EXPERIMENT-03

Aim :- Wireshark Malware Traffic Analysis

1. Initial Setup

□ Load the PCAP file in Wireshark.

□ Go to: Statistics > Protocol Hierarchy – see what protocols are used.

□ Statistics > Conversations – inspect endpoints and how much data was transferred.

2. Suspicious DNS Lookups

Malware often uses strange domains or DGAs.

Use this filter:

```
DNS
```

Look for:

□ Random-looking domain names (e.g., x12f32asd.biz)

Tip: Right-click a domain > “Apply as Filter” > “Selected” to track that domain across the capture.

3. Look for Beaconing Behavior (C2)

```
ip.addr == <suspect IP>
```

Or:

```
tcp.stream eq <n>
```

Check “Statistics > IO Graphs”:

□ Plot packets per second/minute.

□ Repetitive traffic every X seconds = possible beaconing.

4. Detect Suspicious HTTP Activity

```
http.request
```

Look for:

- POST or PUT methods to unknown or external IPs.
- Suspicious User-Agent strings like curl, python, etc.
- Base64-encoded.

Example filter for POST:

```
http.request.method == "POST"
```

5. Track Large Outbound Transfers

```
frame.len > 1000 && ip.dst != <internal IP range>
```

```
ip.dst != 192.168.0.0/16 && ip.dst != 10.0.0.0/8
```

6. Inspect TCP Streams

Right-click a suspicious packet

Choose: “Follow > TCP Stream”

Inspect contents of communication (look for commands, encoded data, etc.)

7. SSL/TLS Inspection (if possible)

```
ssl.handshake
```

Look for:

□ Unusual SNI fields (domain names in TLS handshake)

□ Suspicious self-signed certificates

□ No Server Name Indication (possible obfuscation)

8. Check for Exfiltration via ICMP, FTP, SMTP, etc.

Some malware uses strange protocols for data exfiltration:

```
ftp
```

Icmp

smtp

Look for payloads in ICMP (shouldn't have much normally), or large amounts of outbound data in FTP or SMTP.

Step-by-Step in Wireshark

Step 1: Open the .pcap File

□ Launch Wireshark

□ Open your .pcap file (File > Open)

Step 2: Go to TCP Conversations

1. Click on Statistics in the top menu bar

2 Select Conversations

. A new window opens — go to the TCP tab

3 You'll see a table with source/destination IPs, number of packets, bytes, etc.

Step 3: Look for Suspicious Traffic

□ Sort by “Packets” or “Bytes”

□ Look for:

o A single external IP communicating very frequently

o Unusual IP addresses (not in your local network)

o Communication with consistent packet sizes or intervals

■Step 4: Use “Follow TCP Stream”

1. Pick one suspicious connection (row)

2 Click to highlight that row

. Now, look at the bottom left of the Conversations window — click “Follow Stream”

3 ıThis button only appears after selecting a row.

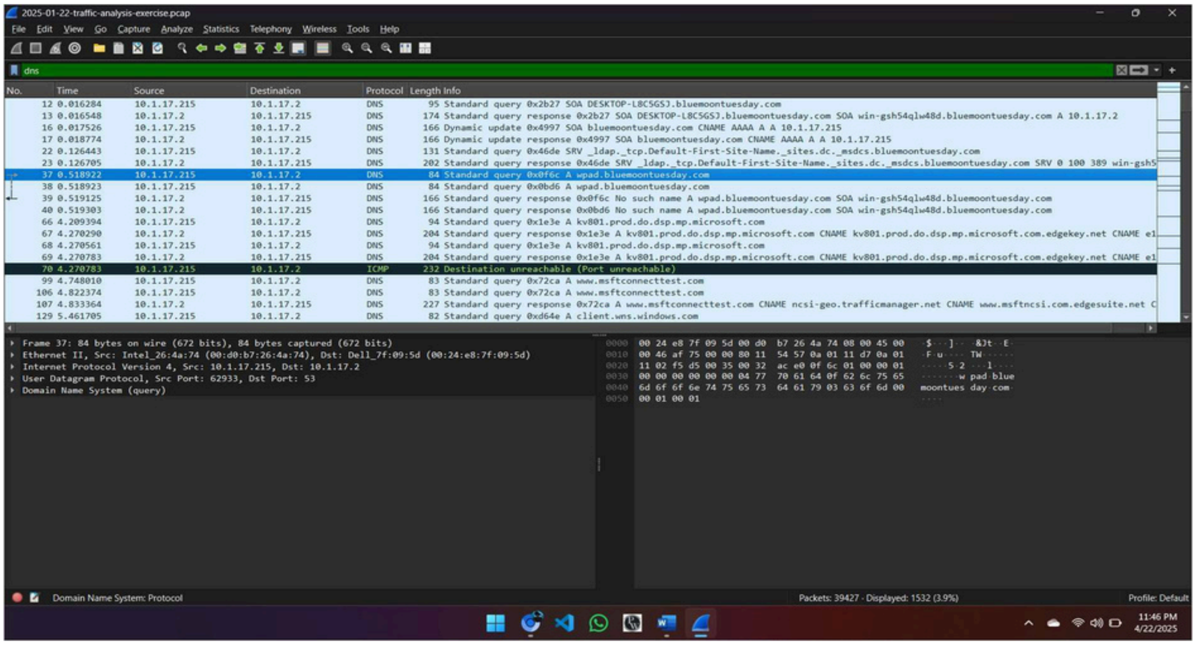
4. A new window will pop up showing the entire conversation (request + response) between the two hosts.

