Manual Book

Dataset disk Image= https://digitalcorpora.org/corpora/scenarios/m57-jean/

Skenario :

Pada eksperimen ini kami menggunakan Skenario M57-jean. Skenario M57-Jean adalah skenario disk image tunggal yang melibatkan eksfiltrasi dokumen perusahaan dari laptop seorang eksekutif senior. Skenario ini melibatkan sebuah perusahaan kecil yang masih baru, M57.Biz. Beberapa minggu setelah didirikan, sebuah file spreadsheet rahasia yang berisi nama dan gaji karyawan inti perusahaan ditemukan di posting pada bagian "komentar" salah satu kompetitor perusahaan. File spreadsheet tersebut hanya ada pada satu pegawai M57 yaitu Jean. Jean mengatakan bahwa dirinya tidak mengetahui bagaimana data tersebut dapat keluar dari laptopnya dan dia pasti telah diretas.

Identifikasi:

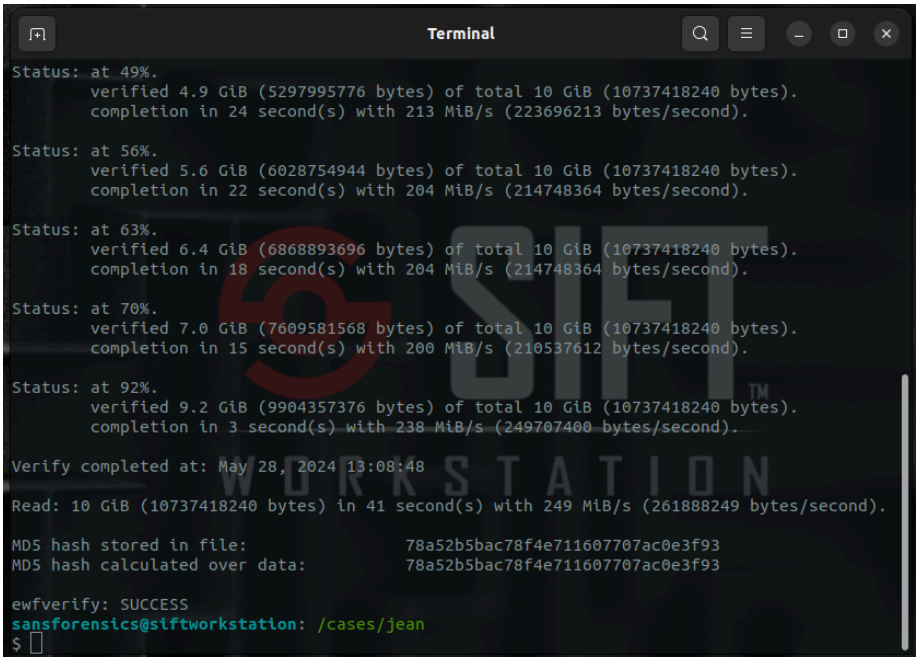
1. Fakta-fakta dari kasus ini:
    - Pendanaan tahap awal sebesar $3 juta; sekarang menutup putaran pendanaan $10 juta
    - 2 pendiri/pemilik
    - 10 karyawan dipekerjakan pada tahu n pertama
2. Staf perusahaan:
    - President: Alison Smith
    - CFO: Jean
    - Programmer: Bob, Carole, David, & Emmy
    - Marketing: Gina, Harris
    - BizDev: Indy
3. Pemasaran & BizDev:
    - Bekerja di kamar hotel atau Starbucks (kebanyakan di jalan)
    - Pertemuan tatap muka setiap dua minggu sekali.
    - Sebagian besar dokumen dipertukarkan melalui email
4. Hasil wawancara:
    - Alison (Presiden):
        - ➢ “Saya tidak tahu apa yang Jean bicarakan.”
        - ➢ “Saya tidak pernah meminta spreadsheet kepada Jean.”
        - ➢ “Saya tidak pernah menerima spreadsheet melalui email.”
    - Jean (CFO):
        - ➢ “Alison meminta saya untuk menyiapkan spreadsheet sebagai bagian dari putaran pendanaan baru.”
        - ➢ “Alison meminta saya untuk mengirimkan spreadsheet kepadanya melalui email.”
        - ➢ “Hanya itu yang saya tahu”

5. Akun Email:
    - Alison (President): alison@m57.biz ; password: "ab=8989
    - Jean (CFO): jean@m57.biz ; password: gick*121

Akuisisi:

sudah diberikan disk image berupa:

kemudian kita melakukan hashing untuk disk image tersebut

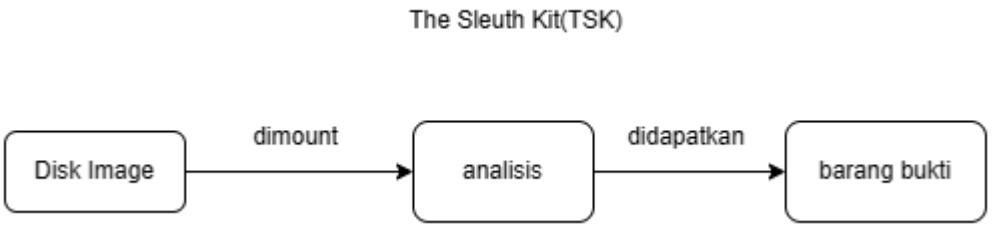


Tugas kami adalah mencari tahu bagaimana data tersebut bisa dicuri, apakah jean yang bersalah atas tersebarnya data, dan bagaimana langkah yang tepat untuk menghindari kasus pencurian seperti dalam skenario.

Pada skenario ini kami menggunakan SIFT WORKSTATION sebagai lingkungan kerja, dimana SIFT WORKSTATION ini merupakan kumpulan alat insiden respons dan forensik open source yang gratis yang dirancang untuk melakukan pemeriksaan forensik digital secara mendetail dalam berbagai pengaturan.SIFT menunjukkan bahwa kemampuan insiden respons tingkat lanjut dan teknik forensik digital yang mendalam dapat dilakukan dengan menggunakan alat open source yang tersedia secara gratis dan updated.

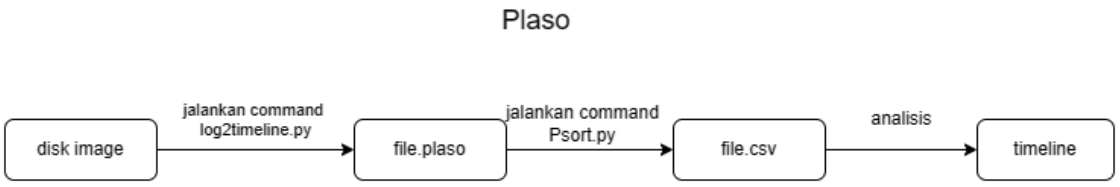
Tools yang akan kami gunakan dalam SIFT WORKSTATION adalah Plaso dan The Sleuth Kit (TSK). Plaso akan kami gunakan untuk event reconstruction berdasarkan timeline, sedangkan The Sleuth Kit (TSK) akan kami gunakan untuk melakukan mounting disk image sehingga dapat dilakukan proses analisis untuk mencari file-file yang dapat dijadikan bukti.

