Wireshark Project Lab Report

Objective

Analyze a PCAP file using Wireshark to identify suspicious or malicious network activity, particularly focusing on a Windows host that may have downloaded a malicious `.exe` file.

Tools Used

- **Wireshark**
- **PCAP File: `2024-01-04-traffic-analysis-exercise.pcap` (from malware-traffic-analysis.net)**
- ***(Optional)* Windows 10 VM for testing and validation**

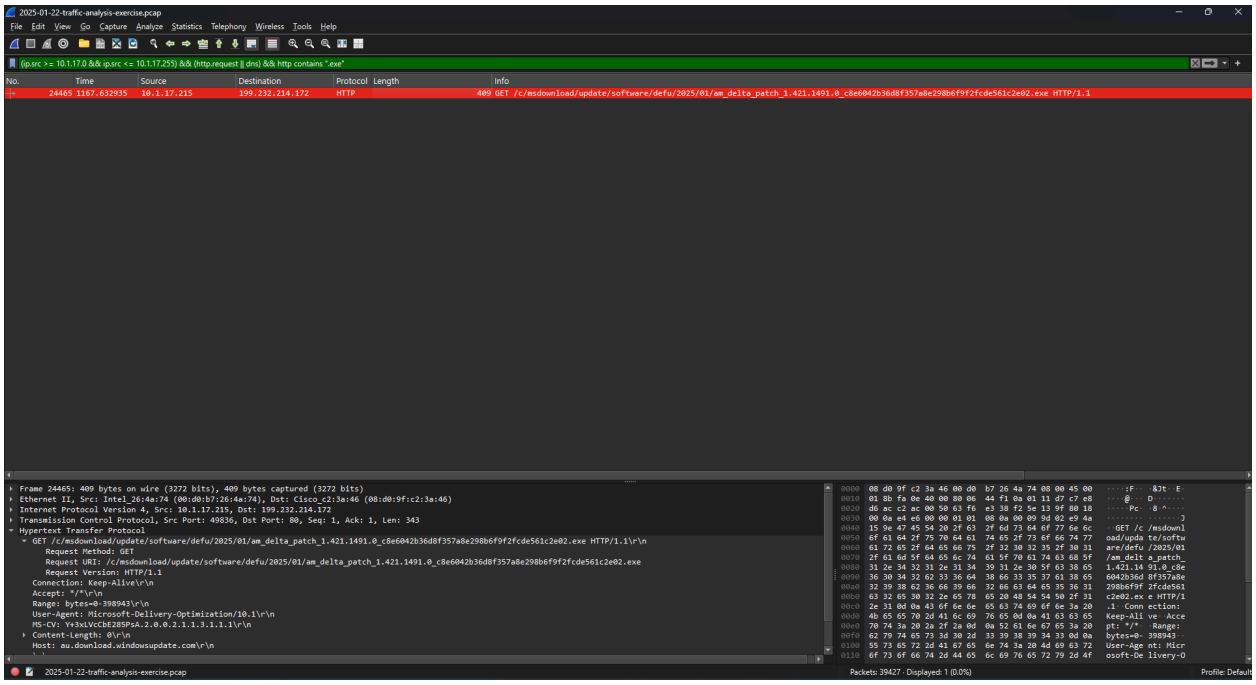
PCAP Summary

- **File Name: `2024-01-04-traffic-analysis-exercise.pcap`**
- **Description: Captures DNS and HTTP traffic from an infected Windows machine.**

1. IP Address of Infected Windows Client

- **Answer**: `10.1.17.215`

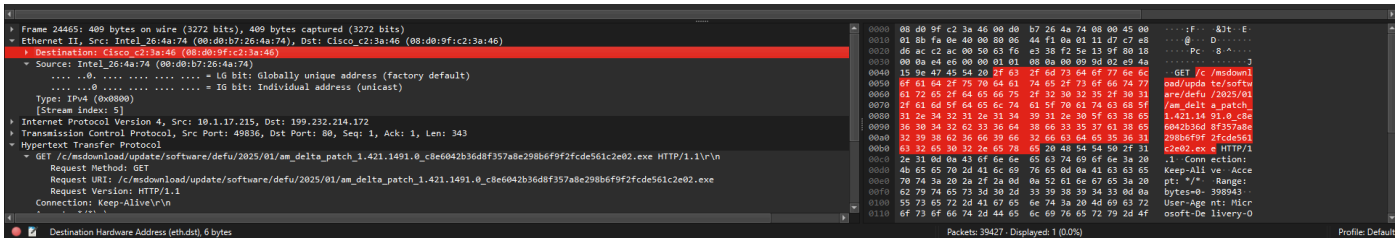
- **How Found**: Applied IP range filter to identify devices on the 10.1.17.x subnet making `.exe` HTTP requests.



