#Wireshark Network Forensics:
Detecting C2 and Lateral Movement in Simulated Breach

Scenario Summary:
A compromised internal host starts communicating with an unknown external IP. Traffic shows signs of:

- Initial DNS queries
- Beaconing patterns
- Suspicious HTTP requests or file download
- Possible lateral movement via SMB or RDP

My Goal:
Analyze the PCAP file using Wireshark to:

- Detect IOCs and attacker behavior
- Correlate to MITRE techniques (like T1071, T1043, T1021)
- Show a real-world analysis flow like a Tier 1/2 SOC Analyst
- Present findings in GitHub (with visuals, markdown, logs)

!LAN SEGMENT DETAILS FROM THE PCAP

- LAN segment range: **10.6.13[.]0/24** (**10.6.13[.]0** through **10.6.13[.]255**)
- Domain: **massfriction[.]com**
- Active Directory (AD) domain controller: **10.6.13[.]3 - WIN-DQL4WFWJXQ4**
- AD environment name: **MASSFRICTION**
- LAN segment gateway: **10.6.13[.]1**
- LAN segment broadcast address: **10.6.13[.]255**

LESSON LEARNED Questions.

I should be able to answer the following:

1. What is the IP address of the infected Windows client?
2. What is the mac address of the infected Windows client?
3. What is the host name of the infected Windows client?
4. What is the user account name from the infected Windows client?

Incident Analysis Report

Incident Type: Suspicious Network Traffic (Possible Malware Infection & Data Exfiltration)
Tool Used: Wireshark
Date of Analysis: July 14, 2025
PCAP File: 2025-06-13-traffic-analysis-exercise.pcap
Analyst: Elena Teplyakova

Summary

The analysis of network traffic on June 13, 2025, reveals that the host `10.6.13.133` has been compromised. The host engaged in suspicious HTTP POST activity to unknown and likely malicious external domains. Sensitive system data was exfiltrated via plaintext HTTP requests. Additionally, TLS handshakes were observed with unusual SNI fields, indicating potential command-and-control (C2) communications.

Timeline of Events

Time (UTC)	Source IP	Destination IP	Description
11:34:00	10.6.13.133	23.192.223.206	HTTP GET to /connecttest.txt
11:35:38	10.6.13.133	104.21.16.1	HTTP POST with encoded payload
11:35:42	10.6.13.133	104.21.16.1	More HTTP POST traffic (potential beaconing)
11:35:48	10.6.13.133	104.21.21.186	HTTP GET `/zhbQGFZdKt` → suspicious string
11:36–11:42	10.6.13.133	Multiple external IPs	HTTP POST Exfiltration attempts with encoded payloads
11:36:01	10.6.13.133	104.21.80.1	Exfiltration to windows-msgas.com
11:34:45	10.6.13.133	205.174.24.80	TLS handshake to SNI www.truglomedspa.com
11:34–11:50	10.6.13.133	eventdata-microsoft[.]live	HTTP System metadata POST via PowerShell

Figure 1. Exfiltration of system metadata via HTTP POST to fake domain eventdata-microsoft.live. Evidence of C2 behavior.

