

GlobalTech Corp DFIR Research Paper

COSC 435 – Computer & Network Security

Fall 2025

By: Duran Anderson, D'Marco Rodgers

Abstract

This research paper explains the foundations behind the Digital Forensics and Incident Response (DFIR) Playbook created for GlobalTech Corp. The goal is to break down real incident response standards, especially those used during targeted ransomware attacks. The paper uses industry frameworks like NIST SP 800-61, NIST SP 800-86, and RFC 3227 to explain how incident responders collect evidence, handle volatile memory, analyze forensic artifacts, and follow a structured Incident Response lifecycle. It also includes real tools like FTK Imager, WinPMMEM, Autopsy, and Volatility, which are all required in the project. Finally, this paper connects modern DFIR methods to real-world cyberattacks and shows how a playbook improves GlobalTech's readiness and reduces damage during incidents.

Introduction

This project is about **Project 8: DFIR Playbook** - a clear step-by-step guide for dealing with serious ransomware attacks at GlobalTech. As the professor wanted, it walks through every stage of incident response - starting with Prep, then spotting threats, limiting damage, removing malware, getting systems back online, and finally reviewing what happened. Instead of just listing tools, it brings in memory capture, copying hard drives, gathering digital clues, along with how to examine them closely. The info here supports each move outlined in that plan.

Background on DFIR

Incident Response Frameworks

The go-to guide for DFIR tasks is NIST SP 800-61 Rev 2. This doc lays out the real Incident Response Lifecycle.

NIST SP 800-86 shows ways to blend forensics into each IR step by handling evidence carefully while keeping it intact.

RFC 3227 lays out clear rules about the "Order of Volatility," so you know what evidence to grab right away - since some data disappears fast. Instead of waiting, start with what's most likely to vanish, because timing really matters when gathering digital clues.

Mitre Att&ck shows how real hackers act - like ransom gangs do things.

These sources - when combined - form the base of a solid DFIR playbook.

Why Ransomware Requires DFIR

Modern ransomware strikes quickly. The 2024 CrowdStrike report shows attackers break out in under 79 minutes - so they spread between systems while teams are still catching up. Groups such as Ryuk, Conti, or LockBit steal login details (MITRE ATT&CK T1003), wipe backup data (T1490), then jump across networks (T1021).

This quick pace means teams must follow clear steps - showing precisely what to gather, while separating devices carefully so proof stays intact.

DFIR Playbook Structure Aligned to the Project

435 Group Project

(Using exact requirements from Project 8)

3.1 Preparation

This includes enabling detailed logging, setting up Sysmon, training the IR team, preparing storage for evidence, and maintaining offline backups. NIST says preparation is the most important phase because it directly affects every response action.

3.2 Identification

Teams confirm whether a security event is an actual ransomware attack. Indicators include:

- Encrypted files with changed extensions
- Ransom notes
- Unauthorized remote access
- Suspicious PowerShell or WMI usage
- Sudden changes in CPU or network activity

Logs examined include:

- Windows Event Logs
- Sysmon events 1, 3, 7, 11
- Firewall and DNS logs
- EDR alerts

3.3 Containment

GlobalTech must isolate compromised systems without shutting them down.

According to **NIST SP 800-61**, containment should be immediate and may include:

- Disconnecting from network
- Killing malicious processes
- Blocking known malicious IP addresses
- Taking VM snapshots

3.4 Volatile Evidence Acquisition

Memory contains:

- Encryption keys
- Injected malware
- Network connections
- Credentials in memory

Tools include:

- **WinPMMEM**
- **FTK Imager (memory mode)**

This follows **RFC 3227's Order of Volatility**.

3.5 Disk Imaging

After memory, responders take a full forensic image using:

- **FTK Imager** (E01 format)
- SHA-256 hashing
- Write blockers

Disk images preserve:

- Ransomware executables
- Deleted shadow copies
- Registry Run keys
- Persistence methods

3.6 Eradication & Recovery

Eradication removes the malware and persistence. Recovery restores from clean backups and confirms that the ransomware is no longer present. According to NIST, all restored systems must be validated before going back online.

3.7 Lessons Learned

This phase updates the playbook based on what went well or poorly. GlobalTech should also add new detection rules and patch exploited vulnerabilities.

