

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

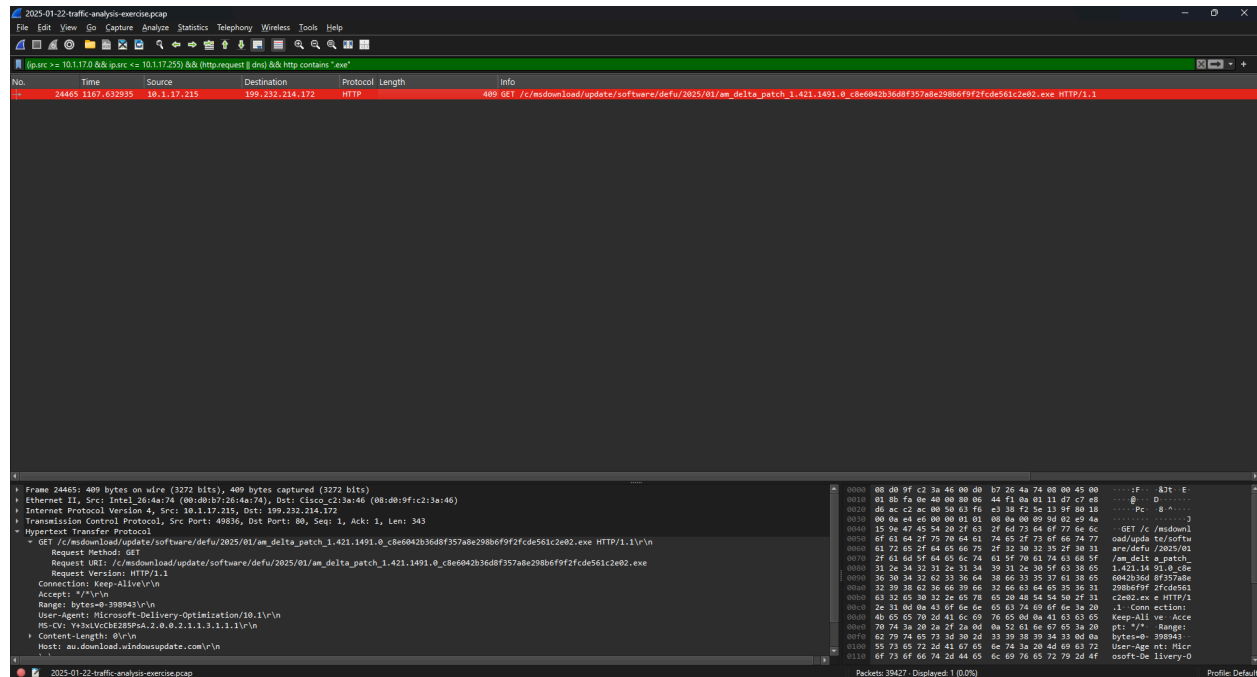
- Wireshark
 - PCAP File: **2024-01-04-traffic-analysis-exercise.pcap** (from malware-traffic-analysis.net)
 - *(Optional)* Windows 10 VM for testing and validation
-

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.

```
Frame 24465: 400 bytes on wire (3272 bits), 400 bytes captured (3272 bits) on interface 0
Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Cisco_c2:3a:46 (00:d0:9f:c2:3a:46)
  Destination: Cisco_c2:3a:46 (00:d0:9f:c2:3a:46)
    Source: Intel_26:4a:74 (00:d0:b7:26:4a:74)
      .... 0 .... = LO bit: Globally unique address (factory default)
      .... 0 .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 5]
  Internet Protocol Version 4, Src: 10.1.17.215, Dst: 199.232.214.172
  Transmission Control Protocol, Src Port: 49836, Dst Port: 80, Seq: 1, Ack: 1, Len: 343
  Hypertext Transfer Protocol
    GET /c/msdownload/update/software/defu/2025/01/am_delta_patch_1.421.1491.0_c8e6042b36d8f357a8e298b6f9f2fcd561c2e02.exe HTTP/1.1\r\n
      Request Method: GET
      Request URI: /c/msdownload/update/software/defu/2025/01/am_delta_patch_1.421.1491.0_c8e6042b36d8f357a8e298b6f9f2fcd561c2e02.exe
      Request Version: HTTP/1.1
      Connection: Keep-Alive\r\n
      ...
Destination Hardware Address (eth.dst), 6 bytes
Packets: 39427, Displayed: 1 (0.0%)
Profile: Default
```