Step 5: Analyze the TCP Stream

□ Suspicious POST requests (sending data out)

□ Weird or obfuscated content (e.g., base64 blobs, binary data)

□ Repeated messages or heartbeats (beaconing behavior)



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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Display filter: dns

```
No.  Time      Source        Destination   Protocol Length Info
  12 0.016284  10.1.17.215   10.1.17.2     DNS       95 Standard query 0x2b27 SOA DESKTOP-L8C5GSJ.bluemoontuesday.com
  13 0.016548  10.1.17.2     10.1.17.215   DNS      174 Standard query response 0x2b27 SOA DESKTOP-L8C5GSJ.bluemoontuesday.com SOA win-gsh54qlw48d.bluemoontuesday.com A 10.1.17.2
  16 0.017526  10.1.17.215   10.1.17.2     DNS      166 Dynamic update 0x4997 SOA bluemoontuesday.com CNAME AAAA A A 10.1.17.215
  17 0.018774  10.1.17.2     10.1.17.215   DNS      166 Dynamic update response 0x4997 SOA bluemoontuesday.com CNAME AAAA A A 10.1.17.215
  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.bluemoontuesday.com
  23 0.126705  10.1.17.2     10.1.17.215   DNS      202 Standard query response 0x46de SRV _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.bluemoontuesday.com SRV 0 100 389 win-gsh5
  37 0.518922  10.1.17.215   10.1.17.2     DNS       84 Standard query 0x0f6c A wpad.bluemoontuesday.com
  38 0.518923  10.1.17.215   10.1.17.2     DNS       84 Standard query 0x0bd6 A wpad.bluemoontuesday.com
  39 0.519125  10.1.17.2     10.1.17.215   DNS      166 Standard query response 0x0f6c No such name A wpad.bluemoontuesday.com SOA win-gsh54qlw48d.bluemoontuesday.com
  40 0.519303  10.1.17.2     10.1.17.215   DNS      166 Standard query response 0x0bd6 No such name A wpad.bluemoontuesday.com SOA win-gsh54qlw48d.bluemoontuesday.com
  66 4.209394  10.1.17.215   10.1.17.2     DNS       94 Standard query 0x1e3e A kv801.prod.do.dsp.mp.microsoft.com
  67 4.270290  10.1.17.2     10.1.17.215   DNS      204 Standard query response 0x1e3e A kv801.prod.do.dsp.mp.microsoft.com CNAME kv801.prod.do.dsp.mp.microsoft.com.edgekey.net CNAME e1
  68 4.270561  10.1.17.215   10.1.17.2     DNS       94 Standard query 0x1e3e A kv801.prod.do.dsp.mp.microsoft.com
  69 4.270783  10.1.17.2     10.1.17.215   DNS      204 Standard query response 0x1e3e A kv801.prod.do.dsp.mp.microsoft.com CNAME kv801.prod.do.dsp.mp.microsoft.com.edgekey.net CNAME e1
  70 4.270783  10.1.17.215   10.1.17.2     ICMP     232 Destination unreachable (Port unreachable)
  99 4.748010  10.1.17.215   10.1.17.2     DNS       83 Standard query 0x72ca A www.msftconnecttest.com
 106 4.822374  10.1.17.215   10.1.17.2     DNS       83 Standard query 0x72ca A www.msftconnecttest.com
 107 4.833364  10.1.17.2     10.1.17.215   DNS      227 Standard query response 0x72ca A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net C
 129 5.461705  10.1.17.215   10.1.17.2     DNS       82 Standard query 0xd64e A client.wns.windows.com
```