Skenario penggunaan tools:



- Melakukan mounting disk image agar disk image bisa dibuka

- Setelah disk image sudah dapat dibuka, kita akan melakukan analisis untuk menemukan barang bukti
- Mengumpulkan barang bukti yang didapat



- menjalankan log2timeline.py untuk mengumpulkan artefak dalam file.plaso
- menjalankan psort.py untuk mengekstrak informasi.
- melakukan analisis file.csv untuk rekonstruksi insiden

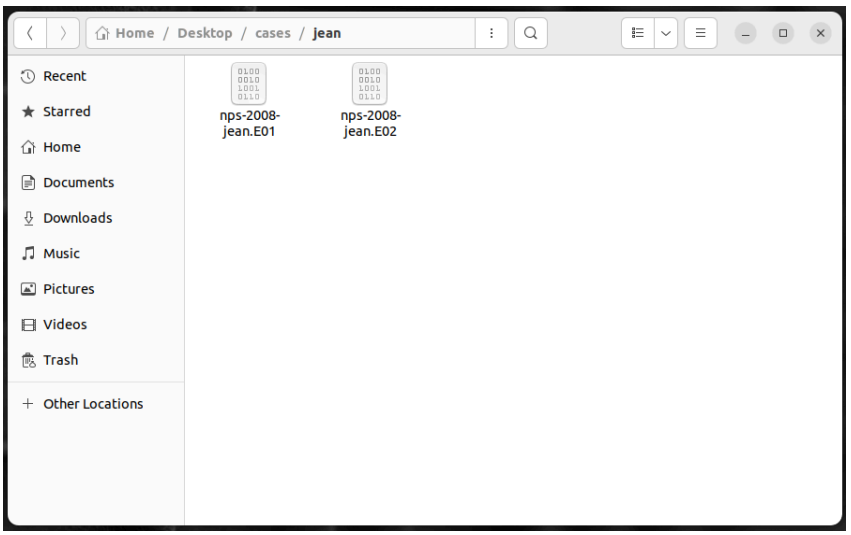
Spesifikasi perangkat keras laptop yang digunakan:
Laptop 1:
- Processor : 12th Gen intel i7-1200H
- GPU : Nvidia GeForce RTX 3050
- RAM : 16 GB
- OS : Windows 11
- VM : VirtualBox(versi 7.0)

Virtual Machine Ubuntu (plaso):
- Processor : Ryzen 5 3550H (4 Core)
- GPU : Nvidia GeForce GTX 1050 (Video Memory: 16MB)
- RAM : 4GB
- OS : Ubuntu 20.04.6 amd64
- VM : VirtualBox(versi 7.0)

Komputer 1
- Processor: 13th Gen Intel I7-13700KF
- GPU: Nvidia GeForce RTX 3060
- RAM: 32 GB
- OS: Windows 10 Home Edition
- VM: VMware Workstation

Penggunaan The Sleuth Kit(TSK)

1. **Siapkan file disk Image**



masukan disk image ke folder cases/jean agar mudah ditemukan.

2. Mount Disk Image

- **cd /cases/jean**
  - ❖ Perintah ini digunakan untuk berpindah direktori ke /cases/jean.

- **ls**

```
sansforensics@siftworkstation: /cases/jean
$ ls
nps-2008-jean.E01  nps-2008-jean.E02
```

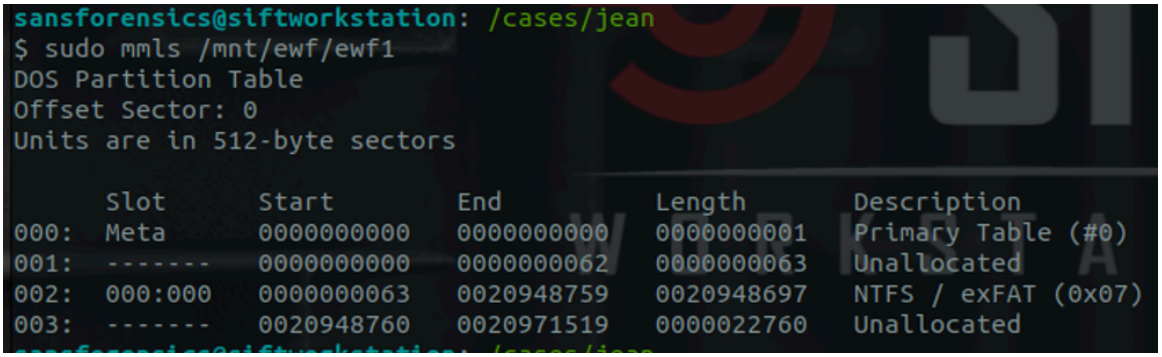
  - ❖ Perintah ini digunakan untuk menampilkan daftar file dan direktori yang ada di dalam direktori saat ini (/cases/jean).
  - ❖ Hasil outputnya menunjukkan dua file: nps-2008-jean.E01 dan nps-2008-jean.E02.

- **sudo ewfmount /cases/jean/nps-2008-jean.E01 /mnt/ewf**
  - ❖ Perintah ini menggunakan sudo untuk menjalankan “ewfmount” dengan hak akses superuser atau root.
  - ❖ ewfmount adalah alat yang digunakan untuk me-mount file EWF (Expert Witness Format), yang sering digunakan dalam kegiatan forensik digital.
  - ❖ File nps-2008-jean.E01 akan di-mount ke direktori /mnt/ewf.
- **sudo ls -l /mnt/ewf**

```
sansforensics@siftworkstation: /cases/jean
$ sudo ls -l /mnt/ewf
total 0
-r--r--r-- 1 root root 10737418240 May 14 13:22 ewf1
```

  - ❖ Perintah ini menampilkan daftar file di direktori /mnt/ewf dengan format yang lebih detail (long format) dan menggunakan sudo untuk memastikan hak akses superuser.
  - ❖ Hasil output menunjukkan file ewf1 dengan ukuran besar (10737418240 bytes).

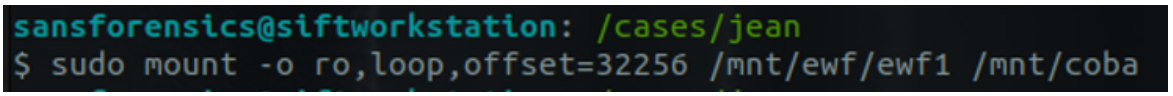
- **mmls /mnt/ewf/ewf1**



- ❖ Perintah ini menggunakan alat mmls untuk menampilkan tabel partisi dari file yang di-mount (/mnt/ewf/ewf1).

- ❖ Hasil output menunjukkan tabel partisi DOS dengan beberapa partisi:
  Slot 00: Primary Table
  Slot 01: Unallocated
  Slot 02: NTFS / exFAT
  Slot 03: Unallocated

- **sudo mount -o ro,loop,offset=32256 /mnt/ewf/ewf1 /mnt/coba**



- ❖ Perintah ini menggunakan sudo untuk menjalankan mount dengan hak akses superuser.

