

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:

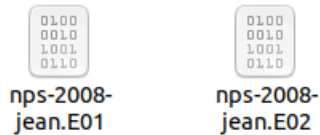
1. Fakta-fakta dari kasus ini:
 - Pendanaan tahap awal sebesar \$3 juta; sekarang menutup putaran pendanaan \$10 juta
 - 2 pendiri/pemilik
 - 10 karyawan dipekerjakan pada tahun pertama
2. Staf perusahaan:
 - President: Alison Smith
 - CFO: Jean
 - Programmer: Bob, Carole, David, & Emmy
 - Marketing: 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

```
Terminal
sansforensics@siftworkstation: ~
$ cd /cases/jean
sansforensics@siftworkstation: /cases/jean
$ ls
nps-2008-jean.E01  nps-2008-jean.E02
sansforensics@siftworkstation: /cases/jean
$ ewfverify nps-2008-jean.E01
ewfverify 20140816

Verify started at: May 28, 2024 13:08:07
This could take a while.

Status: at 5%.
verified 579 MiB (607223808 bytes) of total 10 GiB (10737418240 bytes).
completion in 1 minute(s) and 16 second(s) with 128 MiB/s (134217728 bytes/second)
.

Status: at 15%.
verified 1.6 GiB (1706164224 bytes) of total 10 GiB (10737418240 bytes).
completion in 45 second(s) with 193 MiB/s (202592796 bytes/second).

Status: at 21%.
verified 2.1 GiB (2287665152 bytes) of total 10 GiB (10737418240 bytes).
completion in 45 second(s) with 179 MiB/s (188375758 bytes/second).

Status: at 27%.
verified 2.7 GiB (2933129216 bytes) of total 10 GiB (10737418240 bytes).
completion in 43 second(s) with 173 MiB/s (181990139 bytes/second).

Status: at 42%.
```

```
Terminal
Status: at 49%.
verified 4.9 GiB (5297995776 bytes) of total 10 GiB (10737418240 bytes).
completion in 24 second(s) with 213 MiB/s (223696213 bytes/second).

Status: at 56%.
verified 5.6 GiB (6028754944 bytes) of total 10 GiB (10737418240 bytes).
completion in 22 second(s) with 204 MiB/s (214748364 bytes/second).

Status: at 63%.
verified 6.4 GiB (6868893696 bytes) of total 10 GiB (10737418240 bytes).
completion in 18 second(s) with 204 MiB/s (214748364 bytes/second).

Status: at 70%.
verified 7.0 GiB (7609581568 bytes) of total 10 GiB (10737418240 bytes).
completion in 15 second(s) with 200 MiB/s (210537612 bytes/second).

Status: at 92%.
verified 9.2 GiB (9904357376 bytes) of total 10 GiB (10737418240 bytes).
completion in 3 second(s) with 238 MiB/s (249707400 bytes/second).

Verify completed at: May 28, 2024 13:08:48
Read: 10 GiB (10737418240 bytes) in 41 second(s) with 249 MiB/s (261888249 bytes/second).

MD5 hash stored in file:          78a52b5bac78f4e711607707ac0e3f93
MD5 hash calculated over data:    78a52b5bac78f4e711607707ac0e3f93

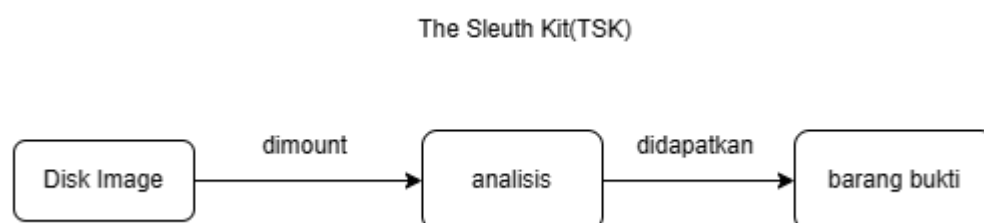
ewfverify: SUCCESS
sansforensics@siftworkstation: /cases/jean
$
```

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.

