

## DIGITAL FORENSIC

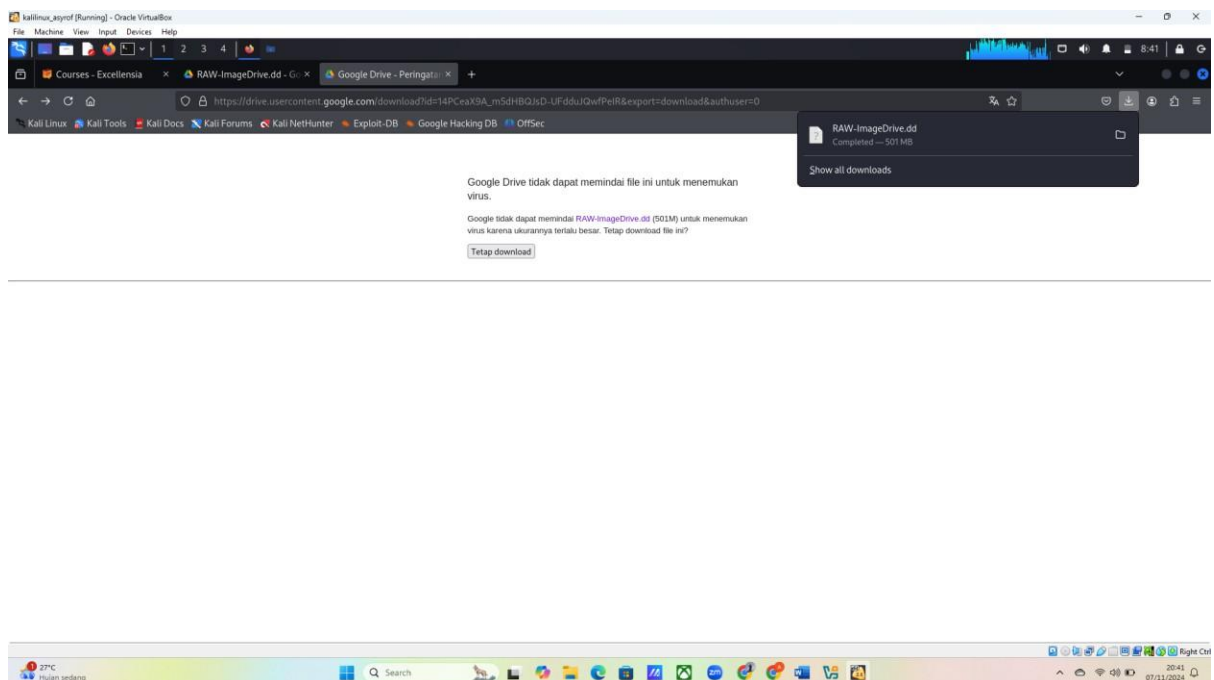
1. Gunakan beberapa Tools Forensik dibawah ini untuk melakukan Analisa image penyimpanan file File RAW-ImageDrive.dd ( Download di <https://s.id/imageforensic> )
  - tsk\_recovery
  - foremost
  - dmde
  - autopsy
  - ftk imager
2. Sebutkan jumlah dan kategori file terhapus yang anda dapat recovery dari file image no.1
3. Tools apa saja yang berhasil melakukan recovery file video dalam file percobaan anda ? (Tunjukkan dengan screenshot hasil)
4. Tools apa saja yang berhasil melakukan recovery file Gambar (JPG) dalam percobaan anda (Tunjukkan dengan screenshot hasil)

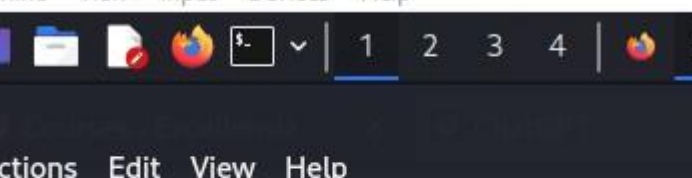
Terangkan dengan tables hasil dari penggunaan tools tools diatas.

Jawab :

- Tool tsk\_recover :

Pertama download file RAW-ImageDrive.dd :





The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. The terminal window displays the following commands and output:

```
File Actions Edit View Help
zsh: corrupt history file /home/asyrof/.zsh_history
(asyrof@asyrof)-[~]
$ sudo su
[sudo] password for asyrof:
(root@asyrof)-[/home/asyrof]
# mkdir tugas9

(root@asyrof)-[/home/asyrof]
# cd tugas9
```

The screenshot shows a Kali Linux virtual machine running Oracle VM VirtualBox. The terminal window displays the following commands and output:

```

root@asyrof:~/home/asyrof
File Actions Edit View Help
zsh: corrupt history file /home/asyrof/.zsh_history
root@asyrof:~# cat /dev/urandom tr -dc 'a-z0-9' | fold -w 64 | xargs -n 1 shuf -e | paste -s -d ':' - | xargs echo
[sudo] password for asyrof:
root@asyrof:~# apt install task_recover
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package task_recover

root@asyrof:~# apt install leuthit
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
leuthit is already the newest version (4.12-1dfsg-akali6).
The following packages were automatically installed and are no longer required:
fonts-liberation2 libcephfs2 libgdx90 liblua5.2-0 libpython3.11-dev libqt6opengl6t64 librados2 libwasutil5t64 python3-lib2to3 python3.11-dev
freeresp2-ssl1 libfreeresp-client2-2t64 libglasters10 libeaf1 libpython3.11-minimal libqt6openglwidgets6t64 libssh-crypt-4 python3-paho-mqttc python3.11-minimal
libarmadillo12 libfreeresp2-t64 libgmp12-3 libpython3.11-stdlib libqtspeech6t64 libswscale7 openjdk-17-jre libpython3-pluggy who
libarmadillo12 libgmp12t64 liblcm40320 libpython3.11t64 libqt6qt6t64 libswscale6 openjdk-17-jre-headless python3-rsa whois
libavfilter9 libgmp5-12 libbinparser1 libplist1 libqt6dbus6t64 libqt6test6t64 libwinpr2-2t64 python3-hatch-vcx python3-setuptools-scm samba-vfs-modules
libavformat58 libgmp10 libbjlmb.82t64 libboppler124 libqt6gui6t64 libwireshark17t64 python3-hatchling python3-trove-classifiers
libblosc2-2 libgmpc8 libbjlsoncp25 libbostproc37 libqt6network6t64 libqt6xml6t64 libwireshark17t64 python3-jose python3.11

Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2

root@asyrof:~# apt search task_recover
root@asyrof:~#

```

```
(root@asyrof)~[/home/asyrof/Downloads]
# mkdir tugas9

(root@asyrof)~[/home/asyrof/Downloads]
# cd tugas9
```

## Memindahkan disk image

```
(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# mv ../RAW-ImageDrive.dd .
```

Memastikan file direktori

```
(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# ls -al

total 513036
drwxr-xr-x 2 root root 4096 Nov 7 09:32 .
drwxr-xr-x 3 asyrof asyrof 4096 Nov 7 09:32 ..
-rw-rw-r-- 1 asyrof asyrof 525336576 Nov 7 08:41 RAW-ImageDrive.dd

(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# ls
RAW-ImageDrive.dd
```

Membuat direktori output untuk hasil pemulihan

```
(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# mkdir RECOVER-BY-TSK

(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# ls
RAW-ImageDrive.dd RECOVER-BY-TSK
```

File yang terecovery :

```
(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# tsk_recover RAW-ImageDrive.dd RECOVER_BY_TSK
Files Recovered: 8
```

Melihat output recover apakah sudah tersimpan

```
(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# cd RECOVER_BY_TSK

(root@asyrof)-[/home/asyrof/Downloads/tugas9/RECOVER_BY_TSK]
# ls -al

total 66180
drwxr-xr-x 4 root root 4096 Nov 7 09:40 .
drwxr-xr-x 4 root root 4096 Nov 7 09:40 ..
-rw-r--r-- 1 root root 60000261 Nov 7 09:40 'Cyber Crisis Management at EU Level_HD.mp4'
drwxr-xr-x 2 root root 4096 Nov 7 09:40 'Foto-CyberCrisis Management'
drwxr-xr-x 2 root root 4096 Nov 7 09:40 'FotoBSSN-Digital Forensik'
-rw-r--r-- 1 root root 7747842 Nov 7 09:40 'Practical Forensic Imaging - Securing Digital Evidence with Linux Tool'
```

