Digital Forensics CTF Report

Manual File Extraction from HTTP Traffic - PCAP

Investigator: Dayo Sonibare

BNS CyberLab Ltd.

Case File: bns_captured_activity.pcap

Tools Used: Wireshark, HxD Hex Editor

1. Introduction

This forensic Capture the Flag (CTF) exercise involved analyzing a captured network session to manually extract files transmitted through HTTP traffic. The objective was to identify, reconstruct, and recover hidden files embedded within TCP streams without the use of automation or scripting tools.

By relying solely on Wireshark and HxD Hex Editor, I examined raw packet data to uncover transferred content and reconstruct multiple file types. This approach simulates real-world digital forensic investigations where manual evidence recovery is often required.

2. Objectives

The goals of this investigation were to:

Inspect HTTP traffic within a packet capture file

Follow TCP streams to locate file transfers

Identify file types using hexadecimal signatures (magic numbers)

Manually extract and reconstruct .jpg, .png, .pdf, and .zip files

Document all findings in a structured forensic report

3. Methodology

3.1 Traffic Analysis in Wireshark

The file bns_captured_activity.pcap was opened in Wireshark. To isolate relevant packets, I applied the following filters: http, http.request.method == "GET", http.request.method == "POST"

These filters revealed HTTP sessions where data was transferred between hosts.

3.2 Following TCP Streams

Suspicious packets were selected and analyzed using:

Right-click → Follow → TCP Stream

This allowed me to view full conversations and identify embedded file content within the data payloads.

3.3 Identifying File Signatures

Within each stream, I searched for known hexadecimal file headers:

File Type	Hex Signature
JPG	FF D8 FF
PNG	89 50 4E 47
PDF	25 50 44 46
ZIP	50 4B 03 04

These signatures confirmed the presence and type of each transferred file.

3.4 Manual File Reconstruction

Once file content was located:

The raw hexadecimal data was copied from Wireshark

Pasted into HxD Hex Editor

Cleaned to remove unrelated stream data

Saved with the correct file extension

Each reconstructed file was then opened to verify integrity.

4. Recovered Evidence

The following files were successfully extracted:

File Name	File Type	Status
BNS01.jpg	JPEG Image	Recovered
BNS02.png	PNG Image	Recovered
BNS03.pdf	PDF Document	Recovered
BNS04.zip	ZIP Archive	Recovered

All files opened correctly and confirmed successful reconstruction.

5. Findings & Analysis

The captured traffic clearly demonstrated unauthorized file transfers hidden within standard HTTP communications. By embedding files inside TCP streams, the activity attempted to appear as routine web traffic.

Manual extraction revealed:

Multiple file types transmitted without encryption

Evidence of potential data exfiltration techniques

The effectiveness of hex-level analysis in uncovering concealed content

This technique is commonly observed in malware delivery, insider data theft, and covert communications.

6. Conclusion

This forensic investigation successfully recovered four hidden files from HTTP traffic using only manual analysis techniques. The exercise reinforced critical skills in network forensics, including traffic inspection, TCP stream reconstruction, and file carving using hexadecimal signatures.

The results demonstrate how attackers can conceal sensitive data within normal-looking traffic and highlight the importance of deep packet analysis during incident response.

7. Tools Summary

Wireshark – Network traffic inspection and stream reconstruction

HxD Hex Editor – Binary data carving and file recovery

8. Key Takeaways

File signatures are essential for identifying embedded content

TCP stream following provides complete data reconstruction

Manual carving remains a vital forensic skill

HTTP traffic can be abused for covert file transfer