

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Src.port	Destination	Dst.port	Protocol	Length	Info
1	2025-01-22 19:44:56.530137	0.0.0.0	68	255.255.255.255	67	DHCP	344	DHCP Discover - Transaction ID 0x91287c03
2	2025-01-22 19:44:56.531008	10.1.17.2	67	255.255.255.255	68	DHCP	354	DHCP Offer - Transaction ID 0x91287c03
3	2025-01-22 19:44:56.532026	0.0.0.0	68	255.255.255.255	67	DHCP	390	DHCP Request - Transaction ID 0x91287c03
4	2025-01-22 19:44:56.533016	10.1.17.2	67	255.255.255.255	68	DHCP	359	DHCP ACK - Transaction ID 0x91287c03
5	2025-01-22 19:44:56.544758	Intel_26:4a:74		Broadcast		ARP	60	Who has 10.1.17.2? Tell 10.1.17.215
6	2025-01-22 19:44:56.544759	Dell_7f:09:5d		Intel_26:4a:74		ARP	60	10.1.17.2 is at 00:24:e8:7f:09:5d
7	2025-01-22 19:44:56.544983	10.1.17.215	57386	10.1.17.2	53	DNS	131	Standard query 0xbab6 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.bluemoo
8	2025-01-22 19:44:56.545341	10.1.17.2	53	10.1.17.215	57386	DNS	202	Standard query response 0xbab6 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.bluemoo
9	2025-01-22 19:44:56.545732	10.1.17.215	56330	224.0.0.252	5355	LLMNR	75	Standard query 0xceec ANY DESKTOP-L8C5GSJ
10	2025-01-22 19:44:56.545733	10.1.17.215	58958	10.1.17.2	53	DNS	95	Standard query 0x35d3 A win-gsh54qlw48d.bluemoo
11	2025-01-22 19:44:56.546173	10.1.17.2	53	10.1.17.215	58958	DNS	111	Standard query response 0x35d3 A win-gsh54qlw48d.bluemoo
12	2025-01-22 19:44:56.546421	10.1.17.215	50322	10.1.17.2	53	DNS	95	Standard query 0x2b27 SOA DESKTOP-L8C5GSJ.bluemoo
13	2025-01-22 19:44:56.546685	10.1.17.2	53	10.1.17.215	50322	DNS	174	Standard query response 0x2b27 SOA DESKTOP-L8C5GSJ.bluemoo
14	2025-01-22 19:44:56.546686	10.1.17.215	50323	10.1.17.2	389	CLDAP	275	searchRequest(62) "<R00T>" baseObject
15	2025-01-22 19:44:56.547155	10.1.17.2	389	10.1.17.215	50323	CLDAP	250	searchResEntry(62) "<R00T>" searchResDone(62) success [1 result]
16	2025-01-22 19:44:56.547663	10.1.17.215	58958	10.1.17.2	53	DNS	166	Dynamic update 0x4997 SOA bluemoo CNAME AAAA A A 10.1.17.215
17	2025-01-22 19:44:56.548911	10.1.17.2	53	10.1.17.215	58958	DNS	166	Dynamic update response 0x4997 SOA bluemoo CNAME AAAA A A 10.1.17.215
18	2025-01-22 19:44:56.576594	Intel_26:4a:74		Broadcast		ARP	60	Who has 10.1.17.215? (ARP Probe)
19	2025-01-22 19:44:56.609856	10.1.17.215	137	10.1.17.255	137	NBNS	110	Registration NB DESKTOP-L8C5GSJ<00>
20	2025-01-22 19:44:56.609856	10.1.17.215	137	10.1.17.255	137	NBNS	110	Registration NR DESKTOP-L8C5GSJ<20>

▶ Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits)
 ▶ Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
 ▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
 ▶ Dynamic Host Configuration Protocol (Discover)

```

0000  ff ff ff ff ff ff 00 d0  b7 26 4a 74 08 00 45 00  .....&Jt..E.
0010  01 4a 06 d7 00 00 80 11  32 cd 00 00 00 00 ff ff  ..J.....2.....
0020  ff ff 00 44 00 43 01 36  8f d4 01 01 06 00 91 28  ...D.C.6.....(
0030  7c 03 00 00 80 00 00 00  00 00 00 00 00 00 00 00  |.....
0040  00 00 00 00 00 00 00 d0  b7 26 4a 74 00 00 00 00  .....&Jt....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
  
