

Aim:

To perform forensic analysis using FTK Imager and Kali linux

Forensic Analysis

Forensic image acquisition is the process of acquiring a forensically sound copy or image of the device or media to analyze. Forensically sound means that we shall be able to verify that the image is an exact copy of the original and the procedure used to acquire it shall be documented. The image file is the basis on which the examiner works to find the evidence. A forensic image is a bit by bit copy of the media to analyze. It is not simply cloning the file system, it's a copy of all the raw disk sectors. The original media must not be altered in any way. The integrity of the image file shall be verified and I/O errors logged.

FTK Imager:

FTK stands for Forensic Tool Kit. Forensic Toolkit or FTK is a computer forensics software product made by AccessData. This is a Windows based commercial product. For forensic investigations, the same development team has created a free version of the commercial product with a fewer functionalities. This FTK Imager tool is capable of both acquiring and analyzing computer forensic evidence.

The evidence FTK Imager can acquire can be split into two main parts. They are:

- Acquiring volatile memory
- Acquiring non-volatile memory (Hard disk)

There are two possible ways this tool can be used in forensics image acquisitions:

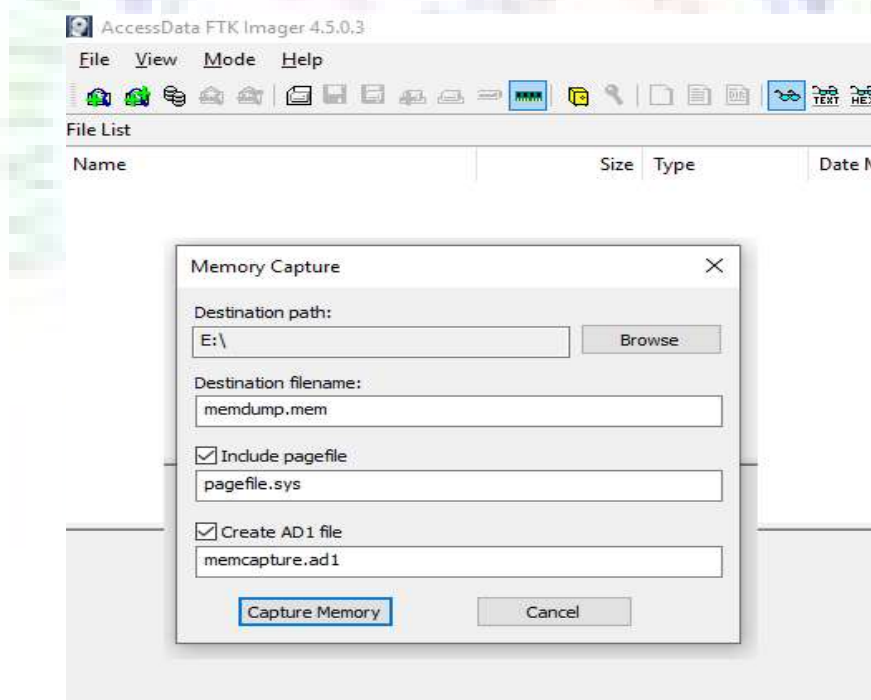
- Using FTK Imager portable version in a USB pen drive or HDD and opening it directly from the evidence machine. This option is most frequently used in live data acquisition where the evidence PC/laptop is switched on.
- Installing FTK Imager on the investigator's laptop. In this case the source disk should be mounted into the investigator's laptop via write blocker. The write blocker prevents data being modified in the evidence source disk while providing read-only access to the investigator's laptop. This helps to maintain the integrity of the source disk

