Digital Evidence Management Documentation

1. Overview This document details digital evidence collection and management activities performed in the IR environment using Parrot OS and macOS. It includes live data capture, memory and disk acquisition, event timeline creation, and chain of custody tracking for all evidence.

---

2. Live Data Collection on Parrot OS

2.1 System State Capture

```
uname -a > system_info.txt
uptime >> system_info.txt
who -a >> system_info.txt
```

2.2 Running Processes

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

2.3 Network Connections

```
netstat -tulnp > net_connections.txt
ss -anpt >> net_connections.txt
```

Evidence Files:

- `system_info.txt`
- `running_processes.txt`
- `net_connections.txt`

---

3. Memory Acquisition and Analysis (Volatility)

3.1 Memory Dump Using LiME

```
insmod lime.ko "path=/root/memdump.lime format=lime"
```

3.2 Basic Memory Analysis Commands

```
vol.py -f memdump.lime --profile=LinuxParrot pslist > pslist_output.txt
vol.py -f memdump.lime --profile=LinuxParrot netscan > netscan_output.txt
```

Evidence Files:

- `memdump.lime`
- `pslist_output.txt`
- `netscan_output.txt`

---

4. Disk Imaging on Parrot OS

4.1 Using `dd` for Disk Acquisition

sudo dd if=/dev/sda of=/mnt/usb/parrot_disk.img bs=4M status=progress

4.2 Hash Verification

sha256sum /mnt/usb/parrot_disk.img > disk_hash.txt

Evidence Files:

- `parrot_disk.img`
- `disk_hash.txt`

---

5. Chain of Custody Documentation

Format:

Evidence ID	Collected By	Date/Time	Description	Location	Integrity Check
EVID-001	Analyst A	2024-11-22 03:00	Parrot memory dump	/root/memdump.lime	SHA256: abc123
EVID-002	Analyst A	2024-11-22 03:15	Parrot disk image	/mnt/usb/parrot.img	SHA256: def456
EVID-003	Analyst B	2024-11-22 03:30	Running process list	running_processes.txt	Manual reviewed

---

6. Timeline Creation & Event Analysis

6.1 Data Sources:

- Parrot OS: `/var/log/auth.log`, `syslog`, Wazuh alerts
- macOS: Syslog forwarded entries

6.2 Sample Timeline (Condensed)

Timestamp	Event Description	Source
03:14:55	SSH attempt from macOS to Parrot OS	macOS logs
03:14:57	Failed password log in `/var/log/auth.log`	Parrot OS
03:15:00	Alert triggered in Wazuh	Wazuh
03:15:30	Memory captured via LiME	Parrot OS
03:16:00	Disk image created via `dd`	Parrot OS

---

7. Conclusion All digital evidence procedures followed industry practices, including proper data capture, secure storage, and documentation. The chain of custody and timeline support the IR workflow and investigation transparency.

End of Document