➤ Tool foremost :

Install foremost :

```
(root@asyrof) ~/home/asyrof
# apt install foremost
The following packages were automatically installed and are no longer required:
fonts-liberation2 libcephfs2 libgxfdr0 liblua5.2-0 libpython3.11-dev libqt6opengl6t64 librados2 libwsutil15t64 python3-lib2to3 python3.11-dev
freerdp-x11 libfreerdp-client2-2t64 libgusterfs0 libmf4 libpython3.11-minimal libqt6openglwidgets6t64 libssh-gcrypt-4 libzstd1t64 python3-pathspec python3.11-minimal
libasound2 libfreerdp2-2t64 libgustt3-3 libpython3.11-stdlib libqt6printsupport6t64 libssm-gcrypt-4 libzstd1t64 python3-pluggy python3.11-minimal
libassuan0 libgda34t64 libmobiledevice6 liblacebo338 libpython3.11t64 libqt6sql6t64 libusbmuxd6 openjdk-17-jre-headless python3-rsa python3.11-minimal
libavfilter9 libgost12t2 liblisp4 liblisp4 libqt6dbus6t64 libqt6gui6t64 libqt6widgets6t64 libwacom2-2t64 python3-hatch-vcs python3-setuptools-scm python3.11-minimal
libavformat9 libgpg10 liblisp4 liblisp4 libqt6gui6t64 libqt6widgets6t64 libwacom2-2t64 python3-hatch-vcs python3-setuptools-scm python3.11-minimal
libblosc2-3 libgprc0 libjsncpp25 libpostproc57 libqt6network6t64 libqt6xml6t64 libwiretap14t64 python3-jose python3.11-minimal
Use 'sudo apt autoremove' to remove them.

Installing:
foremost

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 2
Download size: 42.5 kB
Space needed: 104 kB / 32.1 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 foremost amd64 1.5.7-11+b2 [42.5 kB]
Fetched 42.5 kB in 2s (20.0 kB/s)
Selecting previously unselected package foremost.
(Reading database ... 438144 files and directories currently installed.)
Preparing to unpack .../foremost_1.5.7-11+b2_amd64.deb ...
Unpacking foremost (1.5.7-11+b2) ...
Setting up foremost (1.5.7-11+b2) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.3.1) ...

(root@asyrof) ~/home/asyrof
```

Membuat folder untuk jenis file yang berbeda :

```
(root@asyrof) ~/home/asyrof/Downloads/tugas9
# mkdir FOREMOST_JPG

(root@asyrof) ~/home/asyrof/Downloads/tugas9
# mkdir FOREMOST_MP4

(root@asyrof) ~/home/asyrof/Downloads/tugas9
# mkdir FOREMOST_PNG

(root@asyrof) ~/home/asyrof/Downloads/tugas9
# mkdir FOREMOST_PDF
```

Menjalankan foremost untuk ekstraksi file PDF :

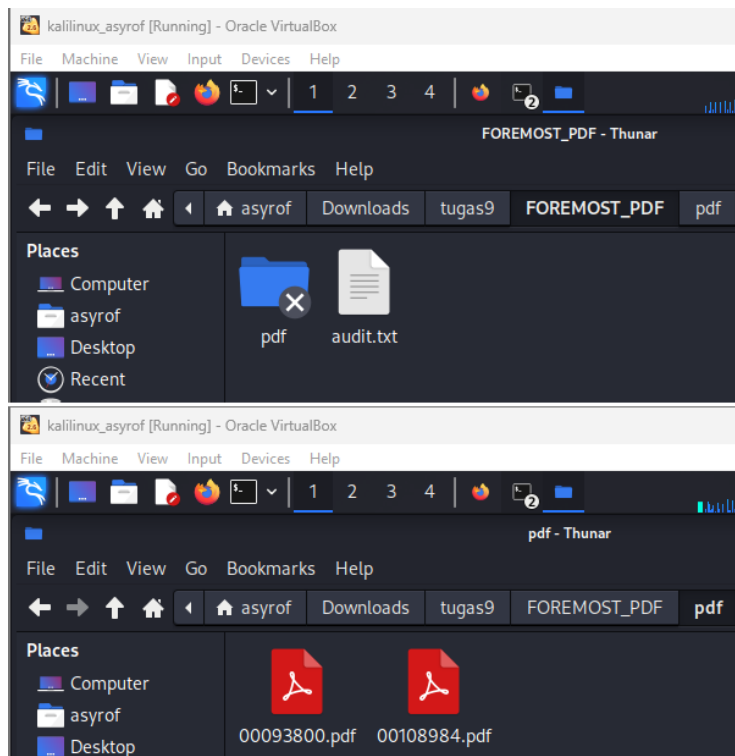
```
(root@asyrof) ~/home/asyrof/Downloads/tugas9
# foremost -i RAW-ImageDrive.dd -t pdf -o FOREMOST_PDF/
Processing: RAW-ImageDrive.dd
|*****|
```

Memeriksa hasil ekstraksi PDF :

```
(root@asyrof) ~/home/asyrof/Downloads/tugas9
# cd FOREMOST_PDF

(root@asyrof) ~/home/asyrof/Downloads/tugas9/FOREMOST_PDF
# ls -al

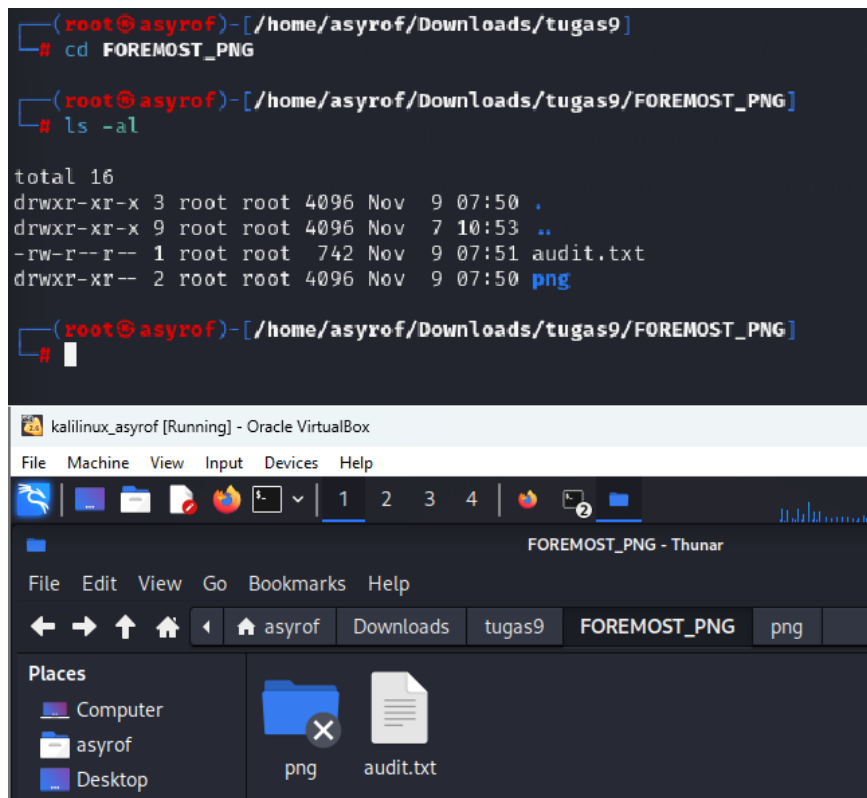
total 16
drwxr-xr-x 3 root root 4096 Nov  7 10:19 .
drwxr-xr-x 8 root root 4096 Nov  7 10:17 ..
-rw-r--r-- 1 root root 774 Nov  7 10:19 audit.txt
drwxr-xr-- 2 root root 4096 Nov  7 10:19 pdf
```



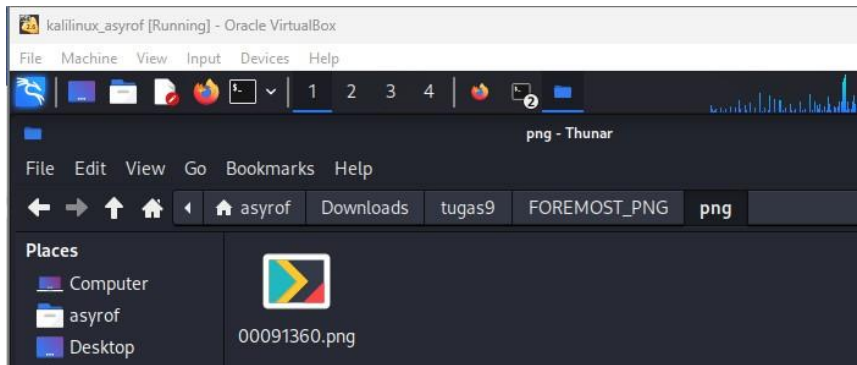
Menjalankan foremost untuk ekstraksi file PNG :

```
(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# foremost -i RAW-ImageDrive.dd -t png -o FOREMOST_PNG/
Processing: RAW-ImageDrive.dd
[*****]
```