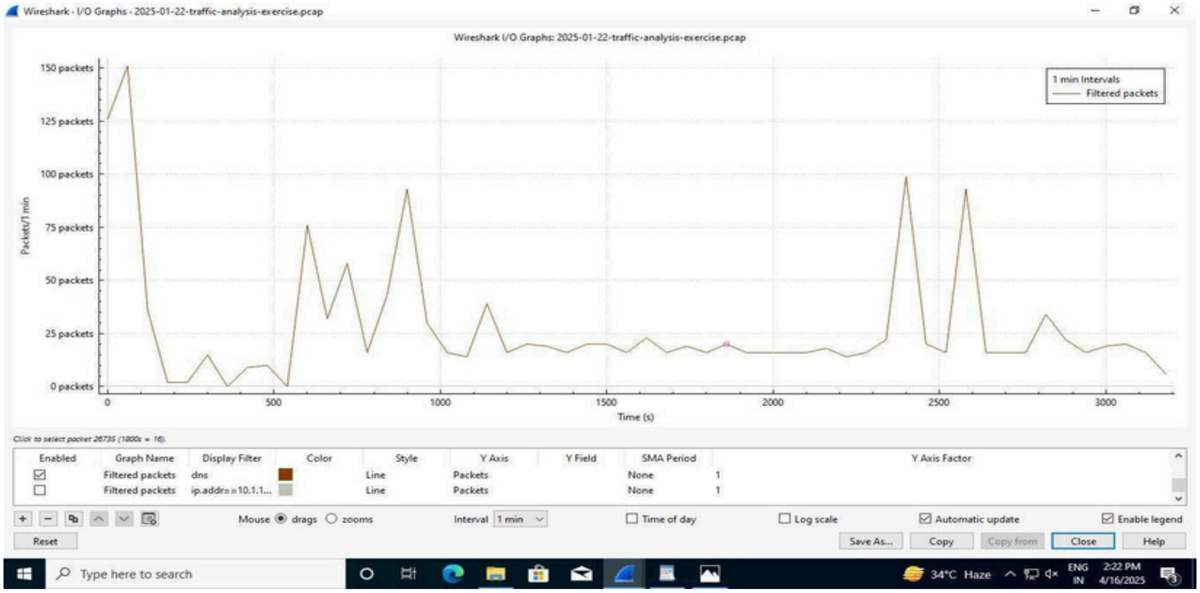
```
▸ Frame 37: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
▸ Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Dell_7f:09:5d (00:24:e8:7f:09:5d)
▸ Internet Protocol Version 4, Src: 10.1.17.215, Dst: 10.1.17.2
▸ User Datagram Protocol, Src Port: 62933, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  00 24 e8 7f 09 5d 00 d0  b7 26 4a 74 08 00 45 00   ·$···]·· ·&Jt··E·
0010  00 46 af 75 00 00 80 11  54 57 0a 01 11 d7 0a 01   ·F·u···· TW······
0020  11 02 f5 d5 00 35 00 32  ac e0 0f 6c 01 00 00 01   ·····5·2 ···l····
0030  00 00 00 00 00 00 04 77  70 61 64 0f 62 6c 75 65   ·······w pad·blue
0040  6d 6f 6f 6e 74 75 65 73  64 61 79 03 63 6f 6d 00   moontues day·com·
0050  00 01 00 01                                        ····
```

Domain Name System: Protocol

Packets: 39427 · Displayed: 1532 (3.9%)

Profile: Default



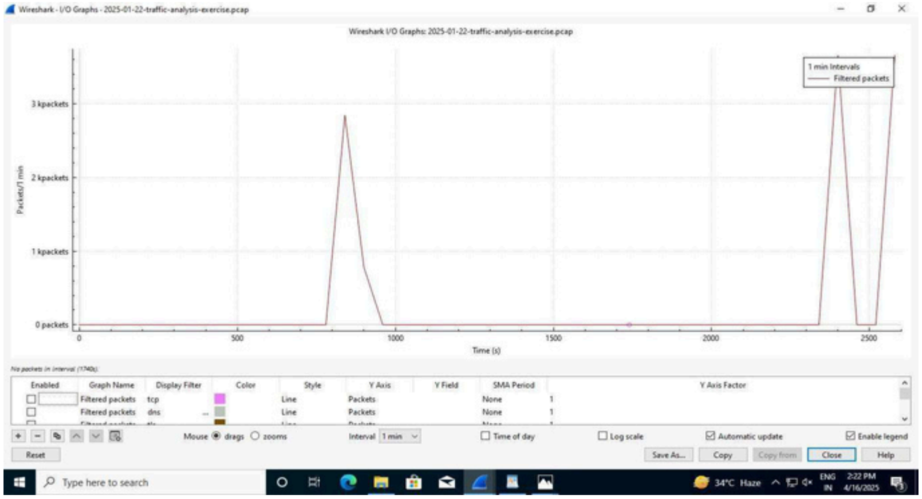
Wireshark · I/O Graphs · 2025-01-22-traffic-analysis-exercise.pcap

Wireshark I/O Graphs: 2025-01-22-traffic-analysis-exercise.pcap

Click to select packet 26735 (1800s = 16).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	Filtered packets	dns	🟫	Line	Packets		None	1
☐	Filtered packets	ip.addr==10.1.1...	⬜	Line	Packets		None	1

Mouse ● drags ○ zooms Interval 1 min ☐ Time of day ☐ Log scale ☑ Automatic update ☑ Enable legend