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

Protocol: UDP (17)
Header Checksum: 0x118d [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.1.17.215
Destination Address: 10.1.17.255
[Stream Index: 4]
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
Transaction ID: 0xd632
Flags: 0x2519, Opcode: Registration, Recursion desired, Broadcast
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
Additional records
DESKTOP-L8C5GSJ-000: type NB, class IN

0000 ff ff ff ff ff ff ff b7 26 4a 74 08 00 45 00 52t E
0010 00 60 f1 a8 00 00 80 11 11 0d 0a 01 11 d7 0a 01
0020 11 ff 00 89 00 89 00 4c 70 c5 d6 32 29 10 00 01 L (:2) ...
0030 00 00 00 00 00 01 20 45 45 45 46 44 45 46 45 E EEPFOELF
0040 45 45 50 46 41 43 4e 45 4d 44 49 45 44 44 46 45 EEPFACNE MOIEDOFE
0050 46 46 44 45 4b 41 41 00 00 28 00 01 00 00 00 20 HPEXIA
0060 00 01 00 04 93 e0 00 00 40 00 0a 01 11 d7 g.....

Packets: 394/77 - Displayed: 82 (0.2%) Profile: Default

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.

The image displays a Wireshark network capture of a Kerberos AS-REQ packet. The top pane shows a list of packets, with packet 250 selected. The bottom pane shows the packet details for the selected packet, which is an AS-REQ (Kerberos AS-REQ) packet. The 'CNameString' field is highlighted in red, showing the value 'shutchenson'. The packet is 230 bytes long and is captured on interface 'eth0'.

No.	Time	Source	Destination	Protocol	Length	Info
250	14.368083	10.1.17.215	10.1.17.2	KRBS	288	AS-REQ
258	14.374722	10.1.17.215	10.1.17.2	KRBS	368	AS-REQ
260	14.376723	10.1.17.2	10.1.17.215	KRBS	399	AS-REP
272	14.380720	10.1.17.2	10.1.17.215	KRBS	329	TGS-REP
296	14.529454	10.1.17.2	10.1.17.215	KRBS	461	TGS-REP
14710	316.418853	10.1.17.2	10.1.17.215	KRBS	435	TGS-REP
15464	522.604316	10.1.17.2	10.1.17.215	KRBS	435	TGS-REP
15476	522.606534	10.1.17.2	10.1.17.215	KRBS	285	TGS-REP
15709	606.272125	10.1.17.215	10.1.17.2	KRBS	381	AS-REQ
15717	606.281407	10.1.17.215	10.1.17.2	KRBS	381	AS-REQ
15719	606.283454	10.1.17.2	10.1.17.215	KRBS	445	AS-REP
15731	606.289671	10.1.17.2	10.1.17.215	KRBS	479	TGS-REP
16075	614.114385	10.1.17.215	10.1.17.2	KRBS	381	AS-REQ
16087	614.123815	10.1.17.215	10.1.17.2	KRBS	381	AS-REQ
16089	614.125892	10.1.17.2	10.1.17.215	KRBS	445	AS-REP
16101	614.130766	10.1.17.2	10.1.17.215	KRBS	479	TGS-REP
16137	614.148389	10.1.17.2	10.1.17.215	KRBS	453	TGS-REP
16894	633.036562	10.1.17.215	10.1.17.2	KRBS	296	AS-REQ
16902	633.043231	10.1.17.215	10.1.17.2	KRBS	376	AS-REQ
16904	633.045281	10.1.17.2	10.1.17.215	KRBS	399	AS-REP
16916	633.049189	10.1.17.2	10.1.17.215	KRBS	461	TGS-REP
17043	650.039149	10.1.17.2	10.1.17.215	KRBS	503	TGS-REP
17201	664.463118	10.1.17.2	10.1.17.215	KRBS	453	TGS-REP
17213	664.465601	10.1.17.2	10.1.17.215	KRBS	381	TGS-REP
17296	666.347913	10.1.17.2	10.1.17.215	KRBS	403	TGS-REP
17334	666.360801	10.1.17.2	10.1.17.215	KRBS	479	TGS-REP
17346	666.367908	10.1.17.2	10.1.17.215	KRBS	383	TGS-REP
17575	683.889152	10.1.17.2	10.1.17.215	KRBS	435	TGS-REP
36297	2593.371769	10.1.17.2	10.1.17.215	KRBS	453	TGS-REP

