

## **EXPERIMENT: 23**

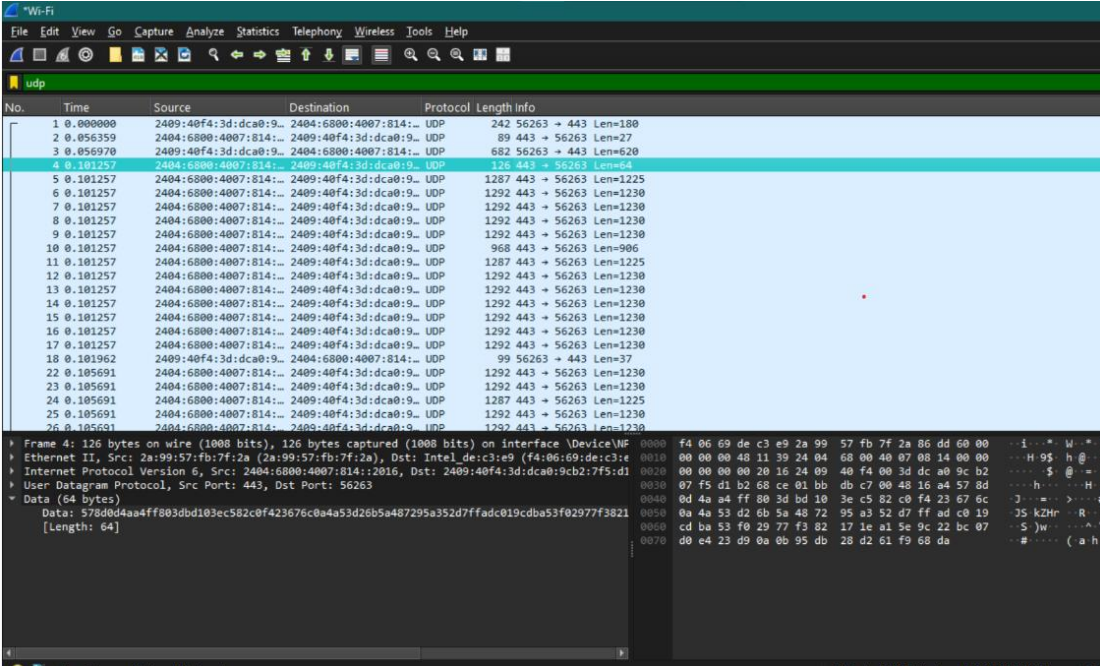
### **TRANSPORT LAYER PROTOCOL HEADER ANALYSIS USING WIRE SHARK-TCP AND UDP**

**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.

## Output:



The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets, all of which are UDP. The bottom pane shows the details of the selected packet (No. 4), including the Ethernet II header, Internet Protocol Version 6 header, and the raw data payload.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2409:40f4:3d:dca0:9...	2404:6800:4007:814:...	UDP	242	56263 → 443 Len=180
2	0.056359	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	89	443 → 56263 Len=27
3	0.056970	2409:40f4:3d:dca0:9...	2404:6800:4007:814:...	UDP	682	56263 → 443 Len=620
4	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
5	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1287	443 → 56263 Len=1225
6	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
7	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
8	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
9	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
10	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	968	443 → 56263 Len=906
11	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1287	443 → 56263 Len=1225
12	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
13	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
14	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
15	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
16	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
17	0.101257	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
18	0.101962	2409:40f4:3d:dca0:9...	2404:6800:4007:814:...	UDP	99	56263 → 443 Len=37
22	0.105691	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
23	0.105691	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
24	0.105691	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1287	443 → 56263 Len=1225
25	0.105691	2404:6800:4007:814:...	2409:40f4:3d:dca0:9...	UDP	1292	443 → 56263 Len=1230
26	0.105691	2404:6800:4007:814:...	2409:40f4:3d: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 (f4:06:69:de:c3:e9)  
Internet Protocol Version 6, Src: 2404:6800:4007:814::2016, Dst: 2409:40f4:3d:dca0:9c2b:7f5:d1  
User Datagram Protocol, Src Port: 443, Dst Port: 56263  
Data (64 bytes)  
Data: 578d0d4aa4ff803dbd103ec582cef423676c0a4a53d26b5a487295a352d7ffadc019cda53f02977f3821 [Length: 64]

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