# EVIDENCE COLLECTION LOG

## Instructions:

## This form is used to track the collection of digital artifacts during an incident response investigation.

## Every piece of evidence (log file, memory dump, email header, etc.) must be logged here.

| Incident ID | Artifact ID | Artifact Type | Source System/Location | Collection Date/Time (UTC) | Collected By | MD5 Hash | SHA256 Hash | Notes |
|---|---|---|---|---|---|---|---|---|
| IR-2025-042 | 001 | Email Header | Affected User Mailbox | 2025-11-05 09:40 | T. Ajose | N/A | N/A | Header extracted to .msg file; contained malicious URL. |
| IR-2025-042 | 002 | Endpoint Memory Dump | WORKSTATION-TOLU-001 | 2025-11-05 11:15 | T. Ajose | [MD5 HASH] | [SHA256 HASH] | Collected before system shutdown for volatile data analysis. |
| IR-2025-042 | 003 | Splunk Export (.csv) | Splunk Index: Security | 2025-11-05 12:30 | T. Ajose | N/A | N/A | Authentication logs for the last 72 hours. |
| IR-2025-042 | 004 | Malware Sample | C:\Temp\WinUpdate.exe | 2025-11-05 14:00 | T. Ajose | [MD5 HASH] | [SHA256 HASH] | Executable quarantined by EDR; hash collected for VT check. |
| [Placeholder] | | | | | | | | |
| [Placeholder] | | | | | | | | |
| [Placeholder] | | | | | | | | |