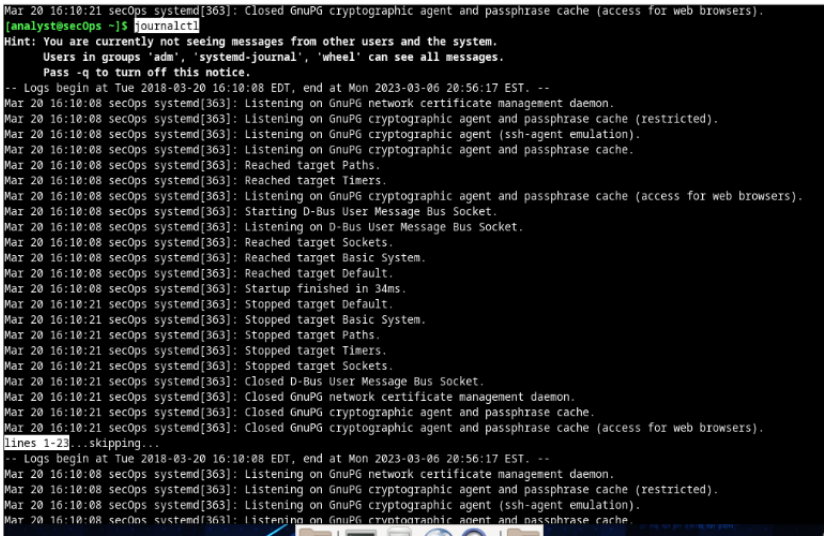
analis@secOps ~$ sudo cat /var/log/syslog.3



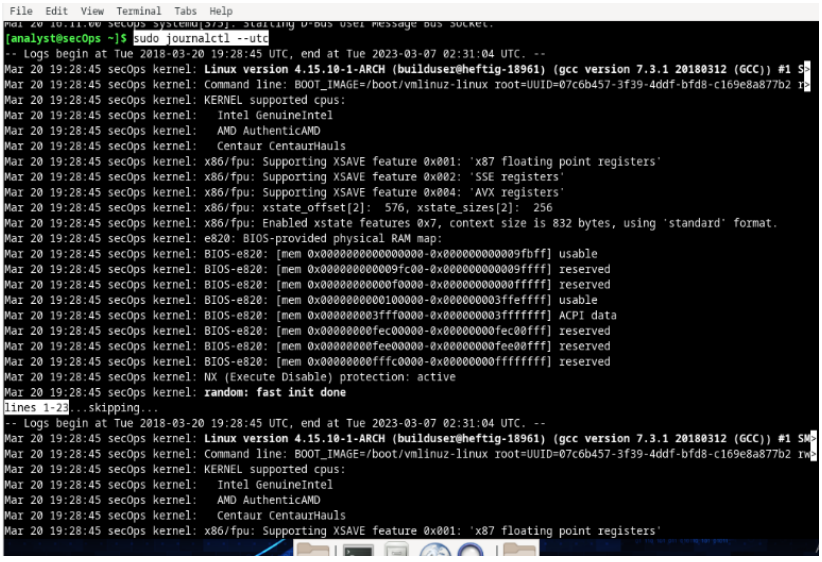
analis@secOps ~$ sudo cat /var/log/syslog.4