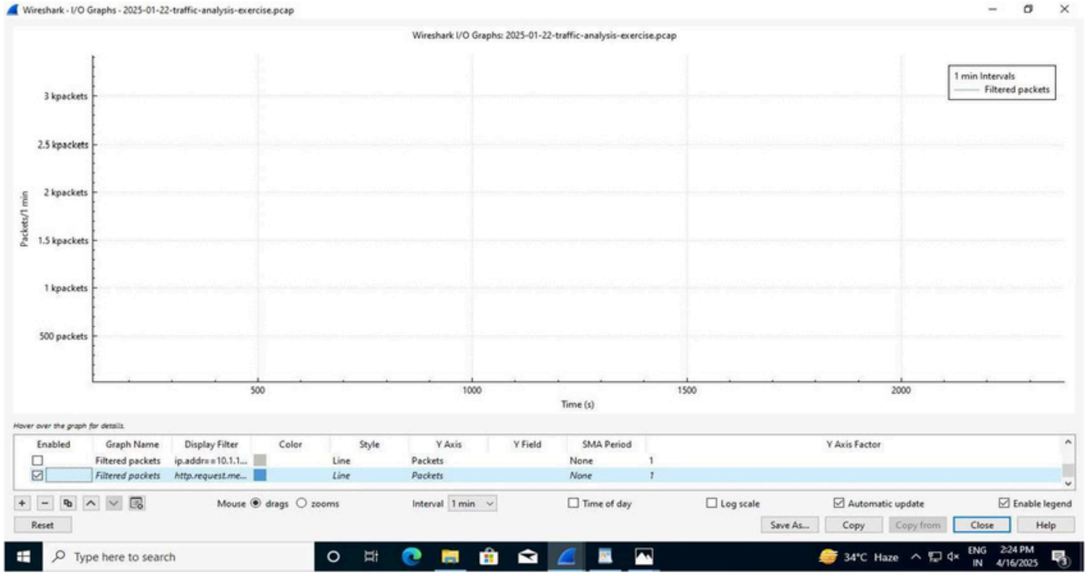
Wireshark · I/O Graphs · 2025-01-22-traffic-analysis-exercise.pcap

Wireshark I/O Graphs: 2025-01-22-traffic-analysis-exercise.pcap

No packets in interval (1740s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☐	Filtered packets	tcp	🟪	Line	Packets		None	1
☐	Filtered packets	dns	⬜	Line	Packets		None	1

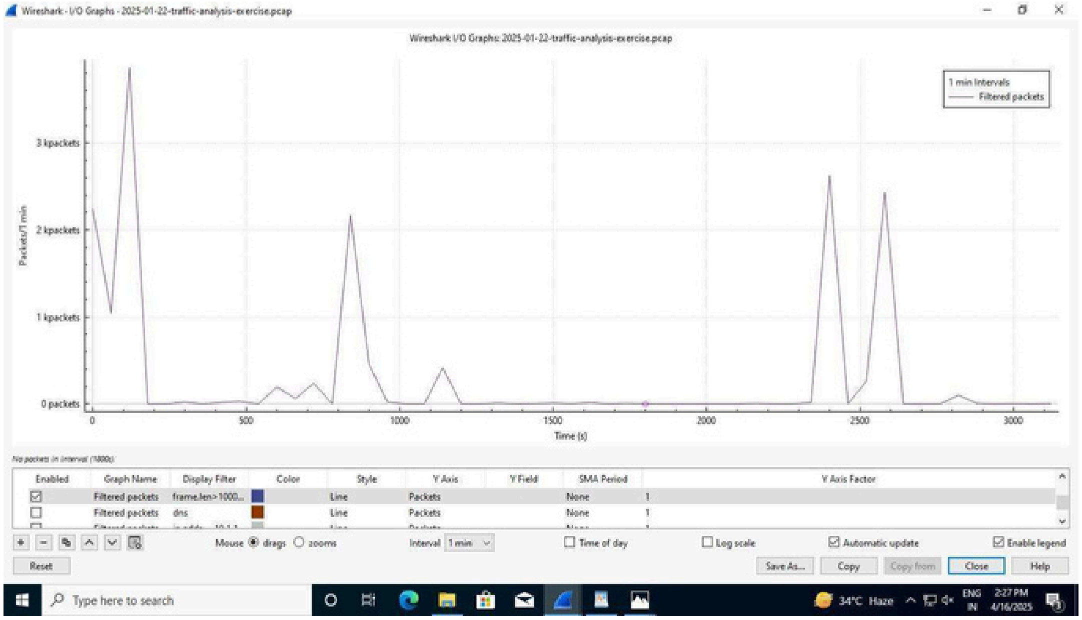
Mouse ● drags ○ zooms Interval 1 min ☐ Time of day ☐ Log scale ☑ Automatic update ☑ Enable legend



Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
□	Filtered packets	ip.addr==10.1.1...		Line	Packets		None	1
☑	*Filtered packets*	*http.request.me...*		*Line*	*Packets*		*None*	*1*