Memeriksa hasil ekstraksi PNG :







Menjalankan foremost untuk ekstraksi file MP4 :

```
(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# foremost -i RAW-ImageDrive.dd -t mp4 -o FOREMOST_MP4/
Processing: RAW-ImageDrive.dd
|*****|
```

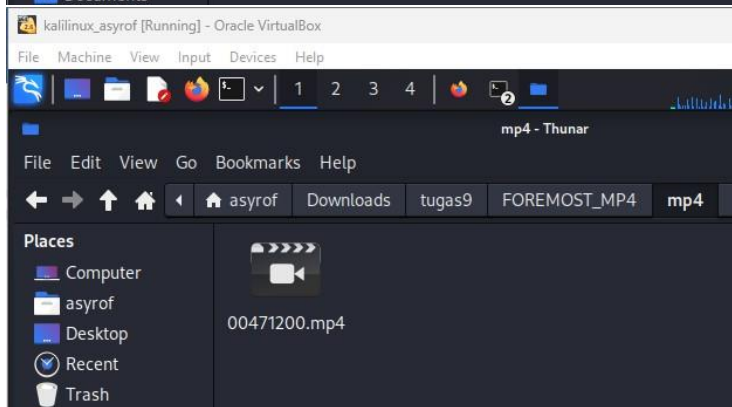
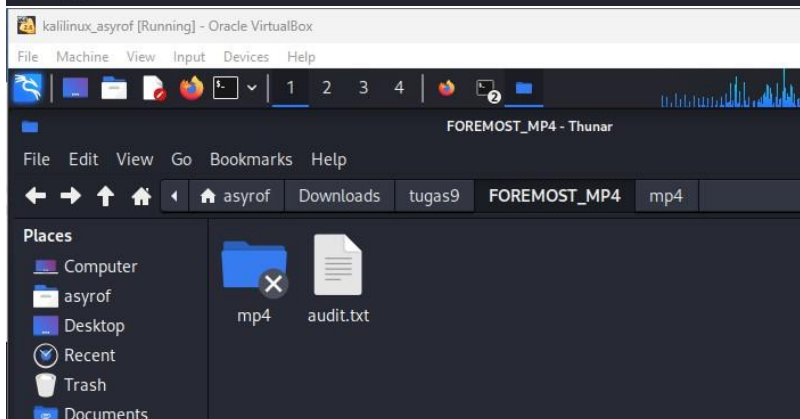
Memeriksa hasil ekstraksi MP4 :

```
(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# cd FOREMOST_MP4

(root@asyrof)-[/home/asyrof/Downloads/tugas9/FOREMOST_MP4]
# ls -al

total 16
drwxr-xr-x 3 root root 4096 Nov  9 07:55 .
drwxr-xr-x 9 root root 4096 Nov  7 10:53 ..
-rw-r--r-- 1 root root  729 Nov  9 07:55 audit.txt
drwxr-xr-- 2 root root 4096 Nov  9 07:55 mp4

(root@asyrof)-[/home/asyrof/Downloads/tugas9/FOREMOST_MP4]
#
```



Menjalankan foremost untuk ekstraksi file JPG :

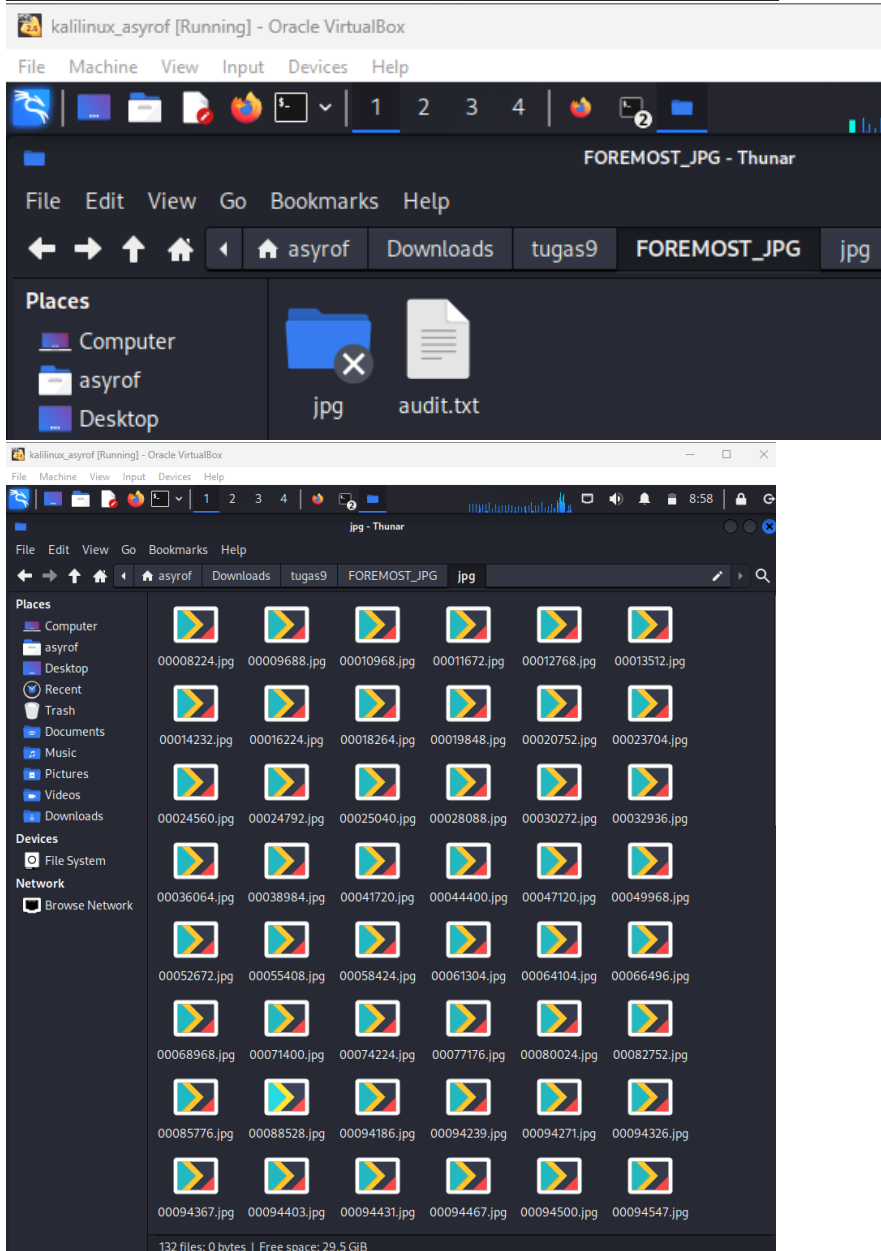
```
(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# foremost -i RAW-ImageDrive.dd -t jpg -o FOREMOST_JPG/
Processing: RAW-ImageDrive.dd
|*****|
```

Memeriksa hasil ekstraksi JPG :