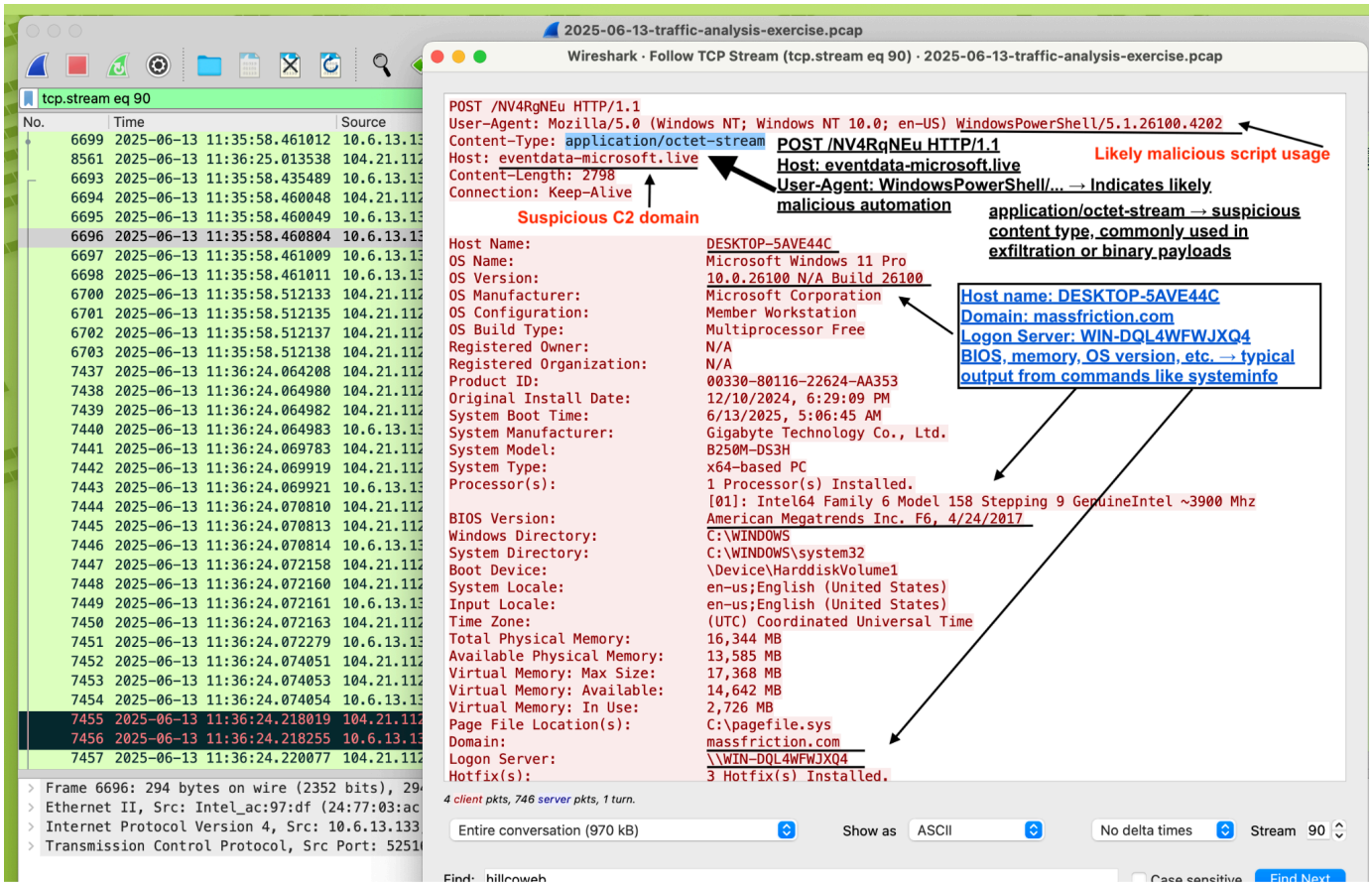


Figure 2. "application/octet-stream" or POST payload

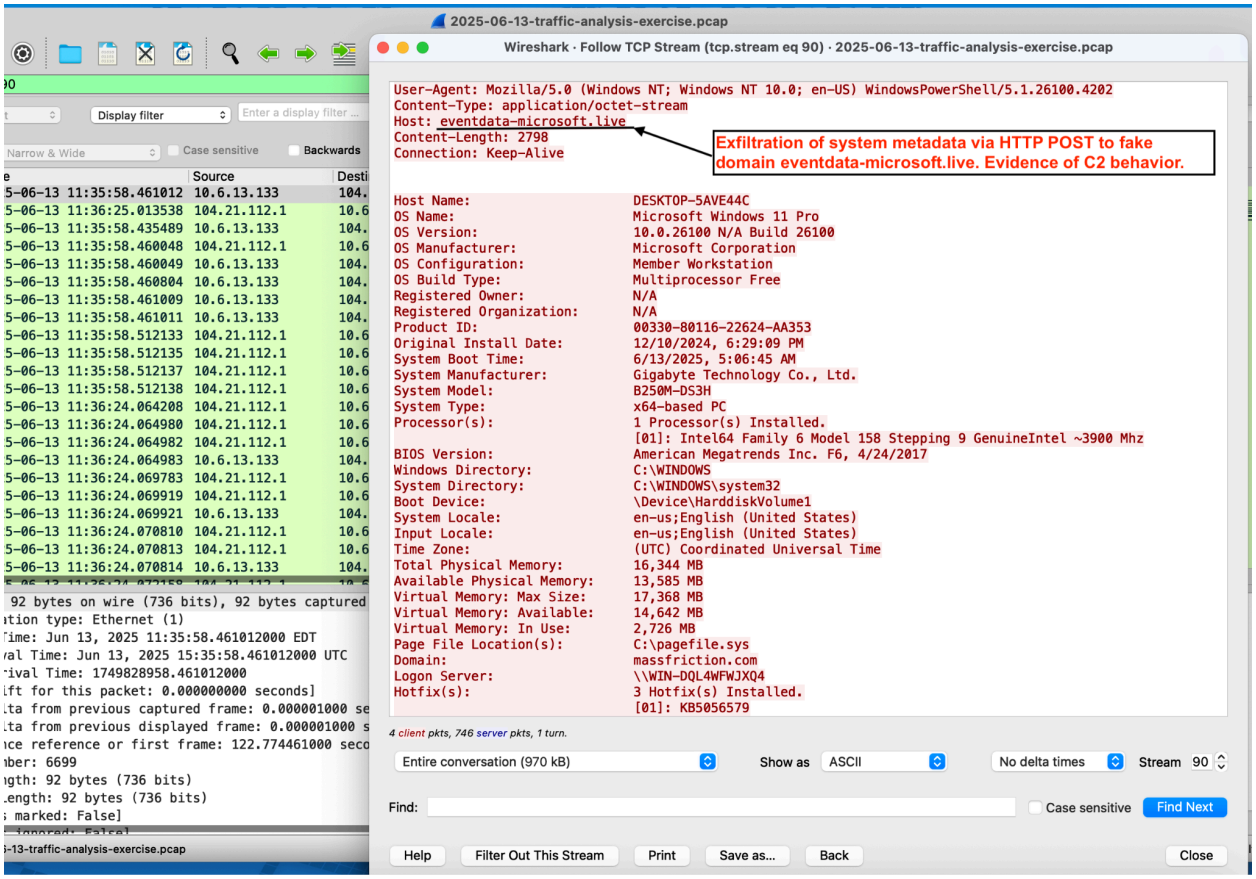


Figure 3. DNS resolution attempts from the infected host (10.6.13.133).
The client resolved v10.events.data.microsoft.com, which returned a suspicious CNAME (win-global-asimo). This was followed by a query to event-datmicrosoft.live, a clearly spoofed domain designed to imitate Microsoft's telemetry. This is consistent with MITRE T1071.001 (C2 over DNS and HTTP).

