

## 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).

The image shows a Wireshark packet capture analysis. The top pane displays a list of 33 packets. The bottom pane shows a detailed view of the selected packet (No. 33), which is a DNS query from 10.1.17.215 to 10.1.17.2. The packet details include Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000000	10.1.17.2	10.1.17.2	DHCP	254	DHCP Offer - Transaction ID 0x01287083
4	0.000000	10.1.17.2	10.1.17.2	DHCP	359	DHCP ACK - Transaction ID 0x01287083
7	0.014846	10.1.17.215	10.1.17.2	DNS	131	Standard query 0xbab6 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumountuesday.com
8	0.015284	10.1.17.2	10.1.17.215	DNS	282	Standard query response 0xbab6 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumountuesday.com SRV 0 100 389 win-gsh54qlw48d
9	0.015595	10.1.17.215	224.0.0.252	LLMNR	75	Standard query 0xccec ANY DESKTOP-LKCSG53
10	0.015596	10.1.17.215	10.1.17.2	DNS	95	Standard query 0x35d3 A win-gsh54qlw48d.blumountuesday.com
11	0.016036	10.1.17.2	10.1.17.215	DNS	111	Standard query response 0x35d3 A win-gsh54qlw48d.blumountuesday.com A 10.1.17.2
12	0.016284	10.1.17.215	10.1.17.2	DNS	95	Standard query 0x2b27 SOA DESKTOP-LKCSG53.blumountuesday.com
13	0.016548	10.1.17.2	10.1.17.215	DNS	174	Standard query response 0x2b27 SOA DESKTOP-LKCSG53.blumountuesday.com SOA win-gsh54qlw48d.blumountuesday.com A 10.1.17.2
14	0.016549	10.1.17.215	10.1.17.2	LDAP	275	searchRequest(62) "(<root>)" baseObject
15	0.017018	10.1.17.2	10.1.17.215	LDAP	250	searchResponse(62) "(<root>)" searchResultEntry(62) success [1 result]
16	0.017526	10.1.17.215	10.1.17.2	DNS	166	Dynamic update 0x4997 SOA blumountuesday.com CNAME AAAA A 10.1.17.215
17	0.018774	10.1.17.2	10.1.17.215	DNS	166	Dynamic update response 0x4997 SOA blumountuesday.com CNAME AAAA A 10.1.17.215
19	0.079719	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-LKCSG53-000
20	0.079719	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-LKCSG53-000
21	0.079896	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUMOUNTUE50AV-000
22	0.126443	10.1.17.215	10.1.17.2	DNS	131	Standard query 0x46de SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumountuesday.com
23	0.126705	10.1.17.2	10.1.17.215	DNS	282	Standard query response 0x46de SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumountuesday.com SRV 0 100 389 win-gsh54qlw48d
24	0.126706	10.1.17.215	10.1.17.2	TCP	66	50084 -> 389 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
25	0.126924	10.1.17.2	10.1.17.215	TCP	66	389 -> 50084 [SYN, ACK] Seq=0 Ack=1 Win=65280 Len=0 MSS=1460 WS=256 SACK_PERM
26	0.127040	10.1.17.215	10.1.17.2	TCP	60	50084 -> 389 [ACK] Seq=1 Ack=1 Win=65280 Len=0
27	0.127247	10.1.17.215	10.1.17.2	LDAP	275	searchRequest(63) "(<root>)" baseObject
28	0.127737	10.1.17.2	10.1.17.215	LDAP	250	searchResponse(63) "(<root>)" searchResultEntry(63) success [1 result]
29	0.128268	10.1.17.215	10.1.17.2	TCP	1514	50084 -> 389 [ACK] Seq=1 Ack=1 Win=65280 Len=1460 [TCP PDU reassembled in 30]
30	0.128268	10.1.17.215	10.1.17.2	LDAP	748	bindRequest(11) "(<root>)" sasl
31	0.128419	10.1.17.2	10.1.17.215	TCP	60	389 -> 50084 [ACK] Seq=1 Ack=2155 Win=1049600 Len=0
32	0.129934	10.1.17.2	10.1.17.215	LDAP	264	bindResponse(11) success
33	0.130233	10.1.17.215	10.1.17.2	LDAP	129	SASL GSS-API Privacy: payload (11 bytes)

Frame 33: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0  
Ethernet II, Src: Intel\_E8\_4A\_74 (08:00:07:26:4A:74), Dst: Dell\_7F\_09\_5D (00:24:00:7F:09:5D)  
Internet Protocol Version 4, Src: 10.1.17.215, Dst: 10.1.17.2

