Incident Analysis Report

Prepared by: Oluwatobiloba Aladejare

Date: 17/03/2025 - 23/03/2025

SUMMARY

The Security Operations Center (SOC) was alerted to an infection following the suspicious file downloaded after searching for Google Authenticator. The caller provided references to social media posts from LinkedIn and X (formerly Twitter) which showed attacks through a malicious ad from a fake Teams page serving fake Google Authenticator pages.

After reviewing the PCAP file named traffic-analysis.pcap.zip the infection was confirmed through the presence of malicious traffic matching details from a GitHub page referenced in the social media posts. This report outlines the findings from the analysis of the associated PCAP file.

Indicators of Compromise (IoCs)

- Fake Google Authenticator Website
- Similar indicators with the GitHub page

Methodology

The file named traffic-analysis.pcap.zip was decrypted using the password **infected_20250122** on a virtual Machine to avoid further risk of infection and network traffic was analyzed using Wireshark.

Analyze the traffic from the infected host based on the **LAN segment details** provided:

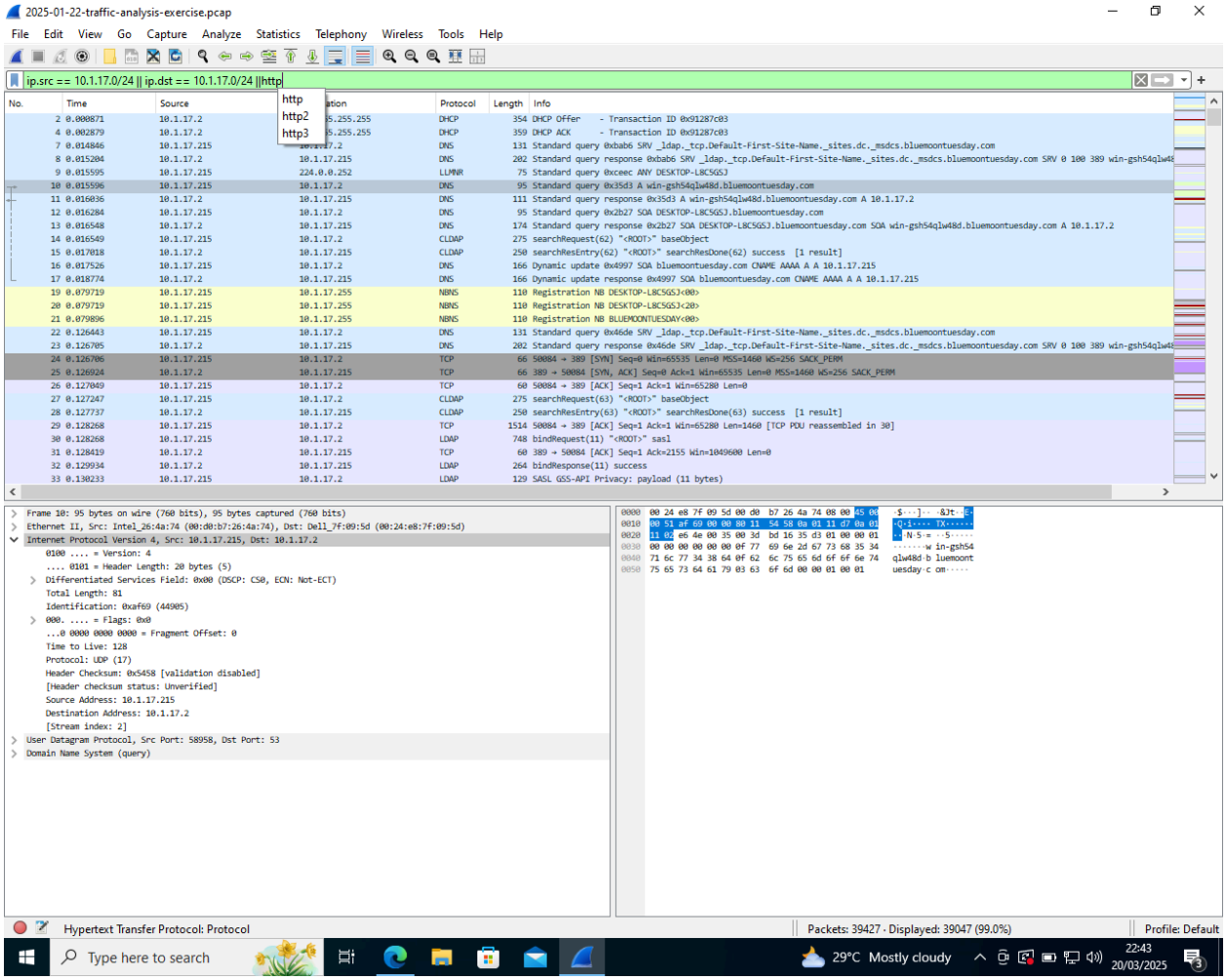
- LAN Segment Range: **10.1.17.0/24**
- Domain: **bluemoontuesday.com**
- Active Directory (AD) Controller: **10.1.17.2**