```

Loading PCAP files through Wireshark

Wireshark - Protocol Hierarchy Statistics - 2025-01-22-traffic-analysis-exercise.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
QUIC IETF	1.1	450	1.1	296598	740	450	296598	740	450
Network Time Protocol	0.1	56	0.0	3264	8	56	3264	8	56
NetBIOS Name Service	0.2	82	0.0	5647	14	82	5647	14	82
NetBIOS Datagram Service	0.3	107	0.0	8774	21	0	0	0	107
SMB (Server Message Block Protocol)	0.3	107	0.0	11854	29	0	0	0	107
SMB MailSlot Protocol	0.3	107	0.0	2675	6	0	0	0	107
Microsoft Windows Browser Protocol	0.3	107	0.0	2652	6	107	2652	6	107
Multicast Domain Name System	0.1	25	0.0	1050	2	25	1050	2	25
Link-local Multicast Name Resolution	0.0	6	0.0	198	0	6	198	0	6
Dynamic Host Configuration Protocol	0.0	4	0.0	1279	3	4	1279	3	4
Domain Name System	3.8	1512	0.5	129133	322	1512	129133	322	1512
Connectionless Lightweight Directory Access Protocol	0.1	48	0.0	10620	26	48	10620	26	48
Transmission Control Protocol	93.2	36749	2.9	755044	1,886	27086	561760	1,403	36749
Transport Layer Security	17.2	6780	61.3	16006079	39 k	6780	14857636	37 k	6990
NetBIOS Session Service	0.8	302	0.3	82088	205	0	0	0	302
SMB2 (Server Message Block Protocol version 2)	0.8	296	0.3	79950	199	248	63074	157	318
SMB (Server Message Block Protocol)	0.0	6	0.0	930	2	6	930	2	6
Lightweight Directory Access Protocol	1.3	497	1.3	352244	879	497	272892	681	525
Kerberos	0.1	50	0.3	72829	181	50	72829	181	50
Hypertext Transfer Protocol	3.2	1253	1.2	304415	760	636	41635	104	1253
Media Type	0.0	5	0.4	98955	247	5	98955	247	5
Line-based text data	1.5	591	0.0	5535	13	591	5535	13	591
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	1.6	650	0.7	188407	470	189	85731	214	650
SAMR (pidl)	0.1	30	0.0	2268	5	30	2268	5	30
Microsoft Network Logon	0.0	11	0.0	3092	7	11	3092	7	11
Local Security Authority	0.1	24	0.0	2776	6	22	2408	6	24
Malformed Packet	0.0	2	0.0	0	0	2	0	0	2
DCE/RPC Endpoint Mapper	0.3	104	0.1	20272	50	104	20272	50	104
Active Directory Replication	0.7	292	0.1	37184	92	292	37184	92	292
Data	0.5	200	25.1	6569763	16 k	200	6569763	16 k	200
Internet Control Message Protocol	0.1	20	0.0	3301	8	20	3301	8	20
Address Resolution Protocol	0.9	340	0.0	9520	23	340	9520	23	340

No display filter.

Close Copy Protocols Help

The first thing I do is go through statistics > protocol hierarchy and see where the traffic is moving the most, and I see through TCP.