0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 81  
Identification: 0x4f69 (44905)  
> 0000 .... = Flags: 0x00  
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 128  
Protocol: UDP (17)  
Header Checksum: 0x5458 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 10.1.17.215  
Destination Address: 10.1.17.2  
[Stream index: 2]  
> User Datagram Protocol, Src Port: 58958, Dst Port: 53  
> Domain Name System (query)

0000 00 24 e8 7f 09 5d 00 d0 b7 26 4a 74 08 00 05 00 ... 02f  
0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ... 00  
0020 11 02 e5 4e 00 35 00 3d bd 16 35 d3 01 00 00 01 ... N 5 = 5  
0030 00 00 00 00 00 00 0f 77 69 6e 2d 67 73 68 35 34 ... w in-gsh54  
0040 71 6c 77 34 38 64 0f 62 6c 75 65 6d 6f 6e 74 ... qlw48d-b blumount  
0050 75 65 73 64 63 79 03 63 6f 6d 00 00 01 00 01 ... uesday-c on

## 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**

2025-01-22-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: arp

No.	Time	Source	Destination	Protocol	Length	Info
5	0.014621	Intel_26:4a:74	Broadcast	ARP	60	Who has 10.1.17.2? Tell 10.1.17.215
6	0.014622	Dell_7f:00:5d	Intel_26:4a:74	ARP	60	10.1.17.2 is at 00:24:e8:7f:00:5d
18	0.046457	Intel_26:4a:74	Broadcast	ARP	60	Who has 10.1.17.215? (ARP Probe)
41	0.046456	Intel_26:4a:74	Broadcast	ARP	60	Who has 169.254.168.209? (ARP Probe)
45	1.050427	Intel_26:4a:74	Broadcast	ARP	60	Who has 10.1.17.215? (ARP Probe)
46	1.550496	Intel_26:4a:74	Broadcast	ARP	60	Who has 169.254.168.209? (ARP Probe)
50	2.047799	Intel_26:4a:74	Broadcast	ARP	60	Who has 10.1.17.215? (ARP Probe)
54	2.552041	Intel_26:4a:74	Broadcast	ARP	60	Who has 169.254.168.209? (ARP Probe)
56	3.046484	Intel_26:4a:74	Broadcast	ARP	60	ARP Announcement for 10.1.17.215
71	4.271868	Intel_26:4a:74	Broadcast	ARP	60	Who has 10.1.17.1? Tell 10.1.17.215
72	4.271177	Cisco_c2:3a:46	Intel_26:4a:74	ARP	60	10.1.17.1 is at 08:00:0c:27:3a:46
127	5.053279	Intel_26:4a:74	Broadcast	ARP	60	ARP Announcement for 10.1.17.215
161	7.659861	Intel_26:4a:74	Broadcast	ARP	60	Who has 10.1.17.1? Tell 10.1.17.215
162	7.659862	Cisco_c2:3a:46	Intel_26:4a:74	ARP	60	10.1.17.1 is at 08:00:0c:27:3a:46
163	7.675442	Intel_26:4a:74	Broadcast	ARP	60	Who has 10.1.17.2? Tell 10.1.17.215
164	7.675443	Dell_7f:00:5d	Intel_26:4a:74	ARP	60	10.1.17.2 is at 00:24:e8:7f:00:5d
168	7.893453	Intel_26:4a:74	Intel_26:4a:74	ARP	60	Who has 10.1.17.215? Tell 10.1.17.2
169	7.893987	Intel_26:4a:74	Dell_7f:00:5d	ARP	60	10.1.17.215 is at 00:d0:b7:26:4a:74
14168	142.044613	Intel_26:4a:74	Dell_7f:00:5d	ARP	60	Who has 10.1.17.2? Tell 10.1.17.215
14169	142.044620	Dell_7f:00:5d	Intel_26:4a:74	ARP	60	10.1.17.2 is at 00:24:e8:7f:00:5d
14170	142.388612	Dell_7f:00:5d	Intel_26:4a:74	ARP	60	Who has 10.1.17.215? Tell 10.1.17.2
14171	142.389220	Dell_7f:00:5d	Intel_26:4a:74	ARP	60	10.1.17.215 is at 00:d0:b7:26:4a:74
14387	203.390216	Dell_7f:00:5d	Intel_26:4a:74	ARP	60	Who has 10.1.17.215? Tell 10.1.17.2
14388	203.390398	Intel_26:4a:74	Dell_7f:00:5d	ARP	60	10.1.17.215 is at 00:d0:b7:26:4a:74
14389	203.532052	Intel_26:4a:74	Dell_7f:00:5d	ARP	60	Who has 10.1.17.2? Tell 10.1.17.215
14390	203.532052	Dell_7f:00:5d	Intel_26:4a:74	ARP	60	10.1.17.2 is at 00:24:e8:7f:00:5d
14487	263.391078	Dell_7f:00:5d	Intel_26:4a:74	ARP	60	Who has 10.1.17.215? Tell 10.1.17.2
14488	263.391701	Intel_26:4a:74	Dell_7f:00:5d	ARP	60	10.1.17.215 is at 00:d0:b7:26:4a:74

> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)  
> Ethernet II, Src: Intel\_26:4a:74 (00:d0:b7:26:4a:74), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Address Resolution Protocol (request)

```
0000  ff ff ff ff ff 00 d0 b7 26 4a 74 08 06 00 01  ....:.....:..  
0010  00 00 06 04 00 01 00 d0 b7 26 4a 74 0a 03 11 d7  ....:.....:..  
0020  00 00 00 00 00 00 0a 01 11 02 00 00 00 00 00 00  ....:.....  
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....:.....
```

Packets: 39427 - Displayed: 340 (0.9%) | Profile: Default

32°C Partly sunny 13:55 20/03/2025

### 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.

2025-01-22-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

nbns

No.	nbns	Source	Destination	Protocol	Length	Info
19	0.879719	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
20	0.879719	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
21	0.879896	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<00>
42	0.855475	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<00>
43	0.855476	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
44	0.855612	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
47	1.613911	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
48	1.613913	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
49	1.614070	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<00>
51	2.172121	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
52	2.172121	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
53	2.172279	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
57	3.157282	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
64	3.917613	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
67	4.679747	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
128	5.437023	10.1.17.2	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
150	16.287062	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
151	16.287066	10.1.17.2	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
14758	326.351309	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
14759	326.351206	10.1.17.2	10.1.17.255	NBNS	110	Registration response, Name is owned by another node NB 10.1.17.2
15543	554.445117	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
15544	554.445118	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
15545	554.445120	169.254.168.209	169.254.255.255	NBNS	110	Registration NB BLUEKONTUESDAY<00>
15547	555.233924	169.254.168.209	169.254.255.255	NBNS	110	Registration NB BLUEKONTUESDAY<00>
15548	555.233925	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
15549	555.233926	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
15550	555.997668	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
15551	555.997661	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>

> Frame 19: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0  
> Ethernet II, Src: Intel\_20:4a:74 (08:00:07:20:4a:74), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Internet Protocol Version 4, Src: 10.1.17.215, Dst: 10.1.17.255  
> User Datagram Protocol, Src Port: 137, Dst Port: 137  
> NetBIOS Name Service

NetBIOS Name Service Protocol | Packets: 39427 - Displayed: 82 (0.2%) | Profile: Default

2025-01-22-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

nbns

No.	Time	Source	Destination	Protocol	Length	Info
20	0.879719	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
21	0.879896	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<00>
42	0.855475	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<00>
43	0.855476	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
44	0.855612	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
47	1.613911	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
48	1.613913	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
49	1.614070	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<00>
51	2.172121	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
52	2.172121	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
53	2.172279	10.1.17.215	10.1.17.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
57	3.157282	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
64	3.917613	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
67	4.679747	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
128	5.437023	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
150	16.287062	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
151	16.287066	10.1.17.2	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
14758	326.351309	10.1.17.215	10.1.17.255	NBNS	110	Registration NB BLUEKONTUESDAY<1a>
14759	326.351206	10.1.17.2	10.1.17.255	NBNS	110	Registration response, Name is owned by another node NB 10.1.17.2
15543	554.445117	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
15544	554.445118	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
15545	554.445120	169.254.168.209	169.254.255.255	NBNS	110	Registration NB BLUEKONTUESDAY<00>
15547	555.233924	169.254.168.209	169.254.255.255	NBNS	110	Registration NB BLUEKONTUESDAY<00>
15548	555.233925	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
15549	555.233926	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
15550	555.997668	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
15551	555.997661	169.254.168.209	169.254.255.255	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
15552	555.997662	169.254.168.209	169.254.255.255	NBNS	110	Registration NB BLUEKONTUESDAY<00>