Analysis

1. IP Address of the Infected Windows Client:

By analyzing the packet capture, we focused on IP addresses within the LAN segment 10.1.17.0/24 and 10.1.17.215.

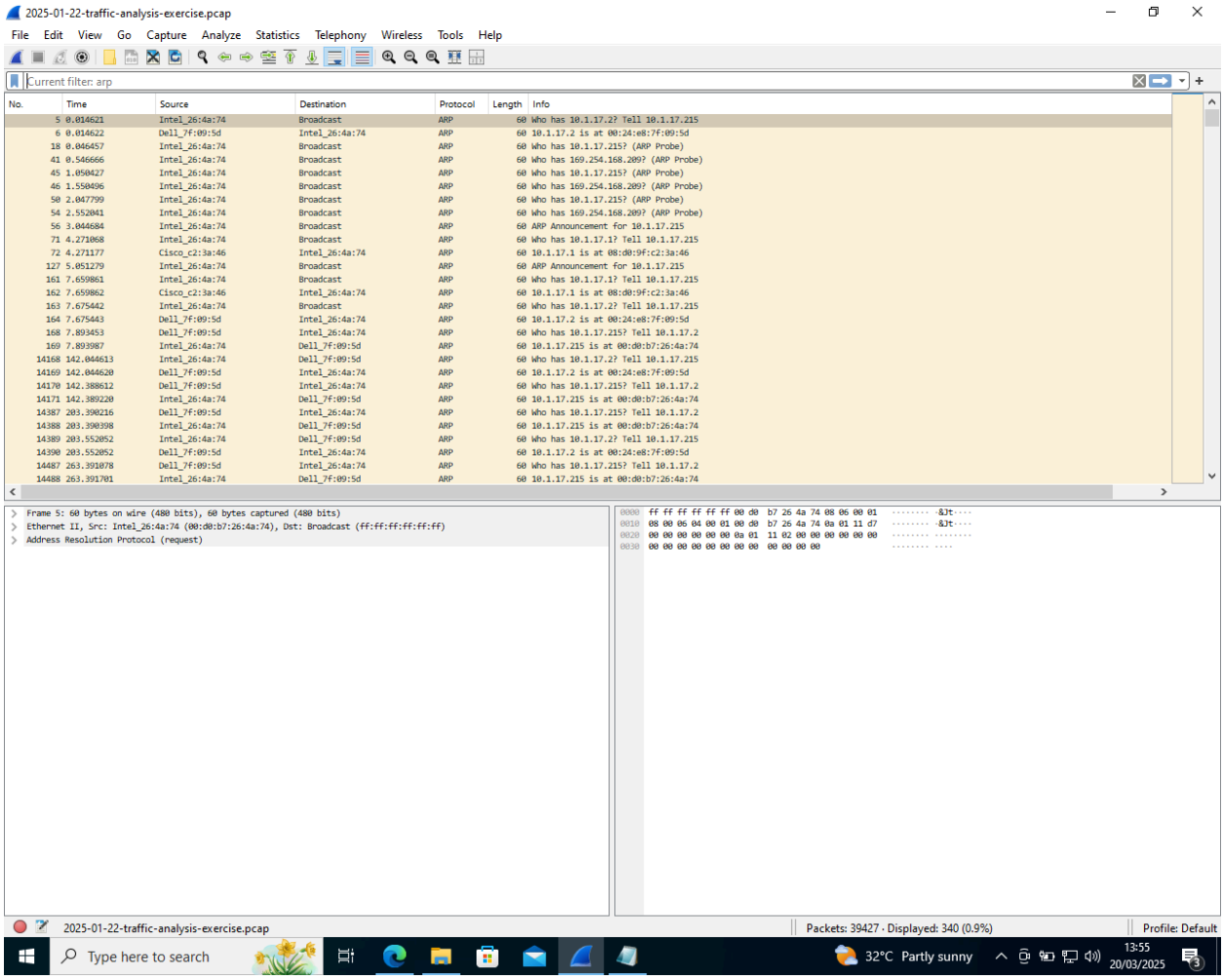
The IP address of the infected Windows client is: **10.1.17.215.** The Domain Controller for the environment is located at 10.1.17.2 (WIN-GSH54QLW48D).