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Src.port	Destination	Dst.port	Protocol	Length	Info
4	2025-01-22 19:44:56.533016	10.1.17.2	67	255.255.255.255	68	DHCP	359	DHCP ACK - Transaction ID 0x91287c03
5	2025-01-22 19:44:56.544758	Intel_26:4a:74		Broadcast		ARP	60	Who has 10.1.17.2? Tell 10.1.17.215
6	2025-01-22 19:44:56.544759	Dell_7f:09:5d		Intel_26:4a:74		ARP	60	10.1.17.2 is at 00:24:e8:7f:09:5d
7	2025-01-22 19:44:56.544983	10.1.17.215	57386	10.1.17.2	53	DNS	131	Standard query 0xbab6 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumoonuesday.com
8	2025-01-22 19:44:56.545341	10.1.17.2	53	10.1.17.215	57386	DNS	202	Standard query response 0xbab6 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumoonuesday.com
9	2025-01-22 19:44:56.545732	10.1.17.215	56330	224.0.0.252	5355	LLMNR	75	Standard query 0xceec ANY DESKTOP-L8C5GSJ
10	2025-01-22 19:44:56.545733	10.1.17.215	58958	10.1.17.2	53	DNS	95	Standard query 0x35d3 A win-gsh54qlw48d.blumoonuesday.com
11	2025-01-22 19:44:56.546173	10.1.17.2	53	10.1.17.215	58958	DNS	111	Standard query response 0x35d3 A win-gsh54qlw48d.blumoonuesday.com A 10.1.17.2
12	2025-01-22 19:44:56.546421	10.1.17.215	50322	10.1.17.2	53	DNS	95	Standard query 0x2b27 SOA DESKTOP-L8C5GSJ.blumoonuesday.com
13	2025-01-22 19:44:56.546685	10.1.17.2	53	10.1.17.215	50322	DNS	174	Standard query response 0x2b27 SOA DESKTOP-L8C5GSJ.blumoonuesday.com SOA win-gsh54qlw48d.blumoonuesday.com
14	2025-01-22 19:44:56.546686	10.1.17.215	50323	10.1.17.2	389	CLDAP	275	searchRequest(62) "<R00T>" baseObject
15	2025-01-22 19:44:56.547155	10.1.17.2	389	10.1.17.215	50323	CLDAP	250	searchResEntry(62) "<R00T>" searchResDone(62) success [1 result]
16	2025-01-22 19:44:56.547663	10.1.17.215	58958	10.1.17.2	53	DNS	166	Dynamic update 0x4997 SOA blumoonuesday.com CNAME AAAA A A 10.1.17.215
17	2025-01-22 19:44:56.548911	10.1.17.2	53	10.1.17.215	58958	DNS	166	Dynamic update response 0x4997 SOA blumoonuesday.com CNAME AAAA A A 10.1.17.215
18	2025-01-22 19:44:56.576594	Intel_26:4a:74		Broadcast		ARP	60	Who has 10.1.17.215? (ARP Probe)
19	2025-01-22 19:44:56.609856	10.1.17.215	137	10.1.17.255	137	NBNS	110	Registration NB DESKTOP-L8C5GSJ<00>
20	2025-01-22 19:44:56.609856	10.1.17.215	137	10.1.17.255	137	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
21	2025-01-22 19:44:56.610033	10.1.17.215	137	10.1.17.255	137	NBNS	110	Registration NB BLUEMOONTUESDAY<00>
22	2025-01-22 19:44:56.656580	10.1.17.215	50322	10.1.17.2	53	DNS	131	Standard query 0x46de SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumoonuesday.com
23	2025-01-22 19:44:56.656842	10.1.17.2	53	10.1.17.215	50322	DNS	202	Standard query response 0x46de SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumoonuesday.com

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)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: Intel_26:4a:74 (00:d0:b7:26:4a:74)
 Sender IP address: 10.1.17.215
 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Target IP address: 10.1.17.2

```

0000  ff ff ff ff ff ff 00 d0  b7 26 4a 74 08 06 00 01  .....&Jt....
0010  08 00 06 04 00 01 00 d0  b7 26 4a 74 0a 01 11 d7  .....&Jt....
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  .....
  
```

Checking through the traffic, where I can see the broadcast requesting the 10.1.17.215, to tell who has 10.1.17.2. It says it resides at this so-and-so MAC address.

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name contains "auth"

No.	Time	Source	Src.port	Destination	Dst.port	Protocol	Length	Info
2321	2025-01-22 19:45:34.720717	10.1.17.215	61582	10.1.17.2	53	DNS	103	Standard query 0xcc42 A google-authenticator.burleson-appliance.net
2322	2025-01-22 19:45:34.720823	10.1.17.215	52497	10.1.17.2	53	DNS	103	Standard query 0xe4c2 HTTPS google-authenticator.burleson-appliance.net
2329	2025-01-22 19:45:34.780280	10.1.17.2	53	10.1.17.215	61582	DNS	215	Standard query response 0xcc42 A google-authenticator.burleson-appliance.net A 104.21.64.1 A 104.21
2330	2025-01-22 19:45:34.799976	10.1.17.2	53	10.1.17.215	52497	DNS	351	Standard query response 0xe4c2 HTTPS google-authenticator.burleson-appliance.net HTTPS
2364	2025-01-22 19:45:35.393278	10.1.17.215	59630	10.1.17.2	53	DNS	78	Standard query 0xbcc7 A authenticatoor.org
2365	2025-01-22 19:45:35.393286	10.1.17.215	59769	10.1.17.2	53	DNS	78	Standard query 0xe6f7 HTTPS authenticatoor.org
2375	2025-01-22 19:45:35.628118	10.1.17.2	53	10.1.17.215	59769	DNS	147	Standard query response 0xe6f7 HTTPS authenticatoor.org SOA siti.ns.orangewebsite.com
2376	2025-01-22 19:45:35.917991	10.1.17.2	53	10.1.17.215	59630	DNS	94	Standard query response 0xbcc7 A authenticatoor.org A 82.221.136.26