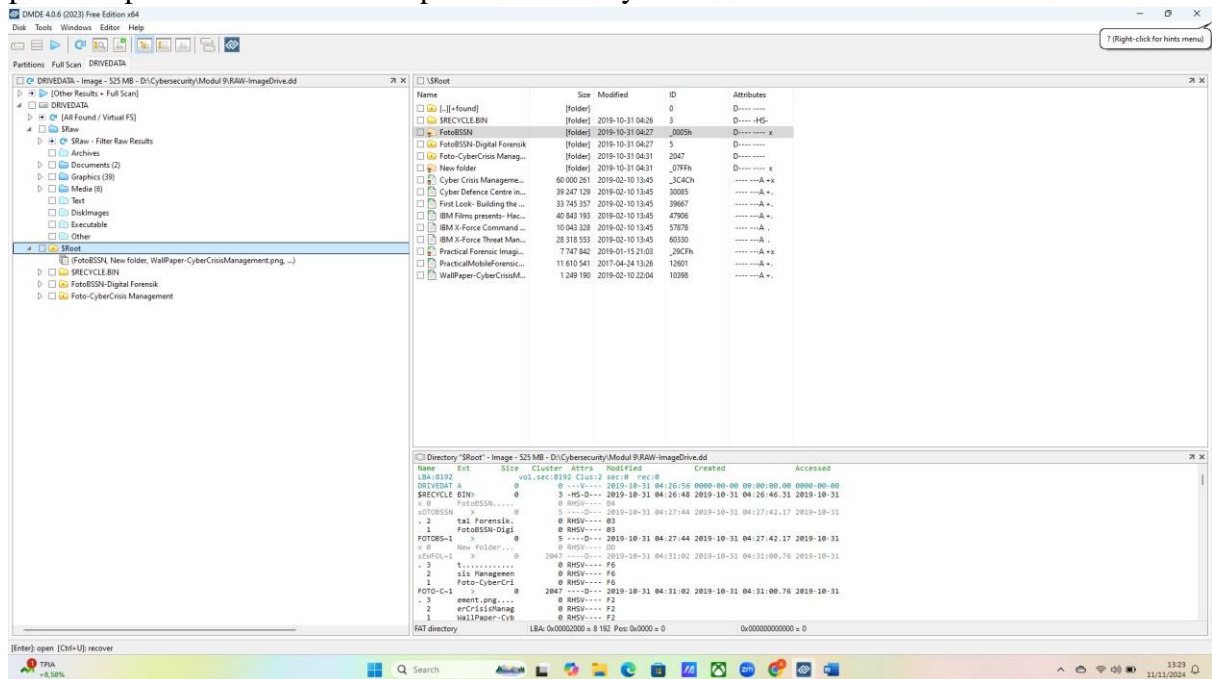
```
(root@asyrof)-[/home/asyrof/Downloads/tugas9]
# cd FOREMOST_JPG

(root@asyrof)-[/home/asyrof/Downloads/tugas9/FOREMOST_JPG]
# ls -al

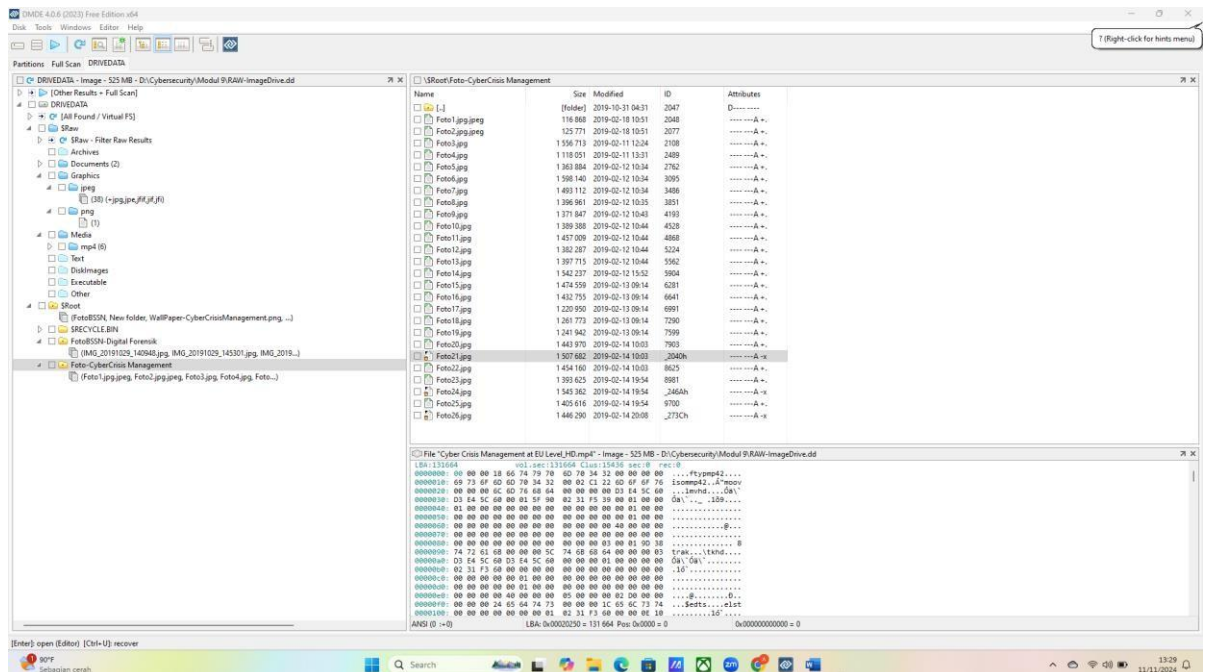
total 20
drwxr-xr-x 3 root root 4096 Nov  9 08:56 .
drwxr-xr-x 9 root root 4096 Nov  7 10:53 ..
-rw-r--r-- 1 root root 6782 Nov  9 08:56 audit.txt
drwxr-xr-- 2 root root 4096 Nov  9 08:56 jpg
```



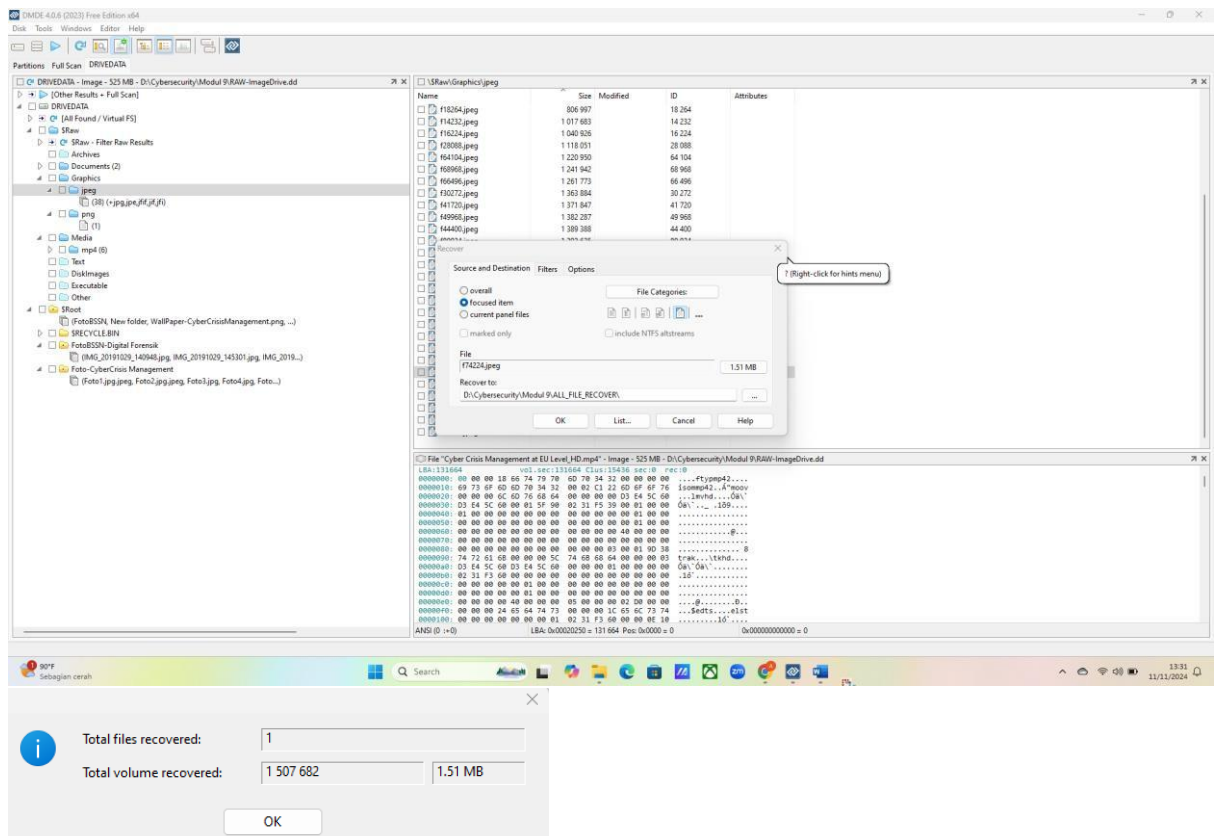
- Tool DMDE :
- pada tampilan tool DMDE terdapat 2 versi data yaitu RAW dan Root



