Experiment No .10

10.1 Aim: Mobile Forensic: Cellular Antenna Search, Confiscating a Mobile Device, Tracking a Suspect using WiFi, SD Card Evidence.

Example Scenario:
You are a digital forensics trainee assisting in a mobile investigation. A suspect is believed to have used a smartphone during several illegal activities. Your job is to identify the phone's possible location history using **cellular antenna information** and **Wi-Fi networks**, properly **confiscate the device** without tampering, and safely **acquire evidence from the SD card**.

You use online resources like

- Open AntennaSearch.com to find nearby cell towers, and
- Open WiFiSpots.com to identify open Wi-Fi networks around the suspect's known locations.

You also handle the mobile phone carefully using **antistatic gloves**, a **docking station**, and **forensic tools** such as **Autopsy** to analyze the extracted data.

Tasks:

Scene Assessment:

- Observe the mobile device's state (on/off, locked/unlocked, connected to a network).
- Photograph the device as found and note its surroundings.

Confiscating the Mobile Device:

- Wear antistatic gloves to avoid static discharge and contamination.
- If the phone is on, place it immediately into a Faraday bag to block signals and prevent remote wiping.
- If it is off, remove the SIM and battery (if accessible) and store them in separate antistatic bags.
- Label the evidence properly and record it in the chain-of-custody form.

Cellular Antenna Search:

- Use https://www.antennasearch.com to identify nearby cell towers and antenna locations around the suspect's last known area.

- Document the tower IDs, operators, and distances.
- This helps in mapping the phone's possible connection range and verifying signal coverage.

Tracking a Suspect using Wi-Fi:

- Visit https://www.openwifispots.com to find open Wi-Fi hotspots in the area.
- Compare these locations with the device's stored Wi-Fi SSIDs or BSSIDs (from the phone or extracted logs).
- Note matches that can help identify where the suspect's phone connected.

SD Card Evidence Collection:

- Use antistatic gloves and a docking station to safely remove the SD card.
- Place it into an antistatic bag labeled with case details.
- Use a forensic imaging tool (e.g., FTK Imager) to create a bit-by-bit image of the SD card.
- Calculate hash values (MD5/SHA1) to verify the image integrity.

Analysis Using Autopsy:

- Open the acquired SD card image in the Autopsy forensic tool.
- Examine stored files such as photos, chat logs, browser history, and location data.
- Check metadata and EXIF information for timestamps and GPS coordinates.
- Generate an analysis report summarizing findings.

Documentation:

- Save screenshots of each major step: confiscation, imaging, hashing, and analysis.
- Maintain detailed notes and include URLs, hash values, and timestamps in your final lab report.

10.2 Lab Outcome :

To learn how to properly handle and analyze a mobile device forensically, perform cell tower lookup, identify Wi-Fi-based location evidence, and safely acquire and analyze SD card data using tools like Autopsy, ensuring that all evidence remains authentic and admissible.

10.3Learning Objectives:

- To understand how cellular antenna search aids in mobile location forensics.
- To follow proper confiscation procedures using Faraday and antistatic protection.
- To track a suspect's location using Wi-Fi hotspot data.
- To perform SD card evidence extraction safely using a docking station.
- To analyze extracted evidence using Autopsy forensic software.
- To verify evidence integrity using hash functions and maintain proper documentation.

10.4 Requirement:

Hardware:

- Smartphone (case device)
- Faraday bag
- Antistatic gloves and antistatic bags
- Docking station for SD card
- Forensic workstation or laptop
- External storage drive for forensic images

Software / Online Tools:

- AntennaSearch.com – to locate cell towers
- OpenWiFiSpots.com – to identify public Wi-Fi networks
- Autopsy – forensic analysis tool
- FTK Imager or dc3dd – imaging tool
- Hash calculator (MD5/SHA1)

10.5 Related Theory :

Cellular Antenna Search:
Helps investigators determine which cell towers a mobile phone could connect to based on its location. Using websites like AntennaSearch gives a list of nearby antennas and towers to estimate coverage areas.

