NETWORK TRAFFIC ANALYSIS REPORT

REPORTED BY ABDULMALIK SALAMAH

DATE: 20TH OF MARCH,2025

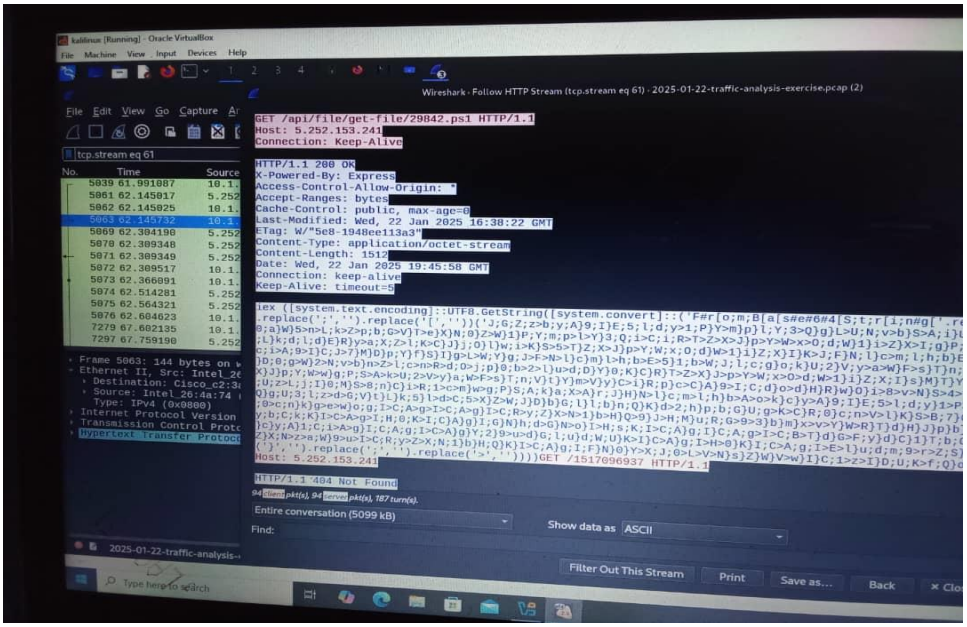
On the 20th of march 2025, it was brought to the attention of i and my team members that a co worker downloaded a suspicious file during her search for google authenticator.

I confirmed there was an infection,got a packet capture from the associated traffic to compare with matching details from a github page on social media accounts that had some posts on them.

