Report: Digital Investigation

Title: Network Traffic Analysis and Digital Investigation

By: Dennis Gilbert

Objective
The objective of this investigation was to analyze captured network activity from a flagged laptop showing unusual traffic patterns. The goal was to reconstruct evidence from the packet capture (PCAP) file and identify any suspicious or hidden files transmitted over the network.

Tools Used

Wireshark – for packet capture analysis and protocol filtering

Hex Editor – for examining raw packet data and extracting file fragments

File Signature Analysis – for identifying file types based on magic numbers

Base64 Decoder – decoding encoded text hidden in traffic

Methodology

1. Initial Analysis with Wireshark

- Loaded the provided PCAP file.
- Applied filters (e.g., http) to narrow down suspicious traffic.
- Followed TCP streams to reconstruct data flows.

2. Raw Data Inspection

- Exported raw binary data segments from network streams.
- Used a hex editor to carefully examine data structures.

3. File Carving via Signatures

- Identified file boundaries using known magic numbers:
    - JPEG: FF D8 FF … FF D9

- PNG: 89 50 4E 47 0D 0A 1A 0A … 49 45 4E 44 AE 42 60 82
- PDF: 25 50 44 46 … 25 25 45 4F 46
- ZIP: 50 4B 03 04

Extracted files accordingly and validated extensions.

4. Base64 Decoding

- Identified text encoded in Base64 within HTTP streams.
- Decoded to reveal hidden text contents.

Findings

The investigation successfully revealed and reconstructed:

1 JPEG image:

1 PDF document

1 ZIP archive

Hidden text strings (decoded from Base64)

These files were hidden within the network traffic, indicating possible data exfiltration or covert file transfer activity.

Conclusion

Through a combination of packet analysis, file carving, and Base64 decoding, hidden files and text were successfully uncovered. These findings demonstrate how attackers may embed and encode data within ordinary network traffic, reinforcing the need for deep forensic inspection during incident response.