2. MAC Address of the Infected Windows Client:

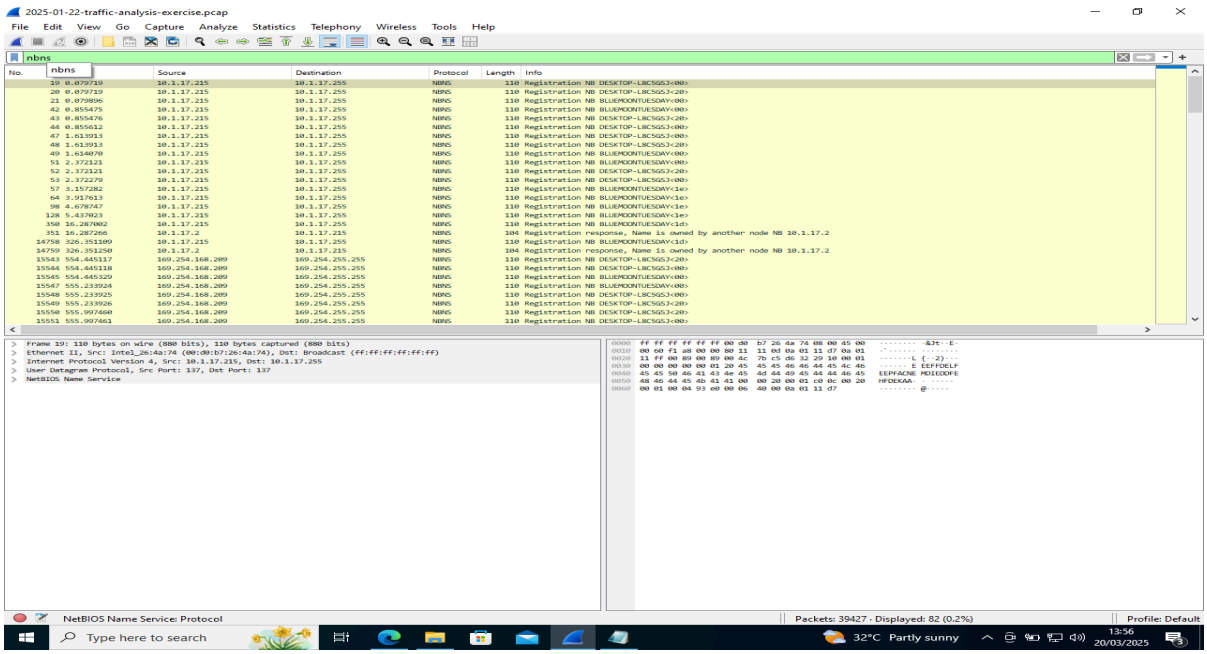
The Ethernet frames in the PCAP are examined for the MAC address. By analyzing the arp replies, the MAC address associated with the infected IP was found.