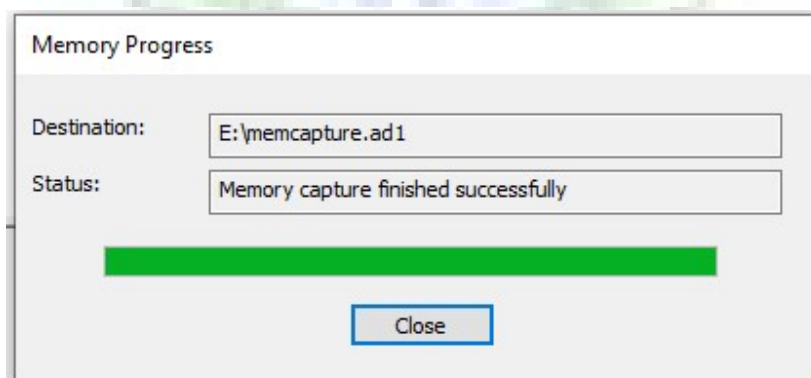
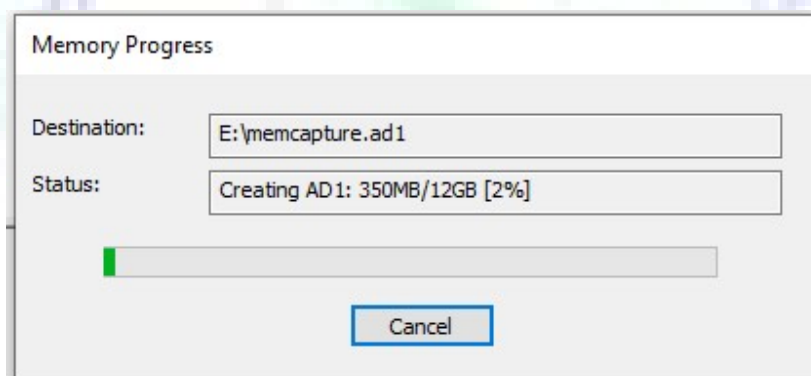
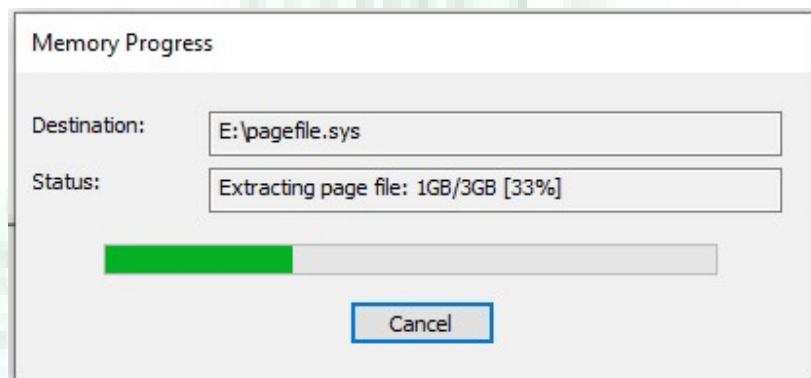
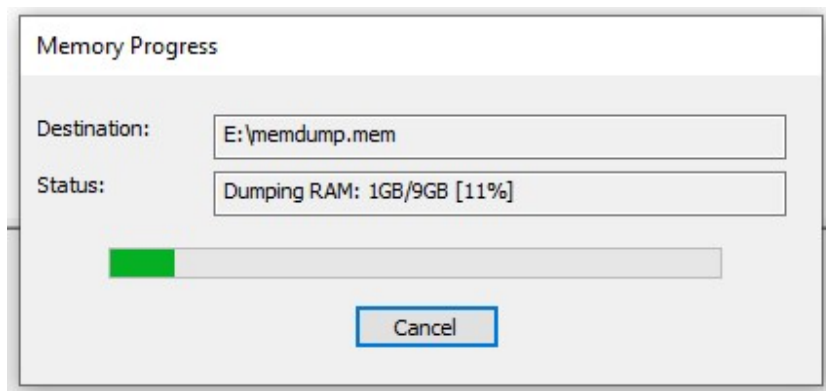
Acquiring volatile memory using FTK Imager:

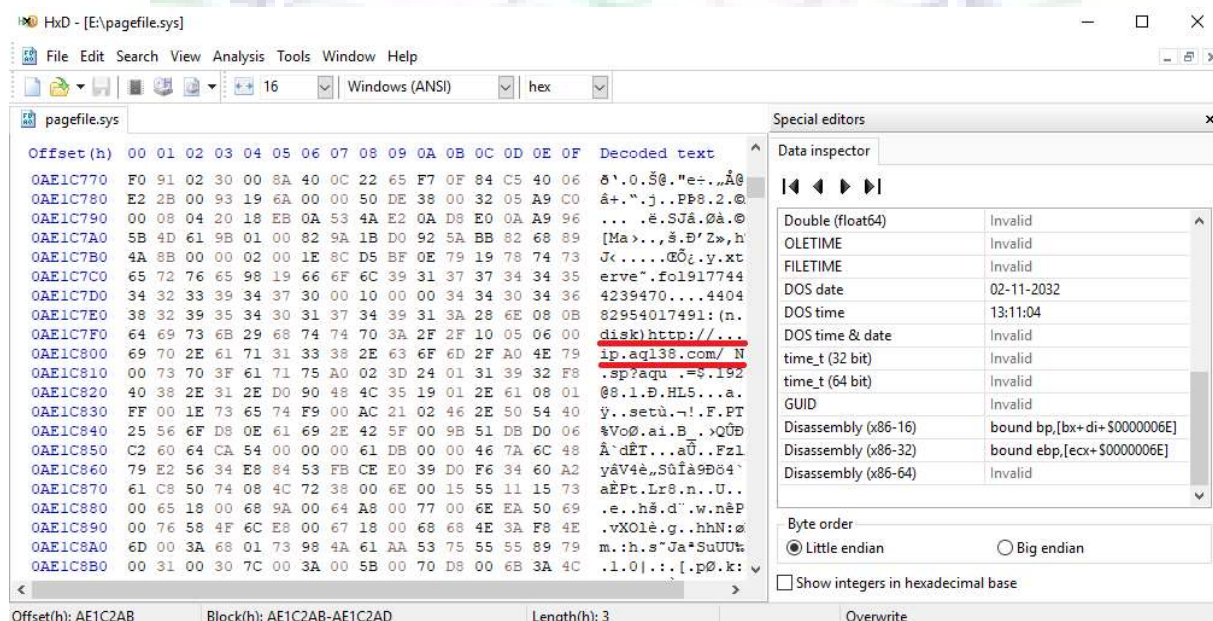
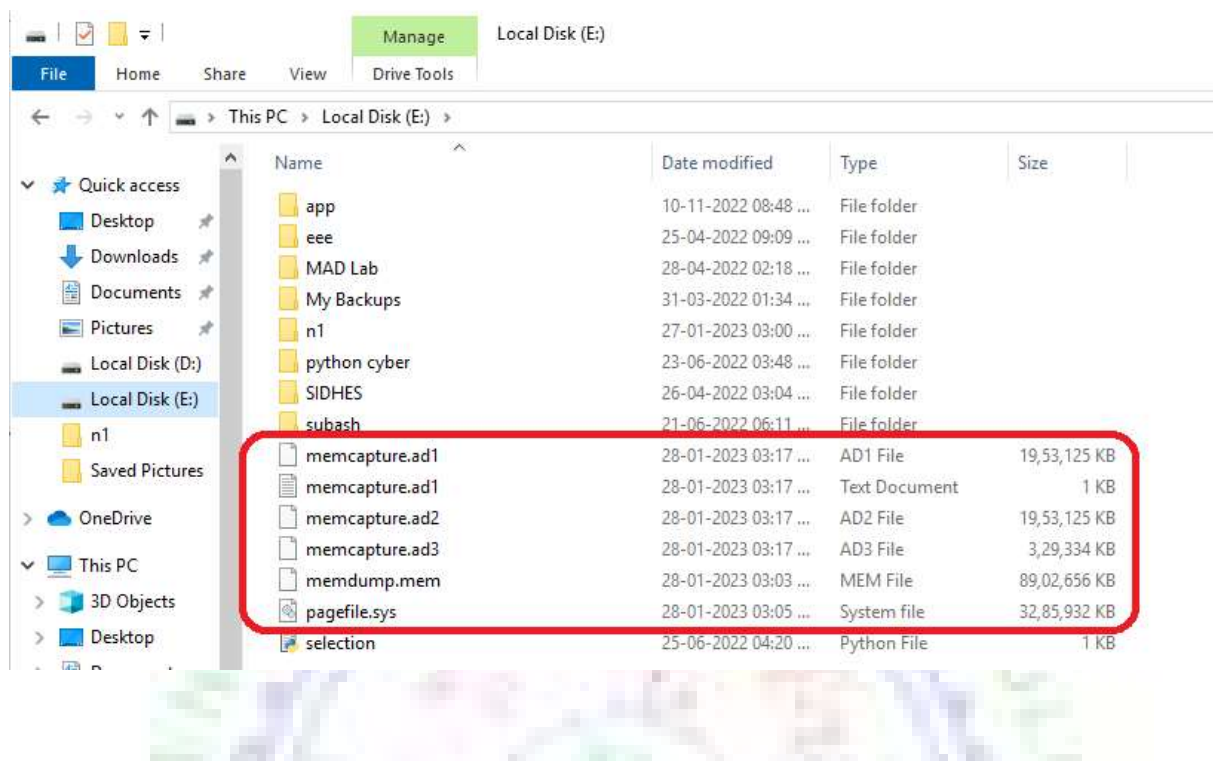
1. Open FTK Imager
2. Select Capture Memory black color icon