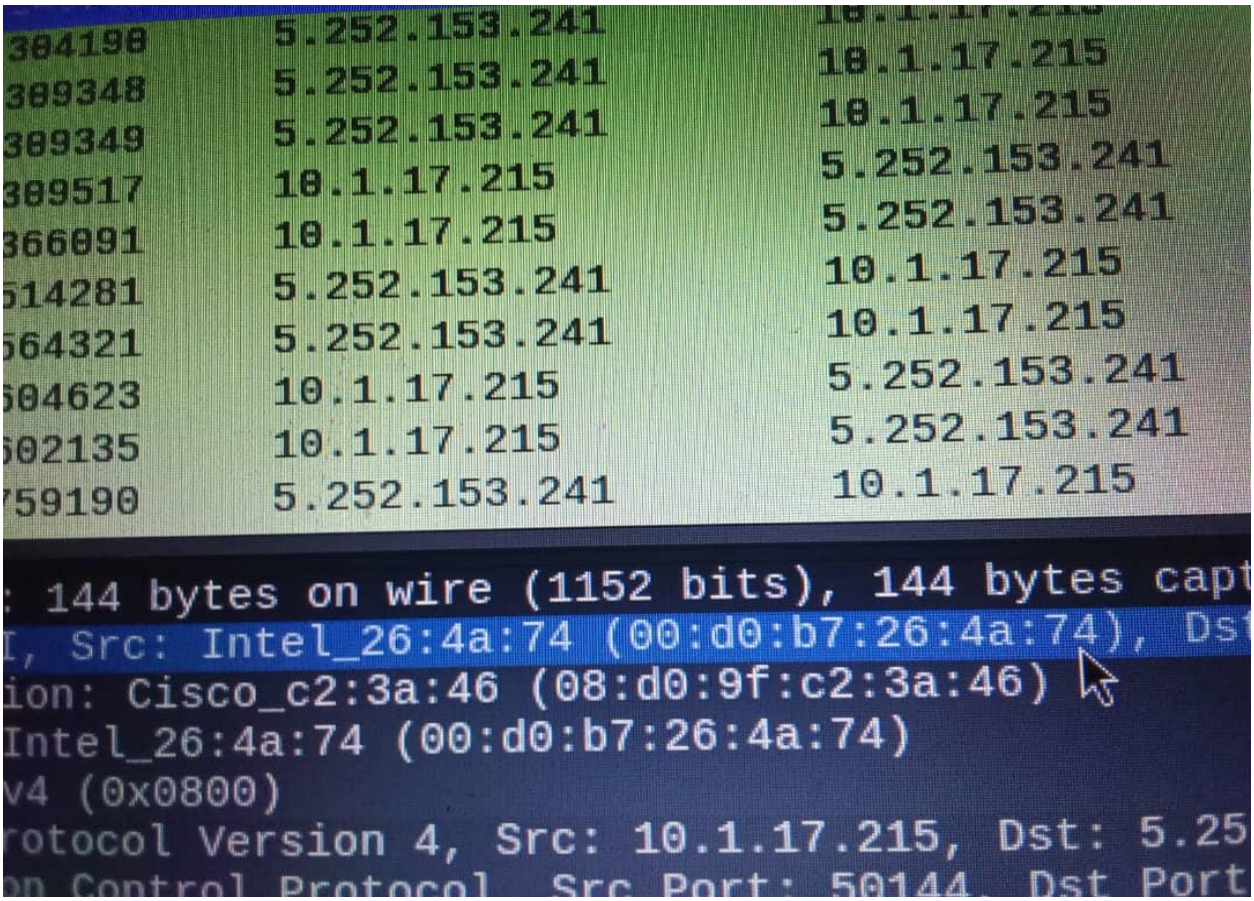
After careful review and investigations, I could come up with these details from the packet capture I took that were aligning to the details of the posts made on the social media accounts .

The details include:

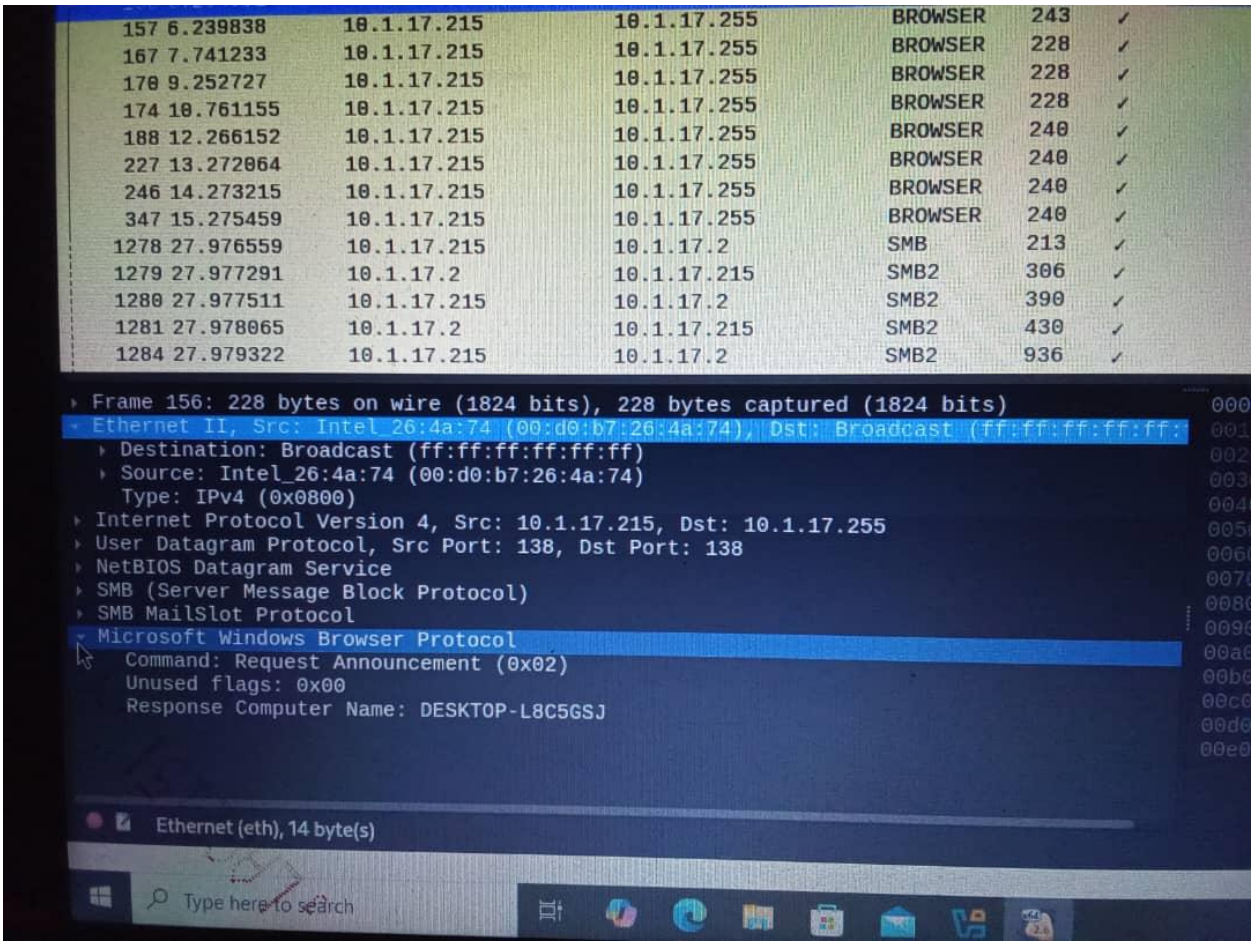
1. The Ip address of the infected windows client