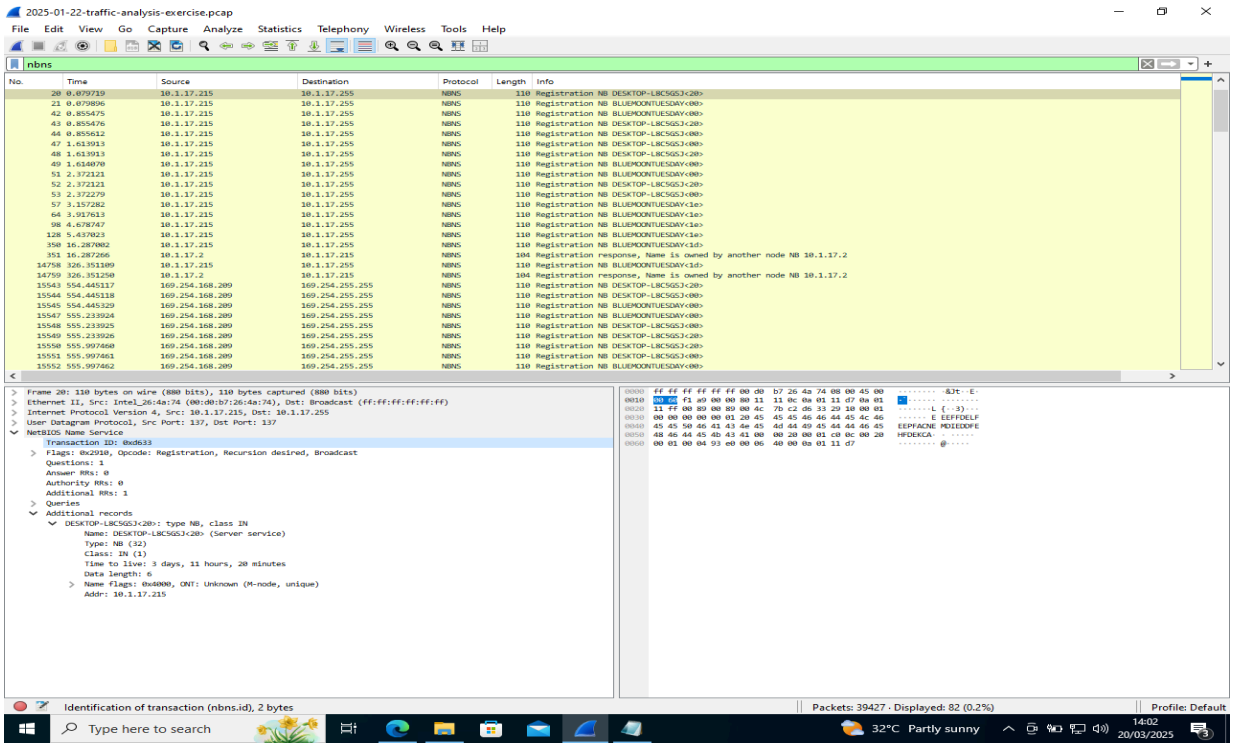
The **MAC address** of the infected Windows client is **00:d0:b7:26:4a:74**



3. Hostname of the Infected Windows Client:

The hostname was identified using the NetBIOS Name Service (nbns) query. The hostname of the infected Windows client is: **DESKTOP-L8C5GSJ<20>**, confirming its identity on the network.