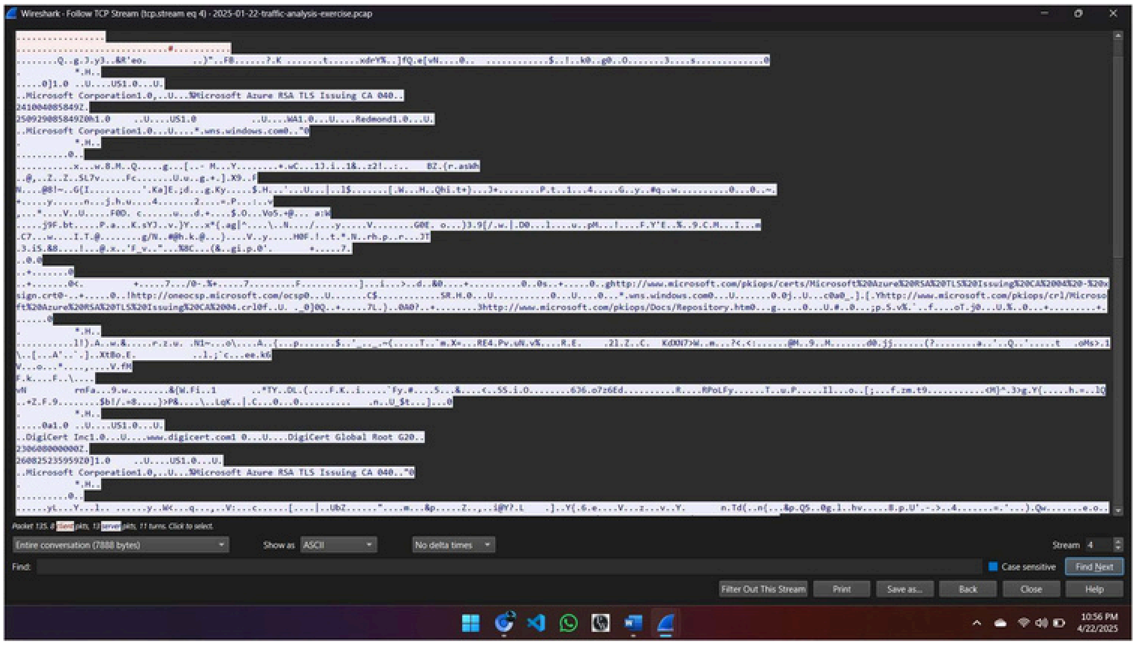
Mouse ● drags ○ zooms Interval 1 min □ Time of day □ Log scale ☑ Automatic update ☑ Enable legend



No packets in interval (1800s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	Filtered packets	frame.len>1000...		Line	Packets		None	1
□	Filtered packets	dns		Line	Packets		None	1

Mouse ● drags ○ zooms Interval 1 min □ Time of day □ Log scale ☑ Automatic update ☑ Enable legend