Confiscating a Mobile Device:
Mobile devices should be handled with antistatic gloves to avoid damage. A Faraday bag blocks all wireless signals, preventing remote wiping or tracking. The device must be labeled, logged, and stored in an antistatic bag after seizure.

Wi-Fi Tracking:
Wi-Fi data such as SSIDs and BSSIDs stored in a device's memory can reveal where it

connected. Comparing this data with public hotspot databases (like OpenWiFiSpots) helps place a suspect at specific locations.

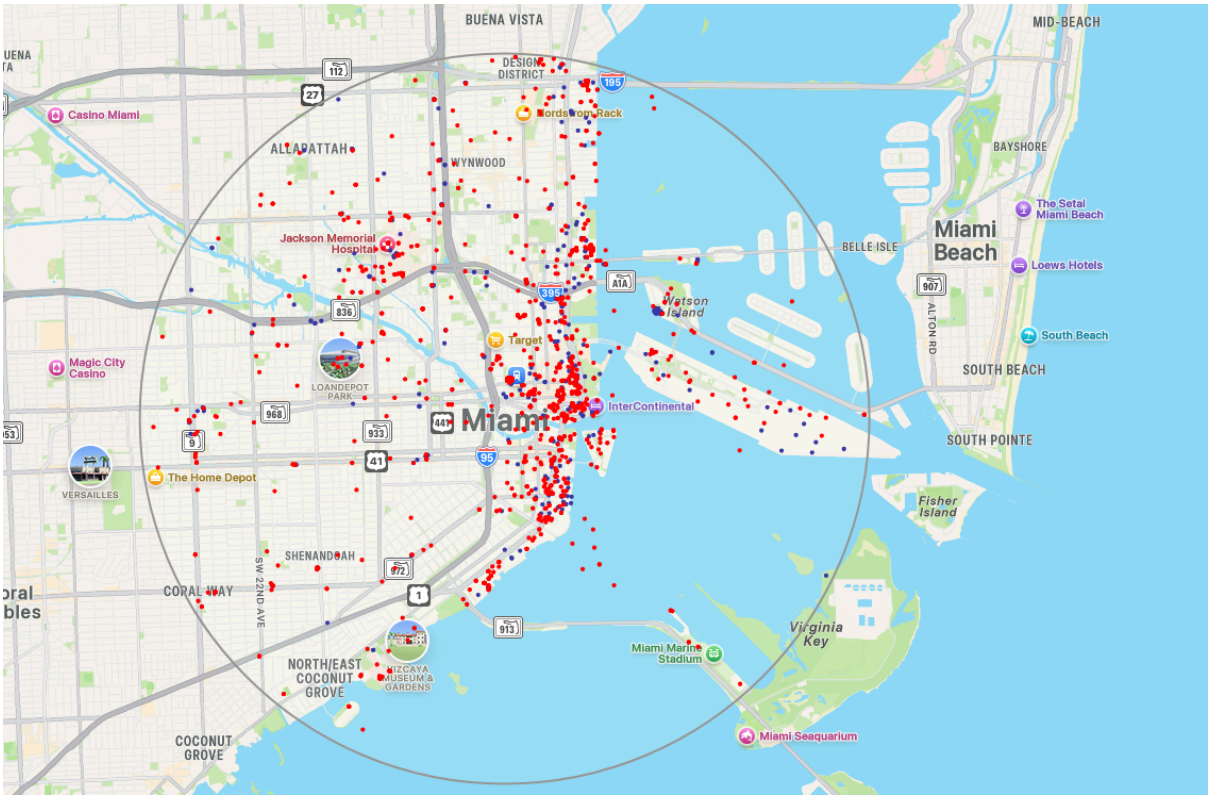
SD Card Forensics:
An SD card can contain photos, files, app data, and deleted artifacts. Using a docking station, it can be safely imaged and analyzed using Autopsy. Metadata from media files can provide timestamps and GPS evidence.