Record Mark: 230 bytes

as-req

msg-type: krb-as-req (10)

padat: 1 item

req-body

Padding: 0

kdc-options: 40810010

cname

name-type: KRBS-NT-PRINCIPAL (1)

cname-string: 1 item

CNameString: shutchenson

realm: BLUEMOONTUESDAY

sname

till: Sep 12, 2100 22:48:05.000000000 Eastern Daylight Time

rttime: Sep 12, 2100 22:48:05.000000000 Eastern Daylight Time

nonce: 859884552

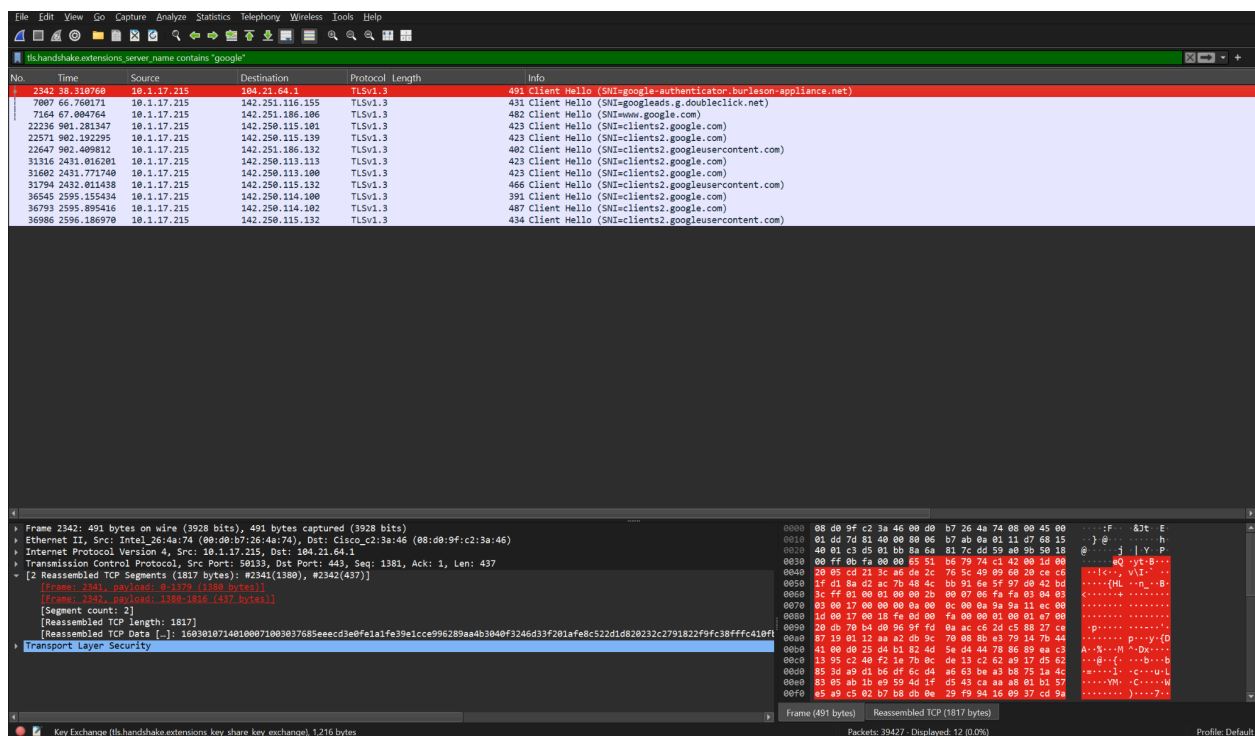
CNameString (Kerberos.CNameString), 11 bytes

Packets: 39477 / Displayed: 29 (0.1%)

Profile: Default

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.