- ❖ Perintah ini akan me-mount file /mnt/ewf/ewf1 ke direktori /mnt/coba dengan opsi ro (read-only), loop, dan offset=32256.

- ❖ Opsi offset=32256 digunakan untuk mengatur offset byte di mana partisi NTFS / exFAT dimulai dalam file ewf1.

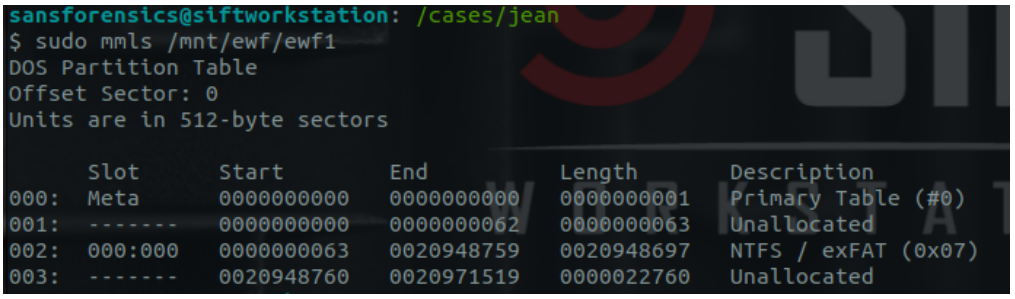
- ❖ '-0' Singkatan dari options. Opsi ini digunakan untuk menentukan parameter tambahan saat menjalankan perintah mount.

- ❖ 'ro' Singkatan dari read-only. Opsi ini mengindikasikan bahwa file sistem akan di-mount dalam mode hanya-baca. Ini berarti Anda tidak dapat melakukan perubahan apapun pada file sistem yang di-mount, yang sangat berguna dalam konteks forensik digital untuk mencegah modifikasi data.

- ❖ Opsi loop memberitahu mount untuk me-mount file sebagai perangkat loopback. Ini memungkinkan file gambar (image file) seperti EWF untuk diperlakukan sebagai perangkat blok (block device), yang memungkinkan file tersebut diakses seolah-olah merupakan perangkat fisik (seperti hard drive).

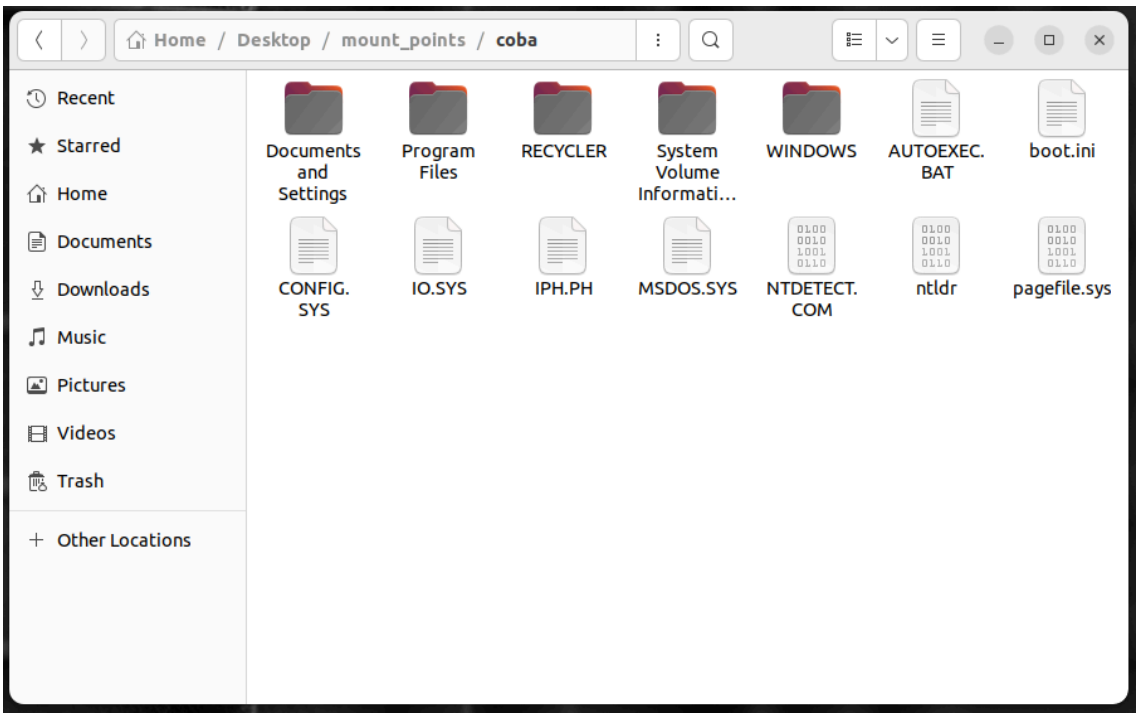
- Opsi ‘offset’ menentukan offset dalam byte dari mana partisi atau file sistem dimulai dalam file gambar. Dalam kasus ini, offset ditetapkan ke 32256 byte. Ini berarti proses mount akan melewati 32256 byte pertama dari file gambar ewf1 dan mulai membaca partisi dari posisi tersebut. Offset ini biasanya digunakan untuk me-mount partisi tertentu yang tidak dimulai dari awal file gambar.

- Berikut cara untuk menghitung ‘offset’
  rumus offset:
  Offset dalam Byte = Offset Sektor x Ukuran Sektor



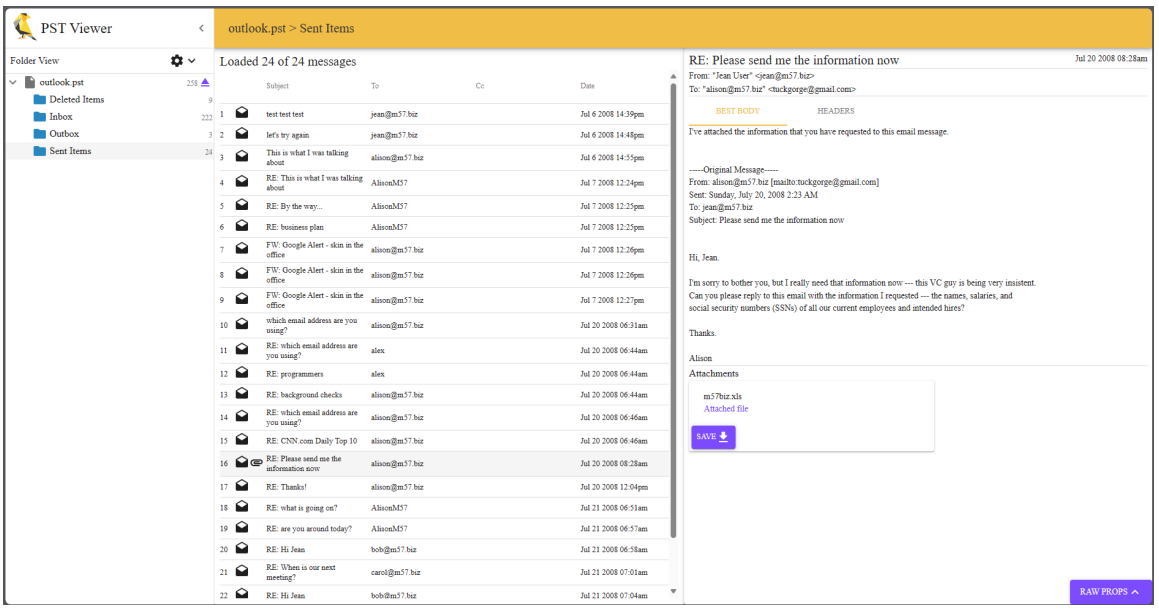
  - Ambil nilai Start dari partisi yang ingin di-mount: 63
  - Ukuran sektor: 512 byte
  - Hitung offset dalam byte:
    Offset dalam Byte = 63 sektor x 512 byte/sektor = 32256 byte