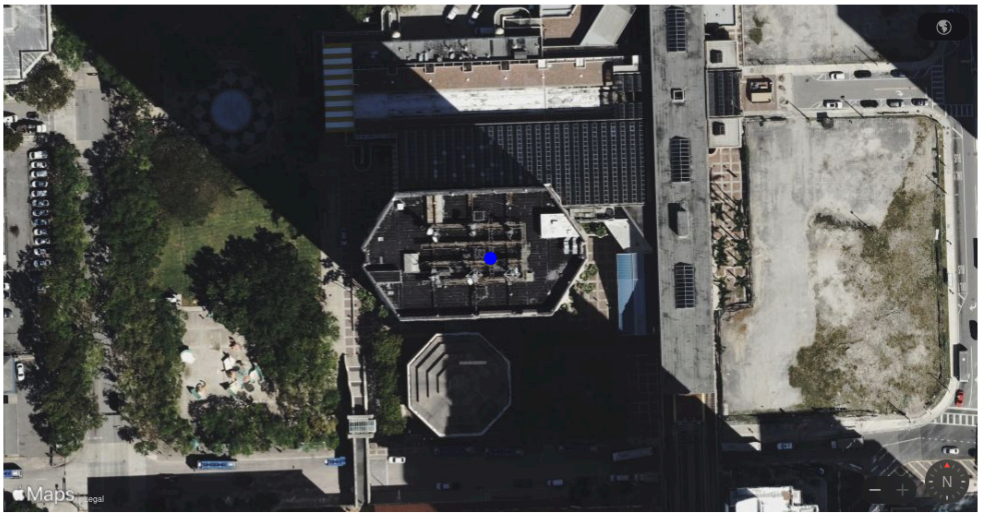
Autopsy Tool Working:
Autopsy is an open-source digital forensics tool used to examine disk images, SD cards, and mobile data. It helps recover deleted files, view user activities, and generate detailed reports for investigation.

Hash Verification:
Hashing (MD5, SHA1) ensures the forensic image is an exact copy of the original data and confirms that no tampering occurred.

