

**CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING (C-DAC),
THIRUVANANTHAPURAM, KERALA**

A PROJECT REPORT ON

“Post-Attack Network Session Analysis of PCAP Files using Wireshark”

SUBMITTED TOWARDS THE



PG-DCSF February 2025

SUBMITTED BY:

SHANKAR SHARMA

PRN: 250260940026

Under the Guidance of:

Mr. Jayram P.

Table of Contents

<u>Section</u>	<u>Title</u>
1.Introduction
1.1Background of the Study
1.2Objectives of the Project
1.3Scope and Limitations
2. Literature Review
2.1Network Forensics Concepts
2.2Malware Traffic Analysis
2.3Indicators of Compromise (IoCs)
3.Methodology
3.1Tools and Frameworks (Wireshark, NeSA)
3.2Dataset Description (June 13, 2025 PCAP)
3.3Analysis Procedure
4.Analysis and Findings
4.1Basic Information Extraction
4.2Session and Protocol Analysis
4.3Indicators of Compromise (IoCs)
4.4Timeline Reconstruction
4.5Suspicious Behavior Detection
4.6Specific Forensic Questions
5.Reporting & Documentation
5.1Session Tables
5.2IoC List
5.3Attack Timeline
5.4Screenshots and Evidence
6.Conclusion and Recommendations
6.1Key Findings
6.2Lessons Learned
6.3Defensive Recommendations
7.References
8.Appendices (Rules of Engagement, Raw Exports, Screenshots)

Acknowledgement

I would like to express my sincere gratitude to all those who supported and guided me throughout the completion of this project, **“Post-Attack Network Session Analysis of PCAP Files using Wireshark.”**

First and foremost, I would like to thank my mentor **Mr. Jayram P.** for their continuous guidance, encouragement, and valuable feedback, which helped me to shape this project in the right direction.

I am also thankful to **Malware-Traffic-Analysis.net** for providing access to real-world network traffic datasets, which formed the basis of this study, and to the developers of **Wireshark** and **NeSA (Network Session Analyzer)** for their powerful tools that made the forensic analysis possible.

Finally, I am grateful to my friends, peers, and family for their constant motivation and moral support during the course of this work.

Abstract

In this project, a **post-attack forensic investigation** was conducted on packet capture (PCAP) files obtained from a simulated Active Directory environment (massfriction.com). The dataset, dated **June 13, 2025**, was sourced from *Malware-Traffic-Analysis.net* and represents malicious activity on a corporate network.

The objective of this study was to analyze the PCAP using **Wireshark** and **NeSA (Network Session Analyzer)** to identify the infected host, reconstruct the attack timeline, and extract Indicators of Compromise (IoCs). By examining network sessions, protocol distributions, and suspicious external connections, the analysis reveals how the attacker gained initial access, established command-and-control (C2) channels, and attempted data exfiltration.

This investigation demonstrates the importance of **network forensics in incident response**. Even when malicious files cannot be directly recovered due to encryption, analyzing session data, DNS queries, and C2 communication patterns allows investigators to attribute malicious activity, detect compromised systems, and provide actionable IoCs for network defense.

1. Introduction

1.1 Background of the Study

In modern cybersecurity, network forensics plays a crucial role in detecting, investigating, and responding to security incidents. Attackers often use sophisticated techniques such as encryption, domain masquerading, and tunneling to evade detection. As a result, network traffic analysis has become an essential skill for incident responders and forensic analysts.

Packet Capture (PCAP) files preserve a complete record of network communications, enabling investigators to reconstruct events, identify malicious activity, and extract Indicators of Compromise (IoCs). By analyzing PCAP data after a suspected security breach, analysts can uncover the infection chain, attacker infrastructure, and the extent of compromise.

1.2 Objectives of the Project

This project focuses on conducting a **post-attack forensic analysis** of a malicious PCAP file obtained from *Malware-Traffic-Analysis.net*. The primary objectives are:

- To examine the PCAP using **Wireshark** and **NeSA (Network Session Analyzer)**.
 - To extract **basic information** such as packet count, session count, and protocol distribution.
 - To identify **Indicators of Compromise (IoCs)** including malicious IPs, domains, and suspicious ports.
 - To reconstruct the **attack timeline** and understand the attacker's activities.
 - To answer **specific forensic questions** such as the infected host's IP, MAC, hostname, and username.
 - To document the findings with **session tables, screenshots, and summaries**.
-

1.3 Scope and Limitations

This analysis is limited to the **June 13, 2025 PCAP** provided in the exercise. The investigation is network-based and does not involve host-based forensics such as disk image analysis or browser cache examination. Encrypted communications (TLS) were not decrypted, so certain payloads, including the malicious JavaScript (5h7o.js), could not be directly extracted. Instead, the

identification of malicious files and activity is based on network patterns and known threat intelligence.