Frame 2321: 103 bytes on wire (824 bits), 103 bytes captured (824 bits)

Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Dell_7f:09:5d (00:24:e8:7f:09:5d)

Internet Protocol Version 4, Src: 10.1.17.215, Dst: 10.1.17.2

User Datagram Protocol, Src Port: 61582, Dst Port: 53

Domain Name System (query)

```

0000  00 24 e8 7f 09 5d 00 d0 b7 26 4a 74 08 00 45 00  .$. .] . . &Jt . E .
0010  00 59 b0 13 00 00 80 11 53 a6 0a 01 11 d7 0a 01  .Y . . . . S . . . . .
0020  11 02 f0 8e 00 35 00 45 dc c3 cc 42 01 00 00 01  . . . . 5 E . . B . . .
0030  00 00 00 00 00 00 14 67 6f 6f 67 6c 65 2d 61 75  . . . . . g oogle-au
0040  74 68 65 6e 74 69 63 61 74 6f 72 12 62 75 72 6c  thentica tor burl
0050  65 73 6f 6e 2d 61 70 70 6c 69 61 6e 63 65 03 6e  eson-app liance-n
0060  65 74 00 00 01 00 01  et . . . . .

```

As it says, fake Google Authenticator, I looked through the search as “dns.qry.name contains ‘auth’”, where it gave me a few packets as I can see the typo name as “authenticatoor.org” – flag 1

Where the source address or infected IP that accessed the fake auth is 10.1.17.215 – flag 2

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Src.port	Destination	Dst.port	Protocol	Length	Info
4	2025-01-22 19:44:56.533016	10.1.17.2	67	255.255.255.255	68	DHCP	359	DHCP ACK - Transaction ID 0x91287c03
5	2025-01-22 19:44:56.544758	Intel_26:4a:74		Broadcast		ARP	60	Who has 10.1.17.2? Tell 10.1.17.215
6	2025-01-22 19:44:56.544759	Dell_7f:09:5d		Intel_26:4a:74		ARP	60	10.1.17.2 is at 00:24:e8:7f:09:5d
7	2025-01-22 19:44:56.544983	10.1.17.215	57386	10.1.17.2	53	DNS	131	Standard query 0xbab6 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumoonuesday.com
8	2025-01-22 19:44:56.545341	10.1.17.2	53	10.1.17.215	57386	DNS	202	Standard query response 0xbab6 SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumoonuesday.com
9	2025-01-22 19:44:56.545732	10.1.17.215	56330	224.0.0.252	5355	LLMNR	75	Standard query 0xceec ANY DESKTOP-L8C5GSJ
10	2025-01-22 19:44:56.545733	10.1.17.215	58958	10.1.17.2	53	DNS	95	Standard query 0x35d3 A win-gsh54qlw48d.blumoonuesday.com
11	2025-01-22 19:44:56.546173	10.1.17.2	53	10.1.17.215	58958	DNS	111	Standard query response 0x35d3 A win-gsh54qlw48d.blumoonuesday.com A 10.1.17.2
12	2025-01-22 19:44:56.546421	10.1.17.215	50322	10.1.17.2	53	DNS	95	Standard query 0x2b27 SOA DESKTOP-L8C5GSJ.blumoonuesday.com
13	2025-01-22 19:44:56.546685	10.1.17.2	53	10.1.17.215	50322	DNS	174	Standard query response 0x2b27 SOA DESKTOP-L8C5GSJ.blumoonuesday.com SOA win-gsh54qlw48d.blumoonuesday.com
14	2025-01-22 19:44:56.546686	10.1.17.215	50323	10.1.17.2	389	CLDAP	275	searchRequest(62) "<R00T>" baseObject
15	2025-01-22 19:44:56.547155	10.1.17.2	389	10.1.17.215	50323	CLDAP	250	searchResEntry(62) "<R00T>" searchResDone(62) success [1 result]
16	2025-01-22 19:44:56.547663	10.1.17.215	58958	10.1.17.2	53	DNS	166	Dynamic update 0x4997 SOA blumoonuesday.com CNAME AAAA A 10.1.17.215
17	2025-01-22 19:44:56.548911	10.1.17.2	53	10.1.17.215	58958	DNS	166	Dynamic update response 0x4997 SOA blumoonuesday.com CNAME AAAA A 10.1.17.215
18	2025-01-22 19:44:56.576594	Intel_26:4a:74		Broadcast		ARP	60	Who has 10.1.17.215? (ARP Probe)
19	2025-01-22 19:44:56.609856	10.1.17.215	137	10.1.17.255	137	NBNS	110	Registration NB DESKTOP-L8C5GSJ<00>
20	2025-01-22 19:44:56.609856	10.1.17.215	137	10.1.17.255	137	NBNS	110	Registration NB DESKTOP-L8C5GSJ<20>
21	2025-01-22 19:44:56.610033	10.1.17.215	137	10.1.17.255	137	NBNS	110	Registration NB BLUEMOONTUESDAY<00>
22	2025-01-22 19:44:56.656580	10.1.17.215	50322	10.1.17.2	53	DNS	131	Standard query 0x46de SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumoonuesday.com
23	2025-01-22 19:44:56.656842	10.1.17.2	53	10.1.17.215	50322	DNS	202	Standard query response 0x46de SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.blumoonuesday.com