10.6 Output:

- AntennaSearch.com – to locate cell towers





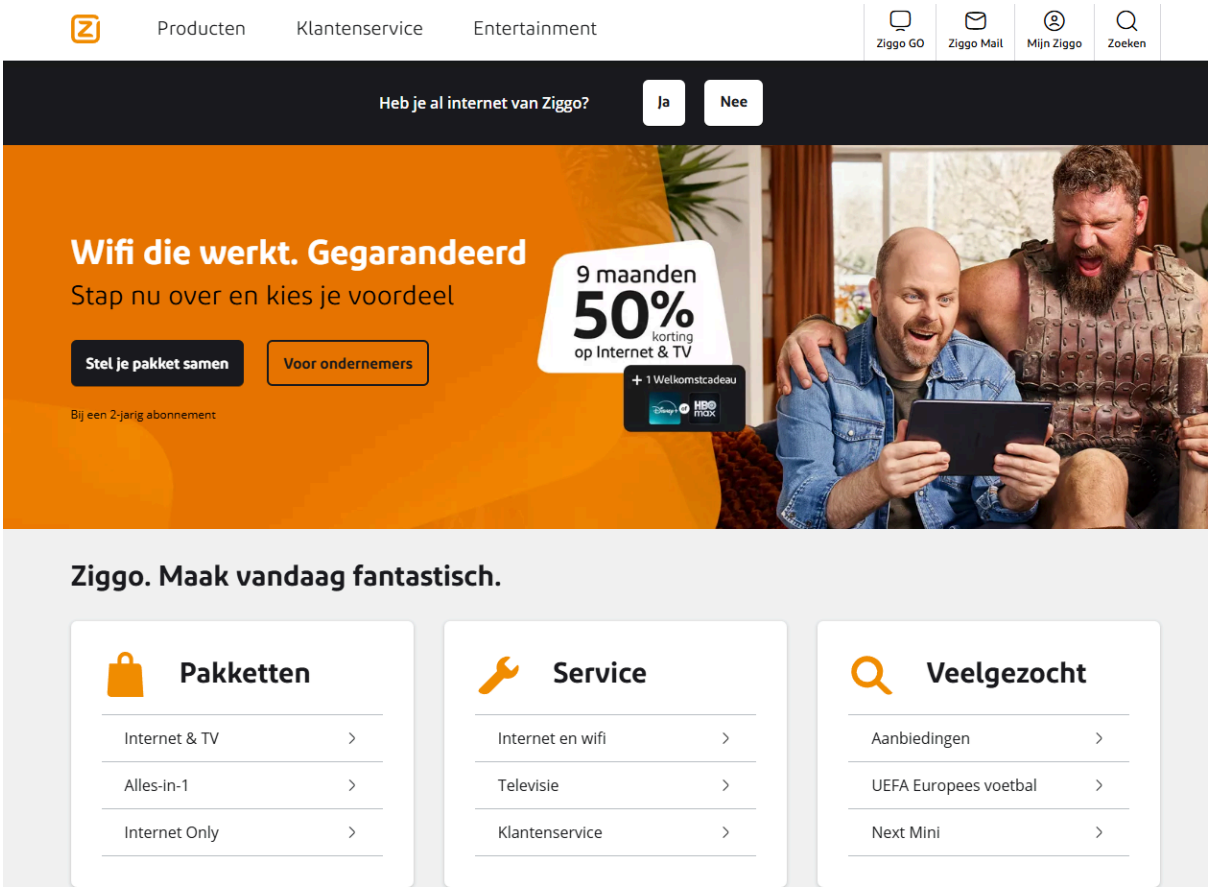
Representative Info

Company	Miami-dade County
Contact	Miguel Luna
Phone	3055968909
Email	Luna@miamidade.gov
Address	5680 Sw 87th Ave Miami Fl 33173