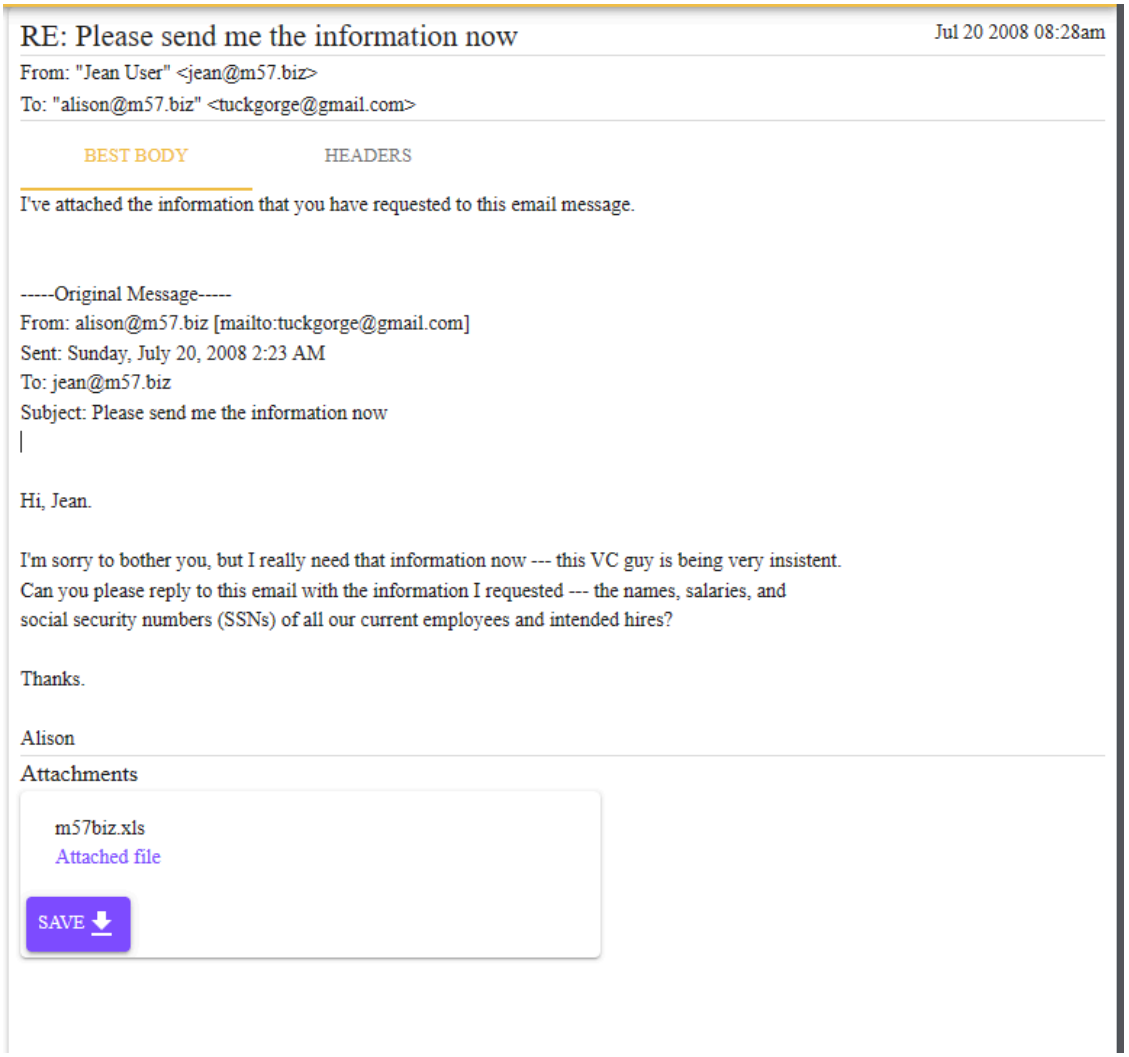
berikut adalah tampilan file yang sudah di mount dan siap untuk dilakukan analisis



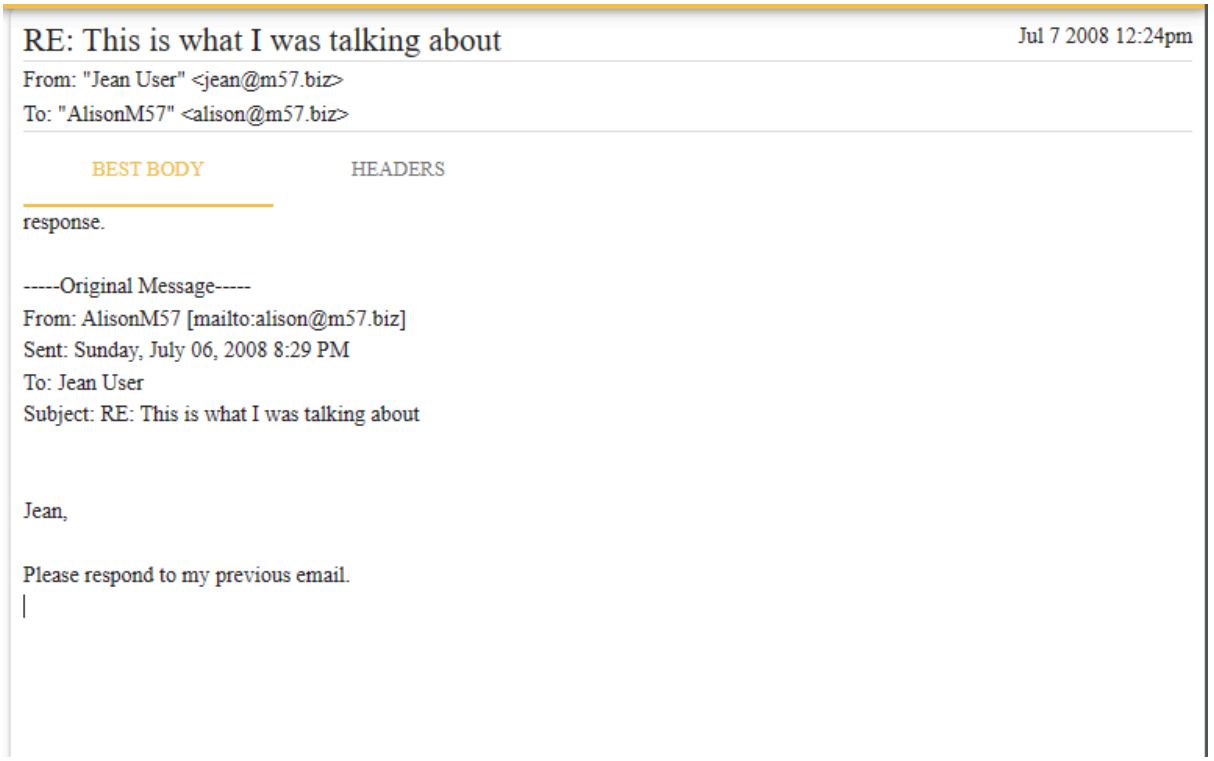
3. **Melakukan analisis terhadap disk yang sudah di-mount**
   setelah melakukan explorasi kami menemukan file outlook.pst pada folder: **mount_points/coba/Documents and Settings/Jean/Local Settings/Aplication Data/Microsoft/Outlook**

berikut tampilan outlook dari file outlook.pst kami menggunakan **pst online vewer** untuk menganalisis file outlook.pst