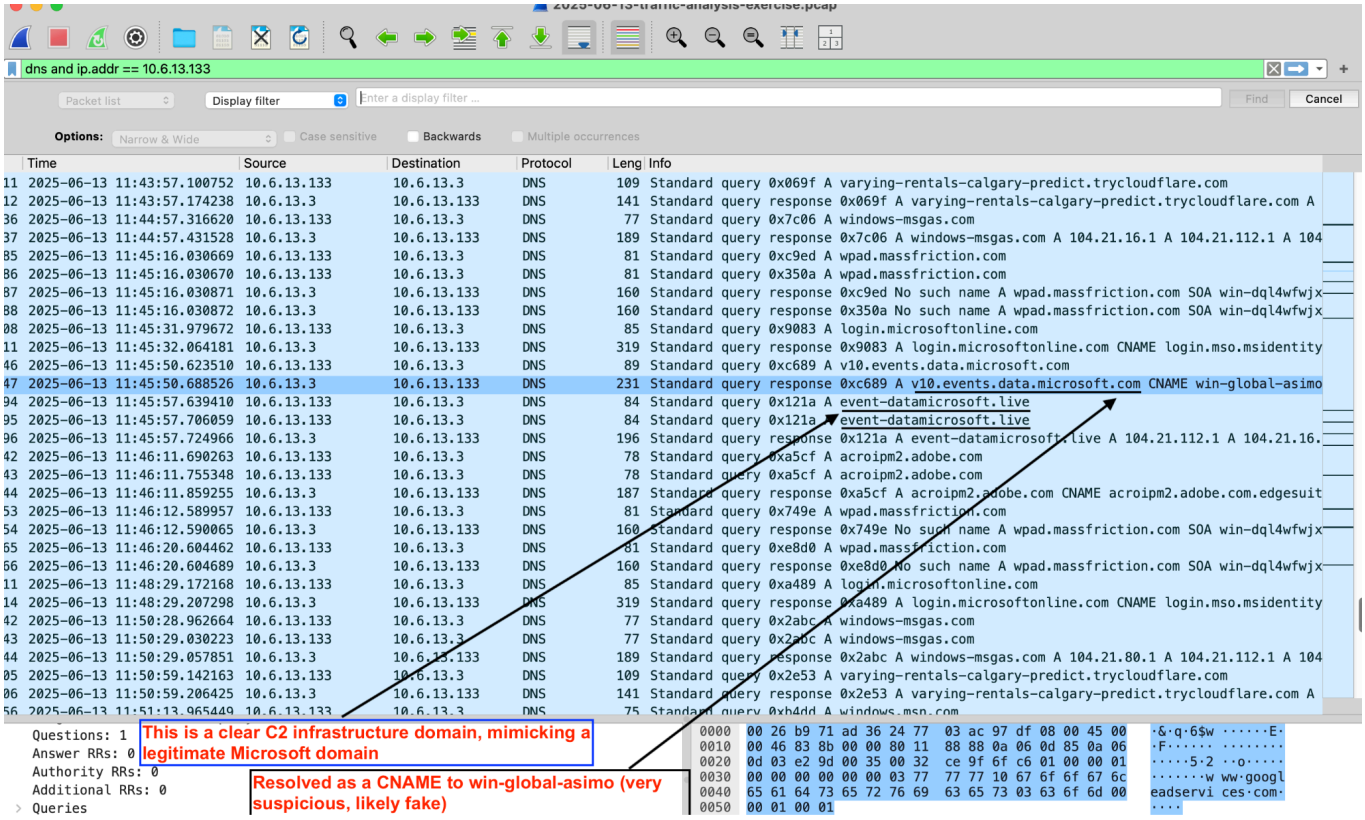


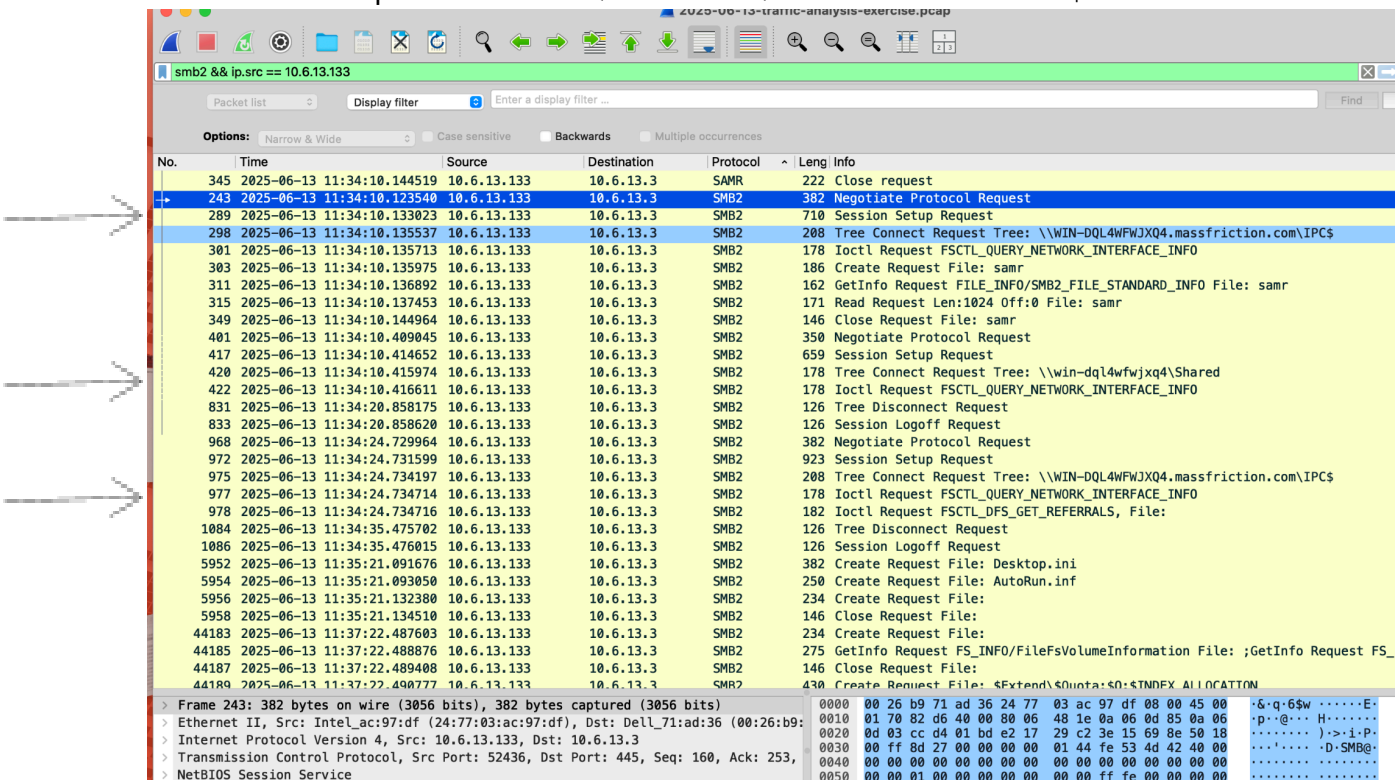
Figure 4. SMB Lateral Movement Attempt

Infected host **10.6.13.133** initiated an SMB connection to the Domain Controller **10.6.13.3**, attempting to access the IPC$ share. This is a typical method attackers use for lateral movement within internal networks.

Technique: T1021.002 – Remote Services: SMB/Windows Admin Shares

Evidence includes:

- Negotiate Protocol Request
- Session Setup Request
- Tree Connect Request to \\WIN-DQL4WFWJXQ4.massfriction.com\IPC$



Key Indicators from this Screenshot:

- Source: 10.6.13.133
- Destination: 10.6.13.3 (Domain Controller: WIN-DQL4WFWJXQ4.massfriction.com)
- Protocol: SMB2
- Port: 445

Packets highlighted and arrowed:

3: Negotiate Protocol Request

289: Session Setup Request

298: **Tree Connect Request Tree: \WIN-DQL4WFWJXQ4.massfriction.com\IPC$` - **Classic sign of lateral move attempt**

Others include: **Create Request File, Ioctl Request, Logoff Request**

Key Indicators

Identified Infected Host

(Captured from `Follow TCP Stream` (HTTP POST to suspicious domain):

- **IP Address:** `10.6.13.133`
- **MAC Address:** `00:02:ba:54:95:22` *(identified via ARP response)*
- **OS Info:** Windows 11 Pro, Hostname: `DESKTOP-5AVE44C`
- **User-Agent:** `WindowsPowerShell/5.1.26100.4202`
- **Logon Domain:** `massfriction.com`

Suspicious Domains / Hosts:

- eventdata-microsoft.live
- windows-msgas.com
- truglomedspa.com

Indicators of Compromise (IoCs)

- Large `application/octet-stream` HTTP POST requests
- System data POSTed in plaintext
- Fake Microsoft domain names used as C2
- Abnormal SNI values in TLS handshakes
- **Suspicious Domains:**