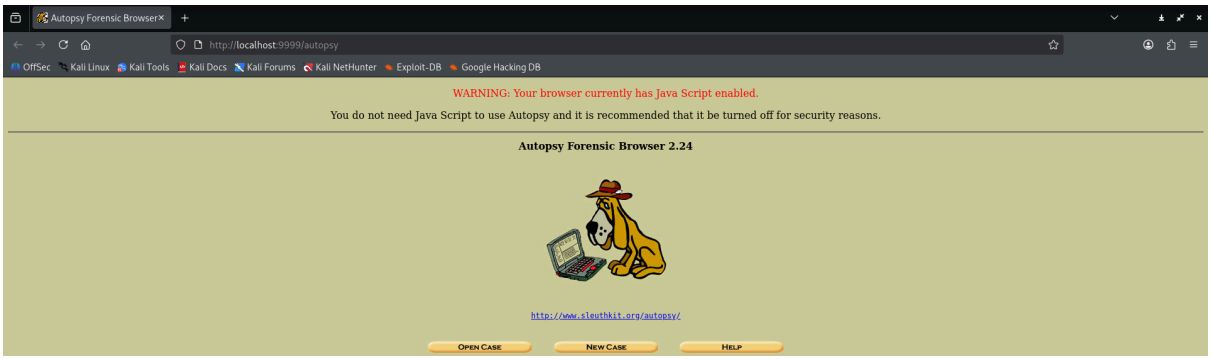
Ownership Info

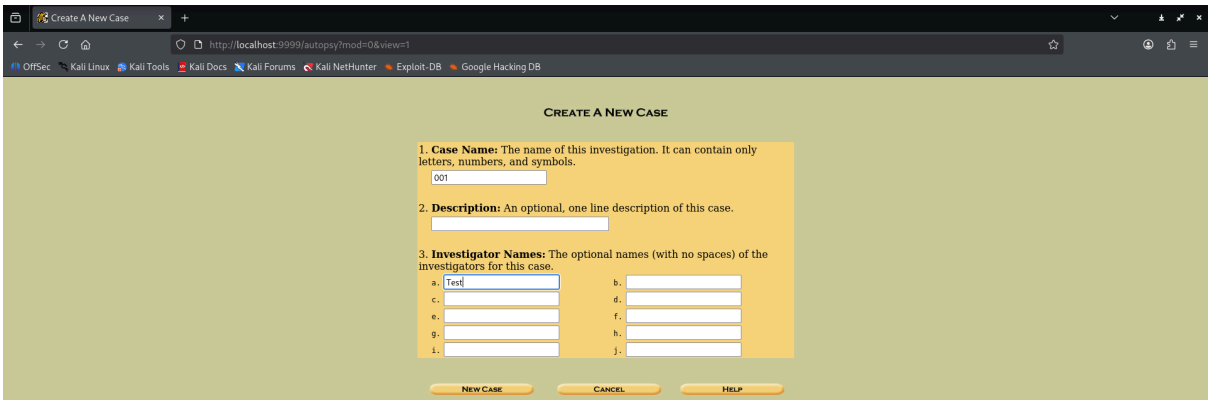
Company	Miami-dade County
Contact	NA
Phone	3055968909
Email	Luna@miamidade.gov
Attn	Itd Radio Division - Miguel Luna
Address	5680 Sw 87th Ave

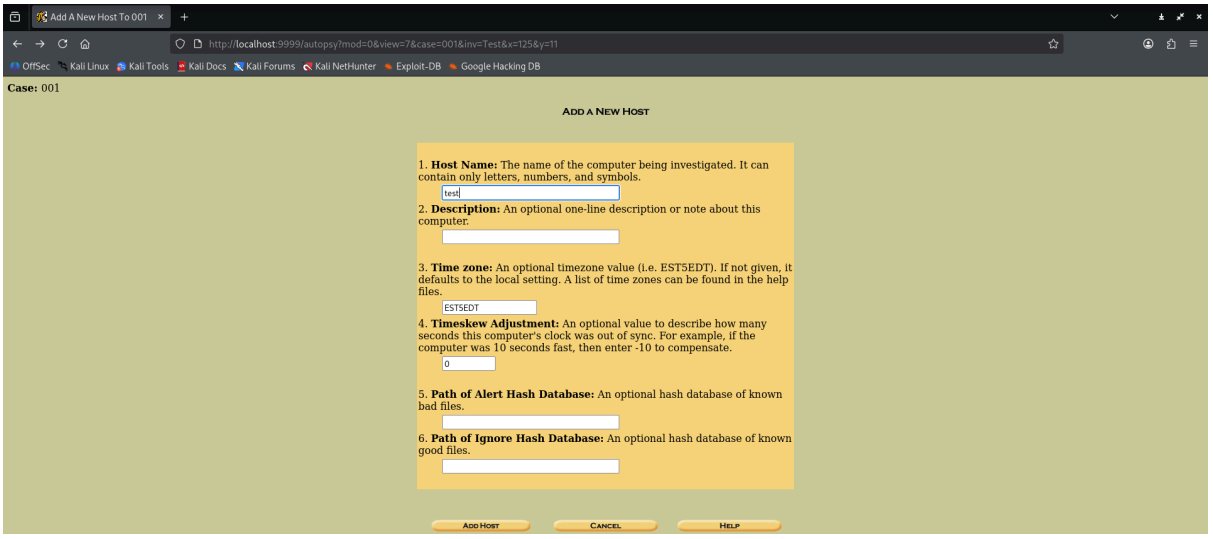
- Open WiFiSpots.com – to identify public Wi-Fi networks