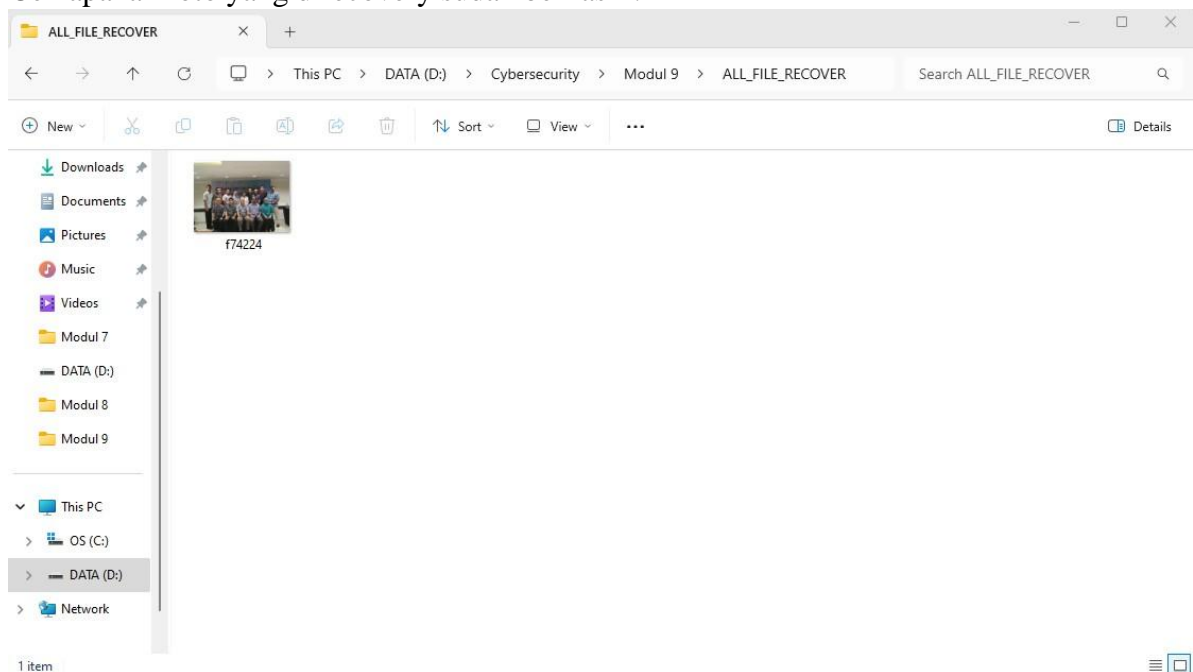
Jika ingin melakukan recovery, kita akses dahulu data root, dan lihat tanda ikon sampah yang terdapat pada beberapa file yang menandakan file tersebut telah terhapus, lalu kita cari file yang terhapus tersebut pada data RAW nya, kemudian klik kanan lalu pilih recover :



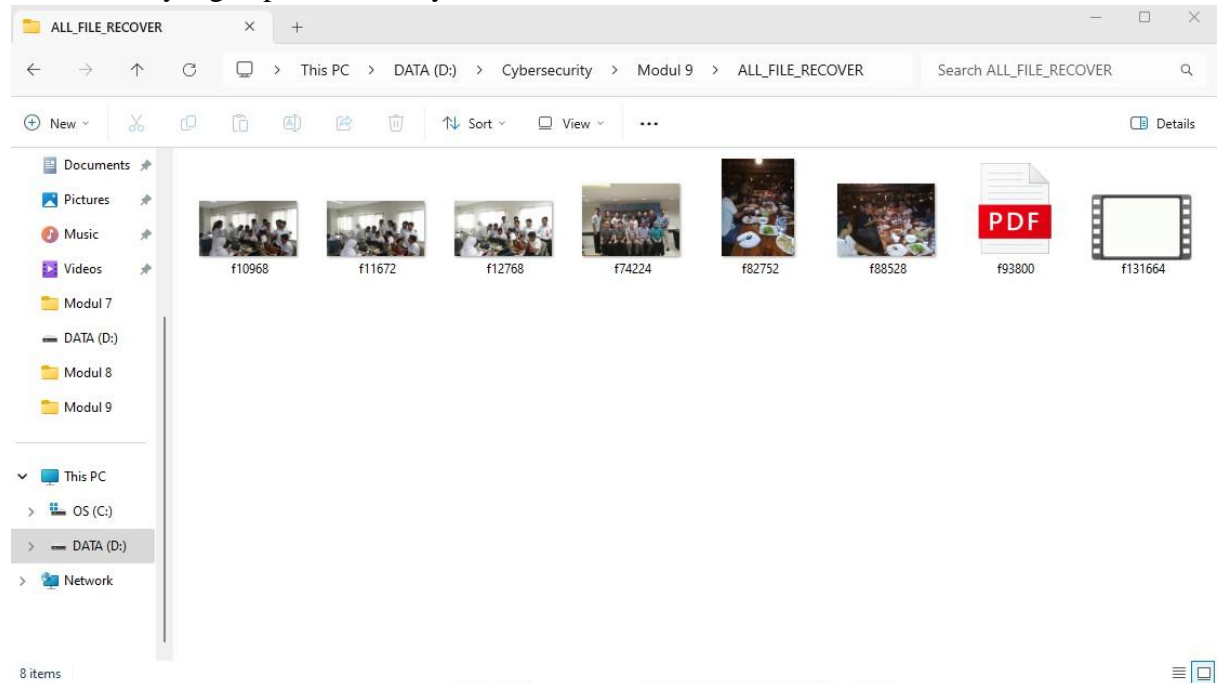




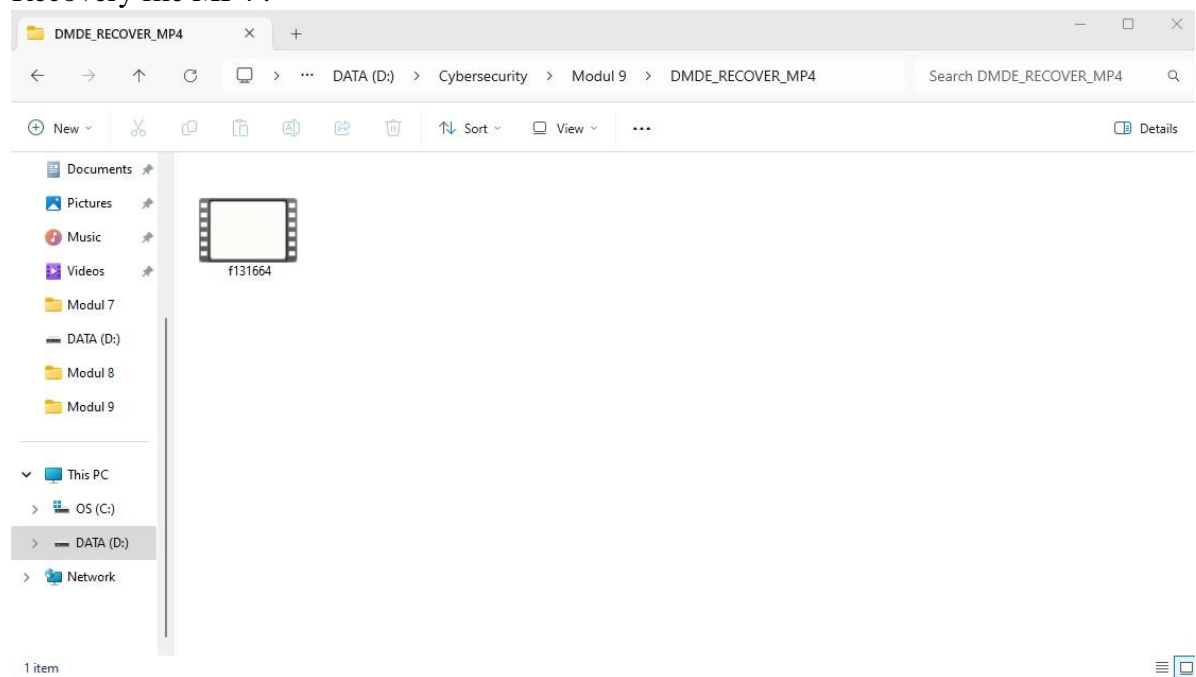
Cek apakah foto yang direcovery sudah berhasil :