Forensic Artifacts Collected During Ransomware Analysis

Based on **NIST SP 800-86** and real case studies:

Artifacts to Collect

- Memory dump
- \$MFT and \$LogFile
- Browser history
- Prefetch files
- Registry hives
- Event logs
- Sysmon logs
- PowerShell history
- Network PCAPs
- Ransom note and binary

Analysis Focus

specifies artifacts including:

- Ransomware executables
- Shadow volume deletion commands
- C2 communication

These appear in logs as:

- vssadmin delete shadows
- wmic shadowcopy delete
- powershell.exe -enc ...
- Suspicious outbound connections

5. Tools Used (Required by Project 8)

Memory Acquisition Tools

- **WinPMEM**
- **FTK Imager (live memory mode)**

Disk Forensics

- **FTK Imager (E01 format)**
- **Autopsy (GUI analysis)**

Memory Analysis

- **Volatility Framework**
(Industry standard for analyzing memory dumps)

Log Analysis

- **ELK Stack**
- **Sysmon**
- **Windows Event Viewer**

Network Forensics

- **Wireshark**
- **Zeek**

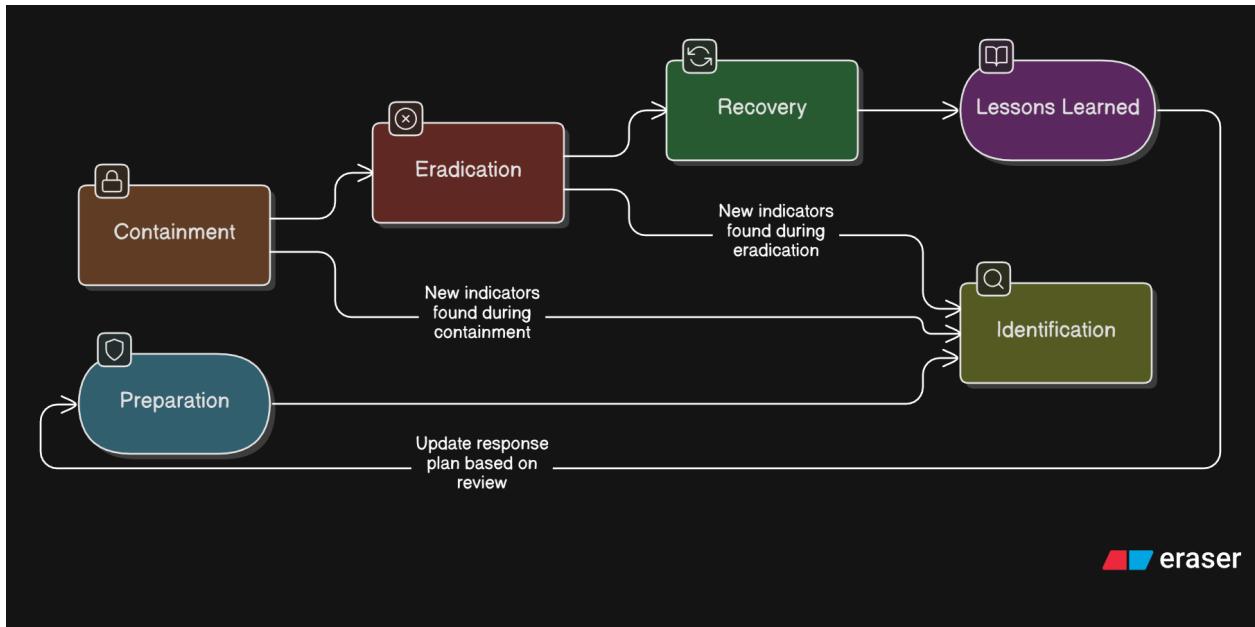
These tools directly match the project requirements and real IR workflows.

Timeline Reconstruction

Timeline reconstruction is one of the most important parts of DFIR. Analysts combine timestamps from different sources to map out the attack:

Phishing Event → Initial Execution → Privilege Escalation → Lateral Movement → Payload Deployment → Encryption

DFIR Workflow Diagram:



Summary

This research explains main points from the GlobalTech DFIR Playbook. Built on reliable standards such as NIST SP 800-61, alongside MITRE ATT&CK and RFC 3227. Shows how structured steps help handle digital clues while choosing proper analysis tools. Rather than confusion, teams stay organized during probes. Since ransomware changes fast, the guide matches today's threat behaviors. A step-by-step incident response plan cuts breach impact; also trims recovery time while boosting security gradually. Once threats strike, following this guide lets GlobalTech respond quicker and more effectively with greater resilience.

References (APA-Style)

NIST SP 800-61 Rev. 2. (2012). *Computer Security Incident Handling Guide*. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

NIST SP 800-86. (2006). *Guide to Integrating Forensics Techniques into Incident Response*. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

RFC 3227. (2002). *Guidelines for Evidence Collection and Archiving*. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc3227>

MITRE ATT&CK Framework. MITRE Corporation. <https://attack.mitre.org>

CrowdStrike. (2024). *Global Threat Report*. CrowdStrike Inc. <https://www.crowdstrike.com/resources/reports/global-threat-report>