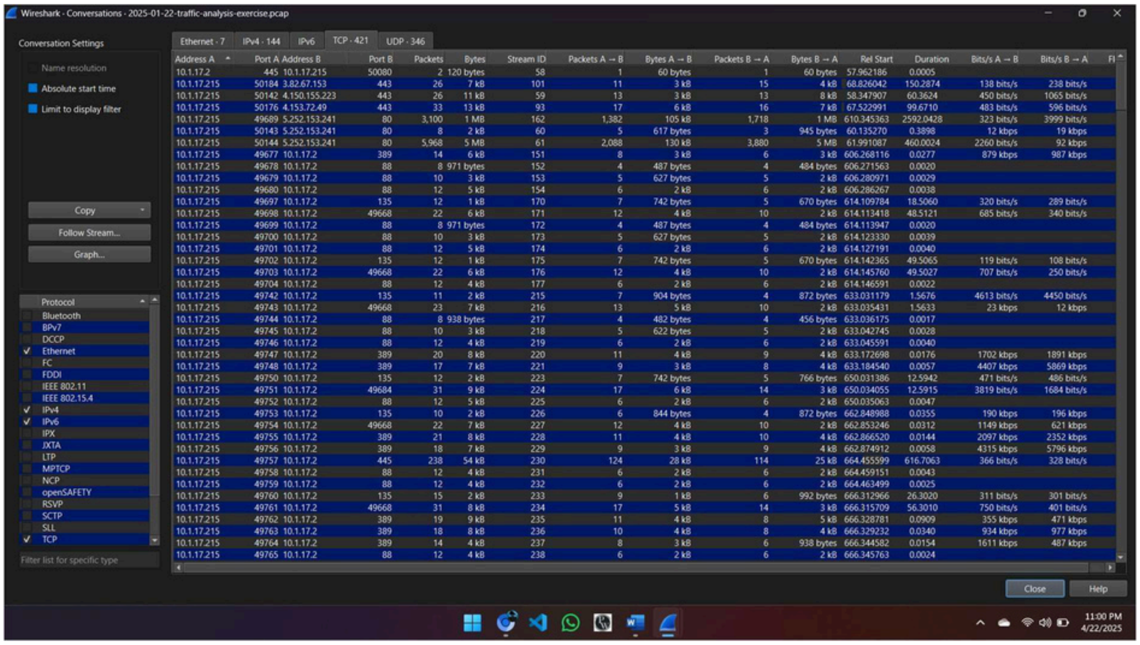

Wireshark · Follow TCP Stream (tcp.stream eq 4) · 2025-01-22-traffic-analysis-exercise.pcap
Filter Out This Stream
Print
Save as...
Back
Close
Help
Find Next
10:56 PM 4/22/2025

```
.................
..............................#...........
........Q..g.J.y3..&R'eo.        ..)"..F0......?.K .......t......xdrY%..]fQ.e[vN....0..  .............$..!..k0..g0..0.......3....s.............0
.           *.H..
.....0]1.0 ..U....US1.0...U.
..Microsoft Corporation1.0,..U...%Microsoft Azure RSA TLS Issuing CA 040..
241004085849Z.
250929085849Z0h1.0    ..U....US1.0          ..U....WA1.0...U....Redmond1.0...U.
..Microsoft Corporation1.0...U....*.wns.windows.com0.."0
.           *.H..
..........0..
...........x...w.8.M..Q.....g...[..- M...Y........+.wC...1J.i..1&..z2!..:..   BZ.{r.asWh
..@,..Z..Z..SL7v.....Fc.......U.u..g.+.].X9..F
N....@8!~..G[I..........'.Ka]E.;d...g.Ky.....$.H...'...U...|..1$.......[.W...H..Qhi.t+}...J+........P.t..1...4.....G..y..#q..w..........0...0..~.
+.....y......n...j.h.u....4.......2....=.P...!..v
,...*....V..U.....F0D. c.......u...d.+....$.O...Vo5.+@... a:W
.....j9F.bt.....P.a...K.sYJ..v.}Y...x*{.ag|^....\..N..../....y.....V........G0E. o...}3.9[/.w.|.D0...1....u..pM...!....F.Y'E..%..9.C.M...I...m
.C7...w....I.T.@........g/N..#@h.k.@...}....V..y.....H0F.!..t.*.N..rh.p..r...JT
.3.i5.&8....!...@.x..'F_v.."...%8C...(&..gi.p.0'.       +.....7.
..0.0
..+.......0
..+.......0<.        +.....7.../0-.%+.....7.........F...........]...i...>..d..&0....+..........0..0s..+.....0..ghttp://www.microsoft.com/pkiops/certs/Microsoft%20Azure%20RSA%20TLS%20Issuing%20CA%2004%20-%20x
sign.crt0-..+.....0..!http://oneocsp.microsoft.com/ocsp0...U.......C$...........SR.H.0...U..........0...U....0...*.wns.windows.com0...U.......0.0j..U...c0a0_.].[.Yhttp://www.microsoft.com/pkiops/crl/Microso
ft%20Azure%20RSA%20TLS%20Issuing%20CA%2004.crl0f..U. ._0]0Q..+.....7L.}..0A0?..+........3http://www.microsoft.com/pkiops/Docs/Repository.htm0...g.....0...U.#..0...;p.5.v%.'..f....oT.j0...U.%..0...+.........+.
......0
.           *.H..
...........1!}.A..w.&.....r.z.u. .N1~...o\....A..{...p.......$..'_.._.~(.....T..`m.X=...RE4.Pv.uN.v%....R.E.     .2l.Z..C.  KdXN7>W..m...?<.<:......@M..9..M.......d0.jj......(?........a..'..Q..'.....t   .oMs>.1
\..[...A'..`.]..XtBo.E.           ..1.;`c...ee.k6
V...o...*....,....V.fM
F.k....F..\....
vN          rnFa...9.w........&[W.Fi..1        ..*TY..DL.{....F.K..i.....`Fy.#....5...&....<..5S.i.O.........636.o7z6Ed..........R....RPoLFy......T..u.P.....I1...o..[;...f.zm.t9...........<M]^.3>g.Y{.....h.=..1Q
..+Z.F.9........$b!/.=8....}>P&....\..LqK..|.C...0...0..........  .n..U_$t...]...0
.           *.H..
.....0a1.0 ..U....US1.0...U.
..DigiCert Inc1.0...U....www.digicert.com1 0...U....DigiCert Global Root G20..
230608000000Z.
260825235959Z0]1.0    ..U....US1.0...U.
..Microsoft Corporation1.0,..U...%Microsoft Azure RSA TLS Issuing CA 040.."0
.           *.H..
..........0..
......yL...Y...1.. ......y..W<...q...,..V:...c......[....|..UbZ......"....m...&p.....Z..,..i@Y?.L    .]..Y{.6.e....V...z...v..Y.      n.Td(..n{...&p.Q5..0g.1..hv.....8.p.U'.-.>..4.......=.'...).Qw.......e.o..
```

Packet 135. 8 client pkts, 13 server pkts, 11 turns. Click to select.

