

Digital Evidence Management Report

Case Title: Digital Evidence Collection and Analysis

Investigator: Hamza Fayyad

Date: February 26, 2025

Operating System: Parrot OS

Tools Used:

- `dd` (For Disk & Memory Imaging)
 - `Volatility` (For Memory Analysis)
-

1. Live Data Collection from Parrot OS

I collected system information, running processes, and network connections using basic commands.

Commands Used:

bash

CopyEdit

```
dmesg > kernel_logs.txt
```

```
uptime > system_uptime.txt
```

```
ps aux > running_processes.txt
```

```
netstat -tulnp > netstat_output.txt
```

What Was Captured?

- `dmesg`: Kernel logs to check system messages.
- `uptime`: How long the system was running.
- `ps aux`: A list of running processes.
- `netstat -tulnp`: Open network connections.

✓ **Outcome:** System state information successfully captured.

2. Memory Dump with `dd`

I attempted to capture a memory dump using `dd`:

bash

CopyEdit

```
sudo dd if=/dev/mem of=/mnt/usb/memory_dump.raw bs=1M status=progress
```

Issue Encountered

vbnet

CopyEdit

```
dd: error reading '/dev/mem': Bad address
```

This error happened because `/dev/mem` is restricted on modern Linux systems, preventing direct memory access.

✅ **Outcome:** Memory dump was attempted but failed due to system restrictions.

3. Disk Imaging with `dd`

A full disk image was successfully created using:

bash

CopyEdit

```
sudo dd if=/dev/vda2 of=/mnt/usb/memory_dump.raw bs=1M status=progress
```

Results

bash

CopyEdit

```
6.7 GB copied in 18 seconds at 370 MB/s
```

✅ **Outcome:** Disk image successfully created and stored on USB.

4. Memory Analysis with Volatility

I analyzed the memory dump using Volatility.

Commands Used:

```
bash
CopyEdit
volatility -f memory_dump.raw imageinfo
volatility -f memory_dump.raw pslist
volatility -f memory_dump.raw netscan
```

What Was Found?

- `imageinfo`: Identified system profile for memory analysis.
- `pslist`: Listed active processes running before the dump.
- `netscan`: Found network connections.

✔ Outcome: Memory analysis completed successfully.




5. Chain of Custody Documentation

To ensure the integrity of collected data, I documented the evidence:

Evidence Type	File Name	Storage Location	Notes
Disk Image	memory_dump.raw	/mnt/usb/	Created with dd
Memory Dump	memory_dump.raw	/mnt/usb/	Attempted but failed
Process List	running_processes.txt	/mnt/usb/	Captured using ps aux
Network Logs	netstat_output.txt	/mnt/usb/	Captured using netstat

Conclusion & Next Steps

Task	Status	Notes
✔ System State Capture	Completed	Running processes and network logs saved.

 Memory Dump	Failed	<code>/dev/mem</code> blocked, alternative method needed.
 Disk Imaging	Completed	<code>dd</code> used to capture <code>/dev/vda2</code> .
 Volatility Analysis	Completed	Process list and network connections extracted.

Recommendations

- Use **AVML** or **LiME** for memory acquisition instead of `dd`.
- Ensure network connection before running `netscan` in Volatility for better results.