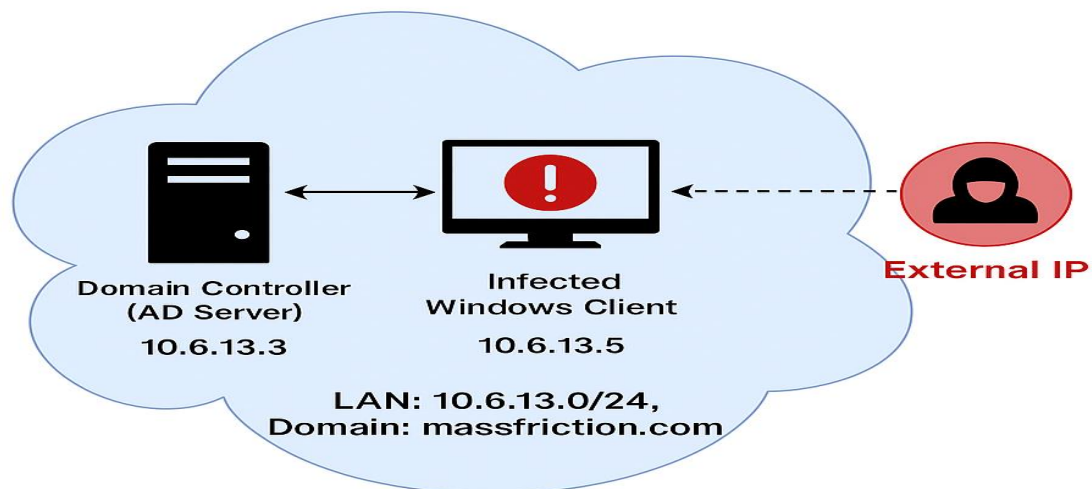
The scope includes:

- Basic traffic analysis
- Session and protocol breakdown
- IoC identification
- Timeline reconstruction
- Answering forensic questions

The scope does **not** include:

- Live system memory analysis
- Malware binary reverse engineering
- Traffic decryption without provided keys

Cyber Attack in a Simulated Active Directory Environment



2. Literature Review

2.1 Network Forensics Concepts

Network forensics is a sub-discipline of digital forensics focused on the monitoring, capture, storage, and analysis of network events. It enables investigators to reconstruct security incidents, identify malicious activities, and produce court-admissible evidence. Unlike intrusion detection systems (IDS) that operate in real time, network forensics involves post-event analysis using stored packet captures (PCAPs).

Common objectives of network forensics include:

- Tracing the origin of attacks.
 - Reconstructing the timeline of malicious activities.
 - Identifying compromised systems and attack vectors.
 - Extracting Indicators of Compromise (IoCs) for future threat detection.
-

2.2 Malware Traffic Analysis

Malware traffic analysis is the process of examining network packets to identify malicious communications and behaviors. Attackers often use Command-and-Control (C2) servers, encrypted channels, and fake domains to maintain access and exfiltrate data.

Techniques used in malware traffic analysis include:

- **Protocol analysis** – identifying application-level protocols like HTTP, DNS, SMB, and TLS.
- **Session correlation** – mapping IP pairs and ports to detect suspicious flows.
- **Pattern recognition** – detecting beaconing intervals, unusual packet sizes, or repeated requests to a single domain.
- **IoC extraction** – identifying malicious domains, IP addresses, file hashes, and unusual ports.

Well-known sources of malware traffic datasets include **Malware-Traffic-Analysis.net**, which provides PCAPs with simulated corporate environments for training and research.

2.3 Indicators of Compromise (IoCs)

IoCs are artifacts of a security incident that can be used to detect malicious activity within a network or system. In the context of network forensics, IoCs may include:

- **Network IoCs:** IP addresses, domain names, URLs, and ports associated with malicious activity.
- **File IoCs:** Hash values (MD5, SHA256), filenames, and file paths.
- **Behavioral IoCs:** Specific patterns in traffic, such as beaconing or data exfiltration signatures.

