Forensic Investigation Report

Case ID: DF-2025-041

Investigator: Jordan Blake

Date: April 26, 2025

1. Introduction

This report documents the full forensic investigation process conducted on a digital asset suspected of being involved in unauthorized access activities at **AcmeTech Solutions Inc.** The investigation strictly followed industry best practices, ensuring evidence integrity, reproducibility of findings, and compliance with legal and ethical standards.

Procedures applied:

- NIST 800-86 Forensic Process Model
- SWGDE Best Practices for Digital Evidence
- Evidence Handling Procedures (Maintaining Data Integrity)
- Chain of Custody Maintenance
- Secure Initial Response Techniques

2. Case Overview

Item	Details
Incident Type	Unauthorized Remote Access Investigation

System	Windows 10 Pro Workstation, Hostname: ACM-WS-32
Suspected Media	Internal HDD (500GB Western Digital SATA)
Seizure Location	Office Room 402B, AcmeTech Solutions HQ
Initial Notifier	IT Security Officer - Melissa Grant

---

3. Forensic Investigation Methodology

3.1 Initial Response Techniques

- **Scene Securing**:

  Workstation photographed in powered-on state.

  Time: **April 25, 2025, 10:13 AM EST**.

- **System State Documentation**:

  Windows session logged in as user jdoe.

  IP address at time of seizure: 192.168.1.45.

- **Live Data Collection**:
  - **Memory Capture**:
    - Tool: **Belkasoft RAM Capturer v1.8**
    - Filename: ACM-WS-32_RAM.dmp
    - Size: 7.8 GB

    - **Network Connections Snapshot**:
        - netstat -ano output saved.
        - Noted suspicious outbound connection to 185.102.219.55:443.
- **Safe Shutdown**:

  After capture, Windows was shut down using shutdown /s /f /t 0 command.

Justification: RAM collection prioritized because of its volatile nature. TCP connections could be evidence of live C2 activity.

3.2 Evidence Collection

- **Disk Imaging**:
    - Tool: **FTK Imager 4.7.1**
    - Device Connection: **Tableau T35u USB 3.0 Write Blocker**
    - Image Filename: ACM-WS-32_Disk.E01
    - Compression: Enabled (10%)
- **Hash Verification**:

Evidence ID	Description	Hash (SHA-1)	Hash (MD5)	Status
EVID-001	RAM Capture	cdb4a8c8d4d5e87b92a548b95b67a8cde3b1b467	9f4b5e5c89e7287d5c96e985a1ef3f78	Verified
EVID-002	Disk Image	a1b7d92983c98d2d5f85b4e5be8e8dcb2a7e71af	7c4ff2db03be7273a9875a2be94e90e2	Verified

(E01
Format)

Justification: Forensic-grade disk imaging ensures an exact duplicate, preserving all filesystem metadata and slack space artifacts.

3.3 Chain of Custody Log

Date/Time	Handler	Action	Comments
04/25/2025 10:15 AM	Jordan Blake	Seized workstation	Photos taken; Bagged evidence
04/25/2025 10:40 AM	Jordan Blake	RAM captured	Copied to encrypted USB SSD
04/25/2025 11:30 AM	Jordan Blake	Full disk image created	Stored on FIPS 140-2 SSD
04/25/2025 12:00 PM	James Stone (Evidence Custodian)	Evidence checked into Locker #A12	Locked under 24/7 video surveillance

3.4 Forensic Analysis Procedures

RAM Analysis:

- **Tool**: Volatility Framework 2.6
- Profile: Win10x64_18362
- Key Results:
  - Suspicious svchost.exe instance (PID 1048) connecting externally.

-
    - Memory artifacts showed Mimikatz tool signatures indicating possible credential dumping.

Disk Image Analysis:

- **Tools Used**:
    - Autopsy 4.20
    - FTK 7.4
- **Findings**:
    - **Malware**:
        - Executable C:\Users\jdoe\AppData\Roaming\svhost32.exe
        - Hash: e59ff97941044f85df5297e1c302d260
        - VirusTotal Detection: 55/67 engines flagged.
    - **Browser Artifacts**:
        - Chrome history revealed frequent visits to suspicious URL hxxps://malicious-example.com.
        - Login session cookies stored unencrypted.
    - **Deleted Files**:
        - Recovered C2_config.txt showing IP addresses: 185.102.219.55 and 77.111.247.57.

Timeline Analysis:

- **Tool**: Plaso (Log2Timeline)
- Events of Interest:
    - Malware installed: April 20, 2025, 3:22 PM EST
    - First C2 communication detected: April 21, 2025, 2:15 AM EST

    - Hidden admin account creation: admin$ created on April 21, 2025, 2:17 AM EST

3.5 Reporting and Preservation

- **Artifacts and logs archived**:
    - Case folder encrypted with AES-256.
    - Secondary backup stored offline.
- **Documentation completed**:
    - RAM Analysis Report
    - Disk Artifact Report
    - Timeline Spreadsheet
    - Chain of Custody Log

---

4. Findings

Evidence	Artifact	Analysis Outcome
RAM	Unauthorized svchost.exe connection	Active C2 communication
RAM	Credential dumping evidence	Potential privilege escalation
Disk	Malware executable (svhost32.exe)	Persistence via startup task

Disk	Hidden admin account (admin$)	Unauthorized privilege escalation
Disk	Browser History	Connection to known malicious domain
Disk	Recovered C2 configuration file	Hardcoded external server IPs

5. Conclusion

The forensic examination concluded that ACM-WS-32 was compromised through the installation of a trojan that established a Command and Control channel with external malicious servers. Volatile memory analysis confirmed credential harvesting activities. Disk artifacts evidenced malware persistence and creation of unauthorized administrative access.

All forensic actions were conducted following established best practices, and the evidence integrity was rigorously maintained throughout the process.

6. Recommendations

- Immediate system reimaging to eliminate rootkits.
- Enterprise password reset for affected accounts.
- Enable Endpoint Detection and Response (EDR) solutions company-wide.
- Conduct cybersecurity awareness refresher training.
- Conduct an external audit of AcmeTech’s current network security posture.