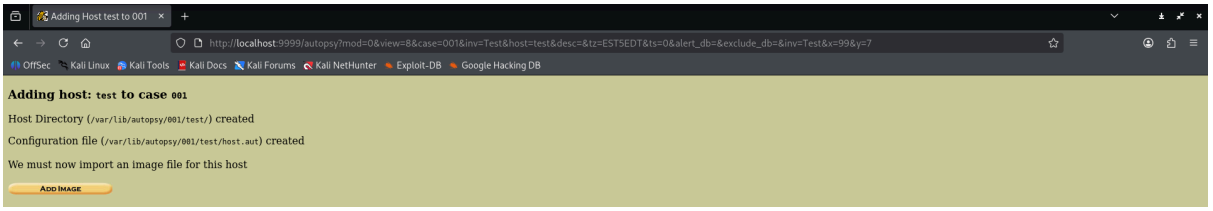


- **Autopsy** – forensic analysis tool

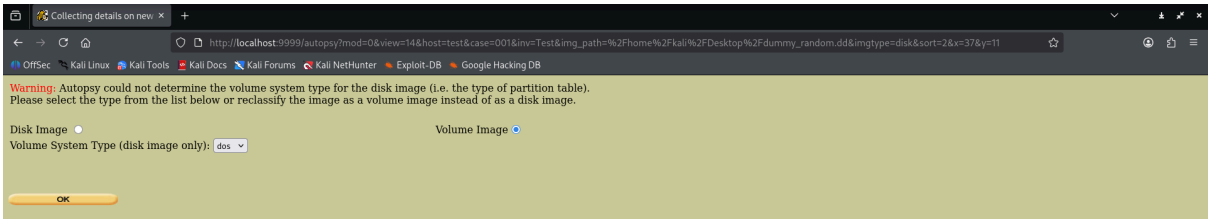


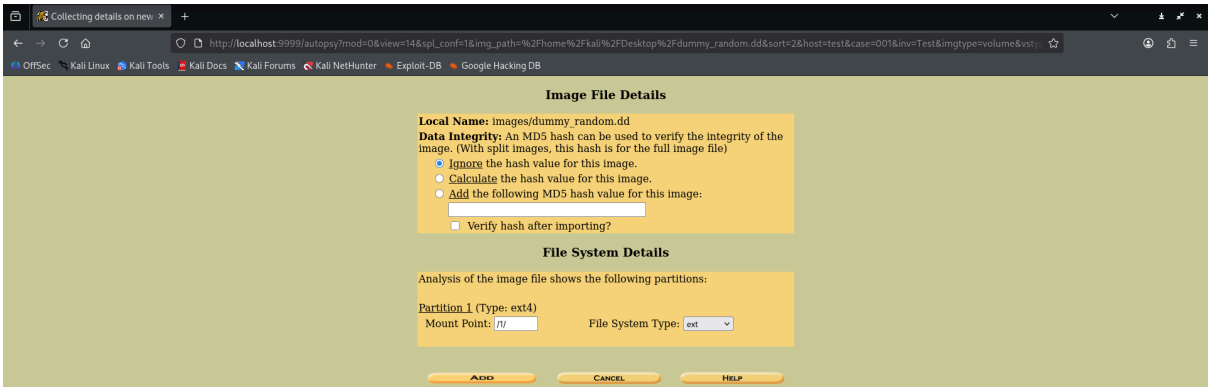


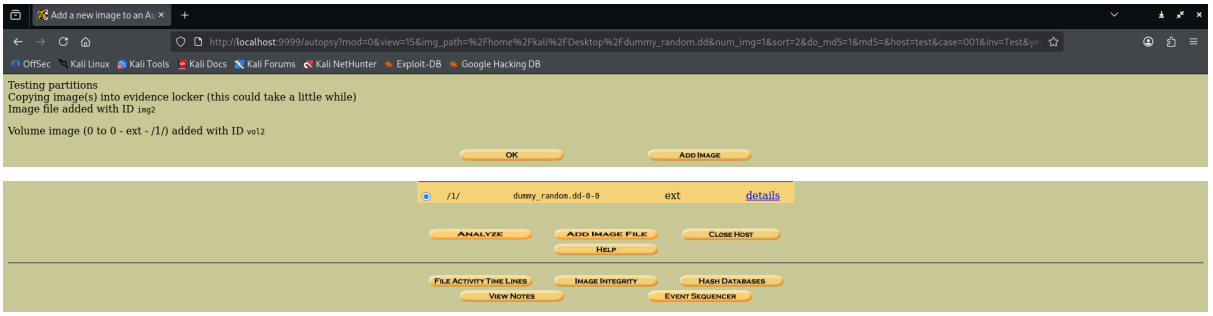




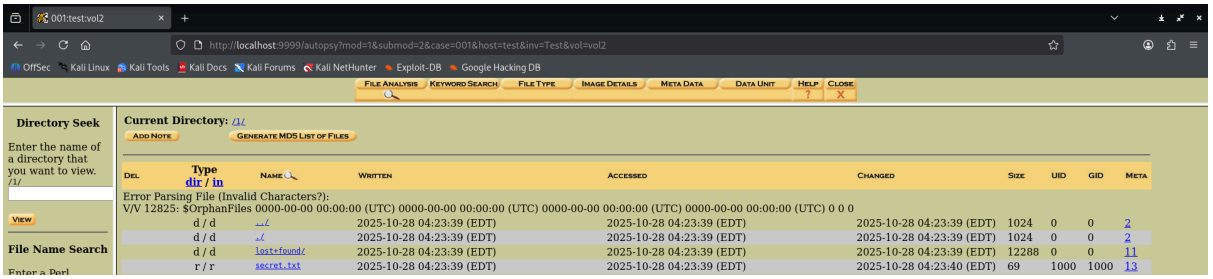

Add Image To 001:test
http://localhost:9999/autopsy?mod=0&view=13&host=test&case=001&inv=Test&x=100&y=7
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Case: 001
Host: test
ADD A NEW IMAGE
1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
/home/kali/Desktop/dummy_random.dd
2. Type