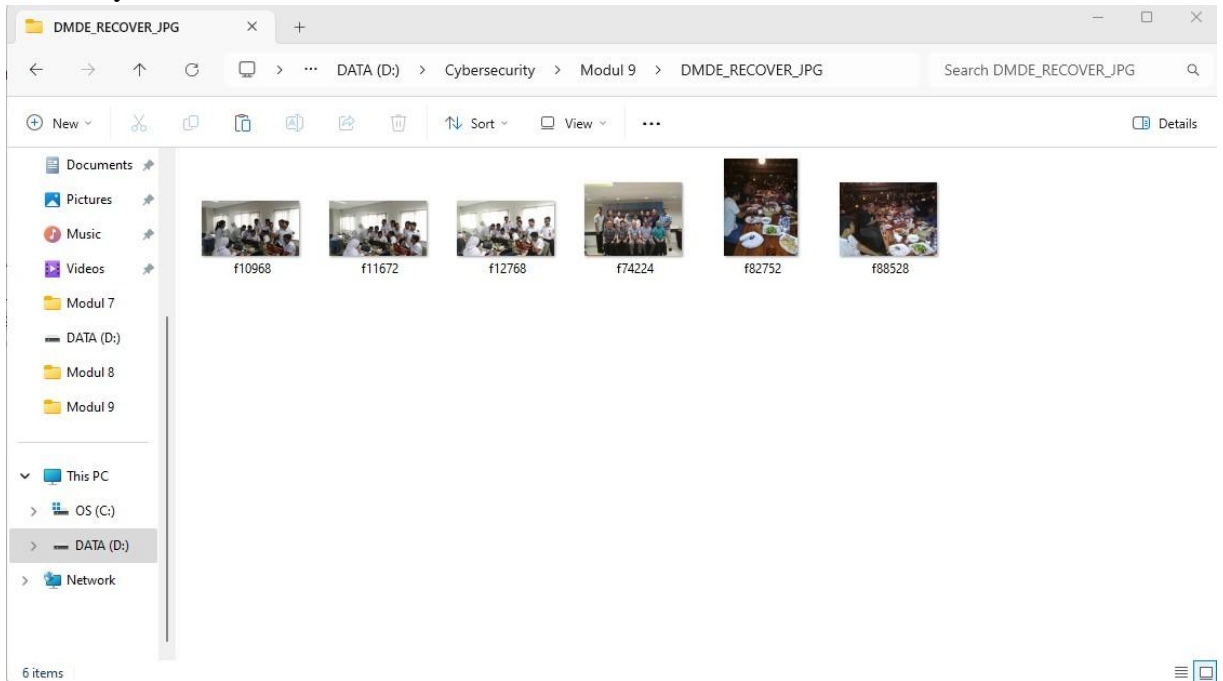
Jumlah file yang dapat direcovery 8 :



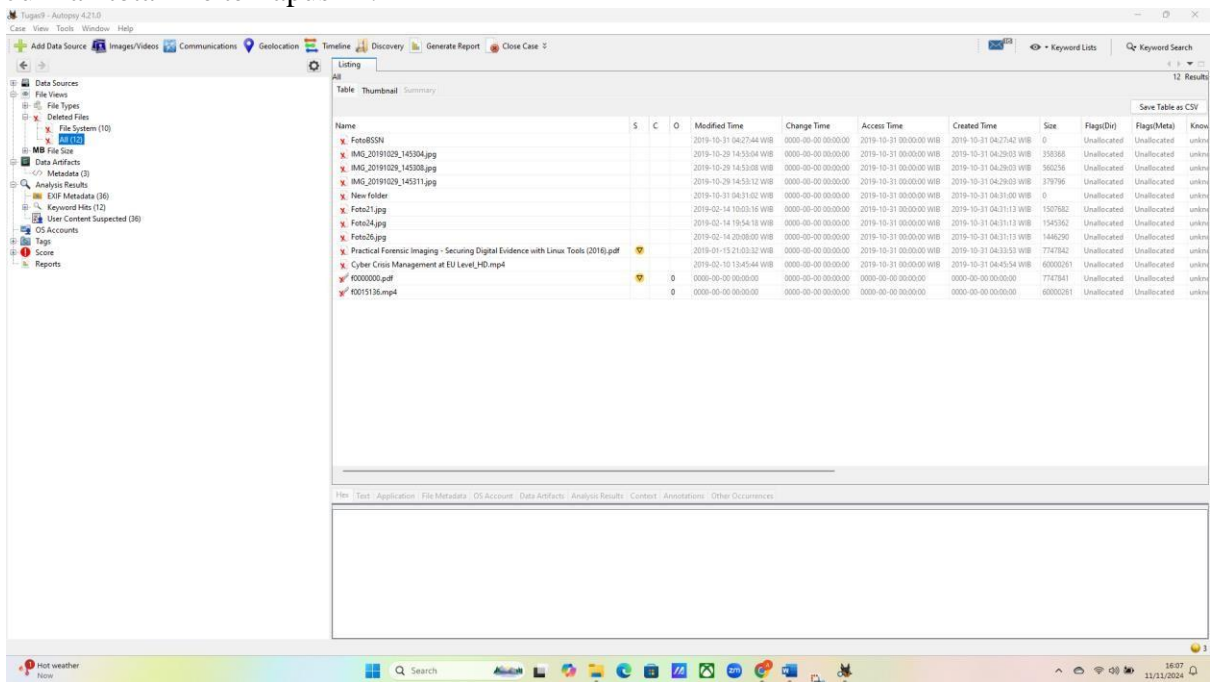
Recovery file MP4 :



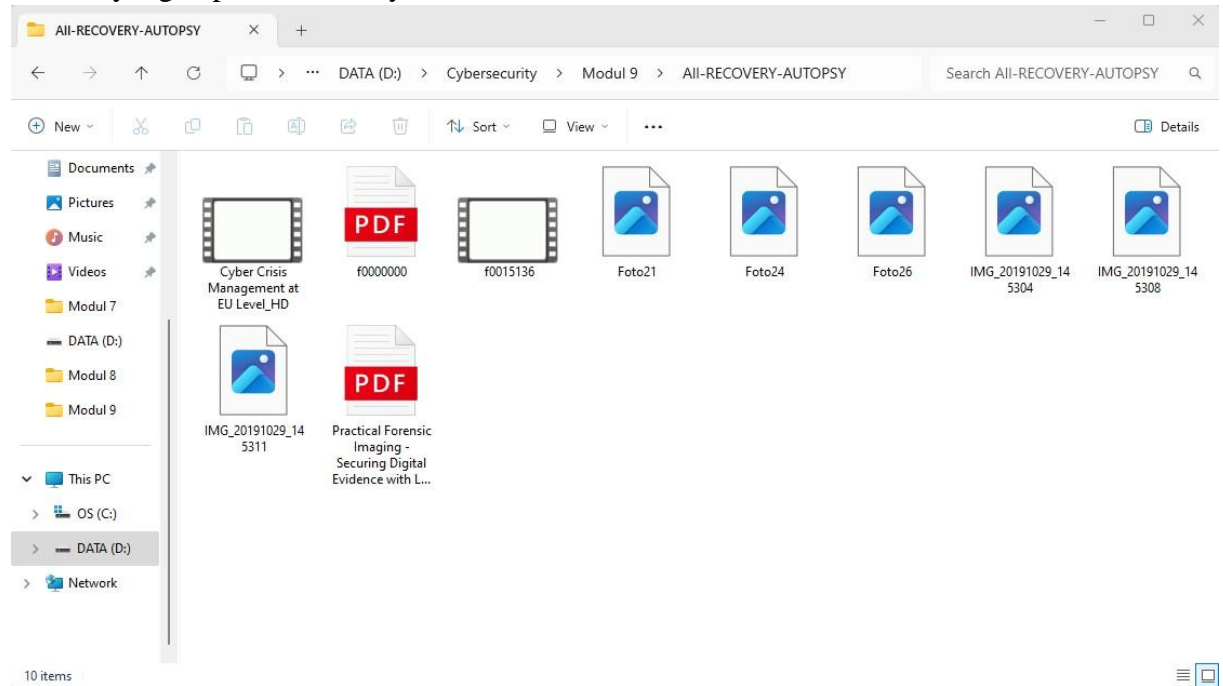
## Recovery file JPG :