Entire conversation (7888 bytes) Show as ASCII No delta times Stream 4

Find: ■ Case sensitive



Wireshark · Conversations · 2025-01-22-traffic-analysis-exercise.pcap

Conversation Settings

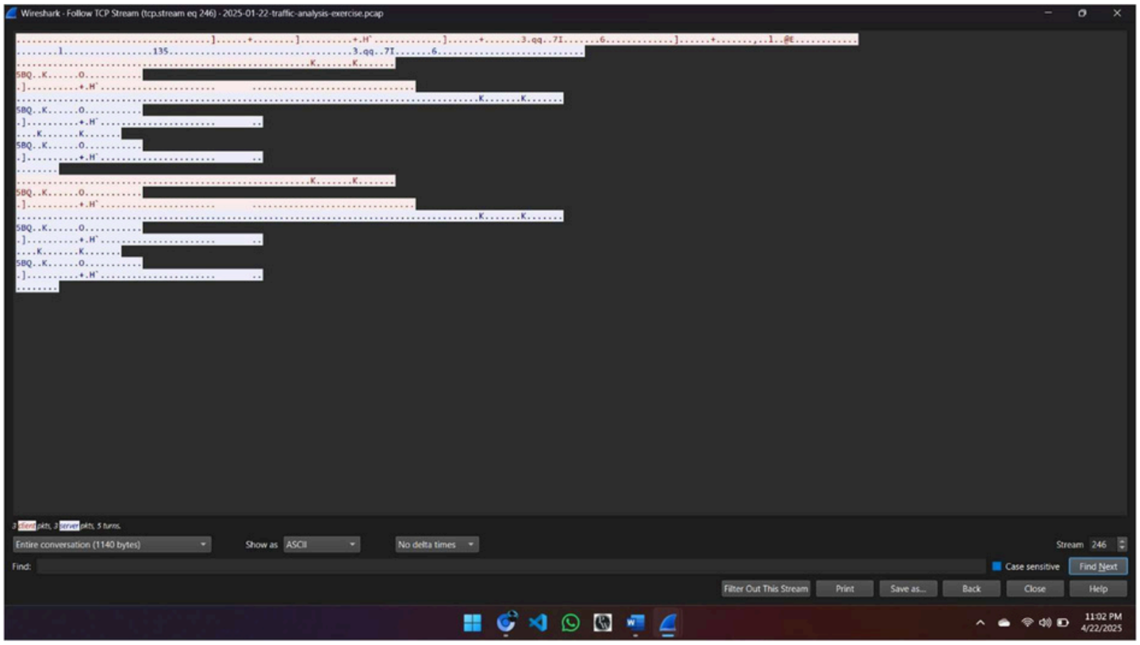
- Name resolution
- ☑ Absolute start time
- ☑ Limit to display filter

Protocol

- Bluetooth
- BPv7
- DCCP
- ☑ Ethernet
- FC
- FDDI
- IEEE 802.11
- IEEE 802.15.4
- ☑ IPv4
- ☑ IPv6
- IPX
- JXTA
- LTP
- MPTCP
- NCP
- openSAFETY
- RSVP
- SCTP
- SLL
- ☑ TCP