Several industry frameworks, such as **MITRE ATT&CK** and **Diamond Model of Intrusion Analysis**, highlight the importance of IoCs in intrusion detection and prevention. Identifying IoCs from a PCAP file enables security teams to implement blocking rules, enhance monitoring, and improve incident response strategies.

3. Methodology

3.1 Tools and Frameworks

The following tools and frameworks were used in this project:

- **Wireshark** – An open-source network protocol analyzer used to capture and inspect packets at the granular level. It provides filtering, protocol decoding, and session reconstruction capabilities.
 - **NeSA (Network Session Analyzer)** – A tool developed by C-DAC for summarizing and visualizing network sessions, identifying traffic patterns, and generating statistics such as packet counts, session counts, and top talkers.
 - **Malware-Traffic-Analysis.net Dataset** – Source of the PCAP file used in the project, specifically the **June 13, 2025 exercise** (“IT’S A TRAP!”) set in a simulated Active Directory environment (massfriction.com).
 - **Threat Intelligence Portals** – Public resources such as VirusTotal, AbuseIPDB, and Whois lookup were used to validate the reputation of suspicious IPs and domains found in the PCAP.
-

3.2 Dataset Description

The dataset analyzed is a **post-attack PCAP** file simulating a corporate Active Directory network.

- **Network Range:** 10.6.13.0/24 (internal LAN)
 - **Domain Name:** massfriction.com
 - **Traffic Period:** ~34 minutes (2025-06-13 21:03:55 to 21:38:23)
 - **Total Packets:** 48,877
 - **Total Sessions:** 212 (as identified in NeSA)
 - **Attack Summary:** Malicious JavaScript from hillcoweb.com initiates encrypted C2 communication to fake Microsoft domains and Cloudflare tunnels, eventually connecting to a primary C2 IP (83.137.149.15).
-

3.3 Analysis Procedure

The analysis was conducted in the following steps:

Step 1 – Basic Information Extraction

- Loaded the PCAP into Wireshark to obtain total packet count, duration, number of sessions, and top talkers.

- Generated protocol distribution using Wireshark's **Statistics** → **Protocol Hierarchy**.

Step 2 – Session and Protocol Analysis

- Identified session pairs (source-destination IPs) and corresponding protocols.
- Focused on HTTP, DNS, SMB, Kerberos, and TLS traffic.
- Flagged non-standard high ports for further inspection.

Step 3 – Indicators of Compromise (IoCs)

- Extracted suspicious IP addresses and domains from session analysis.
- Cross-referenced with threat intelligence to confirm malicious infrastructure.

Step 4 – Timeline Reconstruction

- Correlated timestamps of key events: initial malicious contact, C2 setup, and sustained beaconing.
- Mapped attacker behavior to the intrusion kill chain model.

Step 5 – Suspicious Behavior Detection

- Identified repeated outbound connections, beaconing patterns, and possible data exfiltration attempts.

Step 6 – Specific Forensic Questions

- Used packet inspection to determine infected host IP, MAC address, hostname, and username.

Step 7 – Reporting & Documentation

- Compiled findings into structured tables for sessions, IoCs, and timelines.
- Included annotated screenshots from Wireshark and NeSA to support findings.