2. MAC Address of Infected Windows Client

- **Answer: `00:d0:b7:26:4a:74`**

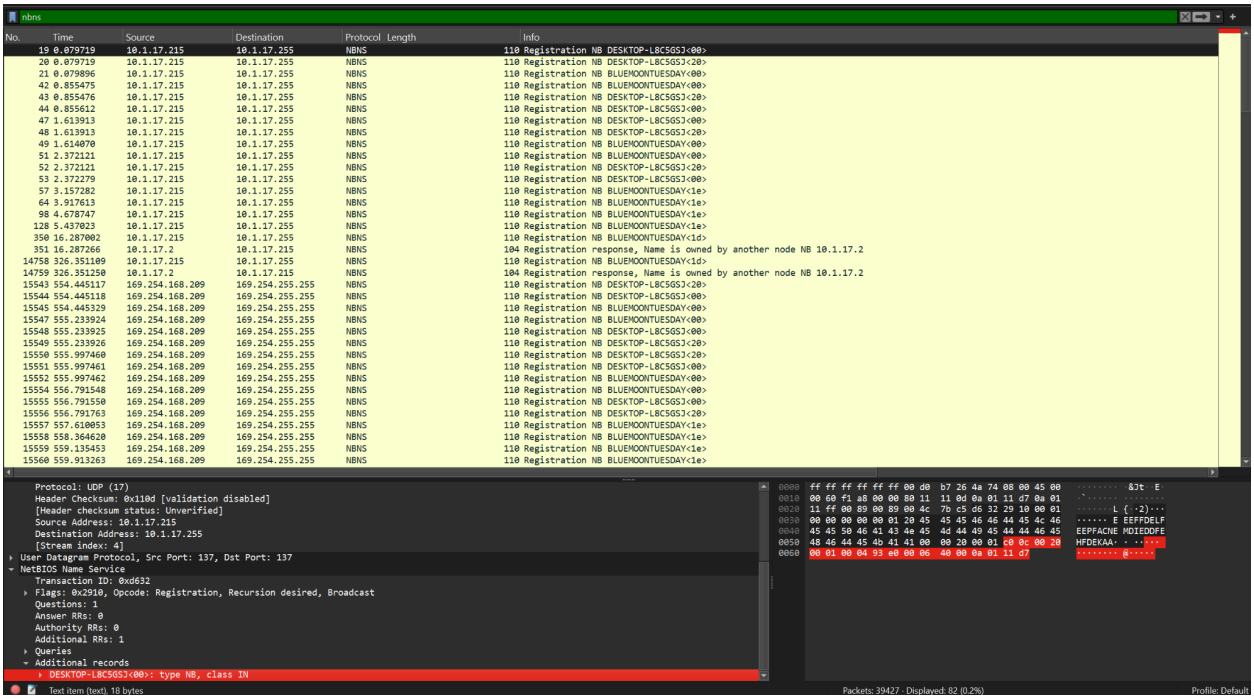
- **How Found: Checked Ethernet headers for the MAC associated with the above IP address.**



3. Host Name of Infected Windows Client

- **Answer: `DESKTOP-L8C5GSJ`**

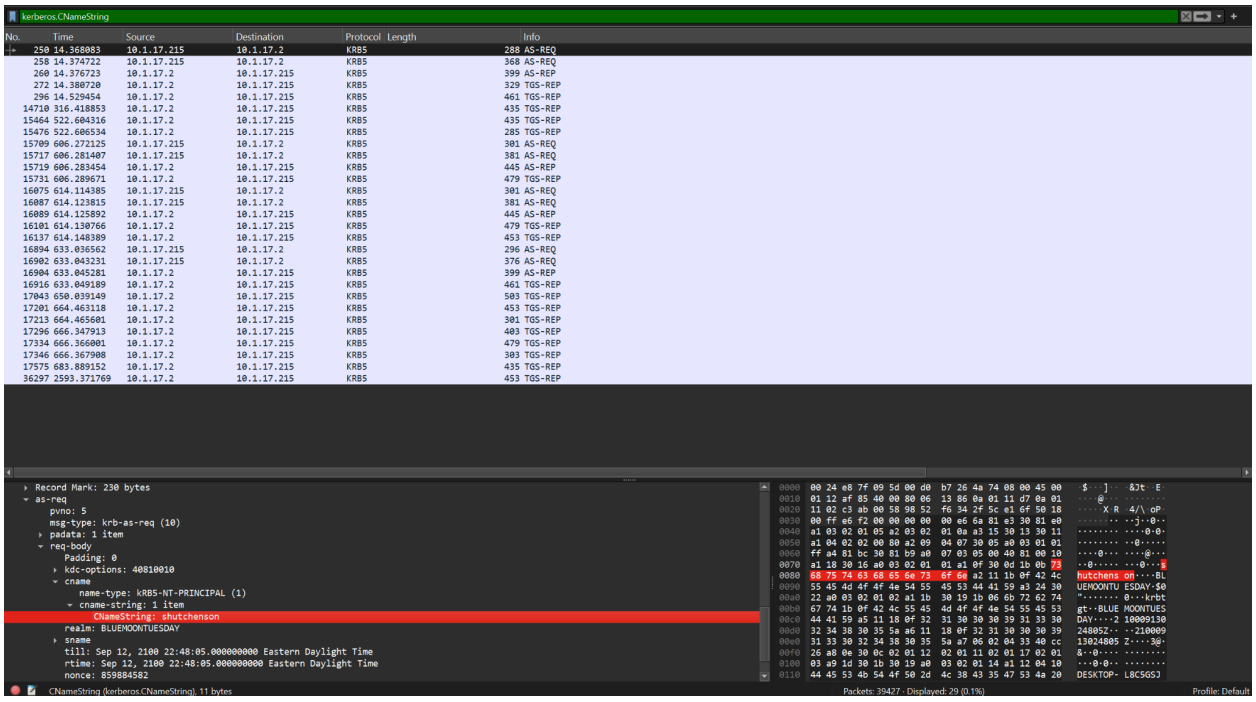
- **How Found: Used the `nbns` display filter. Located a NetBIOS Name Service response associated with the infected IP, which revealed the hostname**



