Lab Assignment - 8

WIRESHARK

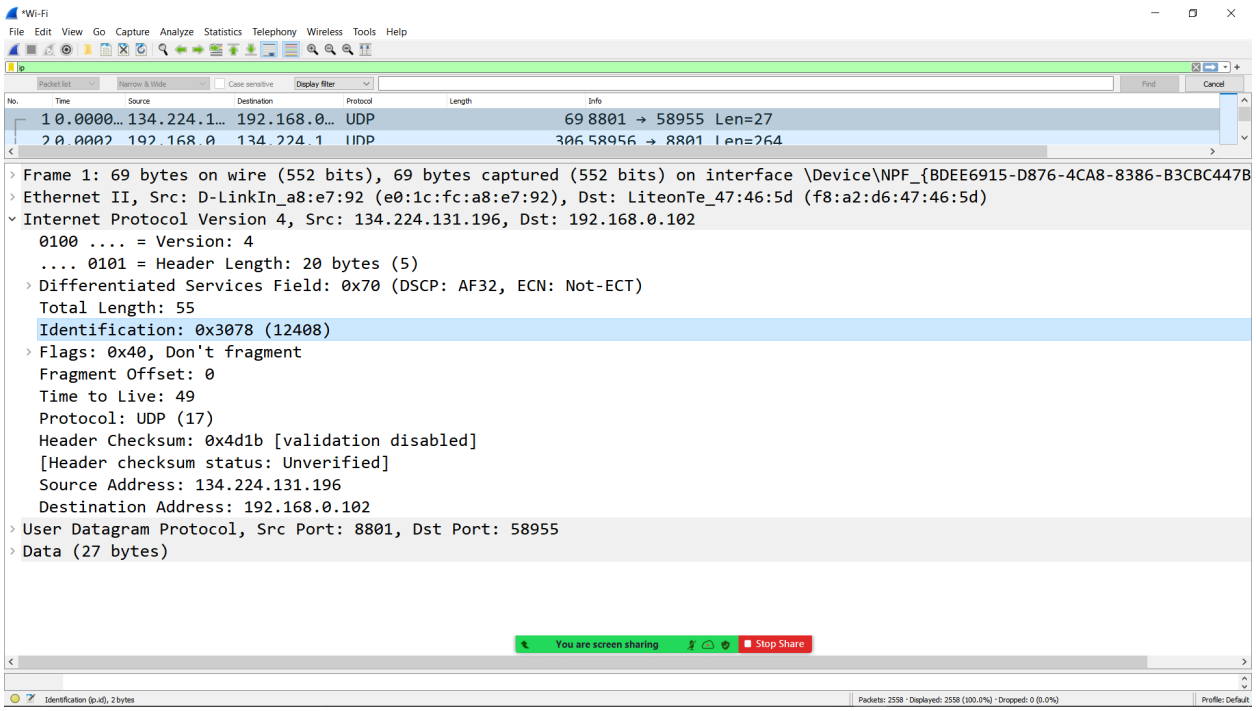
Objective:

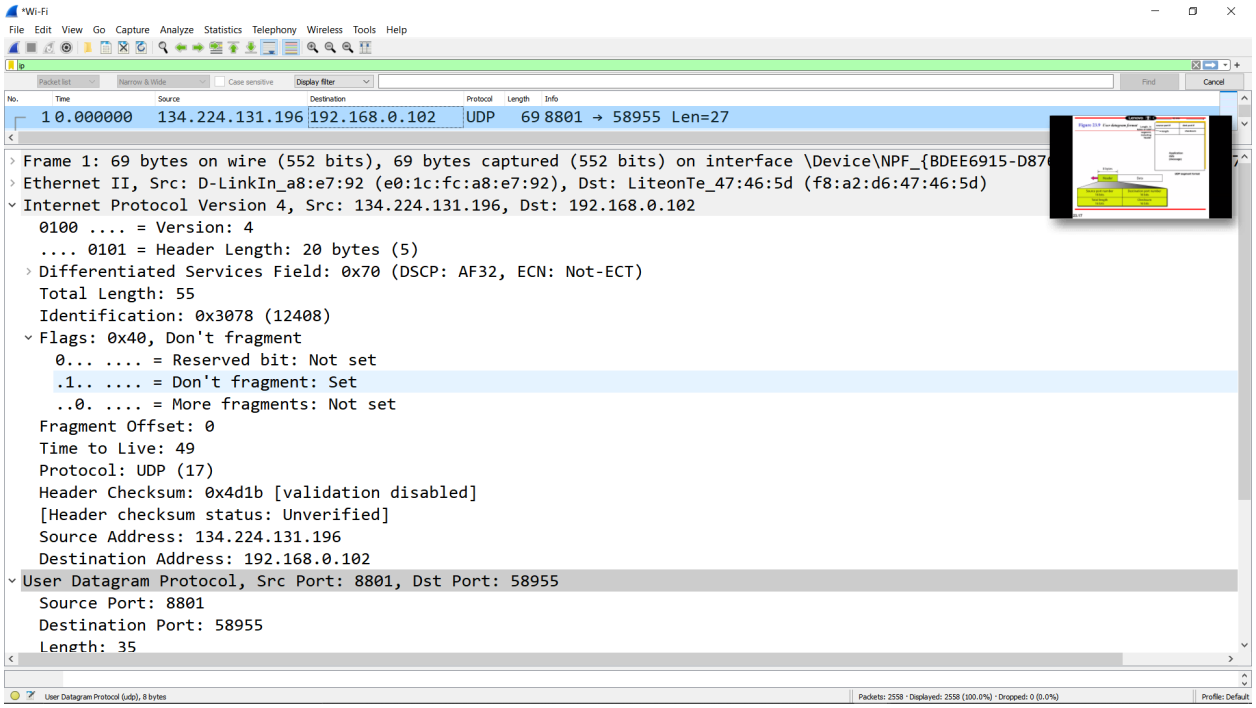
Use wireshark to sniff incoming and outgoing packets and answer the following questions given in the assignment handout.

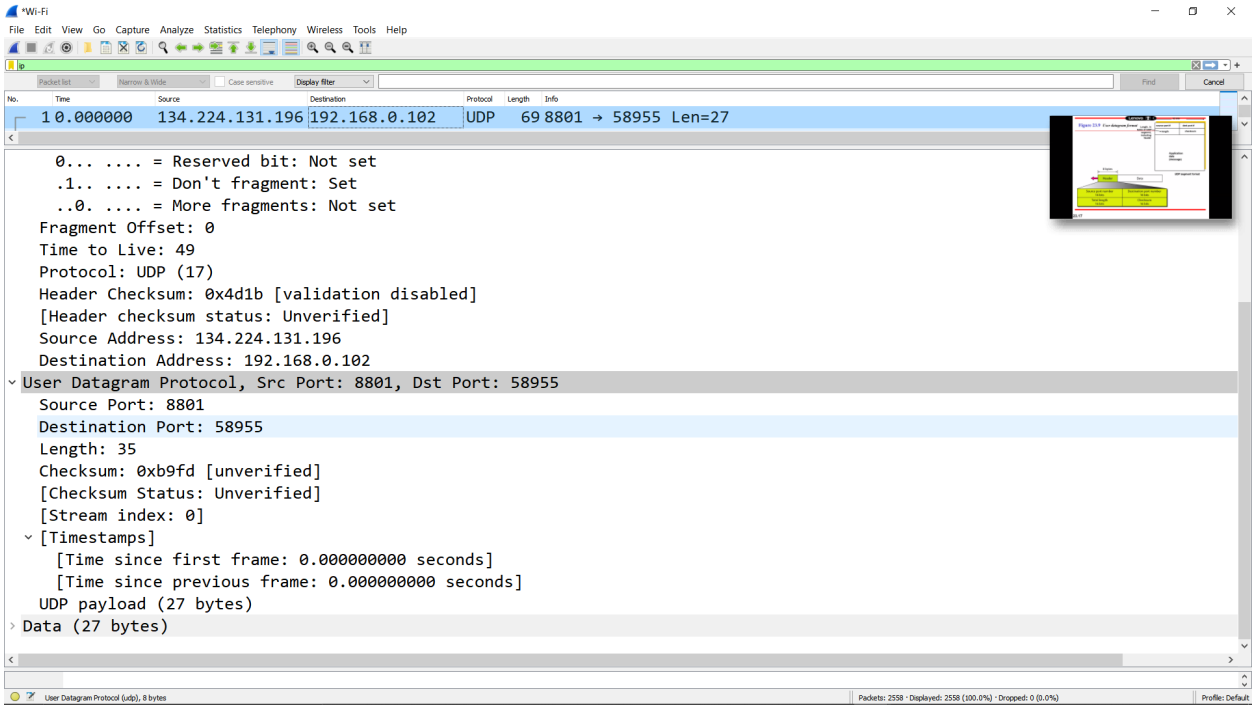
Problem Statement:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Use wireshark to study ongoing packets in the network and collect all the parameters like source and destination ip, port, TCP/IP header etc.