> Frame 20: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0  
> Ethernet II, Src: Intel\_20:4a:74 (08:00:07:20:4a:74), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Internet Protocol Version 4, Src: 10.1.17.215, Dst: 10.1.17.255  
> User Datagram Protocol, Src Port: 137, Dst Port: 137  
> NetBIOS Name Service

Transaction ID: 0x4d33

> Flags: 0x2020, Opcode: Registration, Recursion desired, Broadcast

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 1

Queries

Additional records

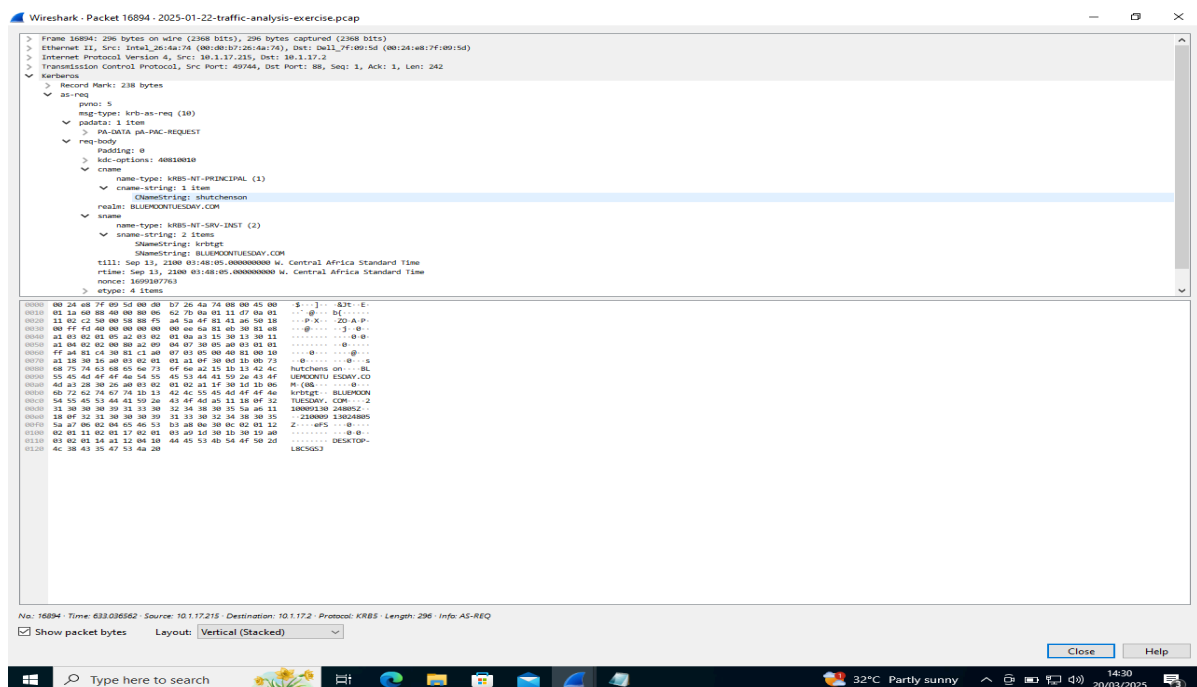
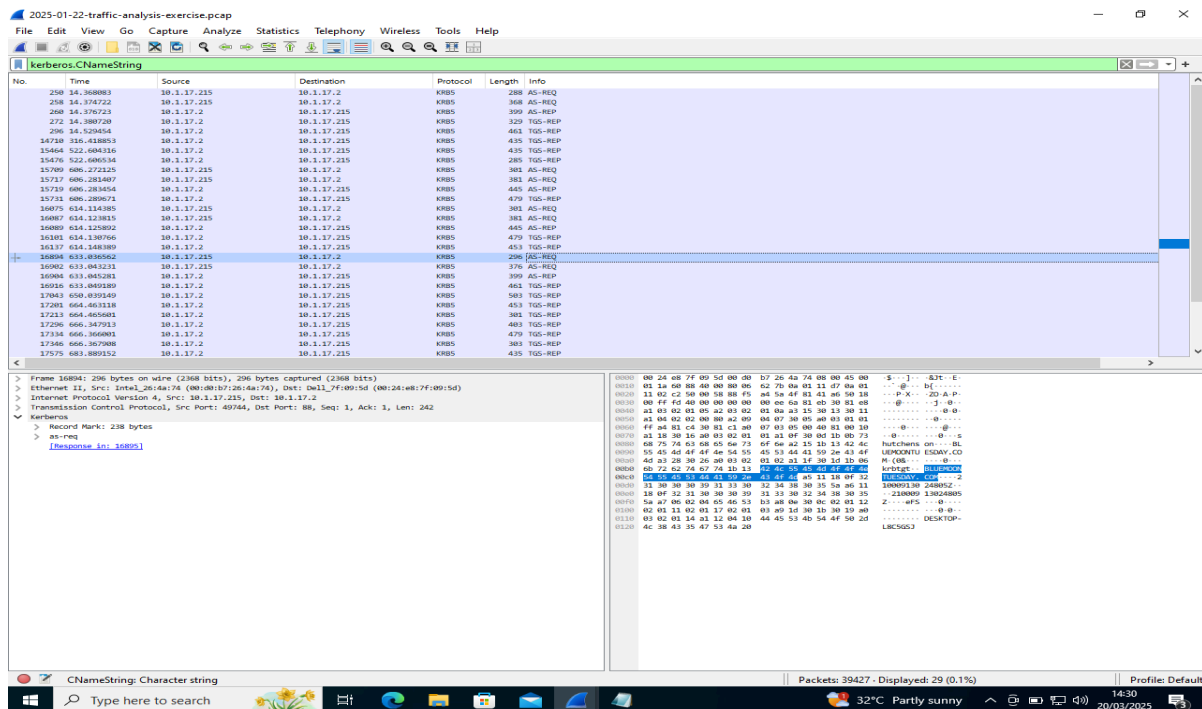
- DESKTOP-L8C5GSJ<20>: type NB, class IN
- Name: DESKTOP-L8C5GSJ<20> (Server service)
- Type: NB (12)
- Class: IN (1)
- Time to live: 3 days, 11 hours, 20 minutes
- Data length: 6
- Name flags: 0x0000, ONT: Unknown (M-node, unique)
- Addr: 10.1.17.215