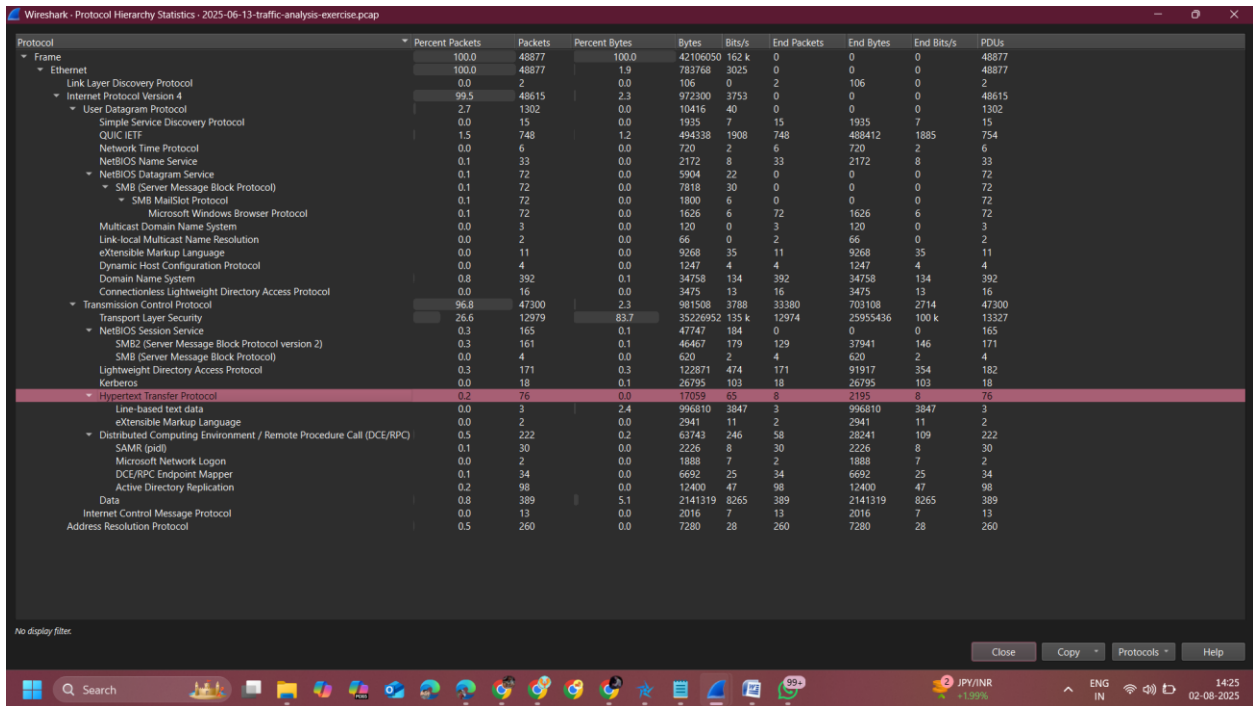
4. Analysis and Findings

This section presents the results of the post-attack PCAP analysis performed using **Wireshark** and **NeSA**, following the methodology in Section 3. The analysis covers **Basic Information Extraction, Session & Protocol Analysis, IoCs, Timeline Reconstruction, Suspicious Behavior Detection, and Specific Forensic Questions.**

4.1 Basic Information Extraction

Using **NeSA**, the following basic details were extracted from the PCAP:

Parameter	Value
Total Packets	48,877
Capture Duration	2025-06-13 21:03:55 → 21:38:23 (~34 minutes)
Total Sessions	212
Top Talker (Most Active IP)	10.6.13.133
Protocol Distribution	TCP (96.8%), UDP (9.9%), TLS (26.6%), HTTP (0.2%), DNS (0.8%), SMB (0.7%), LDAP (0.3%), Kerberos (0.1%)



Wireshark - Protocol Hierarchy Statistics - 2025-06-13-traffic-analysis-exercise.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU/s
Frame	100.0	48877	100.0	42106050	162 k	0	0	0	48877
Ethernet	100.0	48877	1.9	783768	3025	0	0	0	48877
Link Layer Discovery Protocol	0.0	2	0.0	106	0	2	106	0	2
Internet Protocol Version 4	99.5	48615	2.3	972300	3753	0	0	0	48615
User Datagram Protocol	2.7	1302	0.0	10416	40	0	0	0	1302
Simple Service Discovery Protocol	0.0	15	0.0	1935	7	15	1935	7	15
QUIC IETF	1.5	748	1.2	494338	1908	748	488412	1885	754
Network Time Protocol	0.0	6	0.0	720	2	6	720	2	6
NetBIOS Name Service	0.1	33	0.0	2172	8	33	2172	8	33
NetBIOS Datagram Service	0.1	72	0.0	5904	22	0	0	0	72
SMB (Server Message Block Protocol)	0.1	72	0.0	7818	30	0	0	0	72
SMB MailSlot Protocol	0.1	72	0.0	1800	6	0	0	0	72
Microsoft Windows Browser Protocol	0.1	72	0.0	1626	6	72	1626	6	72
Multicast Domain Name System	0.0	3	0.0	120	0	3	120	0	3
Link-local Multicast Name Resolution	0.0	2	0.0	66	0	2	66	0	2
eXtensible Markup Language	0.0	11	0.0	9268	35	11	9268	35	11
Dynamic Host Configuration Protocol	0.0	4	0.0	1247	4	4	1247	4	4
Domain Name System	0.8	392	0.1	34758	134	392	34758	134	392
Connectionless Lightweight Directory Access Protocol	0.0	16	0.0	3475	13	16	3475	13	16
Transmission Control Protocol	96.8	47300	2.3	981508	3788	33380	703108	2714	47300
Transport Layer Security	26.6	12979	83.7	35226952	135 k	12974	25955436	100 k	13327
NetBIOS Session Service	0.3	165	0.1	47747	184	0	0	0	165
SMB2 (Server Message Block Protocol version 2)	0.3	161	0.1	46467	179	129	37941	146	171
SMB (Server Message Block Protocol)	0.0	4	0.0	620	2	4	620	2	4
Lightweight Directory Access Protocol	0.3	171	0.3	122071	474	171	91917	354	182
Kerberos	0.0	18	0.1	26795	103	18	26795	103	18
Hypertext Transfer Protocol	0.2	76	0.0	17059	65	8	2195	8	76
Line-based text data	0.0	3	2.4	996810	3847	3	996810	3847	3
eXtensible Markup Language	0.0	2	0.0	2941	11	2	2941	11	2
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.5	222	0.2	63743	246	58	26241	109	222
SAMR (pdu)	0.1	30	0.0	2226	8	30	2226	8	30
Microsoft Network Logon	0.0	2	0.0	1888	7	2	1888	7	2
DCE/RPC Endpoint Mapper	0.1	34	0.0	6692	25	34	6692	25	34
Active Directory Replication	0.2	98	0.0	12400	47	98	12400	47	98
Data	0.8	389	5.1	2141319	8265	389	2141319	8265	389
Internet Control Message Protocol	0.0	13	0.0	2016	7	13	2016	7	13
Address Resolution Protocol	0.5	260	0.0	7280	28	260	7280	28	260