  - `eventdata-microsoft.live`
  - Other `104.x.x.x` POST targets
    Suspicious User-Agent:
  - `WindowsPowerShell/5.1.26100.4202`
- **Payload Patterns:**
  - Base64-looking POST data
    Odd file paths like `/rpgY6aY/kl53Fb1...`

Filtering Techniques Used

🧪 Filtering and Detection Techniques Used

Display Filters Applied:

- `http.request.method == "POST"` and others
- `(http.request or tls.handshake.type == 1) and !(ssdp)`
- `tcp.stream eq 90` (for stream reassembly)
- `DNS` filters to verify domain resolution
- `smb2 && ip.src == 10.6.13.133`

Followed TCP Streams: Stream #90 (PowerShell payload), #8561 (exfil)

Recommendations

1. **Isolate** host `10.6.13.133` from the network immediately.
2. **Conduct full disk forensic analysis** of the host.
3. **Search for and block all identified IOCs** (IPs, domains).
4. **Update firewall rules** and DNS blocklists with known malicious indicators.
5. **Inspect all other endpoints** for similar behavior (lateral movement).
6. **Patch** systems and review PowerShell logging.

Conclusion

This PCAP reveals a confirmed compromise of internal host `10.6.13.133`, including system profiling and data exfiltration. Evidence suggests active C2 communication using deceptive Microsoft-themed domains. The activity is consistent with post-exploitation behavior following a malware infection.

The host `10.6.13.133` is confirmed to be infected, exhibiting:

- Unauthorized data exfiltration
- PowerShell-based C2 communication
- Potential fake Microsoft domain usage

Next Steps: Block `104.21.x.x`, domain `eventdata-microsoft.live`, and isolate host `10.6.13.133`.

Report Generated by:
Elena Teplyakova
Certified Cybersecurity Analyst (CySA+, Splunk Core)