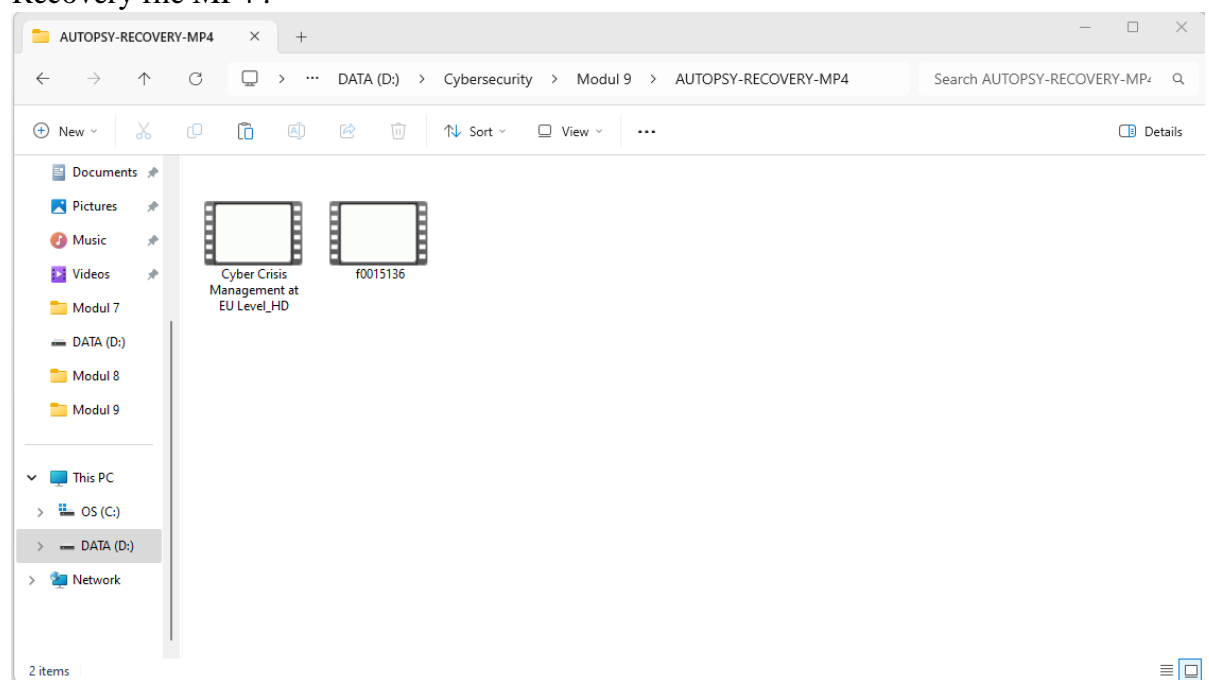
- Tool Autopsy :  
Jumlah total file terhapus 12:



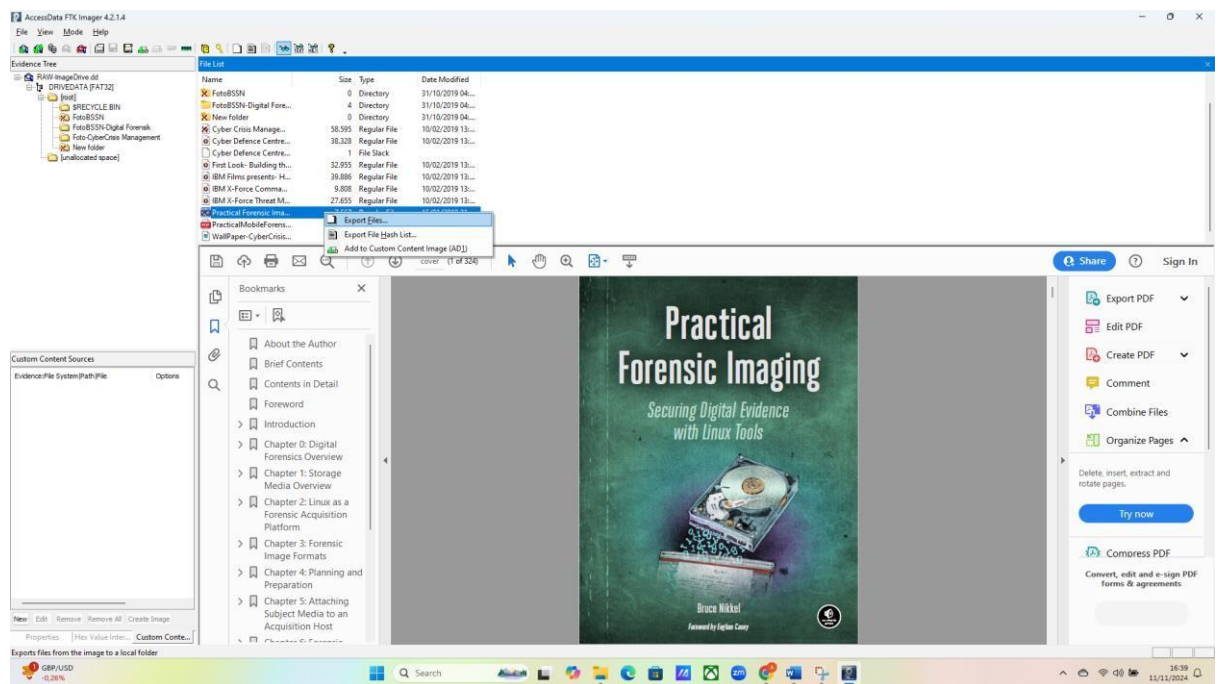
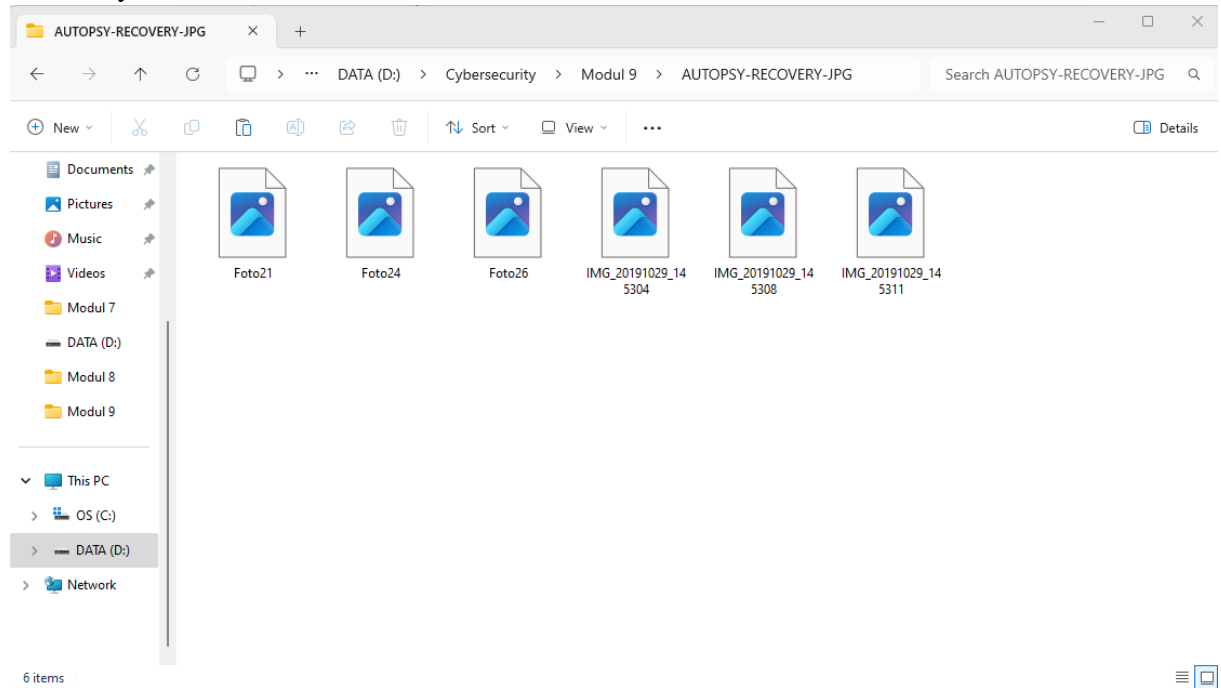
Jumlah yang dapat di recovery 10 file:



Recovery file MP4 :