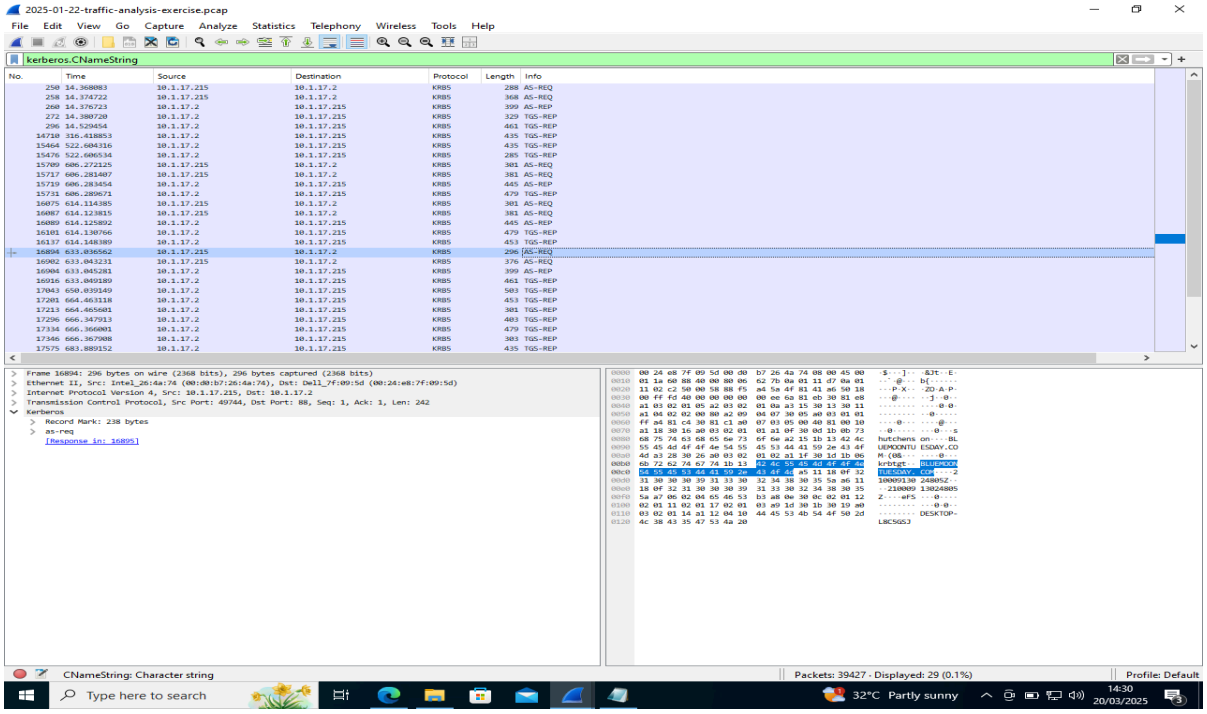


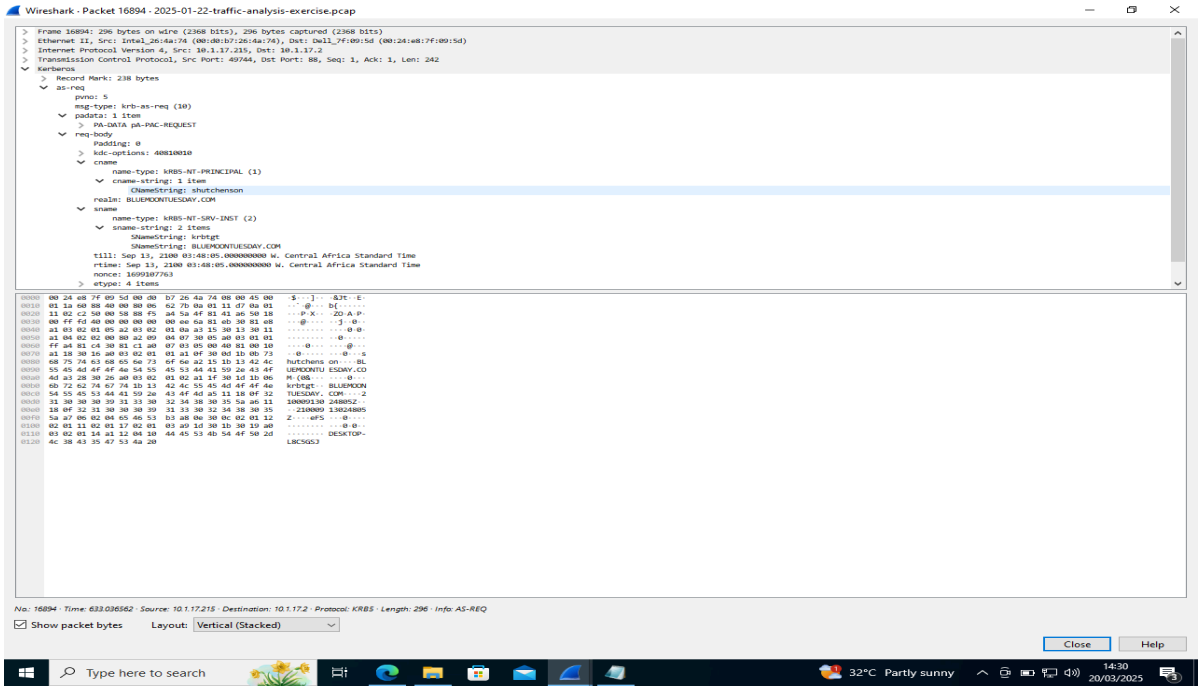


4. User Account Name from the Infected Windows Client:

The machine is in an Active Directory environment and so the username was searched for in the Kerberos packets.

