

# Incident Response & Digital Forensics Report – Week 2

**Incident Type:** Ransomware Simulation

**Environment:** Windows 10 – Local Simulation

## 1. Introduction

This report documents all activities performed during the second week of the Incident Response & Digital Forensics project. The primary objective for this week was to conduct a simulated cybersecurity incident, collect all available evidence, ensure its integrity, and prepare the necessary documentation to track and analyze the incident.

The specific goals for Week 2 were as follows:

- **Simulate a Cybersecurity Incident:** Execute a controlled attack using a safe ransomware script.
- **Collect Evidence:** Gather all possible digital evidence from the target environment.
- **Ensure Evidence Integrity:** Generate hashes for each piece of evidence to verify its authenticity.
- **Prepare an Incident Timeline:** Document the sequence of events accurately.
- **Create a Chain of Custody:** Document the handling and transfer of evidence.
- **Acquire a Memory Image:** Extract a memory dump for forensic analysis.

All activities were performed in an isolated and controlled environment to ensure no actual harm to the system.

## 2. Incident Simulation

To achieve the project's objectives, a safe PowerShell script was used to simulate the behavior of ransomware without actually encrypting files. This allowed for the study of its effects and the collection of evidence in a secure setting.

Component	Description
Simulation Method	A PowerShell script named <code>safe-ransom.ps1</code> was utilized.
Actions Performed	1. <b>Create Locked Copies:</b> The script generated copies of user documents, appending the

.locked extension to simulate encryption.

1. **Generate Ransom Note:** A text file named `README_RECOVER.txt` was created, containing a ransom message.
2. **Log Operations:** All actions performed by the script were logged in a dedicated log file ( `sim_log.txt` ). | **Purpose of Simulation** | To mimic the behavior of real ransomware in a non-destructive manner, providing an opportunity to apply incident response procedures. |

### 3. Evidence Collected

Evidence was gathered from the primary directories affected by the incident ( `C:\Users\whoami\Documents` and `C:\Evidence` ). All evidence was organized into a dedicated folder to ensure easy access and proper documentation. The collected evidence included:

- Original user files.
- The locked copies simulating encrypted files.
- The ransom note.
- The simulation script ( `safe-ransom.ps1` ).
- The simulation operations log ( `sim_log.txt` ).
- A memory image of the `explorer.exe` process.
- A file containing the hashes of all evidence.
- The chain of custody file ( `chain_of_custody.csv` ).
- The incident timeline file ( `incident_timeline.csv` ).

### 4. Evidence Integrity Verification

To guarantee the integrity of the evidence and ensure it was not altered, a SHA256 hash was calculated for every file. This process was executed using the following PowerShell command:

Plain Text

```
Get-FileHash -Algorithm SHA256
```

All hashes were stored in the `C:\Evidence\hashes.txt` file for future reference and to verify the integrity of the evidence at any time.

## 5. Chain of Custody

A formal chain of custody document ( `chain_of_custody.csv` ) was created to track the lifecycle of each piece of evidence from the moment of collection. The document includes the following fields for precise tracking:

EvidenceID	FileName	Collector	DateTime	Location	SHA256	Description
EVID-995761D7	notes.txt	whoami	11/7/2025 16:23	C:...\\notes.txt	E3B0C44...	user file
EVID-D941D248	safe-ransom.ps1	whoami	11/7/2025 16:23	C:...\\safe-ransom.ps1	930C0EA...	simulation script
EVID-MEMDUMP01	explorer.DMP	whoami	11/7/2025 16:40	C:...\\explorer.DMP	7BFB7D41...	memory dump

## 6. Incident Timeline

A detailed incident timeline ( `incident_timeline.csv` ) was prepared to reconstruct the sequence of events that occurred during the simulation. The following table highlights the key events:

Timestamp	Event	Actor	EvidenceRef	Notes
2025-11-07T16:21:09Z	Simulation started	whoami		safe-ransom.ps1 executed
2025-11-07T16:21:09Z	Ransom note created	System	EVID-CDBF4640	README_RECOVER.txt created
2025-11-07T16:21:09Z	Locked copies generated	System	EVID-0D47...	*.locked files created
2025-11-07T16:23:37Z	Hashes recorded	whoami	EVID-D941D248	hashes.txt updated
2025-11-07T16:40:00Z	Memory image captured	whoami	EVID-MEMDUMP01	explorer.exe dump collected

## 7. Memory Image Acquisition

A memory dump of the `explorer.exe` process was acquired as part of the evidence collection process. This was accomplished using the Windows Task Manager, where a dump file (`explorer.DMP`) was created and moved to the evidence folder.

- **Purpose:** To simulate memory forensics procedures, which can reveal evidence not present on the hard drive.
- **Verification:** A SHA256 hash of the memory dump was calculated to ensure its integrity.

## 8. Conclusion

All requirements for the second week of the project were successfully completed. Key accomplishments include the safe simulation of a ransomware attack, the collection of all relevant evidence, and its professional documentation through the creation of hashes, a chain of custody, and an incident timeline. A memory image was also successfully acquired, and all evidence was organized in a clear structure.

This phase is foundational for the subsequent stages of the project, where the collected evidence will be used to perform an in-depth digital forensic analysis.