The screenshot displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets, with a filter of 'http.request' applied. The list includes various HTTP requests, with several highlighted in red, indicating a match with the filter. The bottom pane shows the details of the selected packet (No. 5063), which is an HTTP GET request for a PowerShell script. The packet is captured on the Ethernet II interface, and the details pane shows the full structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, and the HTTP request body. The packet is captured on the Ethernet II interface, and the details pane shows the full structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, and the HTTP request body.

No.	Time	Source	Destination	Protocol	Length	Info
53	3.828629	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
62	3.380729	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
63	3.334093	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
65	3.999157	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
111	4.800969	10.1.17.215	23.200.102.9	HTTP	165	GET /connecttest.txt HTTP/1.1
158	6.345920	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
159	6.371064	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
160	7.011059	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
173	10.018018	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
211	13.020372	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
349	16.033316	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
641	19.043836	10.1.17.215	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
5031	60.297799	10.1.17.215	5.252.153.241	HTTP	373	GET /api/file/get-file/264872 HTTP/1.1
5063	62.145732	10.1.17.215	5.252.153.241	HTTP	144	GET /api/file/get-file/25842.ps1 HTTP/1.1
5073	62.366091	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7279	67.682135	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7680	72.778372	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7688	77.950821	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7696	83.150518	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7762	86.784060	10.1.17.215	199.232.214.172	HTTP	411	HEAD /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=17378849678P2=4048P3=28P4=Q0ZfrdpZetb6N2vCA75UqOgJEUa0b3xK2
7765	86.771540	10.1.17.215	199.232.214.172	HTTP	462	GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=17378849678P2=4048P3=28P4=Q0ZfrdpZetb6N2vCA75UqOgJEUa0b3xK2
7841	88.342574	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7851	90.825252	10.1.17.215	199.232.214.172	HTTP	403	HEAD /filestreamingservice/files/2a0d597c-a09c-4400-be06-87596d2e696?P1=17378849678P2=4048P3=28P4=Q0ZfrdpZetb6N2vCA75UqOgJEUa0b3xK2
7854	90.887961	10.1.17.215	199.232.214.172	HTTP	454	GET /filestreamingservice/files/2a0d597c-a09c-4400-be06-87596d2e696?P1=17378849678P2=4048P3=28P4=Q0ZfrdpZetb6N2vCA75UqOgJEUa0b3xK2
7864	93.533611	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7878	96.724353	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7880	103.914233	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7907	109.104054	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7972	114.301358	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7979	119.552871	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
7996	124.740329	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
8002	124.998139	10.1.17.215	5.252.153.241	HTTP	121	GET /api/file/get-file/TeamViewer_Resource HTTP/1.1
12890	128.458764	10.1.17.215	5.252.153.241	HTTP	133	GET /api/file/get-file/TeamViewer_Resource HTTP/1.1
13643	128.827817	10.1.17.215	5.252.153.241	HTTP	113	GET /api/file/get-file/TV HTTP/1.1
13671	128.984576	10.1.17.215	5.252.153.241	HTTP	118	GET /api/file/get-file/pas.ps1 HTTP/1.1
13677	129.210334	10.1.17.215	5.252.153.241	HTTP	176	GET /1517096937?k=message&20=20&startUp&20=20&shortCut&20=20&status&20=20&success; HTTP/1.1

Frame 5063: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
Ethernet II, Src: Intel26:4a:74 (08:00:b7:26:4a:74), Dst: CiscoC2:3a:46 (08:00:9f:c2:3a:46)
Internet Protocol Version 4, Src: 10.1.17.215, Dst: 5.252.153.241
Transmission Control Protocol, Src Port: 50144, Dst Port: 80, Seq: 1, Ack: 1, Len: 90
Source Port: 50144
Destination Port: 80
[Stream Index: 61]
[Stream Packet Number: 4]
[Conversation completeness: Complete, WITH_DATA (47)]
... .. = RST: Present
... .. = FIN: Absent
... .. = Data: Present
... .. = ACK: Present
... .. = SYN+ACK: Present
... .. = SYN: Present
[Completeness Flags: R+DATA]
[TCP Segment Len: 90]
Request Boolean
Packets: 29427, Displayed: 655 (1.7%)
Profile: Default