

EXPERIMENT: 23

TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK-TCP AND UDP

Aim: To analyze capturing of Transport layer protocol header analysis using Wire shark- TCP and UDP.

SOFTWARE USED:

Wire shark network analyzer

Procedure:

1. Open wire shark.
2. Click on list the available capture interface.
3. Choose the LAN interface.
4. Click on start button.
5. Active packets will be displayed.
6. Capture the packets & select any IP address from the source.
7. Click on the expression and select IPV4 ☐ IP addr source address in the field name.
8. Select the double equals (==) from the selection and enter the selected IP source address.
9. Click on apply button.
10. All the packets will be filtered using source address.

The screenshot displays the Wireshark network analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes. The top pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Length. The second pane displays the details of the selected packet (No. 4), showing the Ethernet II header, Internet Protocol Version 6 header, and User Datagram Protocol header. The third pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates that 17202 packets were captured, 15527 were displayed (90.3%), and 0 were dropped (0.0%).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2404:40f4:3d:dca0:9...	2404:6800:4007:814:...	UDP	242	56263 → 443 Len=180
2	0.056359	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	89	443 → 56263 Len=27
3	0.056978	2404:40f4:3d:dca0:9...	2404:6800:4007:814:...	UDP	682	56263 → 443 Len=620
4	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	126	443 → 56263 Len=64
5	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1287	443 → 56263 Len=1225
6	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
7	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
8	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
9	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
10	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	968	443 → 56263 Len=906
11	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1287	443 → 56263 Len=1225
12	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
13	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
14	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
15	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
16	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
17	0.101257	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
18	0.101962	2404:40f4:3d:dca0:9...	2404:6800:4007:814:...	UDP	99	56263 → 443 Len=37
22	0.105691	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
23	0.105691	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
24	0.105691	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1287	443 → 56263 Len=1225
25	0.105691	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
26	0.105691	2404:6800:4007:814:...	2404:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230

Frame 4: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF...
Ethernet II, Src: 2a:99:57:fb:7f:2a (2a:99:57:fb:7f:2a), Dst: Intel de:c3:e9 (f4:06:b9:de:c3:e9)
Internet Protocol Version 6, Src: 2404:6800:4007:814:2016, Dst: 2404:40f4:3d:dca0:9cb2:7f5:d1
User Datagram Protocol, Src Port: 443, Dst Port: 56263
Data (64 bytes)
578d0d4aa4ff803dbd103ec582cf423676ca4a53d26b5a487295a352d7ffadcc019cda53f82977f3821
[Length: 64]
f4 06 b9 de c3 e9 2a 99 57 fb 7f 2a 86 dd 60 00 ... i . * W * .
00 00 00 48 11 39 24 04 68 00 40 07 08 14 00 00 ... H 9\$ h @
00 00 00 00 20 16 24 09 40 f4 00 3d dc a0 9c b2 ... \$ @
07 f5 d1 b2 68 ce 01 bb db c7 00 48 16 a4 57 8d ... h > . H W
0d 4a a4 ff 80 3d bd 10 3e c5 82 c0 f4 23 67 6c ... J #g1
0a 4a 53 d2 6b 5a 48 72 95 a3 52 d7 ff ad c0 19 ... JS kZhr . R . . .
cd ba 53 f0 29 77 f3 82 17 1e a1 5e 9c 22 bc 07 ... S)w
d0 e4 23 d9 0a 0b 95 db 28 d2 61 f9 68 da ... # (a h

The image shows a Wireshark network packet capture. The main pane displays a list of packets, with packet 43 selected. The packet list shows a retransmission of a TCP segment. The packet details pane shows the structure of the TCP segment, including the header and payload. The packet bytes pane shows the raw data of the segment.

