Digital Evidence Management Report

# 1. Live Data Collection (Parrot OS)

During the investigation, live system data was collected from the Parrot OS environment. This included capturing the current system state, listing running processes, and enumerating active network connections.

Commands executed:

* • who
* • uptime
* • ps aux > /mnt/usb/pslist.txt
* • netstat -tulnp > /mnt/usb/netstat.txt
* • last > /mnt/usb/lastlogins.txt

Mock Output Snapshot:  
- Active users: ceo\_login, root  
- Notable process: /tmp/evil\_script.sh (PID 4578)  
- Network connection: 192.168.1.5:4444 -> 203.0.113.77 (external)

# 2. Memory Analysis Using Volatility

Memory dump was created using the `dd` command and analyzed using Volatility 3.

Command used:

* • dd if=/dev/mem of=/mnt/usb/memdump.img bs=1M

Volatility plugins used:

* • linux.pslist
* • linux.netstat
* • linux.bash

Mock Findings:  
- Suspicious process 'evil\_script.sh' (PID 4578) found in memory  
- Network connection to C2 server IP: 203.0.113.77:4444  
- Bash history confirmed execution of unknown base64-decoded payload

# 3. Disk Acquisition (Parrot OS)

Disk image captured using `dd` tool.

Command:

* • dd if=/dev/sda of=/mnt/usb/disk\_image.img bs=4M status=progress

Hashes calculated for integrity:

* • md5sum disk\_image.img > disk\_image.md5
* • sha256sum disk\_image.img > disk\_image.sha256

# 4. Chain of Custody

Chain of custody for digital evidence is maintained as shown below:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Time | Evidence | Collected By | Stored Location | Hash Verified | Notes |
| 2025-04-25 15:30 | memdump.img | Analyst A | /mnt/usb/ | Yes | Captured post-login compromise |
| 2025-04-25 15:40 | disk\_image.img | Analyst A | /mnt/usb/ | Yes | Image saved & hashed |

# 5. Timeline Correlation (macOS + Parrot OS)

Combined log events from macOS and Parrot OS were analyzed to build a timeline of the incident.

Sample Timeline:

|  |  |  |  |
| --- | --- | --- | --- |
| Time | System | Event | Details |
| 15:20 | Parrot OS | Failed login (ceo\_login) | Brute-force from Russia |
| 15:27 | Parrot OS | Successful login | Via python-requests |
| 15:35 | Parrot OS | Malware executed | evil\_script.sh started |
| 15:36 | macOS | No activity | Confirms external attack |
| 15:40 | Parrot OS | Memory captured | Investigation started |