Identification of transaction (nbns.id), 2 bytes | Packets: 39427 - Displayed: 82 (0.2%) | Profile: Default

#### 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 Wireshark. 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

dns.qry.name

Time	Source	Destination	Protocol	Length	Info
81	10.1.17.215	10.1.17.2	DNS	71	Standard query 0x4c42 HTTPS th.bing.com
87	10.1.17.215	10.1.17.2	DNS	330	Standard query response 0x4c42 A r.bing.com CNAME p-static.bing.trafficmanager.net CNAME r.bing.com.edgekey.net CNAME e86301.dscx.akamaiedge.net
96	10.1.17.2	10.1.17.215	DNS	247	Standard query response 0x4c42 HTTPS r.bing.com CNAME p-static.bing.trafficmanager.net CNAME r.bing.com.edgekey.net CNAME e86301.dscx.akamaiedge.net
98	10.1.17.2	10.1.17.215	DNS	249	Standard query response 0x4c42 HTTPS th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME th.bing.com.edgekey.net CNAME e86301.dscx.akamaiedge.net
102	10.1.17.2	10.1.17.215	DNS	332	Standard query response 0x4c42 A th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME th.bing.com.edgekey.net CNAME e86301.dscx.akamaiedge.net
103	10.1.17.215	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "Q?" question
105	10.1.17.215	10.1.17.2	DNS	84	Standard query 0x3a47 A wpad.blumountuesday.com
106	10.1.17.2	10.1.17.215	DNS	166	Standard query response 0x3a47 No such name A wpad.blumountuesday.com SOA win-gsh54qlw8d.blumountuesday.com
118	10.1.17.215	10.1.17.2	DNS	103	Standard query 0x4c42 A google-authenticator.burleson-appliance.net
122	10.1.17.215	10.1.17.2	DNS	103	Standard query 0x4c42 HTTPS google-authenticator.burleson-appliance.net
129	10.1.17.2	10.1.17.215	DNS	215	Standard query response 0x4c42 A google-authenticator.burleson-appliance.net A 104.21.64.1 A 104.21.68.1 A 104.21.32.1 A 104.21.80.1 A 104.21.16.1
130	10.1.17.2	10.1.17.215	DNS	351	Standard query response 0x4c42 HTTPS google-authenticator.burleson-appliance.net HTTPS
144	10.1.17.215	10.1.17.2	DNS	78	Standard query 0x4c42 A authenticator.org
145	10.1.17.215	10.1.17.2	DNS	78	Standard query 0x4c42 HTTPS authenticator.org
175	10.1.17.2	10.1.17.215	DNS	147	Standard query response 0x4c42 HTTPS authenticator.org SOA siti.ns.orangewebsite.com
176	10.1.17.2	10.1.17.215	DNS	94	Standard query response 0x4c42 A authenticator.org A 82.221.136.26
188	10.1.17.215	10.1.17.2	DNS	88	Standard query 0x4c42 A appointedtimeagriculture.com
189	10.1.17.215	10.1.17.2	DNS	88	Standard query 0x4c42 HTTPS appointedtimeagriculture.com
190	10.1.17.2	10.1.17.215	DNS	104	Standard query response 0x4c42 A appointedtimeagriculture.com A 217.70.186.109
191	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0x4c42 HTTPS appointedtimeagriculture.com SOA ns1.gandi.net
192	10.1.17.2	10.1.17.2	DNS	116	Destination unreachable (port unreachable)
193	10.1.17.215	10.1.17.2	DNS	94	Standard query 0x4c42 A edge-consumer-static.azureedge.net
194	10.1.17.215	10.1.17.2	DNS	94	Standard query 0x4c42 HTTPS edge-consumer-static.azureedge.net
195	10.1.17.2	10.1.17.215	DNS	265	Standard query response 0x4c42 A edge-consumer-static.azureedge.net CNAME edge-consumer-static.afd.azureedge.net CNAME azureedge-t-prod.traffi
196	10.1.17.2	10.1.17.215	DNS	309	Standard query response 0x4c42 HTTPS edge-consumer-static.azureedge.net CNAME edge-consumer-static.afd.azureedge.net CNAME azureedge-t-prod.tr
197	10.1.17.215	10.1.17.2	DNS	86	Standard query 0x4c42 A checkappex.microsoft.com
198	10.1.17.215	10.1.17.2	DNS	86	Standard query 0x4c42 A checkappex.microsoft.com
199	10.1.17.2	10.1.17.215	DNS	288	Standard query response 0x4c42 A checkappex.microsoft.com CNAME prod-atn-wds-apprep.trafficmanager.net CNAME prod-agic-cu-3.centralus.clouda