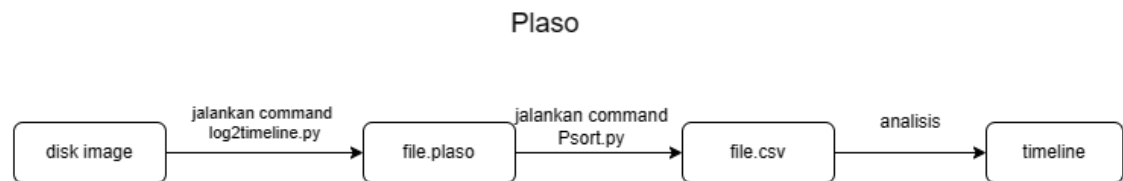
Tools yang akan kami gunakan dalam SIFT WORKSTATION adalah Plaso dan The Sleuth Kit (TSK). Plaso akan kami gunakan untuk event reconstruction berdasarkan timeline, sedangkan The Sleuth Kit (TSK) akan kami gunakan untuk melakukan mounting disk image sehingga dapat dilakukan proses analisis untuk mencari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

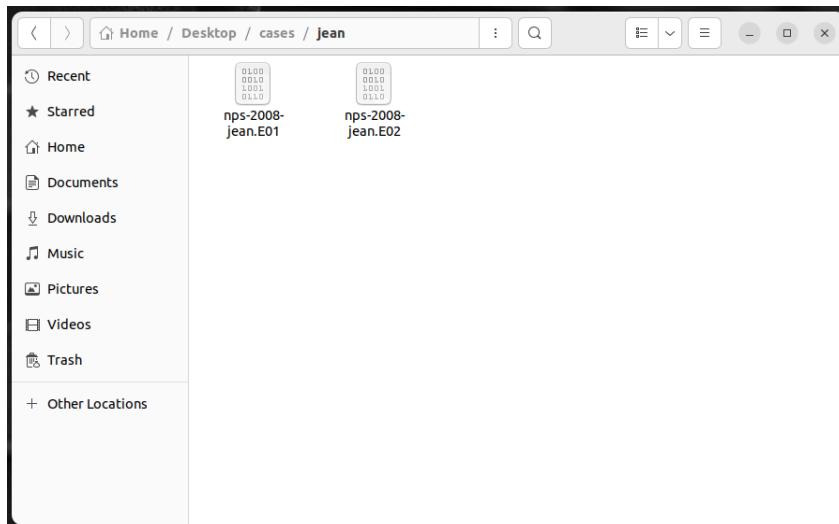
- Processor : Ryzen 5 3550H (4 Core)
- GPU : Nvidia GeForce GTX 1050 (Video Memory: 16MB)
- RAM : 4GB
- OS : Ubuntu 20.04.6 amd64
- VM : VirtualBox(versi 7.0)

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

```

Terminal
sansforensics@siftworkstation: ~
$ cd /cases/jean
sansforensics@siftworkstation: /cases/jean
$ ls
nps-2008-jean.E01  nps-2008-jean.E02
sansforensics@siftworkstation: /cases/jean
$ sudo ewfmount /cases/jean/nps-2008-jean.E01 /mnt/ewf
ewfmount 20140816

sansforensics@siftworkstation: /cases/jean
$ sudo ls -l /mnt/ewf
total 0
-r--r--r-- 1 root root 10737418240 May 14 13:22 ewf1
sansforensics@siftworkstation: /cases/jean
$ ls
nps-2008-jean.E01  nps-2008-jean.E02
sansforensics@siftworkstation: /cases/jean
$ ls /mnt/ewf
ls: cannot access '/mnt/ewf': Permission denied
sansforensics@siftworkstation: /cases/jean
$ sudo ls /mnt/ewf
ewf1
sansforensics@siftworkstation: /cases/jean
$ sudo mmls /mnt/ewf/ewf1
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

   Slot   Start      End      Length  Description
000:  Meta   0000000000  0000000000  0000000001 Primary Table (#0)
001:  -----  0000000000  0000000062  0000000063 Unallocated
002:  000:000  0000000063  0020948759  0020948697 NTFS / exFAT (0x07)
003:  -----  0020948760  0020971519  0000022760 Unallocated

sansforensics@siftworkstation: /cases/jean
$ sudo mount -o ro,loop,offset=32256 /mnt/ewf/ewf1 /mnt/coba
sansforensics@siftworkstation: /cases/jean
$
  
```

- **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).