Frame 19: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)

Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a: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: 0xd632

Flags: 0x2910, Opcode: Registration, Recursion desired, Broadcast

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 1

Queries

- DESKTOP-L8C5GSJ<00>: type NB, class IN
 - Name: DESKTOP-L8C5GSJ<00> (Workstation/Redirector)
 - Type: NB (32)
 - Class: IN (1)

Additional records

- DESKTOP-L8C5GSJ<00>: type NB, class IN

```

0000  ff ff ff ff ff ff 00 d0 b7 26 4a 74 08 00 45 00  .....&Jt..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 7b c5 d6 32 29 10 00 01  .....L {...}...
0030  00 00 00 00 00 01 20 45 45 45 46 46 44 45 4c 46  .....E EEEFDELF
0040  45 45 50 46 41 43 4e 45 4d 44 49 45 44 44 46 45  EEPFACNE MDIEDDFE
0050  48 46 44 45 4b 41 41 00 00 20 00 01 c0 0c 00 20  HFDEKAA.....
0060  00 01 00 04 93 e0 00 06 40 00 0a 01 11 d7  .....@.....

```

2025-01-22-traffic-analysis-exercise.pcap Packets: 39427 Profile: Default

The source address that accessed a malicious website and its hostname are at NBNS > Queries > Desktop>Name