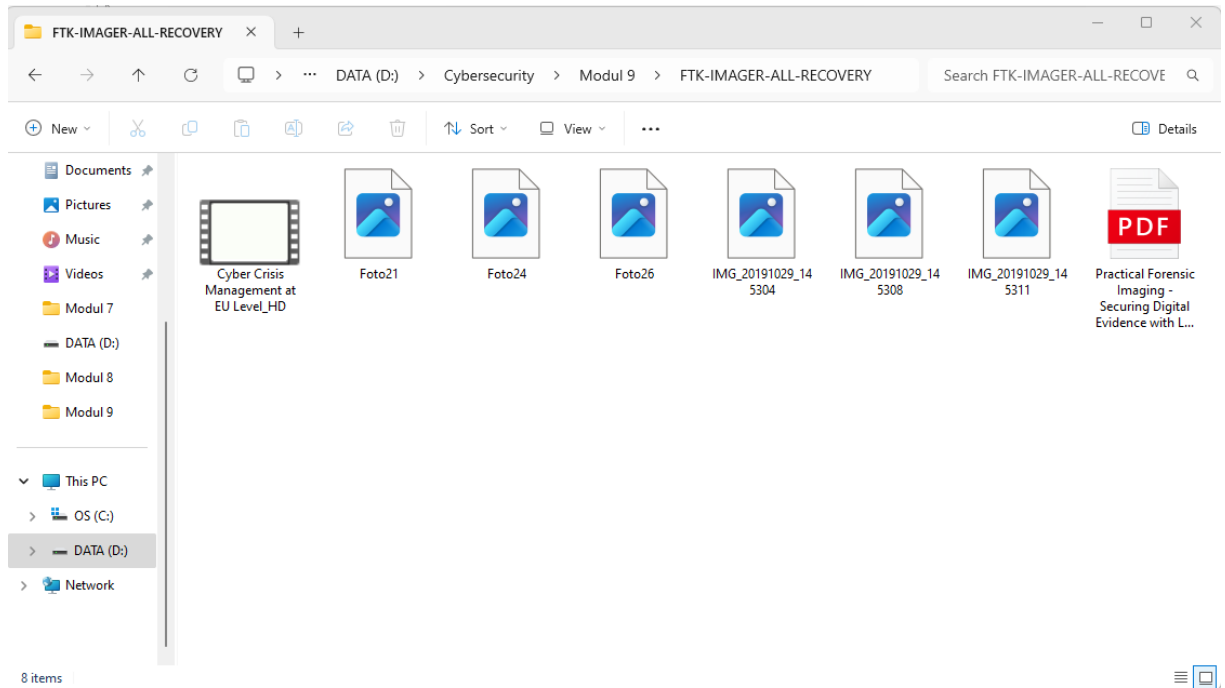
## Recovery file JPG :



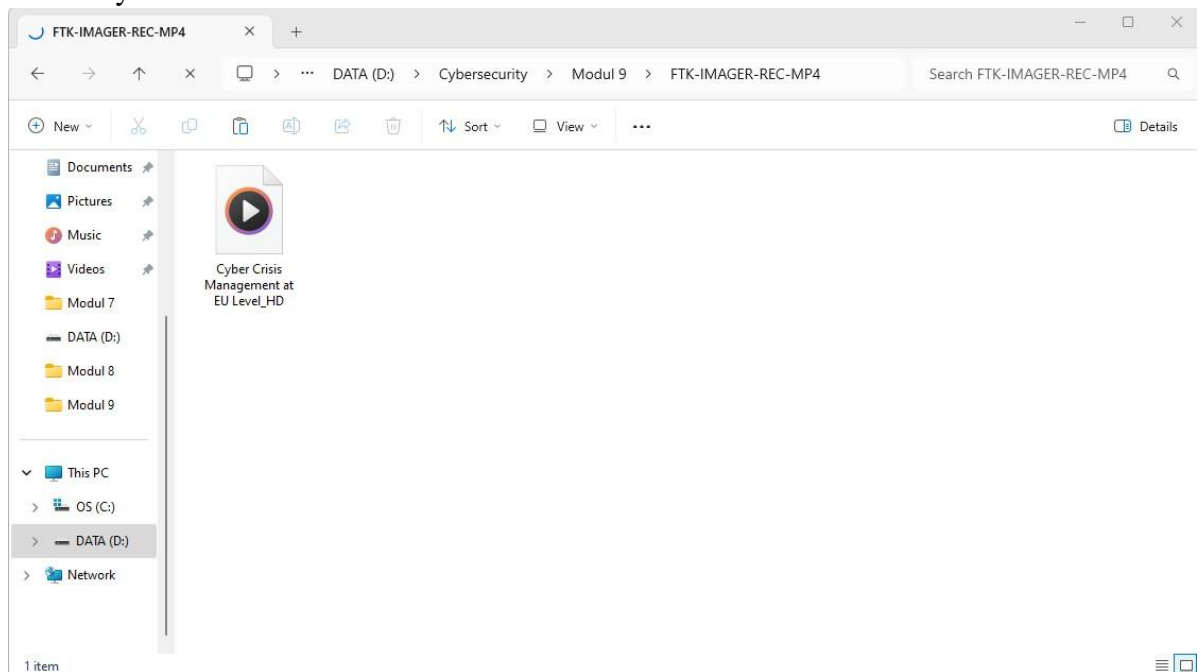
## ➤ Tool FTK\_Imager :



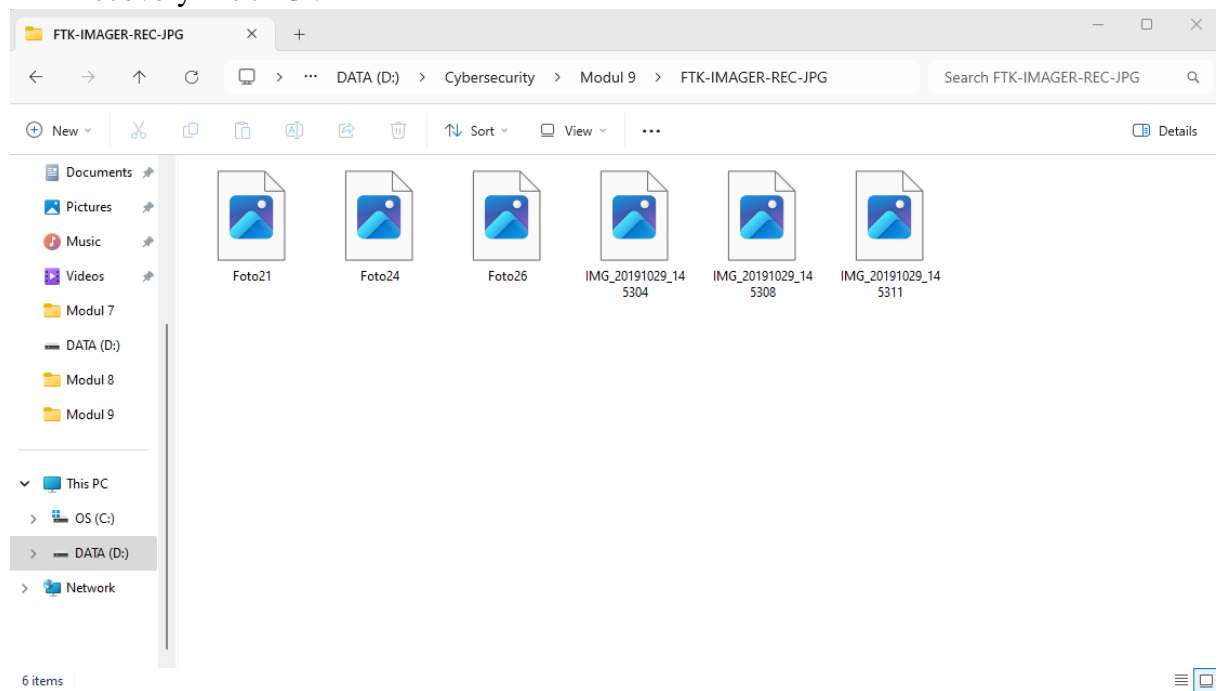
Jumlah file yang terhapus dan sudah direcovery 8 :



Recovery file MP4 :



## Recovery file JPG :



### ➤ Table tool :

No.	Jenis tool	Total file recovery	Mp4 recovered	JPG recovered	Mp4 bisa dibuka	JPG bisa dibuka
1	Tsk_recover	8	yes	yes	yes	no
2	Foremost	8	yes	yes	no	no
3	DMDE	8	yes	yes	yes	yes
4	Autopsy	10	yes	yes	yes	no
5	Ftk_imager	8	yes	yes	yes	no