Please select if this image file is for a disk or a single partition.
Disk
Partition
3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
Symlink
Copy
Move
NEXT
CANCEL
HELP

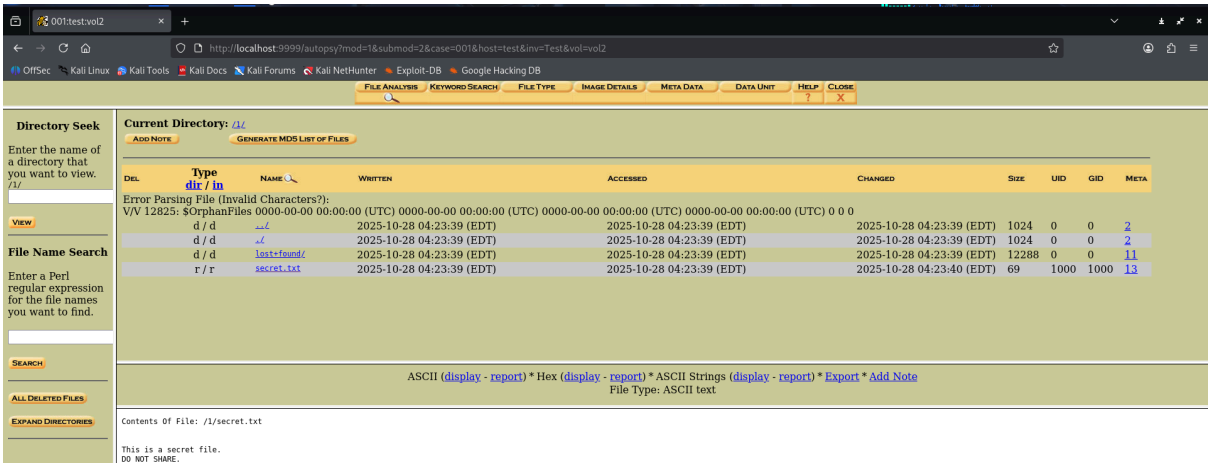

Collecting details on new
http://localhost:9999/autopsy?mod=0&view=14&host=test&case=001&inv=Test&img_path=%2Fhome%2Fkali%2FDesktop%2Fdummy_random.dd&imgtype=disk&sort=2&x=37&y=11
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table).
Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.
Disk Image
Volume Image
Volume System Type (disk image only): dos
OK