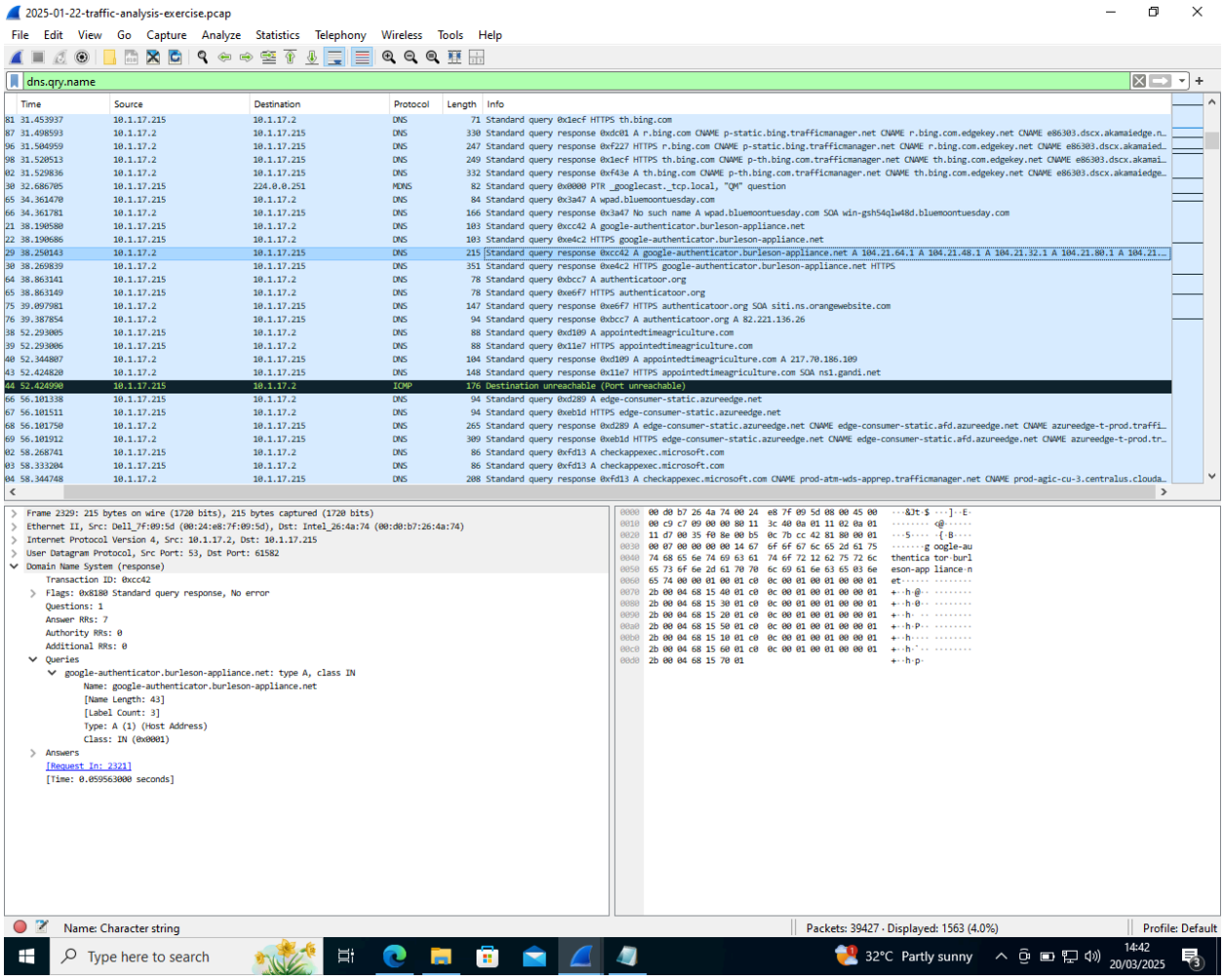
The user account name associated with the infected Windows client is: **SHUTCHENSON**