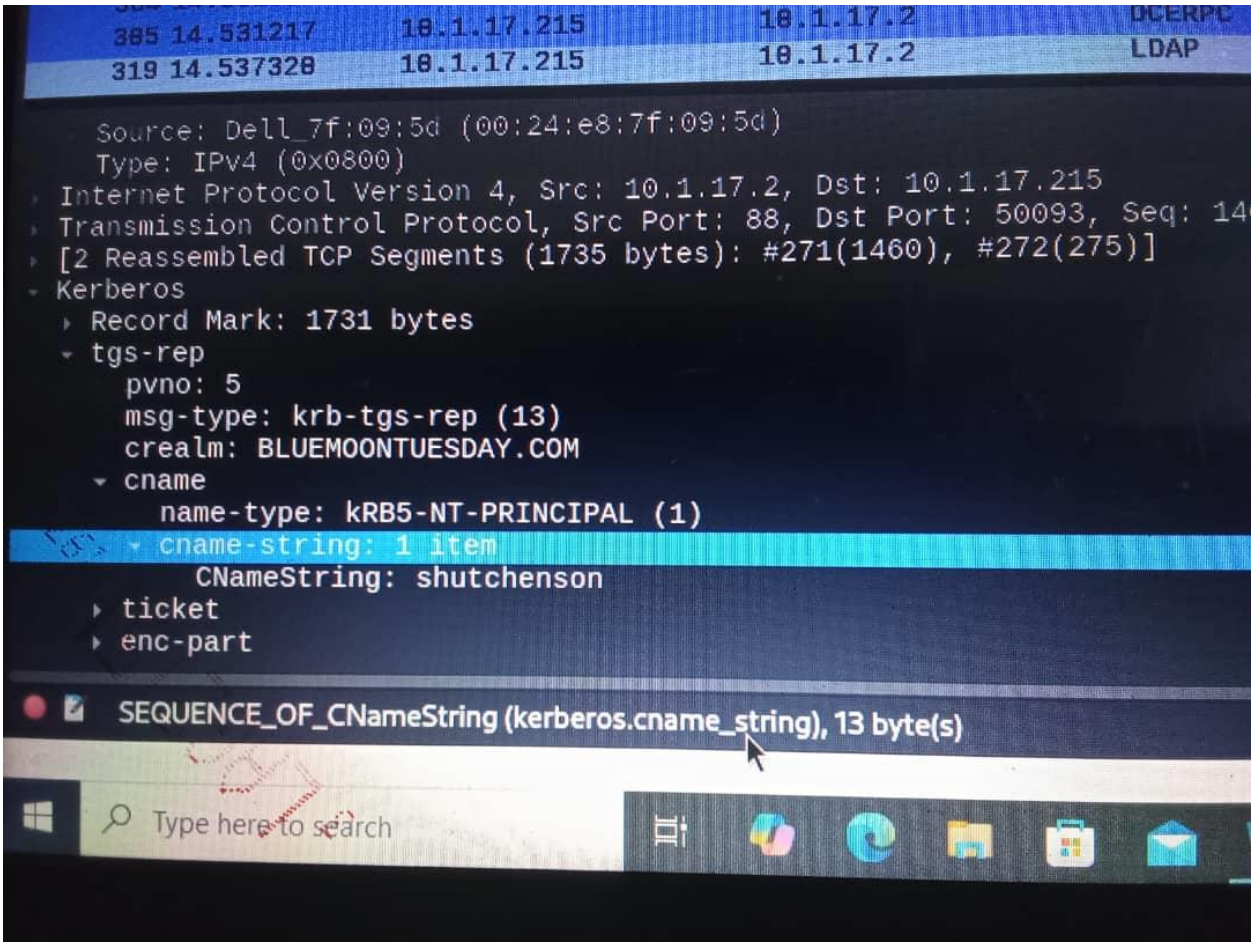
2. The MAC address of the infected windows client:



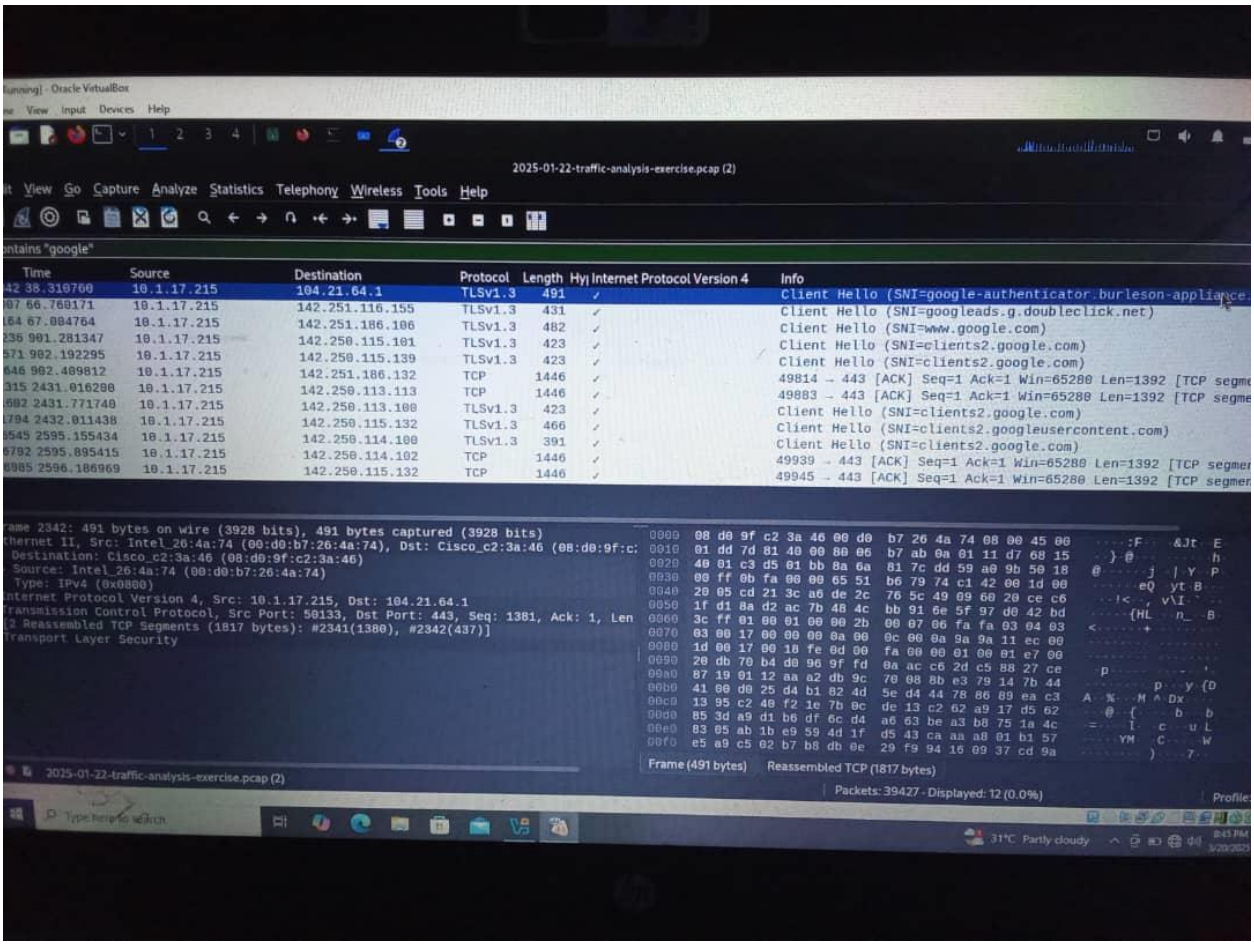
3. The hostname of the infected windows client: THE RESPONSE COMPUTER NAME