- **mmis /mnt/ewf/ewf1**

```
sansforensics@siftworkstation: /cases/jean
$ sudo mmls /mnt/ewf/ewf1
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```

	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
001:	-----	0000000000	0000000062	0000000063	Unallocated
002:	000:000	0000000063	0020948759	0020948697	NTFS / exFAT (0x07)
003:	-----	0020948760	0020971519	0000022760	Unallocated

- ❖ 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**

```
sansforensics@siftworkstation: /cases/jean
$ 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.
- ❖ '-o' 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

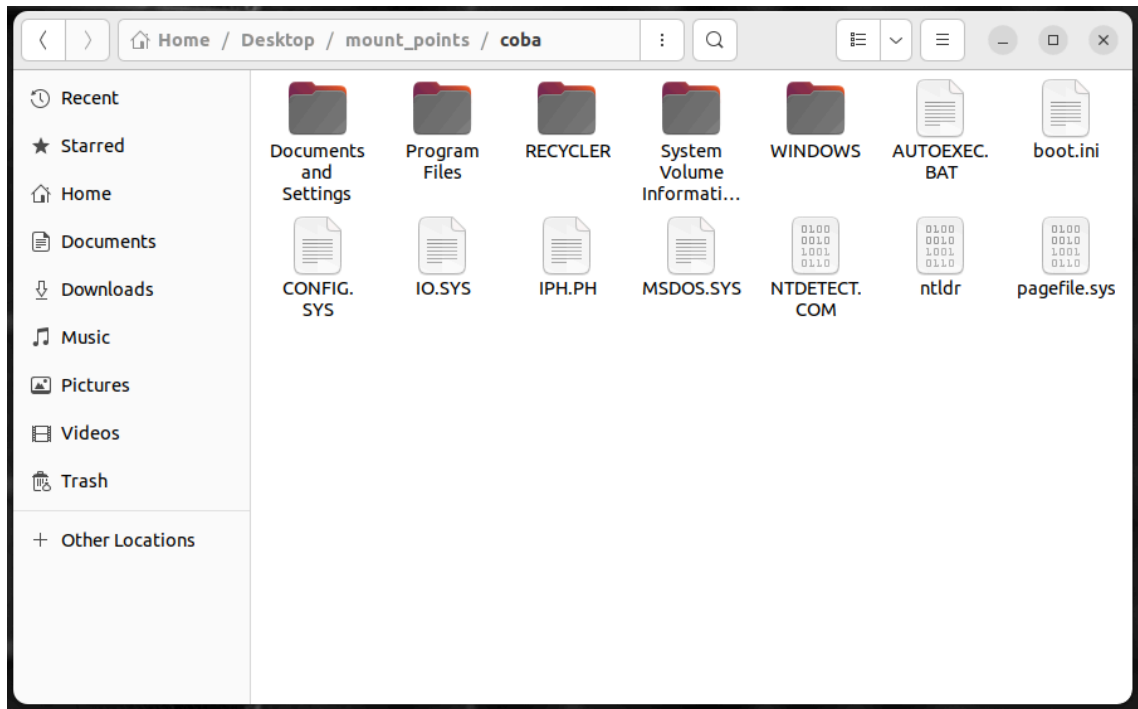
```
sansforensics@siftworkstation: /cases/jean
$ sudo mmls /mnt/ewf/ewf1
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```

	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
001:	-----	0000000000	0000000062	0000000063	Unallocated
002:	000:000	0000000063	0020948759	0020948697	NTFS / exFAT (0x07)
003:	-----	0020948760	0020971519	0000022760	Unallocated

- Ambil nilai Start dari partisi yang ingin di-mount: 63
- Ukuran sektor: 512 byte
- Hitung offset dalam byte:

$$\text{Offset dalam Byte} = 63 \text{ sektor} \times 512 \text{ byte/sektor} = 32256 \text{ byte}$$

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/Application Data/Microsoft/Outlook**

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

PST Viewer < outlook.pst > Sent Items

Folder View 258 ▲

- outlook.pst
 - Deleted Items 9
 - Inbox 222
 - Outbox 5
 - Sent Items 24

Loaded 24 of 24 messages

	Subject	To	Cc	Date
1	test test test	jean@ms57.biz		Jul 6 2008 14:39pm
2	let's try again	jean@ms57.biz		Jul 6 2008 14:48pm
3	This is what I was talking about	alice@ms57.biz		Jul 6 2008 14:55pm
4	RE: This is what I was talking about	Alice@M57		Jul 7 2008 12:24pm
5	RE: By the way...	Alice@M57		Jul 7 2008 12:25pm
6	RE: business plan	Alice@M57		Jul 7 2008 12:25pm
7	FW: Google Alert - skin in the office	alice@ms57.biz		Jul 7 2008 12:26pm
8	FW: Google Alert - skin in the office	alice@ms57.biz		Jul 7 2008 12:26pm
9	FW: Google Alert - skin in the office	alice@ms57.biz		Jul 7 2008 12:27pm
10	which email address are you using?	alice@ms57.biz		Jul 20 2008 06:31am
11	RE: which email address are you using?	alex		Jul 20 2008 06:44am