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

kerberos.CNameString

No.	Time	Source	Src.port	Destination	Dst.port	Protocol	Length	Response	Computer Name	Info
250	2025-01-22 19:45:10.898220	10.1.17.215	50091	10.1.17.2	88	KRB5	288			AS-REQ
258	2025-01-22 19:45:10.904859	10.1.17.215	50092	10.1.17.2	88	KRB5	368			AS-REQ
260	2025-01-22 19:45:10.906860	10.1.17.2	88	10.1.17.215	50092	KRB5	399			AS-REP
272	2025-01-22 19:45:10.910857	10.1.17.2	88	10.1.17.215	50093	KRB5	329			TGS-REP
296	2025-01-22 19:45:11.059591	10.1.17.2	88	10.1.17.215	50096	KRB5	461			TGS-REP
14710	2025-01-22 19:50:12.948990	10.1.17.2	88	10.1.17.215	50205	KRB5	435			TGS-REP
15464	2025-01-22 19:53:39.134453	10.1.17.2	88	10.1.17.215	50226	KRB5	435			TGS-REP
15476	2025-01-22 19:53:39.136671	10.1.17.2	88	10.1.17.215	50227	KRB5	285			TGS-REP
15709	2025-01-22 19:55:02.802262	10.1.17.215	49678	10.1.17.2	88	KRB5	301			AS-REQ
15717	2025-01-22 19:55:02.811544	10.1.17.215	49679	10.1.17.2	88	KRB5	381			AS-REQ
15719	2025-01-22 19:55:02.813591	10.1.17.2	88	10.1.17.215	49679	KRB5	445			AS-REP
15731	2025-01-22 19:55:02.819808	10.1.17.2	88	10.1.17.215	49680	KRB5	479			TGS-REP
16075	2025-01-22 19:55:10.644522	10.1.17.215	49699	10.1.17.2	88	KRB5	301			AS-REQ
16087	2025-01-22 19:55:10.653952	10.1.17.215	49700	10.1.17.2	88	KRB5	381			AS-REQ
16089	2025-01-22 19:55:10.656029	10.1.17.2	88	10.1.17.215	49700	KRB5	445			AS-REP
16101	2025-01-22 19:55:10.660903	10.1.17.2	88	10.1.17.215	49701	KRB5	479			TGS-REP
16137	2025-01-22 19:55:10.678526	10.1.17.2	88	10.1.17.215	49704	KRB5	453			TGS-REP
16894	2025-01-22 19:55:29.566699	10.1.17.215	49744	10.1.17.2	88	KRB5	296			AS-REQ
16902	2025-01-22 19:55:29.573368	10.1.17.215	49745	10.1.17.2	88	KRB5	376			AS-REQ
16904	2025-01-22 19:55:29.575418	10.1.17.2	88	10.1.17.215	49745	KRB5	399			AS-REP

Record Mark: 230 bytes
 0... .. = Reserved: Not set
 .000 0000 0000 0000 0000 1110 0110 = Record Length: 230

as-req
 pvno: 5
 msg-type: krb-as-req (10)
 padata: 1 item
 PA-DATA pA-PAC-REQUEST
 req-body
 Padding: 0
 kdc-options: 40810010
 cname
 name-type: kRB5-NT-PRINCIPAL (1)
 cname-string: 1 item
CNameString: shutchenson
 realm: BLUEMOONTUESDAY
 sname
 name-type: kRB5-NT-SRV-INST (2)
 sname-string: 2 items
 SNameString: krbtgt
 SNameString: BLUEMOONTUESDAY

```

0000 00 24 e8 7f 09 5d 00 d0 b7 26 4a 74 08 00 45 00 .$. .] . .&Jt .E.
0010 01 12 af 85 40 00 80 06 13 86 0a 01 11 d7 0a 01 . . .@ . . .
0020 11 02 c3 ab 00 58 98 52 f6 34 2f 5c e1 6f 50 18 . . .X-R -4/\ .oP.
0030 00 ff e6 f2 00 00 00 00 00 e6 6a 81 e3 30 81 e0 . . . . .j . .0 .
0040 a1 03 02 01 05 a2 03 02 01 0a a3 15 30 13 30 11 . . . . .0 .0 .
0050 a1 04 02 02 00 80 a2 09 04 07 30 05 a0 03 01 01 . . . . .0 . . .
0060 ff a4 81 bc 30 81 b9 a0 07 03 05 00 40 81 00 10 . . .0 . . .@ .
0070 a1 18 30 16 a0 03 02 01 01 a1 0f 30 0d 1b 0b 73 . .0 . . . .0 . .s
0080 68 75 74 63 68 65 6e 73 6f 6e a2 11 1b 0f 42 4c hutchens on . . .BL
0090 55 45 4d 4f 4f 4e 54 55 45 53 44 41 59 a3 24 30 UEMOONTU ESDAY $0
00a0 22 a0 03 02 01 02 a1 1b 30 19 1b 06 6b 72 62 74 " . . . . .0 . .krbt
00b0 67 74 1b 0f 42 4c 55 45 4d 4f 4f 4e 54 55 45 53 gt . .BLUE MOONTUES
00c0 44 41 59 a5 11 18 0f 32 31 30 30 30 39 31 33 30 DAY . . .2 10009130
00d0 32 34 38 30 35 5a a6 11 18 0f 32 31 30 30 30 39 24805Z . . .210009
00e0 31 33 30 32 34 38 30 35 5a a7 06 02 04 33 40 cc 13024805 Z . . .30 .
00f0 26 a8 0e 30 0c 02 01 12 02 01 11 02 01 17 02 01 & . .0 . . . . .
0100 a9 1d 30 1b 30 19 a0 03 02 01 14 a1 12 04 10 . .0 .0 . . . . .
0110 44 45 53 4b 54 4f 50 2d 4c 38 43 35 47 53 4a 20 DESKTOP- L8C5GSJ
  
```

As I searched through the traffic to find the username, I used “kerberos.CNameString”
 It resides at the src.ip = 10.1.17.215.