Collecting details on new
http://localhost:9999/autopsy?mod=0&view=14&spl_conf=1&img_path=%2Fhome%2Fkali%2FDesktop%2Fdummy_random.dd&sort=2&host=test&case=001&inv=Test&imgtype=volume&vsty
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Image File Details
Local Name: images/dummy_random.dd
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
Ignore the hash value for this image.
Calculate the hash value for this image.
Add the following MD5 hash value for this image:
Verify hash after importing?
File System Details
Analysis of the image file shows the following partitions:
Partition 1 (Type: ext4)
Mount Point: /1/
File System Type: ext
ADD
CANCEL
HELP


Add a new image to an A
http://localhost:9999/autopsy?mod=0&view=15&img_path=%2Fhome%2Fkali%2FDesktop%2Fdummy_random.dd&num_img=1&sort=2&do_md5=1&md5=&host=test&case=001&inv=Test&
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Testing partitions
Copying image(s) into evidence locker (this could take a little while)
Image file added with ID img2
Volume image (0 to 0 - ext - /1/) added with ID vol2
OK
ADD IMAGE

/1/ dummy_random.dd-0-0 ext details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER





- **FTK Imager** or **dc3dd** – imaging tool

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0 80.1G  0 disk
└─sda1   8:1    0 80.1G  0 part /
sdb      8:16   1 14.6G  0 disk
└─sdb1   8:17   1 14.6G  0 part
sr0     11:0    1 1024M  0 rom
```

```
┌──(kali㉿kali)-[~]
└─$ sudo dc3dd if=/dev/sdb of=/mnt/forensic/usb_image.dd log=/mnt/forensic/dc3dd_log.txt hash=sha256

dc3dd 7.2.646 started at 2025-10-28 05:00:23 -0400
compiled options:
command line dc3dd if=/dev/sdb of=/mnt/forensic/usb_image.dd log=/mnt/forensic/dc3dd_log.txt hash=sha256
device size: 30515200 sectors (probed),   15,623,782,400 bytes
sector size: 512 bytes (probed)
   266633216 bytes ( 254 M ) copied (  2% ),   28 s, 9 M/s

input results for device `/dev/sdb':
   520768 sectors in
   0 bad sectors replaced by zeros
   e2fa153068794b8301b98f8c63eb8f1b5511d525e43c4eab9a1d995a240174ad (sha256)

output results for file `/mnt/forensic/usb_image.dd':
   520768 sectors out

dc3dd aborted at 2025-10-28 05:00:52 -0400
```

```
┌──(kali㉿kali)-[~]
└─$ sha256sum /mnt/forensic/usb_image.dd > /mnt/forensic/image_sha256.txt
```

```
┌──(kali㉿kali)-[~]
└─$ cat /mnt/forensic/image_sha256.txt
e2fa153068794b8301b98f8c63eb8f1b5511d525e43c4eab9a1d995a240174ad

┌──(kali㉿kali)-[~]
└─$ sha256sum /mnt/forensic/usb_image.dd

e2fa153068794b8301b98f8c63eb8f1b5511d525e43c4eab9a1d995a240174ad
```

- **Hash calculator** (MD5/SHA1)

```
┌──(kali㉿kali)-[~/Desktop]
└─$ md5sum ctf3.jpg
8de3393dde3b78b37fce868eb3f0d263  ctf3.jpg
```

10.7 Conclusion:

The experiment successfully demonstrated core practices in mobile device forensics, including cellular antenna search, proper confiscation procedures, suspect tracking using Wi-Fi data, and safe SD card evidence extraction and analysis. By using antistatic gloves and Faraday bags, handling and confiscation were performed in a forensically sound manner, preventing contamination and remote tampering. The cellular antenna and Wi-Fi hotspot lookup enabled effective mapping of the device's potential locations and movement patterns. Extracting and imaging the SD card allowed for detailed analysis with Autopsy, where files, logs, and metadata were examined without altering original evidence. Hashing further ensured that all forensic copies remained authentic, supporting the integrity and admissibility of collected evidence.