12	RE: programmers	alex		Jul 20 2008 06:44am
13	RE: background checks	alice@ms57.biz		Jul 20 2008 06:44am
14	RE: which email address are you using?	alice@ms57.biz		Jul 20 2008 06:46am
15	RE: CNN.com Daily Top 10	alice@ms57.biz		Jul 20 2008 06:46am
16	RE: Please send me the information now	alice@ms57.biz		Jul 20 2008 08:28am
17	RE: Thanks!	alice@ms57.biz		Jul 20 2008 12:04pm
18	RE: what is going on?	Alice@M57		Jul 21 2008 06:51am
19	RE: are you around today?	Alice@M57		Jul 21 2008 06:57am
20	RE: Hi Jean	bob@ms57.biz		Jul 21 2008 06:58am
21	RE: What is our next meeting?	carol@ms57.biz		Jul 21 2008 07:01am
22	RE: Hi Jean	bob@ms57.biz		Jul 21 2008 07:04am

RE: Please send me the information now Jul 20 2008 08:28am

From: "Jean User" <jean@ms57.biz>
To: "alice@ms57.biz" <tuckgore@gmail.com>

BEST BODY HEADERS

I've attached the information that you have requested to this email message.

-----Original Message-----
From: alice@ms57.biz [mailto:tuckgore@gmail.com]
Sent: Sunday, July 20, 2008 2:23 AM
To: jean@ms57.biz
Subject: Please send me the information now

Hi, Jean,