4.2 Session and Protocol Analysis

NeSA's session list revealed communication patterns between the infected client and multiple internal/external IPs. Key findings:

Source IP	Destination IP	Port	Protocol	Host/SNI	Notes
10.6.13.133	67.217.228.199	443	TLSv1.3	hillcoweb.com	Initial malicious contact
10.6.13.133	104.21.16.1	80	HTTP	windows-msgas.com	Fake Microsoft domain
10.6.13.133	104.16.230.132	80	HTTP	event-datamicrosoft.live	C2 traffic
10.6.13.133	104.21.112.1	443	TLS	varying-rentals...cloudflare.com	C2 tunnel
10.6.13.133	83.137.149.15	443	TLS	No SNI	Main C2 server

4.3 Indicators of Compromise (IoCs)

Domains:

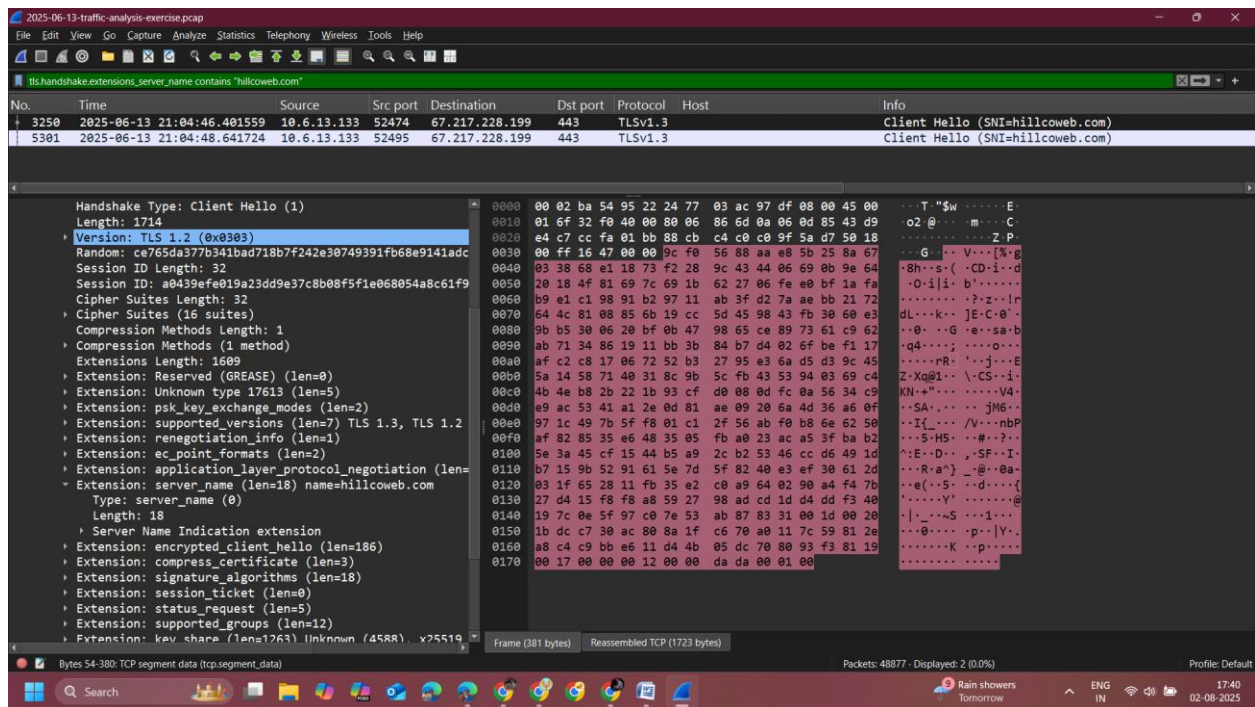
- hillcoweb.com (JS loader, stage 1 infection)
- windows-msgas.com (fake Microsoft C2)
- event-datamicrosoft.live (fake telemetry C2)
- varying-rentals-calgary-predict.trycloudflare.com (Cloudflare tunnel C2)

