Evidence Preservation - Real Collection & Chain of Custody

Collection Details

Collection Date: 2025-11-21
Collection Method: Windows PowerShell + Velociraptor Agent
Collected By: Mr_Chandan_Prasad
System: Windows Host
Purpose: Evidence Preservation

Collected Evidence Files

Evidence ID	Filename	Type	Collection Method	SHA256 Hash
EV-001	netstat_20251121.txt	Network Connections	netstat -ano	2A89028B4F8576845961D7B376C3CA361205B079C111822FC20FC6094B0229D7
EV-002	network_connections.csv	Network Connections (Detailed)	Get-NetTCPConnection	A3AC1B038181958D58EA604125B6C99C404ED3BAB7ADC009ACBFB30204F60F69
EV-003	process_list.csv	Process Memory Snapshot	Get-Process	25BB6DC849B2F01C21EE209AD41649ED9BDB08CC62CBFAAFA371E011A623570D
EV-004	systeminfo.txt	System Information	systeminfo	5B23035F6EB5DD471ED4691889004849D8DEB0A902CC0167017A720AE3453F29

Chain of Custody Log

Timestamp	Evidence ID	Action	Handled By	Status	Notes
2025-11-21 14:03:00	EV-001	Created	SOC Analyst	Collected	Netstat snapshot at collection time
2025-11-21 14:03:00	EV-002	Created	SOC Analyst	Collected	Network connections exported to CSV
2025-11-21 14:03:00	EV-003	Created	SOC Analyst	Collected	Running processes memory snapshot
2025-11-21 14:03:00	EV-004	Created	SOC Analyst	Collected	System configuration snapshot
2025-11-21 14:04:00	ALL	Hashed (SHA256)	SOC Analyst	Verified	Hash verification complete
2025-11-21 14:05:00	ALL	Transfer to Kali	SOC Analyst	In Progress	Transferring to backup location

---

Evidence Content Summary

EV-001: netstat_20251121.txt

Purpose: Network connections at time of collection
Contents:

- Active TCP/UDP connections
- Local and remote addresses with ports
- Connection states (ESTABLISHED, LISTENING, etc.)
- Associated Process IDs (PIDs)

EV-002: network_connections.csv

Purpose: Detailed network connections in structured format
Columns:

- LocalAddress
- LocalPort
- RemoteAddress
- RemotePort
- State

EV-003: process_list.csv

Purpose: Running processes and memory usage snapshot
Columns:

- Name (Process Name)
- Id (Process ID)
- Memory(MB) (Memory consumption)

EV-004: systeminfo.txt

Purpose: System configuration and environment
Contents:

- OS version and build
- System name and domain
- Hardware information
- Network configuration
- Installed software versions

Integrity Verification

Hash Verification Process

All evidence files were hashed using SHA256 algorithm via PowerShell:

powershell

```
Get-FileHash <file> -Algorithm SHA256
```

Verification Steps:

1. Initial hash calculated at time of collection
2. Hash stored in separate .sha256 files
3. Hash will be re-verified before analysis
4. Any hash mismatch indicates tampering

Hash Values (as collected)

EV-001 (netstat_20251121.txt):

2A89028B4F8576845961D7B376C3CA361205B079C111822FC20FC6094B0229D7

EV-002 (network_connections.csv):

A3AC1B038181958D58EA604125B6C99C404ED3BAB7ADC009ACBFB30204F60F69

EV-003 (process_list.csv):

25BB6DC849B2F01C21EE209AD41649ED9BDB08CC62CBFAAFA371E011A623570D

EV-004 (systeminfo.txt):

5B23035F6EB5DD471ED4691889004849D8DEB0A902CC0167017A720AE3453F29

Collection Workflow

Step 1: Created C:\Evidence directory

↓

Step 2: Ran collection commands

- netstat -ano

- Get-NetTCPConnection

- Get-Process

- systeminfo

↓

Step 3: Exported to structured formats (TXT, CSV)

↓

Step 4: Calculated SHA256 hashes

↓

Step 5: Verified file integrity

↓

Step 6: Documented chain of custody

↓

Step 7: Prepared for transfer to Kali

Evidence Storage & Security

Current Location: C:\Evidence\

Security Controls:

- Files stored on Windows host
- Hashes documented and verified
- Chain of custody log maintained
- Ready for transfer to secure backup location

Next Steps:

1. Transfer files to Kali Linux backup
2. Store on external USB drive (if available)
3. Create GitHub repository with documentation
4. Maintain hash verification throughout

Forensic Analysis Notes

Collection Method: Live system collection (forensically sound)
Scope: Network connections, running processes, system configuration
Limitations: Live collection may miss some volatile data (memory dump recommended for full forensics)
Admissibility: Chain of custody maintained, hashes verified, suitable for legal proceedings

Lessons Learned

- Successfully collected REAL evidence from Windows host
- Implemented proper SHA256 hashing
- Maintained chain of custody documentation
- Used forensically sound collection methods
- Future improvement: Add memory dump collection (FTK Imager)
- Future improvement: Add disk image if needed for deeper analysis