I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent. Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires?

Thanks.

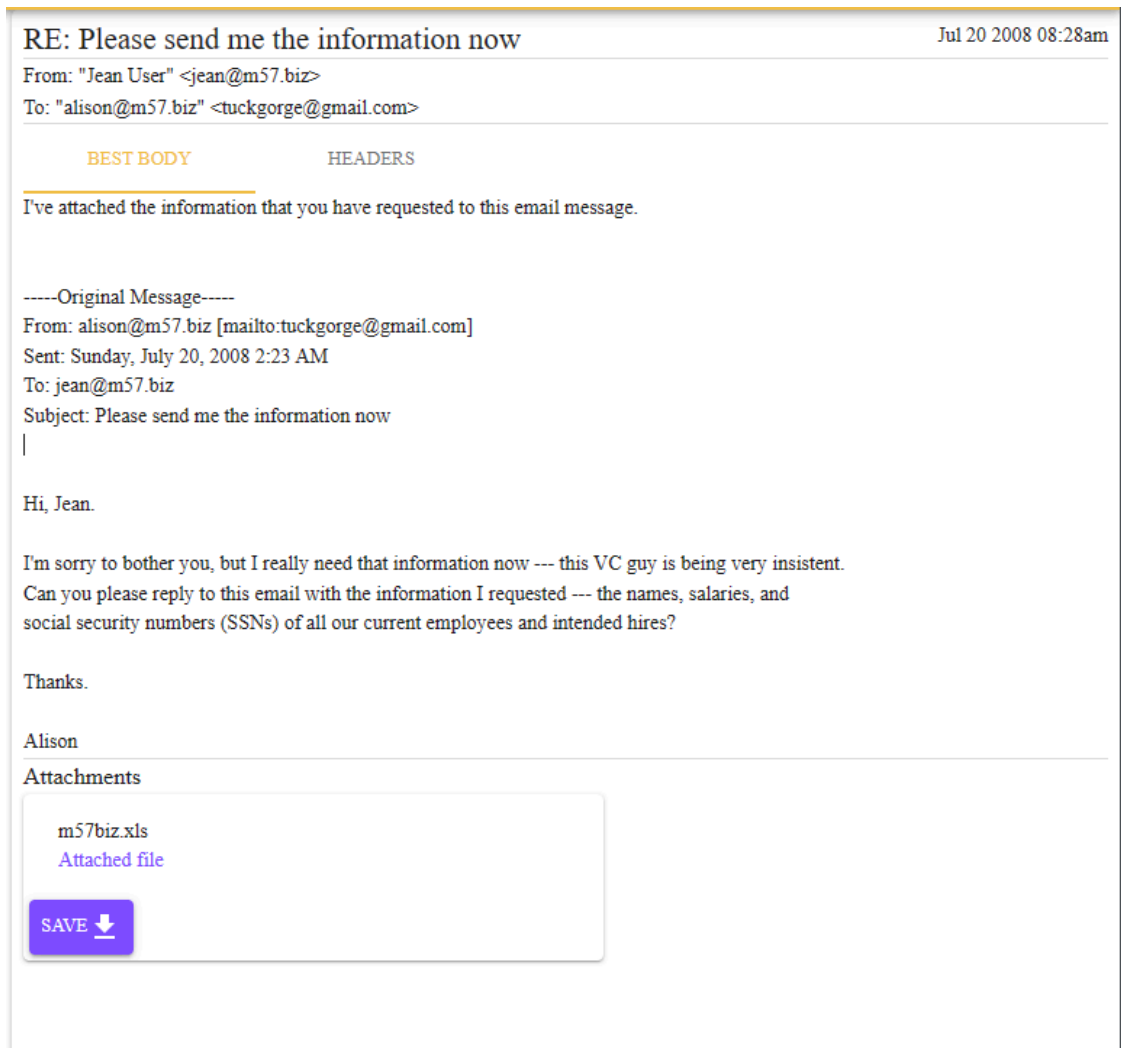
Alice

Attachments

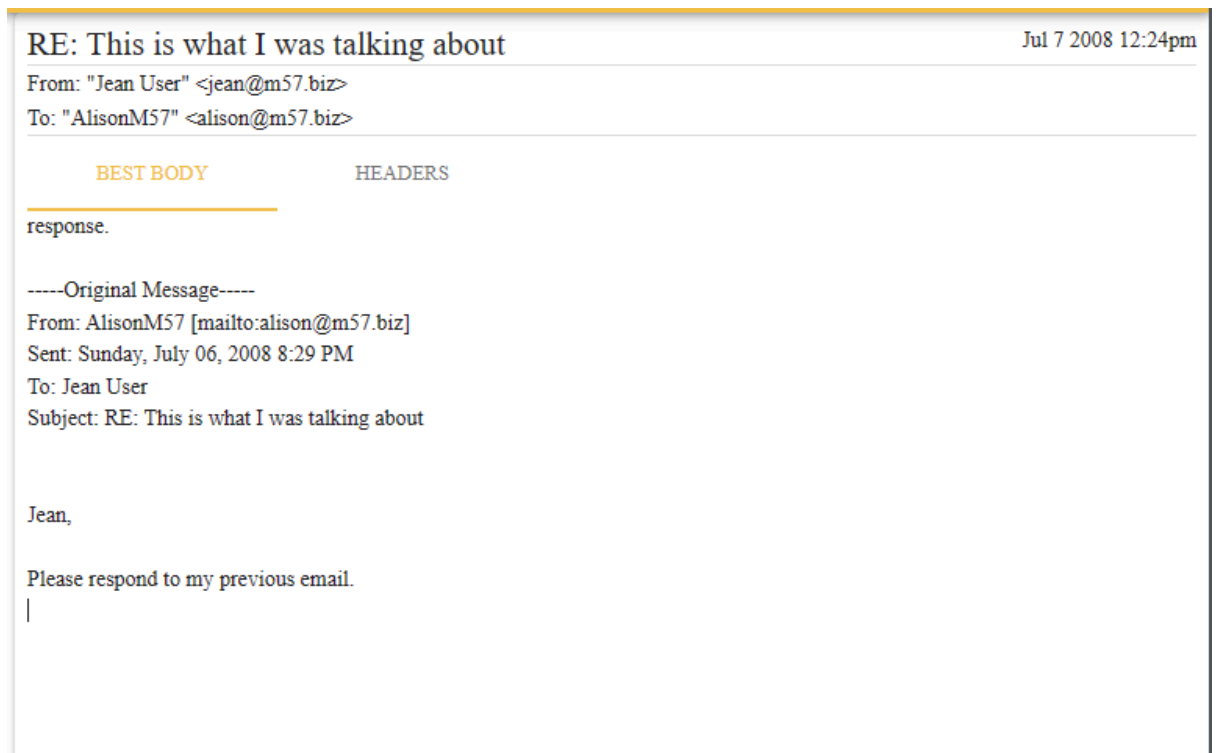
ms7hiz.xls
Attached file

SAVE

RAW PROPS

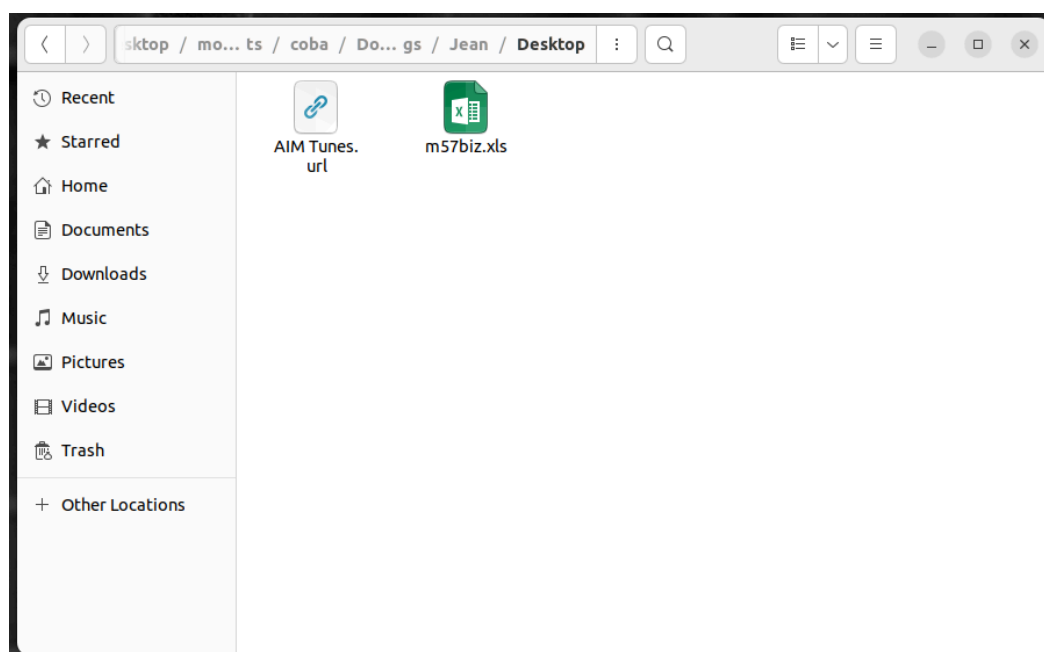


gambar di atas menunjukkan adanya email phishing. Pengirim email menggunakan username dengan nama email dari alison yaitu alison@m57.biz padahal itu hanyalah username dari pengirim email bukan alamat emailnya. sedangkan alamat emailnya yaitu tuckgorge@gmail.com sehingga jean terkecoh hanya dengan melihat 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 spreadsheet-nya

m57biz.xls (read-only) - LibreOffice Calc

File Edit View Insert Format Styles Sheet Data Tools Window Help

D30 f_x Σ =

This document is open in read-only mode. Edit Document

	A	B	C	D	E	F	G	H	I
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	Counterchiro	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									

Sheet1

Sheet 1 of 1 PageStyle_Sheet1 Average: ; Sum: 0 100%

Penggunaan Plaso

Documentation : <https://plaso.readthedocs.io>