3. In the Memory Capture window, Select the destination path as E:\ and click the 'Include pagefile' check box and also click the 'Create ADI file' check box
4. In the Memory progress page, give the Destination as E:\memcapture.ad1
5. Once the acquisition has completed, the destination folder will have the acquired memory with file names memdump.mem and pagefile.sys
6. FTK Imager also creates a log of the acquisition process and places it in the same directory as the image. This file lists the evidence information, details of the drive, checksums, and times the image acquisition started and finished
7. Here memcapture.ad1.txt is created in E:\ folder
8. To analyse pagefile.sys, open HxD hex editor and select the option File -> Open -> pagefile.sys or select the option File -> Add Evidence Item -> Image File -> Next -> Browse -> pagefile.sys -> Finish in FTK Imager and select the icon 'View files in Hex format'
9. The entire content of pagefile.sys is opened.
10. We can view and analyse it using the displayed page in HxD or FTK Imager

Output Screenshot:







Content of memcapture.ad1.txt:

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:

Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:

Information for E:\memcapture.ad1:

[Computed Hashes]
MD5 checksum: c0c7b7e386da1682e2dd3c437fccb124
SHA1 checksum: a0d3e0583a8d0fd2d4aecc29276ebc3742cca284
Image information:
Acquisition started: Fri Jan 27 14:24:24 2023
Acquisition finished: Fri Jan 27 14:35:46 2023
Segment list:
E:\memcapture.ad1
E:\memcapture.ad2

Forensic analysis using Kali Linux:

Using dd command in Kali Linux:

dd command will read from standard input and writes to standard output. We can specify alternative input and output files by using if and of command line options.