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

No.	Time	Source	Src.port	Destination	Dst.port	Protocol	Length	Info
5073	2025-01-22 19:45:58.896228	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7279	2025-01-22 19:46:04.132272	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7602	2025-01-22 19:46:09.308509	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7688	2025-01-22 19:46:14.480958	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7696	2025-01-22 19:46:19.680655	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7841	2025-01-22 19:46:24.872711	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7864	2025-01-22 19:46:30.063748	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7878	2025-01-22 19:46:35.254490	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7888	2025-01-22 19:46:40.444370	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7907	2025-01-22 19:46:45.634791	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7972	2025-01-22 19:46:50.831495	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7979	2025-01-22 19:46:56.083008	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
7996	2025-01-22 19:47:01.270466	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
13693	2025-01-22 19:47:11.031933	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
14075	2025-01-22 19:47:16.221411	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
14172	2025-01-22 19:47:21.408851	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
14191	2025-01-22 19:47:26.573894	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
14228	2025-01-22 19:47:31.774577	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
14278	2025-01-22 19:47:36.951674	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
14281	2025-01-22 19:47:42.152974	10.1.17.215	50144	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1

▶ Frame 5073: 103 bytes on wire (824 bits), 103 bytes captured (824 bits)
 ▶ Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Cisco_c2:3a:46 (08:d0:9f: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: 91, Ack: 1862, Len: 49
 ▶ Hypertext Transfer Protocol

```

0000  08 d0 9f c2 3a 46 00 d0  b7 26 4a 74 08
0010  00 59 20 ed 40 00 80 06  1d ed 0a 01 11
0020  99 f1 c3 e0 00 50 db f2  be 1c de 29 d3
0030  00 ff 8f b9 00 00 47 45  54 20 2f 31 35
0040  39 36 39 33 37 20 48 54  54 50 2f 31 2e
0050  48 6f 73 74 3a 20 35 2e  32 35 32 2e 31
0060  32 34 31 0d 0a 0d 0a
  
```

To find the C2 beaconing, first, I used the “http.request” and found the first C2 server.

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 10.1.17.215 and ip.dst != 10.1.17.0/24

No.	Time	Source	Src.port	Destination	Dst.port	Protocol	Length	Info
37268	2025-01-22 20:28:23.402117	10.1.17.215	49950	45.125.66.32	2917	TLSv1.2	234	Application Data
37266	2025-01-22 20:28:23.186717	10.1.17.215	49950	45.125.66.32	2917	TLSv1.2	83	Application Data
37264	2025-01-22 20:28:22.997069	10.1.17.215	49950	45.125.66.32	2917	TLSv1.2	645	Application Data
37262	2025-01-22 20:28:22.802617	10.1.17.215	49950	45.125.66.32	2917	TLSv1.2	240	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
37261	2025-01-22 20:28:22.787721	10.1.17.215	49950	45.125.66.32	2917	TCP	60	49950 → 2917 [ACK] Seq=224 Ack=1445 Win=65280 Len=0
37257	2025-01-22 20:28:22.602141	10.1.17.215	49950	45.125.66.32	2917	TLSv1.2	277	Client Hello (SNI=45.125.66.32)
37256	2025-01-22 20:28:22.601935	10.1.17.215	49950	45.125.66.32	2917	TCP	60	49950 → 2917 [ACK] Seq=1 Ack=1 Win=65280 Len=0
37254	2025-01-22 20:28:22.431481	10.1.17.215	49950	45.125.66.32	2917	TCP	66	49950 → 2917 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
37253	2025-01-22 20:28:21.010296	10.1.17.215	49689	5.252.153.241	80	TCP	60	49689 → 80 [ACK] Seq=19103 Ack=1169117 Win=523776 Len=0
37250	2025-01-22 20:28:20.667534	10.1.17.215	49689	5.252.153.241	80	HTTP	103	GET /1517096937 HTTP/1.1
37243	2025-01-22 20:28:18.673171	10.1.17.215	49910	45.125.66.252	443	TLSv1.2	81	Application Data
37239	2025-01-22 20:28:17.416544	10.1.17.215	49949	45.125.66.32	2917	TCP	60	49949 → 2917 [FIN, ACK] Seq=118082 Ack=3186 Win=65280 Len=0
37238	2025-01-22 20:28:17.416544	10.1.17.215	49949	45.125.66.32	2917	TLSv1.2	77	Encrypted Alert
37237	2025-01-22 20:28:17.416362	10.1.17.215	49949	45.125.66.32	2917	TCP	60	49949 → 2917 [ACK] Seq=118059 Ack=3186 Win=65280 Len=0
37232	2025-01-22 20:28:17.240949	10.1.17.215	49949	45.125.66.32	2917	TLSv1.2	157	Application Data
37230	2025-01-22 20:28:17.027867	10.1.17.215	49949	45.125.66.32	2917	TLSv1.2	81	Application Data
37229	2025-01-22 20:28:16.066541	10.1.17.215	49949	45.125.66.32	2917	TCP	60	49949 → 2917 [ACK] Seq=117929 Ack=3077 Win=65280 Len=0
37182	2025-01-22 20:28:15.823371	10.1.17.215	49949	45.125.66.32	2917	TLSv1.2	1060	Application Data, Application Data
37181	2025-01-22 20:28:15.823243	10.1.17.215	49949	45.125.66.32	2917	TLSv1.2	1394	Application Data
37180	2025-01-22 20:28:15.823240	10.1.17.215	49949	45.125.66.32	2917	TLSv1.2	1394	Application Data, Application Data