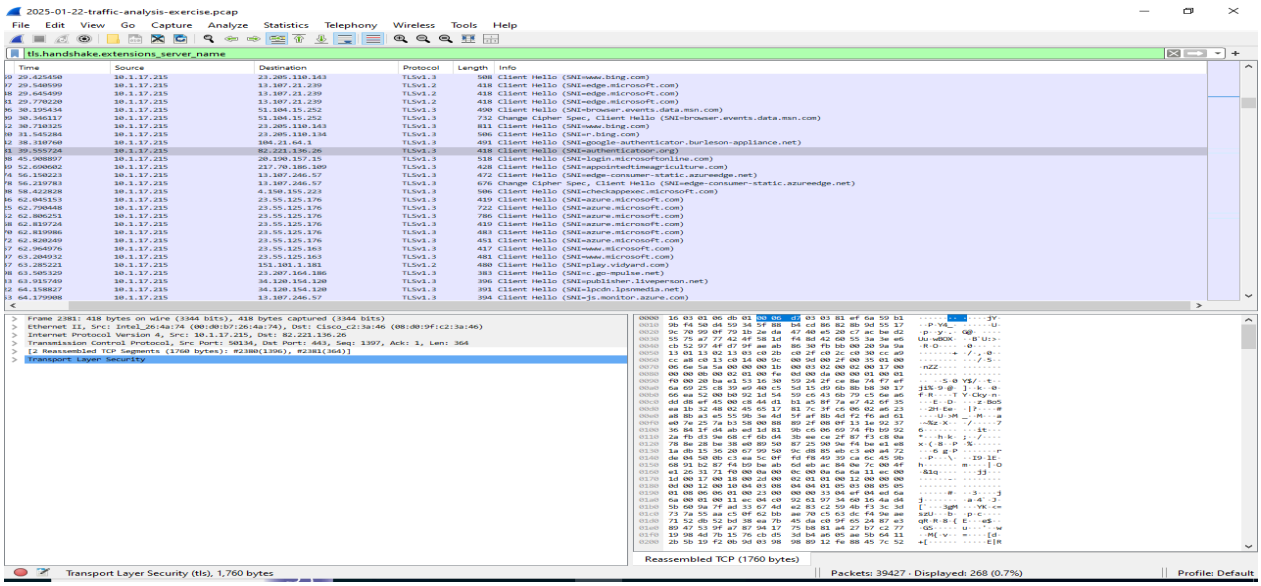


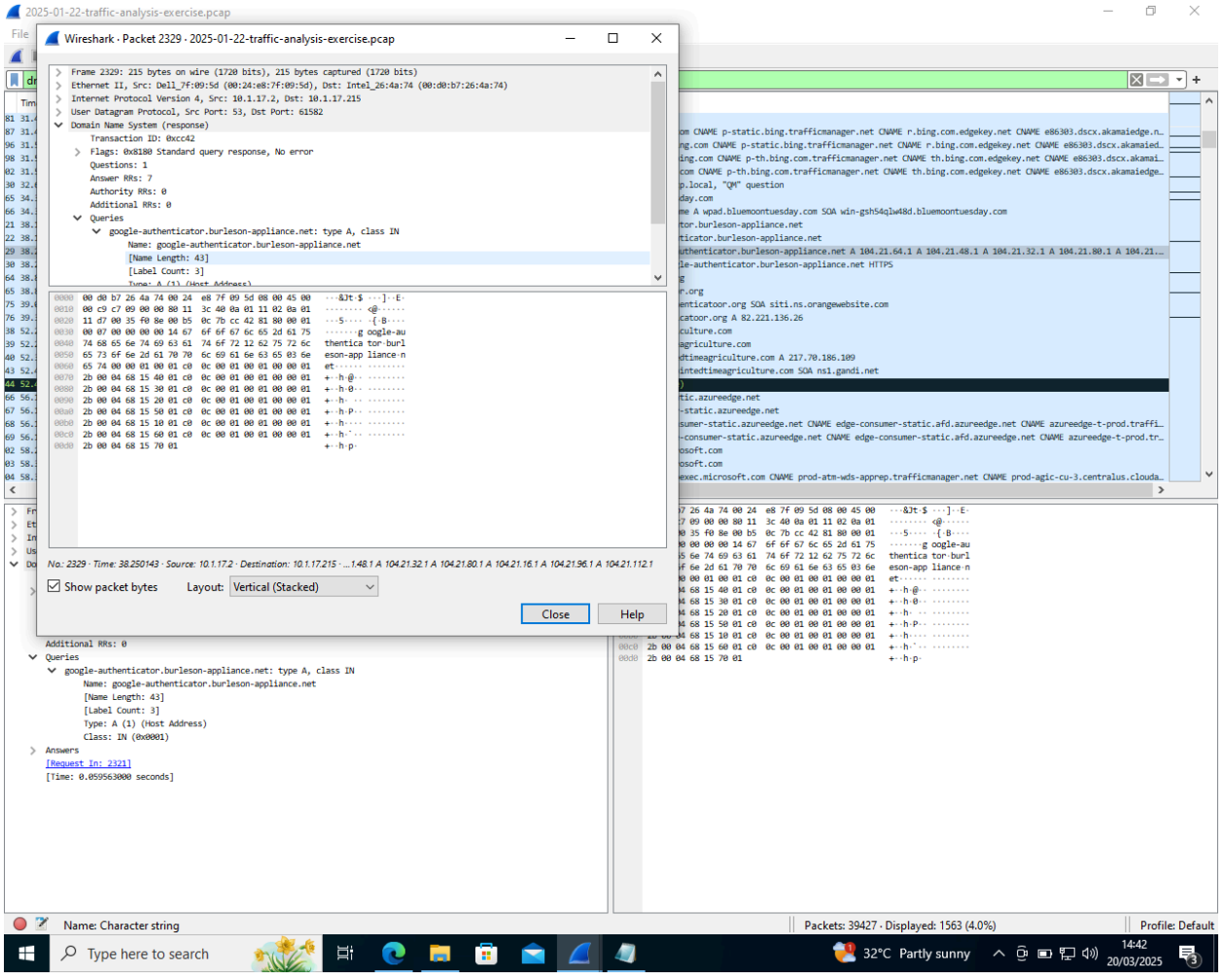


5. Likely Domain Name for the Fake Google Authenticator Page:

To determine the fake website used in the attack, DNS queries were analyzed using . The suspicious domain resembling Google Authenticator page is identified as **google-authenticator.burleson-appliance.net, authenticator.org**




2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls.handshake.extensions_server_name
Transport Layer Security (tls), 1,760 bytes
Reassembled TCP (1760 bytes)
Packets: 39427 · Displayed: 268 (0.7%)
Profile: Default


Wireshark · Packet 2329 · 2025-01-22-traffic-analysis-exercise.pcap
Frame 2329: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits)
Ethernet II, Src: Dell_7f:09:5d (00:24:e8:7f:09:5d), Dst: Intel_26:4a:74 (00:d0:b7:26:4a:74)
Internet Protocol Version 4, Src: 10.1.17.2, Dst: 10.1.17.215
User Datagram Protocol, Src Port: 53, Dst Port: 61582
Domain Name System (response)
Transaction ID: 0xcc42
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 7
Authority RRs: 0
Additional RRs: 0
Queries
google-authenticator.burleson-appliance.net: type A, class IN
Name: google-authenticator.burleson-appliance.net
[Name Length: 43]
[Label Count: 3]
No.: 2329 · Time: 38.250143 · Source: 10.1.17.2 · Destination: 10.1.17.215 · ...1.48.1 A 104.21.32.1 A 104.21.80.1 A 104.21.16.1 A 104.21.96.1 A 104.21.112.1
Show packet bytes
Layout: Vertical (Stacked)
Close
Help
Additional RRs: 0
Queries
google-authenticator.burleson-appliance.net: type A, class IN
Name: google-authenticator.burleson-appliance.net
[Name Length: 43]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)
Answers
[Request In: 2321]
[Time: 0.059563000 seconds]
Name: Character string
Packets: 39427 · Displayed: 1563 (4.0%)
Profile: Default
Type here to search
32°C Partly sunny
14:42
20/03/2025

Recommendations
- The infected Windows should be isolated from the network immediately and all passwords be reset. - All suspicious domains associated with the fake Google Authenticator page must be blocked using a firewall. - A full malware scan and forensic investigation should be done on the infected machine to determine the extent of the breach. - Review any traffic to and from the infected machine to identify other potential compromised systems. - Employees must be educated on malicious search engine ads and on web safe practices and all downloads must be done only from official websites or sources.