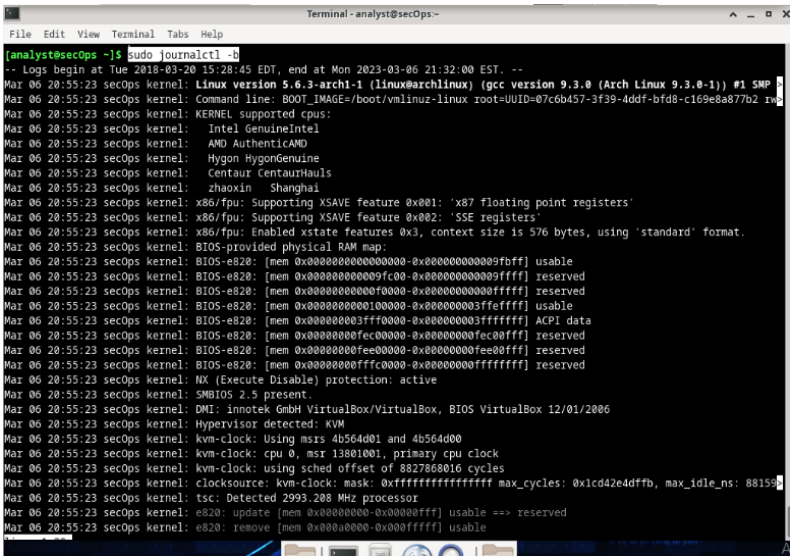
Memahami File Log dan Jurnalctl



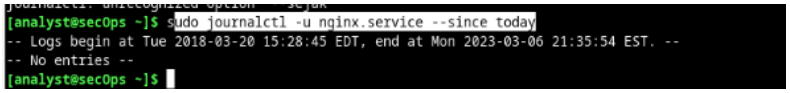
analis@secOps ~$ sudo journalctl –utc



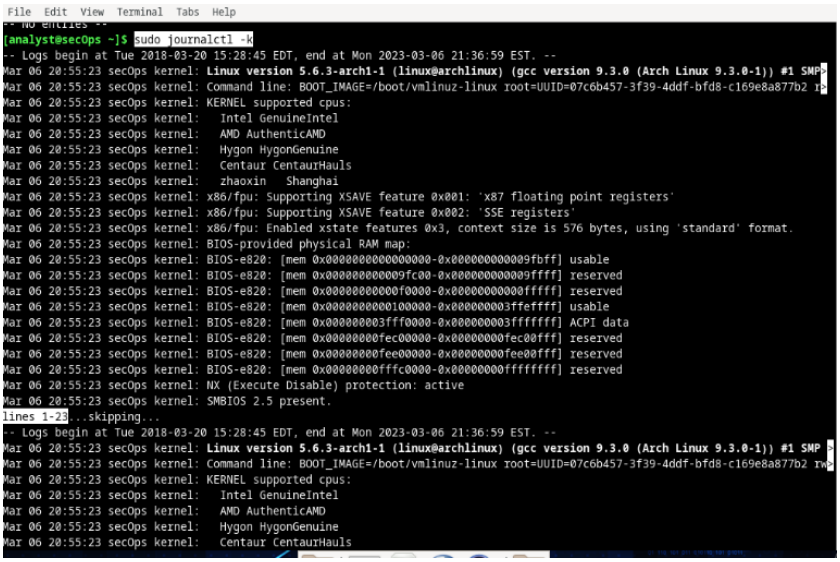
analis@secOps ~$ sudo journalctl –b



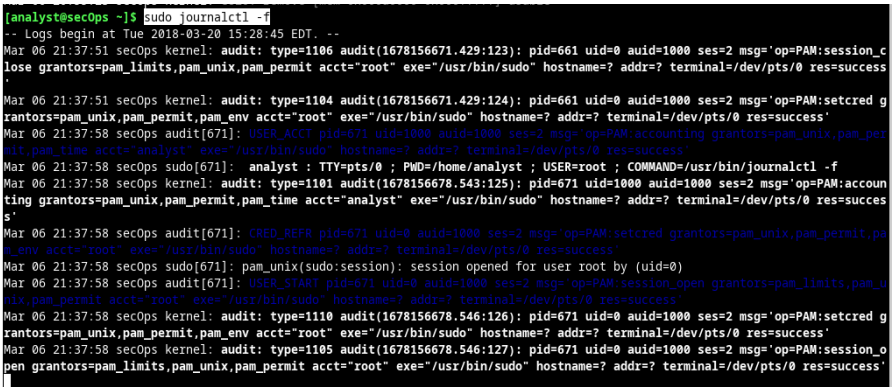
analis@secOps ~$ sudo journalctl -u nginx.service --sejak hari ini



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



Mirip dengan tail -f yang dijelaskan di atas, gunakan -f untuk secara aktif mengikuti log saat sedang ditulis: analis@secOps ~$ sudo journalctl –f



File yang tersimpan:

https://simpan.ugm.ac.id/apps/files/

V. ANALISIS

Pada praktikum kali ini melakukan praktik steganografi dan pembacaan log server/ file log.

Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.

Cara Kerja Steganografi antara lain dengan menyisipkan data yang ingin disembunyikan membutuhkan dua unsur. Unsur pertama ialah media penampung seperti citra, suara, video dan sebagainya yang terlihat tidak mencurigakan untuk menyimpan pesan rahasia. Unsur kedua adalah pesan yang ingin disembunyikan yaitu media penampungnya berupa citra yang disebut *cover-object* dan citra yang telah disisipi pesan disebut *stego-object*.

Secara umum, terdapat dua proses didalam steganografi yaitu proses embedding untuk menyisipkan pesan kedalam cover-object dan proses decoding untuk ekstraksi pesan dari stego-object. Kedua proses ini mungkin memerlukan kunci rahasia yang dinamakan stego-key agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

Pada lab stegano ini mengunduh gambar yang sudah diberikan di modul elok lalu disimpan pada folder yang Bernama "STEGO" kemudian buka cmd dan ketik perintah dir *.jpg untuk menampilkan informasi file berupa gambar yang ada pada folder STEGO. Terlihat sebelum dan sesudah gambar tersebut disispi pesan hiden text dimana terjadi perbedaan ukuran file. Untuk dari segi visual hamper tidak terjadi perbedaan dan hanya bisa diketahui melalui perintah pada CMD. Ditampilkan juga total ukuran 4 files gambar yang ada. Lanjut untuk mengecek keaslian/integritas pda gambar yang ada pada folder STEGO menggunakan MD5SUMS.