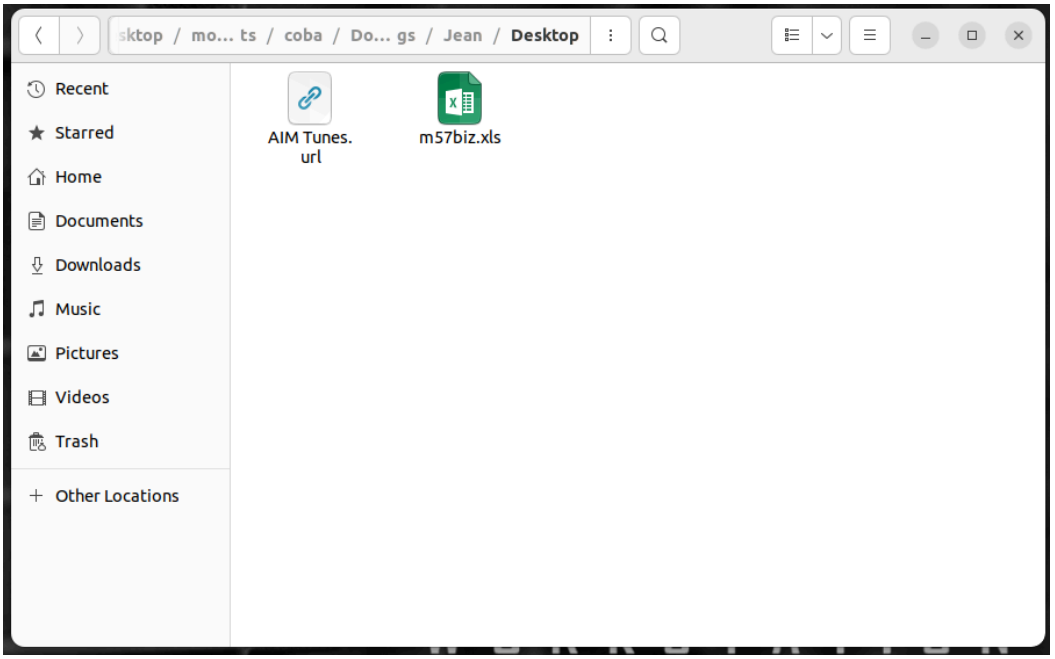


gambar di atas menunjukan adanya email phishing. Pengirim email menggunakan username dengan nama email dari alison yaitu alison@m57.biz padahal itu hanyalah username dari pengirim email bukan alamat emailnya. sedangkan alamat emailnya yaitu tuckgorge@gmail.com sehingga jean terkecoh hanya dengan melihat username nya saja, dia tidak memperhatikan alamat email nya sehingga jean secara tidak sadar mengirimkan file m57biz.xls kepada tuckgorge@gmail.com

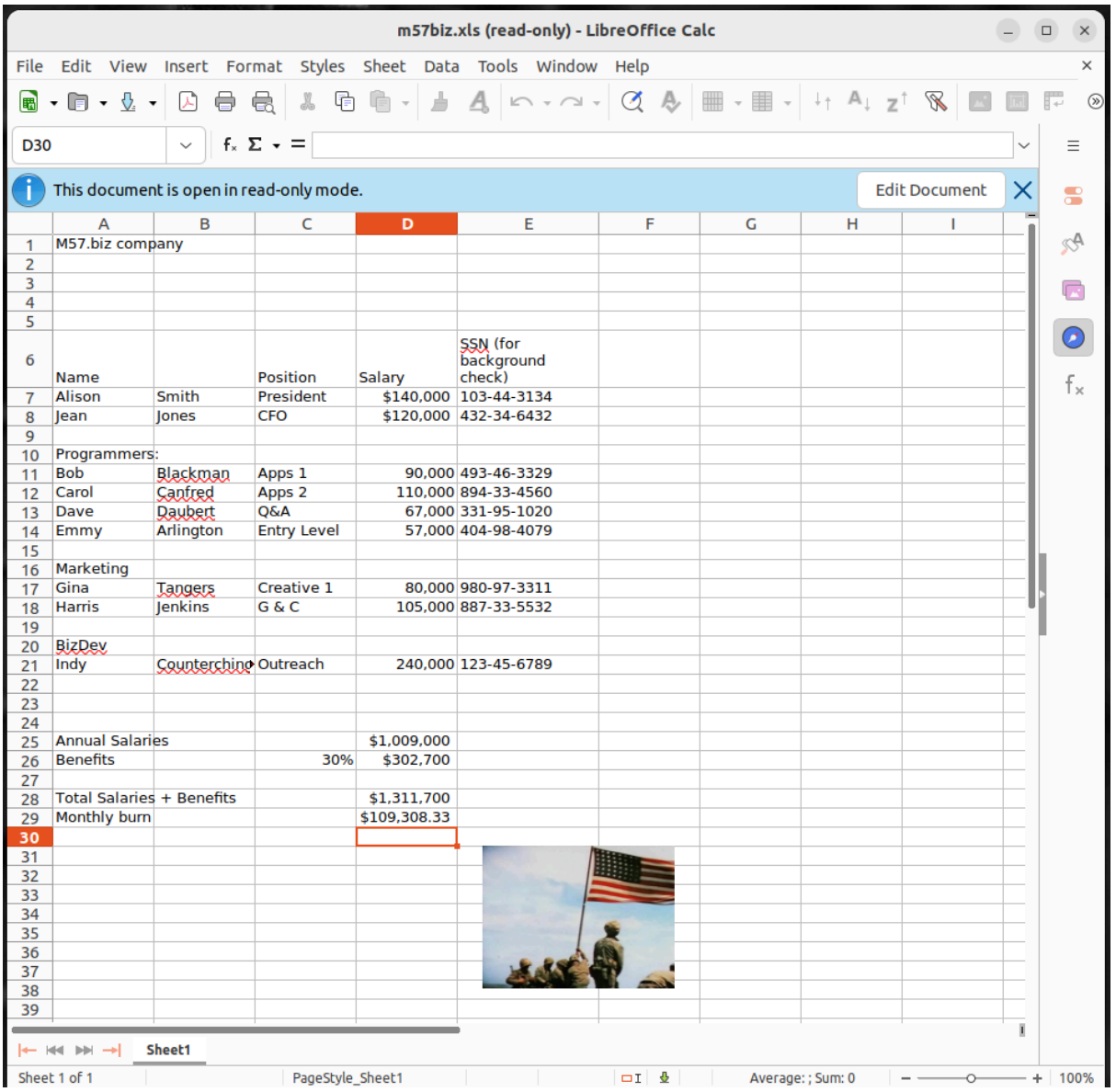


gambar di atas menunjukan username dan alamat email yang asli dari alison dengan username AlisonM57 dan alamat email alison@m57.biz

file spreadsheet ditemukan pada path: **mount_points/coba/Documents and Settings/Jean/Desktop**