4. User Account Name

- **Answer: `Shutchenson`**

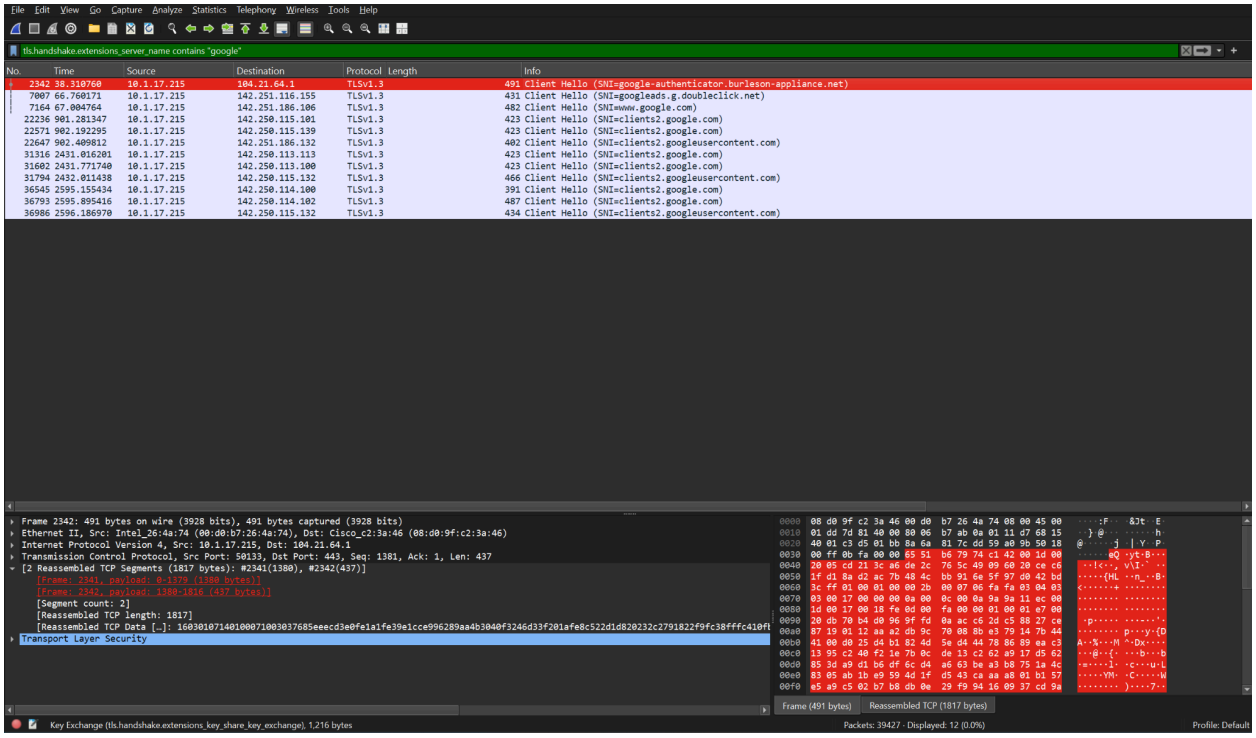
- **How Found: Filtered for `kerberos.CNameString`. Located the infected client's IP in a Kerberos ticket exchange, where the CName (client principal name) showed the username.**



5. Likely Domain Name for the Fake Google Authenticator Page

- **Answer:** `google-authenticator.burleson-appliance.net`

- **How Found: Used the filter** `tls.handshake.extensions_server_name contains "google"` **to reveal the domain in the SNI (Server Name Indication) of TLS handshake packets.**



6. C2 (Command and Control) Server IPs

- **Answers:**
  - `5.252.153.241`
  - `45.125.66.32`
- **How Found: Applied `http.request` filter. Identified outgoing HTTP requests from the infected IP to these external servers, including the retrieval of a PowerShell script indicative of malicious activity.**