

# Assignment- 3

## **Problem Statement:**

The objective of this laboratory exercise is to look at the details of the User Datagram Protocol (UDP). UDP is a transport layer protocol. It is used by many application protocols like DNS, DHCP, SNMP etc., where reliability is not a concern. To do this exercise you need to install the Wireshark tool, which is widely used to capture and examine a packet trace. Wireshark can be downloaded from [www.wireshark.org](http://www.wireshark.org).

## **Step1: Capture a Trace**

1. Launch Wireshark
2. From Capture→Options select Loopback interface
3. Start a capture with a filter of “ip.addr==127.0.0.1 and udp.port==xxxx”, where xxxx is the port number used by the UDP server.
4. Run the UDP server program on a terminal.
5. Run multiple instances of the UDP client program on separate terminals and send requests to the sever.
6. Stop Wireshark capture

## **Step2: Inspect the Trace**

Select different packets in the trace and browse the expanded UDP header and record the following fields:

- Source Port: the port from which the udp segment is sent.
- Destination Port: the port to which the udp segment is sent.
- Length: the length of the UDP segment.

## Capturing UDP packets in WireShark:

UDP is an unreliable and connectionless protocol. There is no need for establishing any connection before data transfer. UDP packets contains a UPD header which contains the port number for both source and destination then there is a length field which is the size of header and payload in Bytes and then some more checksum information.

UDP is faster than TCP as there is no need for creating a connection. But it is unreliable.

\*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 127.0.0.1 and udp.port == 5555

No.	Time	Source	Destination	Protocol	Length	Info
51	8.643472	127.0.0.1	127.0.0.1	UDP	36	54204 → 5555 Len=4
52	8.643749	127.0.0.1	127.0.0.1	UDP	39	5555 → 54204 Len=7
89	15.328399	127.0.0.1	127.0.0.1	UDP	35	54204 → 5555 Len=3
90	15.328610	127.0.0.1	127.0.0.1	UDP	38	5555 → 54204 Len=6
103	17.480964	127.0.0.1	127.0.0.1	UDP	36	54204 → 5555 Len=4
104	17.481146	127.0.0.1	127.0.0.1	UDP	42	5555 → 54204 Len=10

Considering the first frame sent –

The source port is : 54204 (Client in this case)

The destination port is : 5555 (Server in this case)

The length is : 27

The size of the payload is 4 Bytes.

Wireshark · Packet 51 · Adapter for loopback traffic capture

> Frame 51: 36 bytes on wire (288 bits), 36 bytes captured (288 bits) on interface \Device\NPF\_{Loopback}, id 6  
> Null/Loopback  
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
▼ User Datagram Protocol, Src Port: 54204, Dst Port: 5555  
    Source Port: 54204  
    Destination Port: 5555  
    Length: 12  
    Checksum: 0x4b90 [unverified]  
    [Checksum Status: Unverified]  
    [Stream index: 0]  
    > [Timestamps]  
    UDP payload (4 bytes)  
▼ Data (4 bytes)  
    Data: 61726b61  
    [Length: 4]

< >

0000	02 00 00 00 45 00 00 20	75 dd 00 00 80 11 00 00	...E.. u.....
0010	7f 00 00 01 7f 00 00 01	d3 bc 15 b3 00 0c 4b 90	...K..
0020	61 72 6b 61		arka