Outputs:




*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000 134.224.131.196 192.168.0.102 UDP 69 8801 → 58955 Len=27
Frame 1: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{BDEE6915-D87
Ethernet II, Src: D-LinkIn_a8:e7:92 (e0:1c:fc:a8:e7:92), Dst: LiteonTe_47:46:5d (f8:a2:d6:47:46:5d)
Internet Protocol Version 4, Src: 134.224.131.196, Dst: 192.168.0.102
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x70 (DSCP: AF32, ECN: Not-ECT)
Total Length: 55
Identification: 0x3078 (12408)
Flags: 0x40, Don't fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
Fragment Offset: 0
Time to Live: 49
Protocol: UDP (17)
Header Checksum: 0x4d1b [validation disabled]
[Header checksum status: Unverified]
Source Address: 134.224.131.196
Destination Address: 192.168.0.102
User Datagram Protocol, Src Port: 8801, Dst Port: 58955
Source Port: 8801
Destination Port: 58955
Length: 35
User Datagram Protocol (udp), 8 bytes
Packets: 2558 · Displayed: 2558 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000 134.224.131.196 192.168.0.102 UDP 69 8801 → 58955 Len=27
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
Fragment Offset: 0
Time to Live: 49
Protocol: UDP (17)
Header Checksum: 0x4d1b [validation disabled]
[Header checksum status: Unverified]
Source Address: 134.224.131.196
Destination Address: 192.168.0.102
User Datagram Protocol, Src Port: 8801, Dst Port: 58955
Source Port: 8801
Destination Port: 58955
Length: 35
Checksum: 0xb9fd [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
[Time since first frame: 0.000000000 seconds]
[Time since previous frame: 0.000000000 seconds]
UDP payload (27 bytes)
Data (27 bytes)
User Datagram Protocol (udp), 8 bytes
Packets: 2558 · Displayed: 2558 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Q/A :

1. Is the frame an outgoing or an incoming frame?
   -> Incoming

2. What is the source IP address of the network-layer header in the frame?
   -> 134.221.134.194

3. What is the destination IP address of the network-layer header in the frame?
   -> 192.168.0.102

4. What is the total number of bytes in the whole frame?
   -> 69 bytes

5. What is the number of bytes in the Ethernet (data-link layer) header?
   -> 20 bytes

6. What is the number of bytes in the IP header?
   -> 20 bytes

7. What is the total bytes in the message (at the application layer)?
   -> 27 bytes

Conclusion:

Through this experiment we understood how packet analysis is done using wireshark in real time, and capture basic pamerters used to transfer the packet from source IP to destination IP. We also learned how to use the main window and other GUI tools in wireshark.

Report by: Harshad Dhane
AP19110010341
CSE-G