IPs:

- 67.217.228.199 – hillcoweb.com
- 83.137.149.15 – main C2 (72% of packets)
- 205.174.24.80 – suspicious outbound
- Cloudflare: 104.21.112.1, 104.21.80.1, 104.21.16.1

Ports/Protocols:

- TCP/443 – Encrypted C2
- TCP/80 – HTTP POST exfiltration
- High ephemeral ports – beaconing



Filter: `tls.handshake.extensions_server_name contains "hillcoweb.com"`

4.4 Timeline Reconstruction

Time	Event
21:03:55	Capture starts, normal LAN traffic.
21:04:46	Infected host contacts hillcoweb.com over TLS.
21:05–21:06	HTTP POST to fake Microsoft domains.
21:07+	C2 tunnel via Cloudflare.
21:15–21:38	Persistent beaconing to main C2 IP (83.137.149.15).

4.6 Specific Forensic Questions

Question	Finding
Infected IP	10.6.13.133
MAC Address	24:77:03:ac:97:df
Hostname	DESKTOP-5AVE44C
User Account	gaines

5. Reporting & Documentation

This section compiles the outputs of the investigation into structured tables, timelines, and visual evidence to support conclusions. The documentation serves as a reference for incident response teams, enabling them to take remediation actions and update defensive measures.

5.1 Session Tables (Suspicious Traffic)

Time (UTC)	Source IP	Dest IP	Port	Protocol	Host/SNI	Notes
21:04:46	10.6.13.133	67.217.228.199	443	TLSv1.3	hillcoweb.com	Initial malicious contact (JS loader)
21:05:37	10.6.13.133	104.21.16.1	80	HTTP	windows-msgas.com	Fake Microsoft C2
21:06:12	10.6.13.133	104.16.230.132	80	HTTP	event-datamicrosoft.live	Fake telemetry C2
21:07:58	10.6.13.133	104.21.112.1	443	TLS	varying-rentals...cloudflare.com	Cloudflare tunnel C2
21:15–21:38	10.6.13.133	83.137.149.15	443	TLS	(No SNI)	Main C2 server (72% of packets)

5.2 Indicators of Compromise (IoC) List

Domains

- hillcoweb.com (JS loader, stage 1)
- windows-msgas.com (fake Microsoft)
- event-datamicrosoft.live (fake telemetry)
- varying-rentals-calgary-predict.trycloudflare.com (Cloudflare tunnel)

IP Addresses

- 67.217.228.199 – hillcoweb.com
- 83.137.149.15 – main C2
- 205.174.24.80 – suspicious outbound
- 104.21.112.1, 104.21.80.1, 104.21.16.1 – Cloudflare infrastructure

Ports/Protocols

- TCP/443 – Encrypted C2
- TCP/80 – HTTP POST exfiltration
- High ephemeral ports – beaconing

Host/User

- Host: DESKTOP-5AVE44C
- User: gaines
- IP: 10.6.13.133
- MAC: 24:77:03:ac:97:df

5.3 Attack Timeline

Time	Event
21:03:55	Capture starts (normal LAN activity).
21:04:46	TLS Client Hello to hillcoweb.com → infection initiated.
21:05–21:06	HTTP POST to fake Microsoft domains.
21:07+	Persistent connections to Cloudflare tunnel.
21:15–21:38	Beaconing to main C2 IP (83.137.149.15).