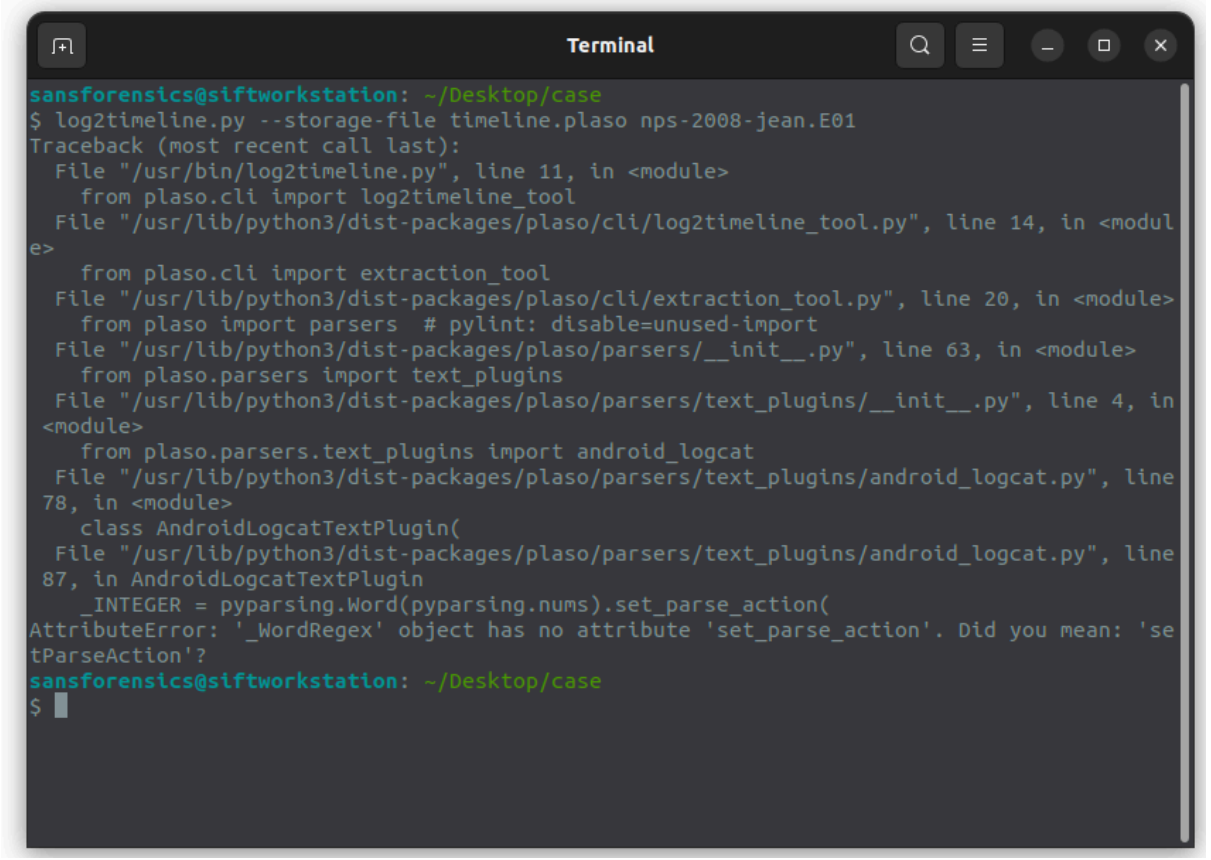
Berikut adalah isi dari file spreadseet-nya



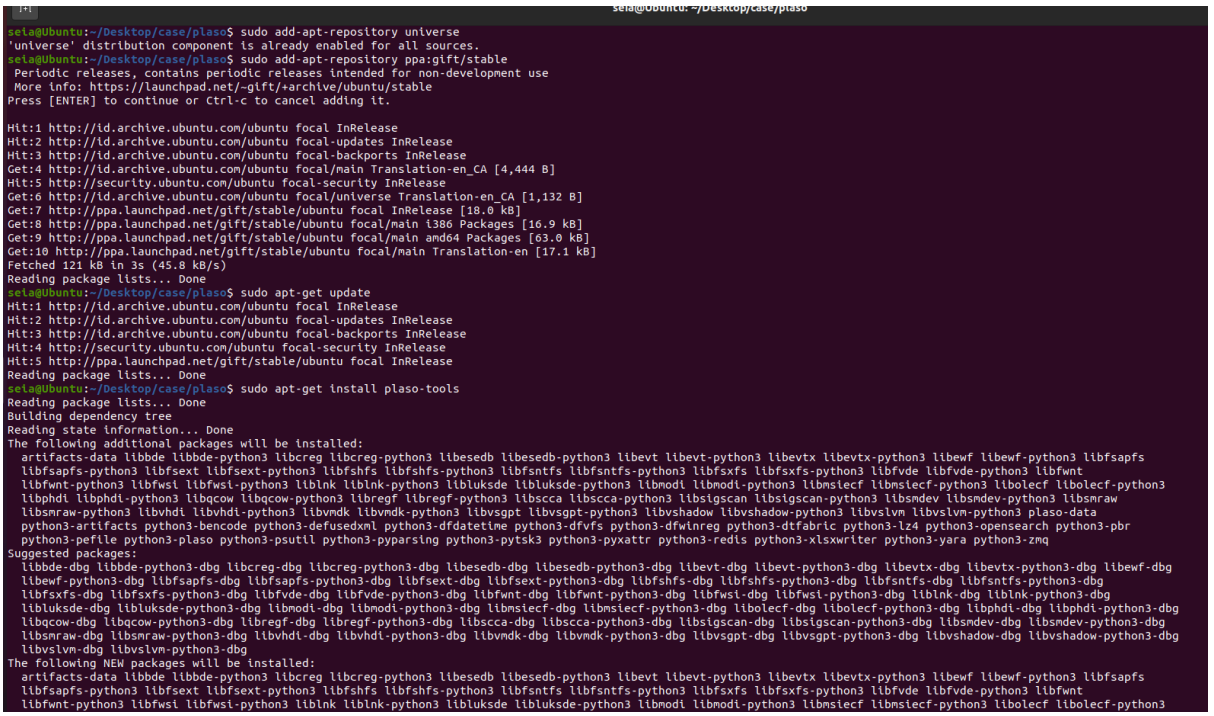
	A	B	C	D	E
1	M57.biz company				
2					
3					
4					
5					
6	Name		Position	Salary	SSN (for background check)
7	Alison	Smith	President	$140,000	103-44-3134
8	Jean	Jones	CFO	$120,000	432-34-6432
9					
10	Programmers:				
11	Bob	Blackman	Apps 1	90,000	493-46-3329
12	Carol	Canfred	Apps 2	110,000	894-33-4560
13	Dave	Daubert	Q&A	67,000	331-95-1020
14	Emmy	Arlington	Entry Level	57,000	404-98-4079
15					
16	Marketing				
17	Gina	Tangers	Creative 1	80,000	980-97-3311
18	Harris	Jenkins	G & C	105,000	887-33-5532
19					
20	BizDev				
21	Indy	Counterchino	Outreach	240,000	123-45-6789
22					
23					
24					
25	Annual Salaries			$1,009,000	
26	Benefits		30%	$302,700	
27					
28	Total Salaries + Benefits			$1,311,700	
29	Monthly burn			$109,308.33	
30					
31					
32					
33					
34					
35					
36					
37					
38					
39					