Pesan yang ditampilkan berupa pesan acak untuk menjaga keamanan dan bernilai 32 karakter

File-file log adalah file yang berada di sebuah sistem yang merupakan file-file penting yang senantiasa mencatat semua kejadian-kejadian(kegiatan) yang berlangsung pada system. File -file log kebanyakan ditulis dalam bentuk file text yang ditulis perbaris (istilah untuk namanya adalah record) oleh program-program sistem bawaan saat kita menginstall sebuah program ataupun sebuah SO (sistem operasi).

Pada perintah ini dilakukan di CyberOps Workstation virtual machine.

Perintah echo untuk menambahkan data baru berupa tulisan yang terdapat pada baris akhir. Setelah perintah echo dijalankan lalu membuka text menggunakan tail -f, maka akan muncul text yang kita tulis tadi pada baris akhir. Perintah syslog untuk mengirim/mengekspor pesan log ke dalam satu server. Untuk pembuatan syslog yang lain berguna agar ukuran file yang dihasilkan tidak terlalu besar dan membebani satu server. Perintah journalctl untuk membaca dan berkomunikasi dengan jurnal log, serta menampilkan

pesan log oleh jurnal log. Perintah –utc pada journalctl berfungsi untuk menampilkan waktu log in UTC dengan menampilkan waktu yang sesungguhnya. Perintah -b pada journalctl berfungsi untuk menampilkan rekaman log terakhir selama boot berakhir. Perintah sudo journalctl -u nginx.service—day untuk menampilkan catatan seluruh log.

Versi-versi Unix menyimpan file-file log-nya pada direktory berbeda-beda. Umumnya file ini berada pada:

/usr/adm ---> Digunakan oleh Unix Versi lama

/var/adm ---> Digunakan oleh kebanyakan Versi Unix/Linux terbaru. dimana partisi /usr di-mount read only

/var/log ---> Digunakan oleh beberapa versi Solaris, Linux, BSD, dan FreeBSD

Di dalam *directory* - *directory* diatas terdapat *subdirectory* didalamnya terdapat file-file sebagai berikut:

sulog ---> Melakukan log penggunaan perintah su

utmp ---> Merekam setiap user yang tengah login

utmpx ---> Extended utmp

wtmp ---> Memberikan record permanen untuk setiap kali user login dan logout, juga merekam shutdown dan star up system

acct atau pacct ---> Merekam perintah-perintah yang dijalankan oleh setiap user

aculog ---> Merekam dial-out modem-modem (automatic call units)

lastlog ---> Melakukan log setiap login user,baik yang sukses maupun tidak

loginlog ---> Merekam usaha-usaha pada saat login yang gagal

messages ---> Merekam output ke "console" sistem atau pesan-pesan lain yang menghasilkan dari fasilitas syslog

wtmpx ---> Extended wtmp

vold.log ---> Melakukan log error-error yang dialami atas penggunaaan external media seperti, disk-disk floppy atau CDROM.

xferlog ---> Melakukan log akses-akses ftp

aculog ---> Melakukan log pada setiap terjadi panggilan telepon yang di-dial

uucp ---> Melakukan log saat terjadi pelanggaran-pelanggaran restriksi atu penggunaan UUCP system (biasanya untuk aktivitas seorang user dan log-log file transfer).

acces_log ---> Melakukan log pada saat menjalankan HTTPD untuk keperluan World Wide Web.

syslog ---> Melakukan log proses-proses system

dmesg ---> Melakukan log pada saat server reboot

www/access.log ---> file log access web server

www/error.log ---> file log error web server

.bash_history ---> Melakukan log hasil ketikan kita diconsole dan lain lain..

VI. KESIMPULAN

Setelah melaksanakan praktikum yang saya dapatkan adalah

- Rotasi file log, dilakukan berdasarkan ukuran file
- File log akan di-rotasi setelah mencapai ukuran tertentu
- Log adalah catatan dalam bentuk file yang berisi rekaman aktifitas dari sebuah aplikasi. Catatan ini dapat berupa pesan peringatan, pesan kesalahan atau pesan lainnya. Salah satu contoh file log yang sering ditemui adalah file “error_log”. File “error_log” ini bisa di temukan pada directory file website yang di buat.
- Steganografi adalah tulisan atau pesan yang disembunyikan

VII. DAFTAR PUSTAKA

Priyambodo, D. (2022, December 29). *Apa itu Log dan Setting Rotasi Log di VPS cPanel*. Rumahweb Journal – News, Article, and Tutorial of Web Dev. https://www.rumahweb.com/journal/apa-itu-log-adalah/

Knowledge, S. S.-. S. I. A. (n.d.). *Mengenal berbagai jenis file log di server linux | Explore your Mind*. https://suryadisyamsu.blogspot.com/2009/05/mengenal-berbagai-jenis-file-log-di.html

Komputer, U. S. &. T. (n.d.). *Seni dan Ilmu Menulis Pesan Tersembunyi (Steganografi)|S1 Teknik Informatika S.Kom*. http://teknik-informatika-s1.stekom.ac.id/informasi/baca/Seni-dan-Ilmu-Menulis-Pesan-Tersembunyi-Steganografi/ff7dc125afd07f6dd43da9fa8a09809e96d41789