Ethernet · 7 | IPv4 · 144 | IPv6 | TCP · 421 | UDP · 346

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	Fl
10.1.17.2	445	10.1.17.215	50080	2	120 bytes	58	1	60 bytes	1	60 bytes	57.962186	0.0005			
10.1.17.215	50184	3.82.67.153	443	26	7 kB	101	11	3 kB	15	4 kB	68.826042	150.2874	138 bits/s	238 bits/s	
10.1.17.215	50142	4.150.155.223	443	26	11 kB	59	13	3 kB	13	8 kB	58.347907	60.3624	450 bits/s	1065 bits/s	
10.1.17.215	50176	4.153.72.49	443	33	13 kB	93	17	6 kB	16	7 kB	67.522991	99.6710	483 bits/s	596 bits/s	
10.1.17.215	49689	5.252.153.241	80	3,100	1 MB	162	1,382	105 kB	1,718	1 MB	610.345363	2592.0428	323 bits/s	3999 bits/s	
10.1.17.215	50143	5.252.153.241	80	8	2 kB	60	5	617 bytes	3	945 bytes	60.135270	0.3898	12 kbps	19 kbps	
10.1.17.215	50144	5.252.153.241	80	5,968	5 MB	61	2,088	130 kB	3,880	5 MB	61.991087	460.0024	2260 bits/s	92 kbps	
10.1.17.215	49677	10.1.17.2	389	14	6 kB	151	8	3 kB	6	3 kB	606.268116	0.0277	879 kbps	987 kbps	
10.1.17.215	49678	10.1.17.2	88	8	971 bytes	152	4	487 bytes	4	484 bytes	606.271563	0.0020			
10.1.17.215	49679	10.1.17.2	88	10	3 kB	153	5	627 bytes	5	2 kB	606.280971	0.0029			
10.1.17.215	49680	10.1.17.2	88	12	5 kB	154	6	2 kB	6	2 kB	606.286267	0.0038			
10.1.17.215	49697	10.1.17.2	135	12	1 kB	170	7	742 bytes	5	670 bytes	614.109784	18.5060	320 bits/s	289 bits/s	
10.1.17.215	49698	10.1.17.2	49668	22	6 kB	171	12	4 kB	10	2 kB	614.113418	48.5121	685 bits/s	340 bits/s	
10.1.17.215	49699	10.1.17.2	88	8	971 bytes	172	4	487 bytes	4	484 bytes	614.113947	0.0020			
10.1.17.215	49700	10.1.17.2	88	10	3 kB	173	5	627 bytes	5	2 kB	614.123330	0.0039			
10.1.17.215	49701	10.1.17.2	88	12	5 kB	174	6	2 kB	6	2 kB	614.127191	0.0040			
10.1.17.215	49702	10.1.17.2	135	12	1 kB	175	7	742 bytes	5	670 bytes	614.142365	49.5065	119 bits/s	108 bits/s	
10.1.17.215	49703	10.1.17.2	49668	22	6 kB	176	12	4 kB	10	2 kB	614.145760	49.5027	707 bits/s	250 bits/s	
10.1.17.215	49704	10.1.17.2	88	12	4 kB	177	6	2 kB	6	2 kB	614.146591	0.0022			
10.1.17.215	49742	10.1.17.2	135	11	2 kB	215	7	904 bytes	4	872 bytes	633.031179	1.5676	4613 bits/s	4450 bits/s	
10.1.17.215	49743	10.1.17.2	49668	23	7 kB	216	13	5 kB	10	2 kB	633.035431	1.5633	23 kbps	12 kbps	
10.1.17.215	49744	10.1.17.2	88	8	938 bytes	217	4	482 bytes	4	456 bytes	633.036175	0.0017			
10.1.17.215	49745	10.1.17.2	88	10	3 kB	218	5	622 bytes	5	2 kB	633.042745	0.0028			
10.1.17.215	49746	10.1.17.2	88	12	4 kB	219	6	2 kB	6	2 kB	633.045591	0.0040			
10.1.17.215	49747	10.1.17.2	389	20	8 kB	220	11	4 kB	9	4 kB	633.172698	0.0176	1702 kbps	1891 kbps	
10.1.17.215	49748	10.1.17.2	389	17	7 kB	221	9	3 kB	8	4 kB	633.184540	0.0057	4407 kbps	5869 kbps	
10.1.17.215	49750	10.1.17.2	135	12	2 kB	223	7	742 bytes	5	766 bytes	650.031386	12.5942	471 bits/s	486 bits/s	
10.1.17.215	49751	10.1.17.2	49684	31	9 kB	224	17	6 kB	14	3 kB	650.034055	12.5915	3819 bits/s	1684 bits/s	
10.1.17.215	49752	10.1.17.2	88	12	5 kB	225	6	2 kB	6	2 kB	650.035063	0.0047			
10.1.17.215	49753	10.1.17.2	135	10	2 kB	226	6	844 bytes	4	872 bytes	662.848988	0.0355	190 kbps	196 kbps	
10.1.17.215	49754	10.1.17.2	49668	22	7 kB	227	12	4 kB	10	2 kB	662.853246	0.0312	1149 kbps	621 kbps	
10.1.17.215	49755	10.1.17.2	389	21	8 kB	228	11	4 kB	10	4 kB	662.866520	0.0144	2097 kbps	2352 kbps	
10.1.17.215	49756	10.1.17.2	389	18	7 kB	229	9	3 kB	9	4 kB	662.874912	0.0058	4315 kbps	5796 kbps	
10.1.17.215	49757	10.1.17.2	445	238	54 kB	230	124	28 kB	114	25 kB	664.455599	616.7063	366 bits/s	328 bits/s	
10.1.17.215	49758	10.1.17.2	88	12	4 kB	231	6	2 kB	6	2 kB	664.459151	0.0043			
10.1.17.215	49759	10.1.17.2	88	12	4 kB	232	6	2 kB	6	2 kB	664.463499	0.0025			
10.1.17.215	49760	10.1.17.2	135	15	2 kB	233	9	1 kB	6	992 bytes	666.312966	26.3020	311 bits/s	301 bits/s	
10.1.17.215	49761	10.1.17.2	49668	31	8 kB	234	17	5 kB	14	3 kB	666.315709	56.3010	750 bits/s	401 bits/s	
10.1.17.215	49762	10.1.17.2	389	19	9 kB	235	11	4 kB	8	5 kB	666.328781	0.0909	355 kbps	471 kbps	
10.1.17.215	49763	10.1.17.2	389	18	8 kB	236	10	4 kB	8	4 kB	666.329232	0.0340	934 kbps	977 kbps	
10.1.17.215	49764	10.1.17.2	389	14	4 kB	237	8	3 kB	6	938 bytes	666.344582	0.0154	1611 kbps	487 kbps	
10.1.17.215	49765	10.1.17.2	88	12	4 kB	238	6	2 kB	6	2 kB	666.345763	0.0024			



Wireshark · Follow TCP Stream (tcp.stream eq 246) · 2025-01-22-traffic-analysis-exercise.pcap

```
...........................................]......+........]..........+.H`.............]......+.......3.qq..7I.......6............]......+.......,..1..@E...........
.........1.................135..................................3.qq..7I.......6..........................
.................................................................K.......K.......
5BQ..K......O...........
.]..........+.H`......................       ................................
..........................................................................................K.......K.......
5BQ..K......O...........
.]..........+.H`......................       ..
....K.......K.......
5BQ..K......O...........
.]..........+.H`......................       ..
........
.................................................................K.......K.......
5BQ..K......O...........
.]..........+.H`......................       ................................
..........................................................................................K.......K.......
5BQ..K......O...........
.]..........+.H`......................       ..
....K.......K.......
5BQ..K......O...........
.]..........+.H`......................       ..
........
```

3 client pkts, 3 server pkts, 5 turns.

Entire conversation (1140 bytes) | Show as: ASCII | No delta times | Stream: 246

Find: | ☑ Case sensitive