



# Digital Forensic Investigation Report

## Forensics Evidence

**Case Number** CTF 2 CFR101

**Investigator(s)** Carmen Amond

**Date of Report** 12/09/2025

### 1. Executive Summary

There is a local company facing a wide network issue. This company claims there is something knocking computers off of our network and leaving them unusable. We need to figure out what's going on and by who or what.

### 2. Case Background

- At this time, the company has no clue why the computers are left unusable.
- Suspect status: The current suspect has to be the last person to successfully use the computer; however, it is impossible to know after another person tries to log on.

### 3. Evidence Acquisition

- Date and time of acquisition Insert date and time
- Method of acquisition e.g., Autopsy, FTK Imager
- Evidence items

1. List each item, e.g., LoneWolf.E01, memdump.mem, etc.
2. Include MD5 or SHA-1 hash values for each item

## 4. Chain of Custody

Chain of Custody document.

## 5. Investigation Methodology

- Tools used List forensic tools, e.g., Autopsy, and versions
- Techniques applied e.g., keyword searching, file carving, timeline analysis

## 6. Findings

### 6.1 Timeline of Suspect's Activities

Create a chronological list of relevant events found in the digital evidence

### 6.2 Key Evidence

List and describe key pieces of evidence, including

- File name
- File location
- Date and time (created, modified, accessed)
- Content summary
- Relevance to the case

### 6.3 Communication Records

Summarize any relevant emails, messages, or social media interactions found

### 6.4 Internet History

List relevant websites visited, searches performed, etc.

### 6.5 Encrypted or Deleted Data

Document any encrypted files found or recovered deleted files

## **7. Analysis**

Provide an in-depth analysis of the evidence, connecting the dots between different pieces of information

## **8. Conclusion**

Summarize the key findings and state whether there is sufficient evidence to detain the suspect

## **9. Recommendations**

Suggest next steps for the investigation or additional areas to explore

## **10. Appendices (If needed)**

- Appendix A Detailed log of all evidence files found
- Appendix B Visual aids (graphs, charts, etc.)
- Appendix C Technical details of forensic processes
- Appendix D Relevant legal considerations

## **11. Verification**

Report prepared by Investigator's Name and Signature Peer reviewed by Reviewer's Name and Signature