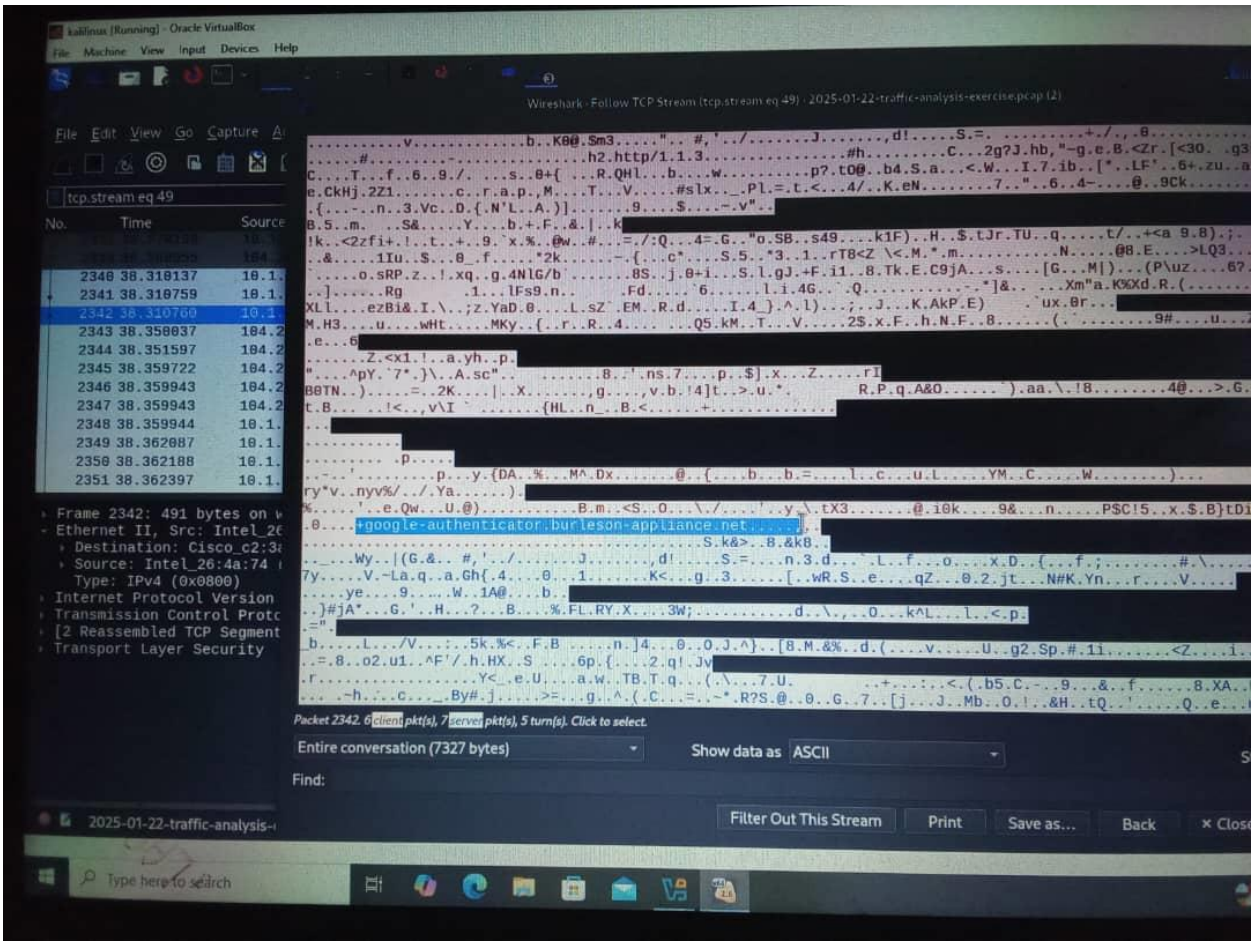

157 6.239838 10.1.17.215 10.1.17.255 BROWSER 243
167 7.741233 10.1.17.215 10.1.17.255 BROWSER 228
170 9.252727 10.1.17.215 10.1.17.255 BROWSER 228
174 10.761155 10.1.17.215 10.1.17.255 BROWSER 228
188 12.266152 10.1.17.215 10.1.17.255 BROWSER 240
227 13.272064 10.1.17.215 10.1.17.255 BROWSER 240
246 14.273215 10.1.17.215 10.1.17.255 BROWSER 240
347 15.275459 10.1.17.215 10.1.17.255 BROWSER 240
1278 27.976559 10.1.17.215 10.1.17.2 SMB 213
1279 27.977291 10.1.17.2 10.1.17.215 SMB2 306
1280 27.977511 10.1.17.215 10.1.17.2 SMB2 390
1281 27.978065 10.1.17.2 10.1.17.215 SMB2 430
1284 27.979322 10.1.17.215 10.1.17.2 SMB2 936
Frame 156: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits)
Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Broadcast (ff:ff:ff:ff:ff:
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Intel_26:4a:74 (00:d0:b7:26:4a:74)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.1.17.215, Dst: 10.1.17.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
Command: Request Announcement (0x02)
Unused flags: 0x00
Response Computer Name: DESKTOP-L8C5GSJ
Ethernet (eth), 14 byte(s)
Type here to search