▶ Frame 37751: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
 ▶ Ethernet II, Src: Intel_26:4a:74 (08:d0:b7:26:4a:74), Dst: Cisco_c2:3a:46 (08:d0:9f:c2:3a:46)
 ▶ Internet Protocol Version 4, Src: 10.1.17.215, Dst: 45.125.66.252
 ▶ Transmission Control Protocol, Src Port: 49951, Dst Port: 443, Seq: 1, Ack: 1, Len: 202
 ▶ Transport Layer Security

```

0000  08 d0 9f c2 3a 46 00 d0 b7 26 4a 74 08 00 45 00  ....F...&Jt..E.
0010  00 f2 16 7b 40 00 80 06 57 3a 0a 01 11 d7 2d 7d  ...{@...W:....}
0020  42 fc c3 1f 01 bb 36 c1 f9 fd c6 66 cb b4 50 18  B.....6...f..P
0030  00 ff 79 93 00 00 16 03 03 00 c5 01 00 00 c1 03  ..y.....
0040  03 67 91 54 e8 b8 21 7a 21 c9 e6 7d 5f 75 ed 8a  .g.T...!z!...}_u
0050  1b dd 21 e9 48 b8 ae 2d 00 47 1e c3 c8 8b c1 cc  ..!..H...G....
0060  14 00 00 50 cc a8 cc a9 cc aa c0 2c c0 30 00 9f  ...P.....,..0..
0070  c0 24 c0 28 00 6b c0 0a c0 14 00 39 c0 2b c0 2f  .$. (..k...9+./
0080  00 9e c0 23 c0 27 00 67 c0 09 c0 13 00 33 00 9d  ...#..g.....3..
0090  00 3d 00 35 c0 32 c0 2a c0 0f c0 2e c0 26 c0 05  ..=5.2.*....&..
00a0  00 9c 00 3c 00 2f c0 31 c0 29 c0 0e c0 2d c0 25  ...<./..1..)-%
00b0  c0 04 00 ff 01 00 00 48 00 0d 00 16 00 14 06 03  .....H.....
00c0  06 01 05 03 05 01 04 03 04 01 03 03 03 01 02 03  .....
00d0  02 01 00 0a 00 18 00 16 00 19 00 1c 00 18 00 1b  .....
00e0  00 17 00 16 00 1a 00 15 00 14 00 13 00 12 00 0b  .....
00f0  00 02 01 00 00 16 00 00 00 17 00 00 00 23 00 00  ....#.
  
```

After applying another search request where the traffic is leaving the source IP found multiple entries. These external IPs were involved in callback traffic post-infection, handling command and control communications.