Penggunaan Plaso

Documentation : https://plaso.readthedocs.io



1. Install Plaso pada Ubuntu 20.04.6



Untuk melakukan penginstallan plaso pada ubuntu sang agen dapat mengikuti dokumentasi dari Plaso pada website berikut https://plaso.readthedocs.io/en/latest/sources/user/Ubuntu-Packaged-Release.html dan memerlukan sang agen untuk menambahkan repository universal dan Personal Package Archive(PPA) GIFT(Glorious Incident Feedback Tools) yang sesuai namanya berisikan package dari berbagai project yang berguna untuk proses *Incident Response* dan Digital Forensics dengan perintah:

- **`sudo add-apt-repository universe`**
- **`sudo add-apt-repository ppa:gift/stable`**

Setelah itu sang agen perlu menjalankan perintah "**`sudo apt-get update`**" untuk melakukan update file index package agar PPA yang baru saja ditambahkan dapat digunakan, dan setelahnya barulah sang agen dapat menginstall plaso pada OS Ubuntu dengan menggunakan perintah "**`sudo apt-get install plaso-tools`**".

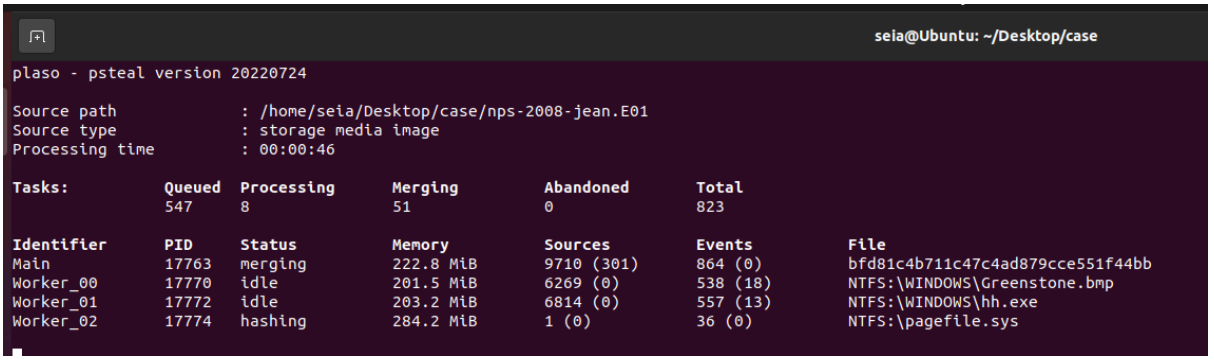
2. Proses

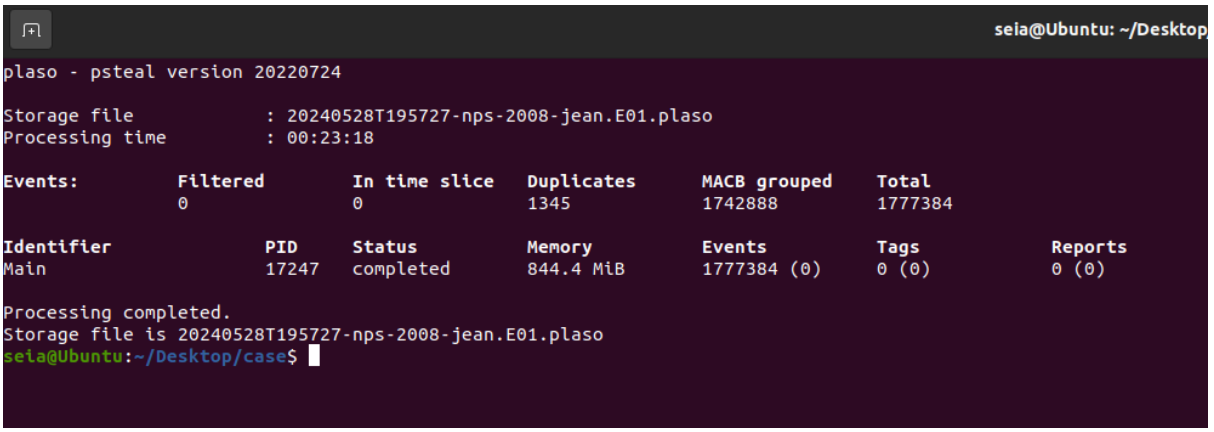
Mengikuti dokumentasi pembuatan timeline yang diberikan oleh plaso(https://plaso.readthedocs.io/en/latest/sources/user/Creating-a-timeline.html), terdapat 2 cara untuk membuat timeline menggunakan plaso yaitu:

- psteal
- log2timeline & psort

Dan disini sang agen dapat memilih diantara kedua opsi tersebut.