4. The user account name:



5. The likely domain name:


Oracle VirtualBox
View Input Devices Help
2025-01-22-traffic-analysis-exercise.pcap (2)
View Go Capture Analyze Statistics Telephony Wireless Tools Help
ntains "google"
Time Source Destination Protocol Length Info
38.310760 10.1.17.215 104.21.64.1 TLSv1.3 491 Client Hello (SNI=google-authenticator.burleson-appliance.
66.760171 10.1.17.215 142.251.116.155 TLSv1.3 431 Client Hello (SNI=googleads.g.doubleclick.net)
67.084764 10.1.17.215 142.251.186.106 TLSv1.3 482 Client Hello (SNI=www.google.com)
901.281347 10.1.17.215 142.250.115.101 TLSv1.3 423 Client Hello (SNI=clients2.google.com)
902.192295 10.1.17.215 142.250.115.139 TLSv1.3 423 Client Hello (SNI=clients2.google.com)
902.489812 10.1.17.215 142.251.186.132 TCP 1446 49814 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1392 [TCP segme
2431.016280 10.1.17.215 142.250.113.113 TCP 1446 49883 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1392 [TCP segme
2431.771740 10.1.17.215 142.250.113.100 TLSv1.3 423 Client Hello (SNI=clients2.google.com)
2432.011438 10.1.17.215 142.250.115.132 TLSv1.3 466 Client Hello (SNI=clients2.googleusercontent.com)
2595.155434 10.1.17.215 142.250.114.100 TLSv1.3 391 Client Hello (SNI=clients2.google.com)
2595.895415 10.1.17.215 142.250.114.102 TCP 1446 49939 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1392 [TCP segmen
2596.186969 10.1.17.215 142.250.115.132 TCP 1446 49945 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1392 [TCP segmen
Internet Protocol Version 4
ame 2342: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits)
thernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Cisco_c2:3a:46 (08:d0:9f:c2:3a:46)
Destination: Cisco_c2:3a:46 (08:d0:9f:c2:3a:46)
Source: Intel_26:4a:74 (00:d0:b7:26:4a:74)
Type: IPv4 (0x0800)
nternet Protocol Version 4, Src: 10.1.17.215, Dst: 104.21.64.1
ransmission Control Protocol, Src Port: 50133, Dst Port: 443, Seq: 1381, Ack: 1, Len
2 Reassembled TCP Segments (1817 bytes): #2341(1380), #2342(437)]
ransport Layer Security
0000 08 d0 9f c2 3a 46 00 d0 b7 26 4a 74 08 00 45 00
0010 01 dd 7d 81 40 00 80 06 b7 ab 0a 01 11 d7 68 15
0020 40 01 c3 d5 01 bb 8a 6a 81 7c dd 59 a0 9b 50 18
0030 00 ff 0b fa 00 00 65 51 b6 79 74 c1 42 00 1d 00
0040 20 05 cd 21 3c a6 de 2c 76 5c 49 09 60 20 ce c6
0050 1f d1 8a d2 ac 7b 48 4c bb 91 6e 5f 97 d0 42 bd
0060 3c ff 01 00 01 00 00 2b 00 07 06 fa fa 03 04 03
0070 03 00 17 00 00 00 0a 00 0c 00 0a 9a 9a 11 ec 00
0080 1d 00 17 00 18 fe 0d 00 fa 00 00 01 00 01 e7 00
0090 20 db 70 b4 d0 96 9f fd 0a ac c6 2d c5 88 27 ce
00a0 87 19 01 12 aa a2 db 9c 70 08 8b e3 79 14 7b 44
00b0 41 00 d0 25 d4 b1 82 4d 5e d4 44 78 86 89 ea c3
00c0 13 95 c2 40 f2 1e 7b 0c de 13 c2 62 a9 17 d5 62
00d0 85 3d a9 d1 b6 df 6c d4 a6 63 be a3 b8 75 1a 4c
00e0 83 05 ab 1b e9 59 4d 1f d5 43 ca aa a8 01 b1 57
00f0 e5 a9 c5 02 b7 b8 db 0e 29 f9 94 16 09 37 cd 9a
Frame (491 bytes)
Reassembled TCP (1817 bytes)
Packets: 39427 · Displayed: 12 (0.0%)
2025-01-22-traffic-analysis-exercise.pcap (2)
Type here to search
31°C Partly cloudy


kalilinux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Wireshark · Follow TCP Stream (tcp.stream eq 49) · 2025-01-22-traffic-analysis-exercise.pcap (2)
File Edit View Go Capture
tcp.stream eq 49
No. Time Source
2340 38.310137 10.1.
2341 38.310759 10.1.
2342 38.310760 10.1.
2343 38.350037 104.2
2344 38.351597 104.2
2345 38.359722 104.2
2346 38.359943 104.2
2347 38.359943 104.2
2348 38.359944 10.1.
2349 38.362087 10.1.
2350 38.362188 10.1.
2351 38.362397 10.1.
Frame 2342: 491 bytes on
Ethernet II, Src: Intel_2
Destination: Cisco_c2:3
Source: Intel_26:4a:74
Type: IPv4 (0x0800)
Internet Protocol Version
Transmission Control Protc
[2 Reassembled TCP Segment
Transport Layer Security
+google-authenticator.burleson-appliance.net
Packet 2342. 6 client pkt(s), 7 server pkt(s), 5 turn(s). Click to select.
Entire conversation (7327 bytes)
Show data as ASCII
Find:
Filter Out This Stream
Print
Save as...
Back
2025-01-22-traffic-analysis-
Type here to search