No.	Time	Source	Destination	Protocol	Length	Info
8	1.359724	2409:40f4:3f:615a:8...	2603:1040:a06:6::1	TLSv1.2	117	Application Data
9	1.843883	2409:40f4:3f:615a:8...	2603:1040:a06:6::1	TCP	117	[TCP Retransmission] 49858 → 443 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=43
10	1.945711	2603:1040:a06:6::1	2409:40f4:3f:615a:8...	TLSv1.2	248	Application Data
11	1.948918	2603:1040:a06:6::1	2409:40f4:3f:615a:8...	TCP	248	[TCP Retransmission] 443 → 49858 [PSH, ACK] Seq=1 Ack=44 Win=7117 Len=174
12	1.948983	2409:40f4:3f:615a:8...	2603:1040:a06:6::1	TCP	86	49858 → 443 [ACK] Seq=44 Ack=175 Win=509 Len=0 SLE=1 SRE=175
13	2.088551	2603:1040:a06:6::1	2409:40f4:3f:615a:8...	TCP	84	[TCP Dup. ACK] 443 → 49858 [ACK] Seq=175 Ack=44 Win=7117 Len=0 SLE=1 SRE=44
22	18.947373	2409:40f4:3f:615a:8...	2a04:4e42:8d::684	TCP	74	55317 → 80 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
23	19.255140	2a04:4e42:8d::684	2409:40f4:3f:615a:8...	TCP	74	80 → 55317 [ACK] Seq=1 Ack=2 Win=288 Len=0
24	19.255140	2a04:4e42:8d::684	2409:40f4:3f:615a:8...	TCP	74	80 → 55317 [FIN, ACK] Seq=1 Ack=2 Win=288 Len=0
25	19.255229	2409:40f4:3f:615a:8...	2a04:4e42:8d::684	TCP	74	55317 → 80 [ACK] Seq=2 Ack=2 Win=510 Len=0
26	19.431256	2409:40f4:3f:615a:8...	64:f9b::14d4:5875	TCP	75	49867 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1 [TCP PDU reassembled in 72]
27	19.534507	64:f9b::14d4:5875	2409:40f4:3f:615a:8...	TCP	86	443 → 49867 [ACK] Seq=1 Ack=2 Win=251 Len=0 SLE=1 SRE=2
40	27.719190	192.168.133.111	192.168.133.219	TCP	66	55090 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
41	28.750793	192.168.133.111	192.168.133.219	TCP	66	[TCP Retransmission] 55090 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
44	31.241308	192.168.133.111	192.168.133.219	TCP	66	[TCP Retransmission] 55090 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
49	35.029421	192.168.133.111	192.168.133.219	TCP	66	[TCP Retransmission] 55090 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
52	39.309740	2620:1ec:42::132	2409:40f4:3f:615a:8...	TCP	74	443 → 55318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	42.815438	192.168.133.111	192.168.133.219	TCP	66	[TCP Retransmission] 55090 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
63	46.369962	2409:40f4:3f:615a:8...	2603:1040:a06:6::1	TLSv1.2	117	Application Data
64	46.700308	2603:1040:a06:6::1	2409:40f4:3f:615a:8...	TLSv1.2	248	Application Data

[Stream Packet Number: 2]
 [Conversation completeness: Incomplete (12)]
 [TCP Segment Len: 43]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 1617641410
 [Next Sequence Number: 44 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 3191353590
 0101 ... = Header Length: 20 bytes (5)
 Flags: 0x018 (PSH, ACK)
 Window: 510
 [Calculated window size: 510]
 [Window size scaling factor: -1 (unknown)]
 Checksum: 0x3fef [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 [Timestamps]
 [SEQ/ACK analysis]
 TCP payload (43 bytes)
 Retransmitted TCP segment data (43 bytes)

0000 2a 99 57 fb 7f 2a b4 8c 9d 8e 01 6f 86 dd 60 02 * W o . .
 0010 4f e8 00 3f 06 3f 24 09 40 f4 00 3f 61 5a 8d 76 0 . 7 . \$ @ . 7 a Z v
 0020 83 32 b0 0f d4 0f 26 03 10 40 0a 00 00 00 00 00 2 o . & . @
 0030 00 00 00 00 01 c2 c2 01 b5 6b 3f c2 b6 35 k 2 . . 8
 0040 30 f6 50 18 01 fe 3f ef 00 00 17 03 03 00 26 00 0 P 7 8
 0050 00 00 00 00 00 33 ce 0f 9f 03 12 c4 91 0a bc 3
 0060 3e d5 6b a3 35 7b 5e 40 16 40 e3 e1 d0 3c 37 > k : \$ (@ . @
 0070 47 09 70 8f 1a 6 p s e

The TCP payload of this packet (tcp.payload), 43 bytes

Packets: 164 · Displayed: 29 (17.7%) · Dropped: 0 (0.0%) Profile: Default

Result: Hence, the capturing of packets using wire shark network analyzer was analyzed for TCP and UDP.