a. psteal

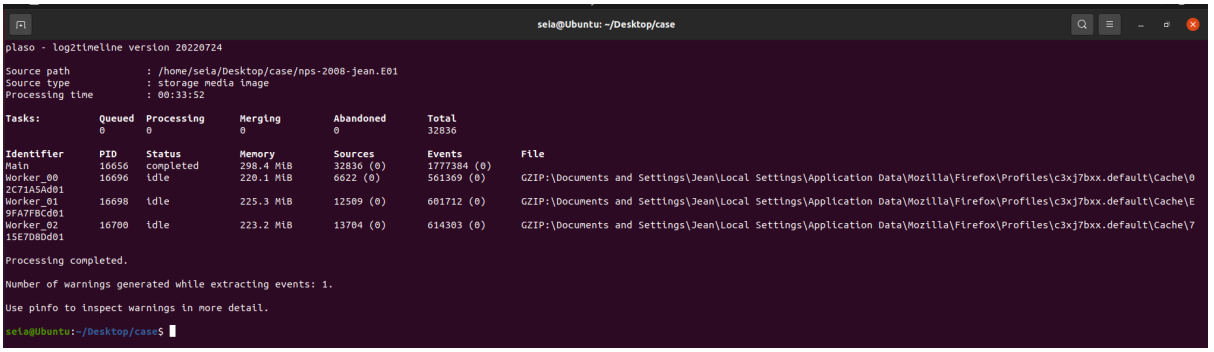


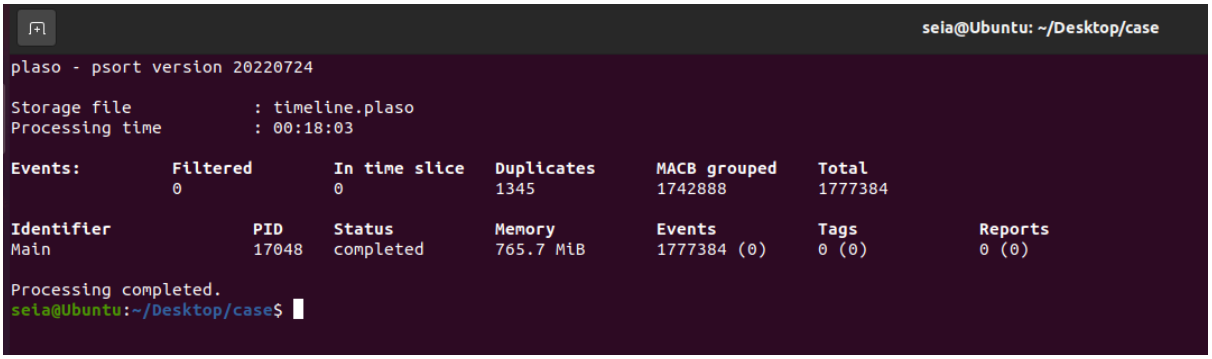


Untuk menggunakan psteal perintah yang perlu dijalankan adalah "**`psteal.py --source <image.raw> -o dynamic -w <registrar.csv>`**" dimana `<image.raw>` adalah file image yang ingin anda buatkan timeline-nya dan `<registrar.csv>` adalah file output yang berisikan data timeline-nya.

Running time dari metode ini adalah 28:40 + 23:18 = 51:58 (51 menit 58 detik), dimana waktu pembuatan file .plaso membutuhkan 28:40 sementara pembuatan file .csv membutuhkan 23:18

b. log2timeline & psort





Sementara itu untuk alternative-nya sang agen dapat memakai log2timeline.py dan psort.py dengan menjalankan kedua perintah dibawah ini:

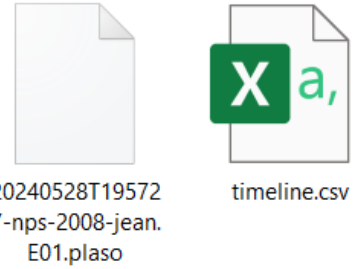
- **`log2timeline.py --storage-file <timeline.plaso> <image.raw>`**
- **`psort.py -o dynamic -w <registrar.csv> <timeline.plaso>`**

Yang dimana `<timeline.plaso>` pada log2timeline.py adalah nama file .plaso yang akan di outputkan dan `<image.raw>` adalah disk yang menjadi sumbernya dan demikian pula pada psort.py `<registrar.csv>` adalah file output yang berisikan list timeline dari semua file yang terdapat pada disk image yang telah dibuat menjadi `.plaso`, dan `<timeline.plaso>` adalah input yang akan menjadi sumber pembuatan file `.csv` nya

Running time dari metode yang satu ini adalh 33:52 + 10:03 = 43:55 (45 menit 55 detik) dan relatif lebih cepat dibanding psteal.py entah ini hanyalah kebetulan atau memanglah demikian, diluar daripada itu waktu yang dibutuhkan untuk membuat file `.plaso` ialah 33:52, sementara waktu pembuatan timeline.csv ialah 10:03

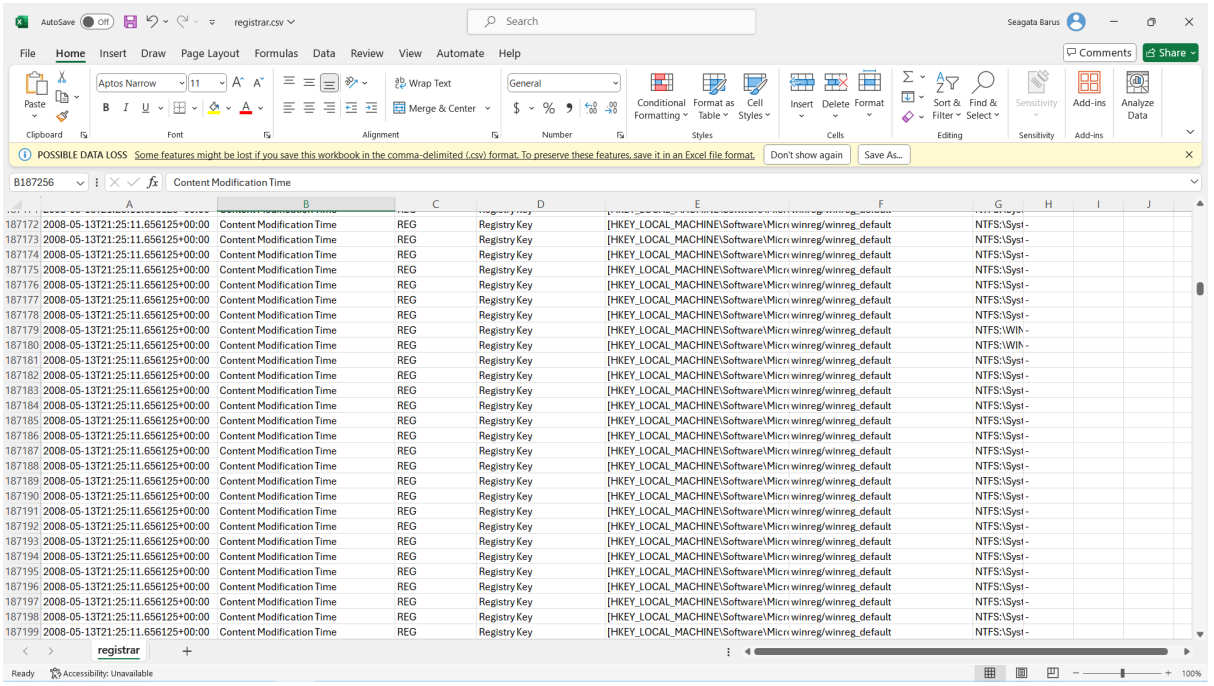
3. Hasil

Hasil output



Dengan ukuran 777,138,176 bytes (741 MB) untuk file `.plaso` dan 657,096,776 bytes(626 MB) untuk `timeline.csv`

Isi file timeline.csv



	A	B	C	D	E	F	G
187172	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187173	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187174	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187175	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187176	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187177	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187178	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187179	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\WIN -
187180	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\WIN -
187181	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187182	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187183	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187184	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187185	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187186	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187187	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187188	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187189	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187190	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187191	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187192	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187193	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187194	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187195	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187196	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187197	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187198	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -
187199	2008-05-13T21:25:11.656125+00:00	Content Modification Time	REG	Registry Key	[HKEY_LOCAL_MACHINE\Software\Micr	winreg/winreg_default	NTFS:\Syst -