```
Terminal
plaso - log2timeline version 20240308

Source path      : /cases/jean/nps-2008-jean.E01
Source type      : storage media image
Processing time   : 00:05:24

Tasks:
Queued 0 Processing 1 Merging 0 Abandoned 1 Total 2

Identifier PID Status Memory Sources Event Data File
Main 6290 completed 250.9 MiB 1 (0) 0 (0)
Worker_00 6294 aborted 177.2 MiB 0 (0) 0 (0) NTFS:\
Worker_01 6296 aborted 177.2 MiB 0 (0) 0 (0) NTFS:\
Worker_02 6298 idle 174.1 MiB 0 (0) 0 (0)
Worker_03 6304 idle 175.2 MiB 0 (0) 0 (0)
Worker_04 6306 idle 175.2 MiB 0 (0) 0 (0)
Worker_05 6315 idle 224.2 MiB 0 (0) 0 (0)

Traceback (most recent call last):
  File "/usr/bin/log2timeline.py", line 103, in <module>
    if not Main():
  File "/usr/bin/log2timeline.py", line 77, in Main
    tool.ExtractEventsFromSources()
  File "/home/sansforensics/.local/lib/python3.10/site-packages/plaso/cli/extraction_tool.py", line 754, in ExtractEventsFromSources
    processing_status = self._ProcessSource(session, storage_writer)
  File "/home/sansforensics/.local/lib/python3.10/site-packages/plaso/cli/extraction_tool.py", line 555, in _ProcessSource
    storage_writer.UpdateAttributeContainer(session)
  File "/home/sansforensics/.local/lib/python3.10/site-packages/plaso/storage/writer.py", line 218, in UpdateAttributeContainer
    self._store.UpdateAttributeContainer(container)
  File "/home/sansforensics/.local/lib/python3.10/site-packages/acstore/interface.py", line 226, in UpdateAttributeContainer
    self._WriteExistingAttributeContainer(container)
  File "/home/sansforensics/.local/lib/python3.10/site-packages/plaso/storage/sqlite/sqlite_file.py", line 304, in _WriteExistingAttributeContainer
    elif data_type not in self._CONTAINER_SCHEMA_TO_SQLITE_TYPE_MAPPINGS:
AttributeError: 'SQLiteStorageFile' object has no attribute '_CONTAINER_SCHEMA_TO_SQLITE_TYPE_MAPPINGS'
sansforensics@siftworkstation: /cases/jean
$
```

```
Terminal
sansforensics@siftworkstation: ~/Desktop/case
$ log2timeline.py --storage-file timeline.plaso nps-2008-jean.E01
Traceback (most recent call last):
  File "/usr/bin/log2timeline.py", line 11, in <module>
    from plaso.cli import log2timeline_tool
  File "/usr/lib/python3/dist-packages/plaso/cli/log2timeline_tool.py", line 14, in <module>
    from plaso.cli import extraction_tool
  File "/usr/lib/python3/dist-packages/plaso/cli/extraction_tool.py", line 20, in <module>
    from plaso import parsers # pylint: disable=unused-import
  File "/usr/lib/python3/dist-packages/plaso/parsers/__init__.py", line 63, in <module>
    from plaso.parsers import text_plugins
  File "/usr/lib/python3/dist-packages/plaso/parsers/text_plugins/__init__.py", line 4, in <module>
    from plaso.parsers.text_plugins import android_logcat
  File "/usr/lib/python3/dist-packages/plaso/parsers/text_plugins/android_logcat.py", line 78, in <module>
    class AndroidLogcatTextPlugin(
  File "/usr/lib/python3/dist-packages/plaso/parsers/text_plugins/android_logcat.py", line 87, in AndroidLogcatTextPlugin
    _INTEGER = pyparsing.Word(pyparsing.nums).set_parse_action(
AttributeError: '_WordRegex' object has no attribute 'set_parse_action'. Did you mean: 'setParseAction'?
sansforensics@siftworkstation: ~/Desktop/case
$
```

Dan disini sang agen dapat memilih diantara kedua opsi tersebut.

a. psteal

```
sela@Ubuntu: ~/Desktop/case
plaso - psteal version 20220724

Source path      : /home/sela/Desktop/case/nps-2008-jean.E01
Source type      : storage media image
Processing time   : 00:00:46

Tasks:           Queued  Processing  Merging  Abandoned  Total
                547      8             51         0           823

Identifier      PID      Status    Memory    Sources    Events    File
Main            17763   merging  222.8 MiB  9710 (301)  864 (0)   bfd81c4b711c47c4ad879cce551f44bb
Worker_00       17770   idle     201.5 MiB  6269 (0)   538 (18)  NTFS:\WINDOWS\Greenstone.bmp
Worker_01       17772   idle     203.2 MiB  6814 (0)   557 (13)  NTFS:\WINDOWS\hh.exe
Worker_02       17774   hashing  284.2 MiB  1 (0)      36 (0)    NTFS:\pagefile.sys

sela@Ubuntu: ~/Desktop/case$

plaso - psteal version 20220724

Storage file      : 20240528T195727-nps-2008-jean.E01.plaso
Processing time    : 00:23:18

