

4. Evidence Preservation

Item	Description	Collected By	Date	Hash Value
Memory Dump	Memory image of affected workstation	SOC Analyst	2025-08-18	c1a92b4d8f2e24db88a6c98e4e70fd59
System Logs	Security and Application Event Logs from the affected workstation	SOC Analyst	2025-08-18	A3b4c5d6e7f80g1h2i3j4k5l6m7n8o9p
Network Traffic (PCAP)	Relevant network packet capture from the time of the incident	Network E... ▾	2025-08-18	1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e

- Evidence was collected without modifying the original system.
- A memory dump was preserved and hashed to maintain data integrity.
- System logs were also secured to provide a timeline of events.
- Access to evidence was restricted to SOC analysts only.
- This ensures proper chain-of-custody for investigation and legal requirements