1. Open Kali Linux
2. Use the command `dd if=scan1.txt of=scan10.txt bs=512`. It is used to copy one file into another
3. To backup the hard disk, use the command `dd if=/dev/sda of=/dev/sdb` where sda is the name of the source hard disk and sdb is the name of the destination hard disk
4. To backup a partition, use the command `dd if=/dev/hda1 of=~/partition.img`
5. To create an image of a hard disk use the command `dd if=/dev/sda of=~/harddisk.img`. To restore using the hard disk image, use the command `dd if=harddisk.img of=/dev/hdb`
6. To create a CDROM backup use the command `dd if=/dev/cdrom of=cdcont.iso bs=2048`

```
(kali@kali)-[~]
$ cat scan1.txt
# Nmap 7.93 scan initiated Thu Jan 19 07:19:42 2023 as: nmap -oN scan1.txt scanme.nmap.org
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0031s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
1000/tcp  open  cadlock

# Nmap done at Thu Jan 19 07:19:53 2023 -- 1 IP address (1 host up) scanned in 10.58 seconds

(kali@kali)-[~]
$ dd if=scan1.txt of=scan10.txt bs=512 noerror
dd: unrecognized operand 'noerror'
Try 'dd --help' for more information.

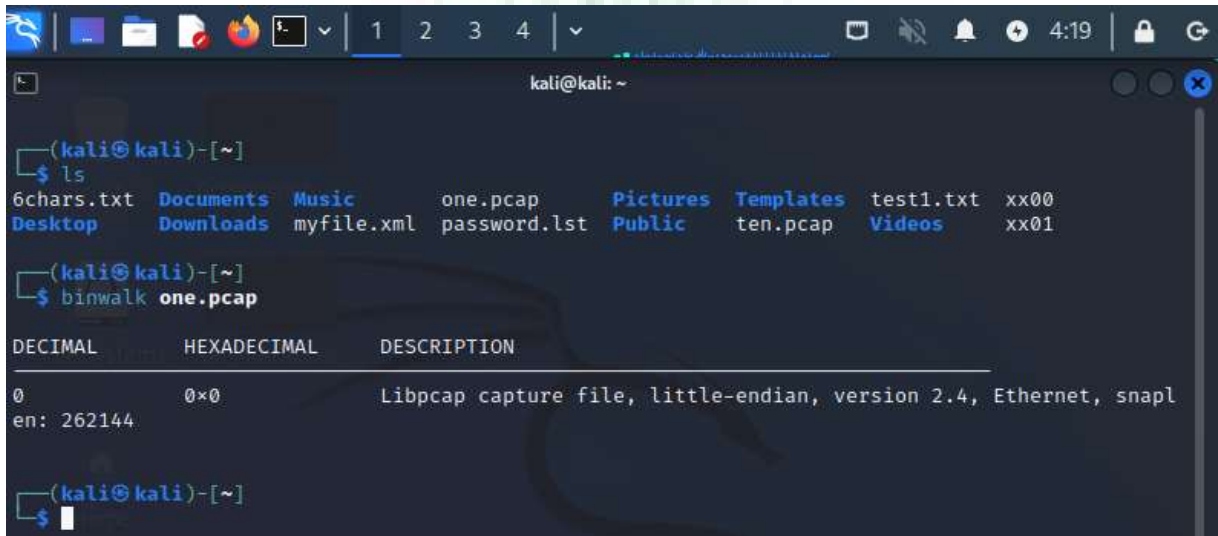
(kali@kali)-[~]
$ dd if=scan1.txt of=scan10.txt bs=512
1+1 records in
1+1 records out
525 bytes copied, 0.00278096 s, 189 kB/s

(kali@kali)-[~]
$ cat scan10.txt
# Nmap 7.93 scan initiated Thu Jan 19 07:19:42 2023 as: nmap -oN scan1.txt scanme.nmap.org
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0031s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
```


Using Binwalk tool in Kali Linux:

Binwalk is used to analyze and extract any firmware images or files.

1. Open Kali Linux
2. Select Applications -> Forensic Analysis -> binwalk
3. Type binwalk filename. Here type as one.pcap
4. The details of the file is displayed for decimal, hexadecimal and description details



```
(kali@kali)-[~]
$ ls
6chars.txt  Desktop  Documents  Downloads  Music  myfile.xml  one.pcap  password.lst  Pictures  Public  Templates  ten.pcap  test1.txt  Videos  xx00  xx01

(kali@kali)-[~]
$ binwalk one.pcap

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0            0x0            Libpcap capture file, little-endian, version 2.4, Ethernet, snapl
en: 262144

(kali@kali)-[~]
$
```

Using Bulk extractor tool in Kali Linux:

Bulk extractor is used to extract files to output directory after analyzing an image file.



```
(kali@kali)-[~]
$ bulk_extractor -o b-out myfile.xml
mkdir "b-out"
bulk_extractor version: 2.0.0
Input file: "myfile.xml"
Output directory: "b-out"
Disk Size: 0
Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml_carved msxml net ntfsin
dx ntfslogfile ntfsmft ntfsusrn pdf rar sqlite utmp vcard_carved windirs winlnk winpe winprefetc
h zip accts email gps
Threads: 2
going multi-threaded... ( 2 )
All data read; waiting for threads to finish...
bulk_extractor      Thu Feb  2 04:34:43 2023

available_memory: 1335939072
bytes_queued: 0
depth0_bytes_queued: 0
depth0_sbufs_queued: 0
elapsed_time: 0:00:00
estimated_date_completion: 2023-02-02 04:34:43
estimated_time_remaining: 0:00:00
fraction_read: 100.000000 %
max_offset: 0
```