< Frame 2220: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface 0  
> Ethernet II, Src: Dell\_7f:80:5d (00:24:68:7f:80:5d), Dst: Intel\_26:4a:74 (00:0b:77:26:4a: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: 0x4c42  
Flags: 0x180 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]  
Type: A (1 (Host Address))  
Class: IN (0x0001)  
Answers  
Request ID: 2321  
[Time: 0.059563000 seconds]

Name: Character string

Packets: 39427 - Displayed: 1563 (4.0%)

Profile: Default

32°C Partly sunny

14:42  
20/03/2025

2025-01-22-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

th.handshake.extensions.server\_name

Time	Source	Destination	Protocol	Length	Info
19	29.242450	10.1.17.215	TLSv1.3	1088	Client Hello (SHA256, bing.com)
20	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
21	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
22	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
23	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
24	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
25	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
26	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
27	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
28	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
29	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
30	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
31	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
32	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
33	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
34	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
35	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
36	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
37	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
38	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
39	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
40	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
41	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
42	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
43	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
44	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
45	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
46	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
47	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
48	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
49	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
50	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
51	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
52	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
53	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
54	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
55	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
56	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
57	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
58	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
59	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
60	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
61	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
62	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
63	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
64	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
65	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
66	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
67	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
68	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
69	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
70	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
71	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
72	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
73	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
74	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
75	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
76	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
77	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
78	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
79	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
80	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
81	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
82	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
83	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
84	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
85	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
86	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
87	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
88	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
89	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
90	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
91	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
92	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
93	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
94	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
95	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
96	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
97	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
98	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
99	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)
100	29.242450	10.1.17.215	TLSv1.3	418	Client Hello (SHA256, microsoft.com)

Transport Layer Security (tls), 1,760 bytes

Packets: 39427 - Displayed: 268 (0.7%)

Profile: Default

2025-01-22-traffic-analysis-exercise.pcap

Wireshark - Packet 2329 - 2025-01-22-traffic-analysis-exercise.pcap

Frame 2329: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on eth0

Ethernet II, Src: Dell\_7F-69-56 (00:24:00:7F:69:56), Dst: Intel\_26:4A:74 (08:00: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: 0xccc2

Flags: 0x0100 Standard query response, No error

Questions: 1

Answers: 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]
- Type: A (1) (Host Address)
- Class: IN (0x0001)

Answers

- 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)

Request ID: 2329

Time: 0.059563000 seconds

Show packet bytes

Layout: Vertical (Stacked)

Close Help

Name Character string

Packets: 39427 - Displayed: 1563 (4.0%)

Profile: Default

## 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.