Events:           Filtered  In time slice  Duplicates  MACB grouped  Total
                0           0             1345        1742888       1777384

Identifier      PID      Status    Memory    Events    Tags    Reports
Main            17247   completed  844.4 MiB  1777384 (0)  0 (0)   0 (0)

Processing completed.
Storage file is 20240528T195727-nps-2008-jean.E01.plaso
sela@Ubuntu:~/Desktop/case$
```

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 buat 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

```
sela@Ubuntu: ~/Desktop/case
plaso - log2timeline version 20220724

Source path      : /home/sela/Desktop/case/nps-2008-jean.E01
Source type      : storage media image
Processing time   : 00:33:52

Tasks:           Queued  Processing  Merging  Abandoned  Total
                0           0             0         0          32836

Identifier      PID      Status    Memory    Sources    Events    File
Main            16056   completed  290.4 MiB  32836 (0)  1777384 (0)  GZIP:\Documents and Settings\Jean\Local Settings\Application Data\Mozilla\Firefox\Profiles\c3xj7bxx.default\Cache\0
2C7IASAd01      16096   idle     220.1 MiB  6622 (0)   561369 (0)   GZIP:\Documents and Settings\Jean\Local Settings\Application Data\Mozilla\Firefox\Profiles\c3xj7bxx.default\Cache\E
9FATERC001      16098   idle     225.3 MiB  12509 (0)  601712 (0)   GZIP:\Documents and Settings\Jean\Local Settings\Application Data\Mozilla\Firefox\Profiles\c3xj7bxx.default\Cache\7
15E70BDd01      16700   idle     223.2 MiB  13704 (0)  614303 (0)   GZIP:\Documents and Settings\Jean\Local Settings\Application Data\Mozilla\Firefox\Profiles\c3xj7bxx.default\Cache\7

Processing completed.

Number of warnings generated while extracting events: 1.
Use pinfo to inspect warnings in more detail.
sela@Ubuntu:~/Desktop/case$
```

```
seia@Ubuntu: ~/Desktop/case
plaso - psort version 20220724
Storage file      : timeline.plaso
Processing time   : 00:18:03

Events:           Filtered      In time slice  Duplicates  MACB grouped  Total
                  0              0              1345         1742888       1777384

Identifier        PID      Status      Memory      Events      Tags      Reports
Main              17048    completed  765.7 MiB   1777384 (0)  0 (0)     0 (0)

Processing completed.
seia@Ubuntu:~/Desktop/case$
```

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

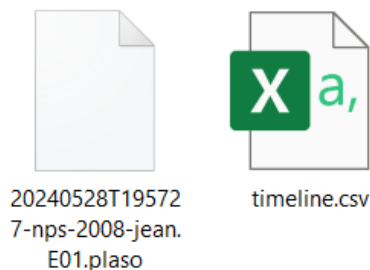
- `log2timeline.py --storage-file <timeline.plaso> <image.raw>`
- `psort.py -o dynamic -w <registrar.csv> <timeline.plaso>`

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 adalah $33:52 + 10:03 = 43:55$ (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

AutoSaveOFF

registrar.csv

Search

Seagata Barus

FileHomeInsertDrawPage LayoutFormulasDataReviewViewAutomateHelp

Paste

Aptos Narrow11A⁺A⁺

Clipboard

Font

Alignment

Number

Wrap Text

Merge & Center

General

Conditional Formatting

Format as Table

Cell Styles

Insert

Delete

Format

Σ

Sort & Filter

Find & Select

Sensitivity

Add-ins

Analyze Data

POSSIBLE DATA LOSS

Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format.

Don't show again

Save As...

8187256

Content Modification Time

A

B

C

D

E

F

G

H

I

J

187172

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187173

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187174

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187175

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187176

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187177

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187178

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187179

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\WiH-

187180

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\WiH-

187181

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187182

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187183

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187184

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187185

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187186

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187187

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187188

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187189

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187190

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187191

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187192

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187193

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187194

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187195

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187196

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187197

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187198

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

187199

2008-05-13T21:25:11.656125+00:00

Content Modification Time

REG

Registry Key

[HKEY_LOCAL_MACHINE\Software\Micri winreg\winreg_default

NTFS:\Syst-

<

>

registrar

+

Ready

Accessibility: Unavailable

100%