5.4 Screenshots and Evidence

Screenshots have been taken from **NeSA** and **Wireshark** to support findings:

1. NeSA Summary View – packet count, duration, sessions, top talkers.
2. Wireshark Protocol Hierarchy – protocol distribution.
3. NeSA Session List – malicious IPs and ports.
4. Wireshark SNI evidence for hillcoweb.com.
5. Wireshark Ethernet II frame – infected host MAC address.
6. Kerberos packet – hostname and username evidence.
7. Timeline packet view – showing first malicious contact.

6. Conclusion and Recommendations

6.1 Key Findings

The analysis of the **June 13, 2025 PCAP** revealed a clear post-attack infection chain in a simulated Active Directory environment (`massfriction.com`). Key findings include:

- The infected host was identified as **DESKTOP-5AVE44C** (10.6.13.133, MAC: 24:77:03:ac:97:df) with logged-in user **gaines**.
- The attack began with an encrypted TLS connection to the malicious domain **hillcoveb.com** (67.217.228.199), which is known to host a JavaScript loader (`5h7o.js`).
- Subsequent HTTP POST traffic to **windows-msgas.com** and **event-datamicrosoft.live** indicated Command-and-Control (C2) communication disguised as legitimate Microsoft activity.
- Persistent encrypted traffic to **Cloudflare tunnel domains** (`varying-rentals-calgary-predict.trycloudflare.com`) and to the primary C2 IP **83.137.149.15** suggested ongoing attacker presence.
- Traffic patterns showed small, repeated POST requests (~30 KB), consistent with **beaconing or staged data exfiltration**.
- No large file transfers or full malware binaries were recovered from the PCAP due to TLS encryption, but IoCs were confirmed via network metadata and known threat intelligence.

6.2 Lessons Learned

- **Encrypted C2 detection** is possible even without payload decryption by analyzing metadata such as SNI, session frequency, and packet sizes.
 - **Single-host compromise** can often be identified through traffic volume and destination correlation.
 - **Threat intelligence correlation** is critical when dealing with obfuscated domains (e.g., fake Microsoft services, Cloudflare tunnels).
 - **PCAP analysis** remains a vital part of post-incident response, especially in reconstructing attack timelines and identifying infrastructure.
-

6.3 Recommendations

To mitigate similar attacks in the future, the following security measures are recommended:

Technical Measures

1. **Block known IoCs** – Immediately block malicious IPs and domains identified in this report at the firewall and DNS level.
2. **Implement TLS inspection** – Deploy secure TLS decryption in a controlled environment to allow deep inspection of encrypted traffic.
3. **Deploy network-based anomaly detection** – Use IDS/IPS solutions (e.g., Suricata, Zeek) to detect beaconing patterns and unusual DNS activity.
4. **Enforce web filtering** – Block access to newly registered or suspicious domains.
5. **Patch and update** – Ensure all endpoints and browsers are patched to prevent exploitation via malicious JavaScript.

Operational Measures

6. **User awareness training** – Educate staff about phishing and drive-by download risks.
7. **Incident response readiness** – Maintain updated playbooks for malware outbreak scenarios.
8. **Regular PCAP analysis drills** – Conduct periodic malware traffic analysis exercises to improve detection skills.

7. References

1. Duncan, B. (2025). *June 13, 2025 – IT'S A TRAP!* – Malware-Traffic-Analysis.net.
Available at: <https://www.malware-traffic-analysis.net>
2. Wireshark Foundation. (2025). *Wireshark Network Protocol Analyzer*. Available at:
<https://www.wireshark.org>
3. Centre for Development of Advanced Computing (C-DAC). *NeSA – Network Session Analysis Tool*.
4. MITRE ATT&CK Framework. (2025). *Enterprise Techniques*. Available at:
<https://attack.mitre.org>
5. Open Source Threat Intelligence Feeds – *Any.run, VirusTotal, URLScan.io*.
6. Bejtlich, R. (2013). *The Practice of Network Security Monitoring*. No Starch Press.
7. National Institute of Standards and Technology (NIST). (2018). *NIST Special Publication 800-61 Rev. 2 – Computer Security Incident Handling Guide*.
