

Exp no: 01  
Date 20/09/2014

## Practical - 05

### Capturing and analysing packets using Wireshark

#### Tool

To filter, capture, view packets in Wireshark tool. Capture 100 packets from the ethernet : IEEE 802.3 LAN interface and save it.

#### Procedure :

- 1 Select Local Area Connection in Wireshark
- 2 Go to capture - option
- 3 Select stop capture automatically after 100 packets.
- 4 Then click start capture
- 5 Save the packets.

#### Output :

No.	Time	Source	Destination	Protocol	Length Info
780	81.178037	192.168.137.221	142.250.196.10	UDP	71 56755 → 443 Len=29
781	81.193928	142.250.196.10	192.168.137.221	UDP	67 443 → 56755 Len=25
782	81.367523	192.168.137.221	13.197.42.20	TCP	54 49895 → 443 [RST, ACK] Seq=1718 Ack=3765 Win=0 Len=0
783	81.368080	192.168.137.221	152.199.40.167	TCP	54 49897 → 443 [RST, ACK] Seq=537 Ack=14111 Win=0 Len=0
784	81.368411	192.168.137.221	13.197.42.18	TCP	54 49898 → 443 [RST, ACK] Seq=1744 Ack=10360 Win=0 Len=0
785	81.409819	192.168.137.221	142.250.196.10	UDP	71 56755 → 443 Len=29
786	81.428378	142.250.196.10	192.168.137.221	UDP	67 443 → 56755 Len=25
787	81.544725	192.168.137.221	142.250.196.10	UDP	71 56755 → 443 Len=29
788	81.662794	142.250.196.10	192.168.137.221	UDP	67 443 → 56755 Len=25
789	81.880383	192.168.137.221	142.250.196.10	UDP	71 56755 → 443 Len=29
790	81.895029	142.250.196.10	192.168.137.221	UDP	67 443 → 56755 Len=25
791	82.312342	192.168.137.221	142.250.196.10	UDP	71 56755 → 443 Len=29
792	82.331554	142.250.196.10	192.168.137.221	UDP	67 443 → 56755 Len=25
793	83.140033	192.168.137.221	142.250.196.10	UDP	71 56755 → 443 Len=29
794	83.164630	192.168.137.180	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
795	83.164630	142.250.196.10	192.168.137.221	BROWSER	67 443 → 56755 Len=25
796	83.357172	192.168.137.1	192.168.137.255	SSDP	243 Host Announcement DESKTOP-CF6U0BT, Workstation, Server, NT Work
797	84.075680	192.168.137.180	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1

1) create a filter to display only TCP/UDP packets, inspect the packets and provide the flow graph:

Procedure:

select local Area connection in wireshark.

GO to capture → option

Select stop capture automatically

after 100 packets

Then start capture.

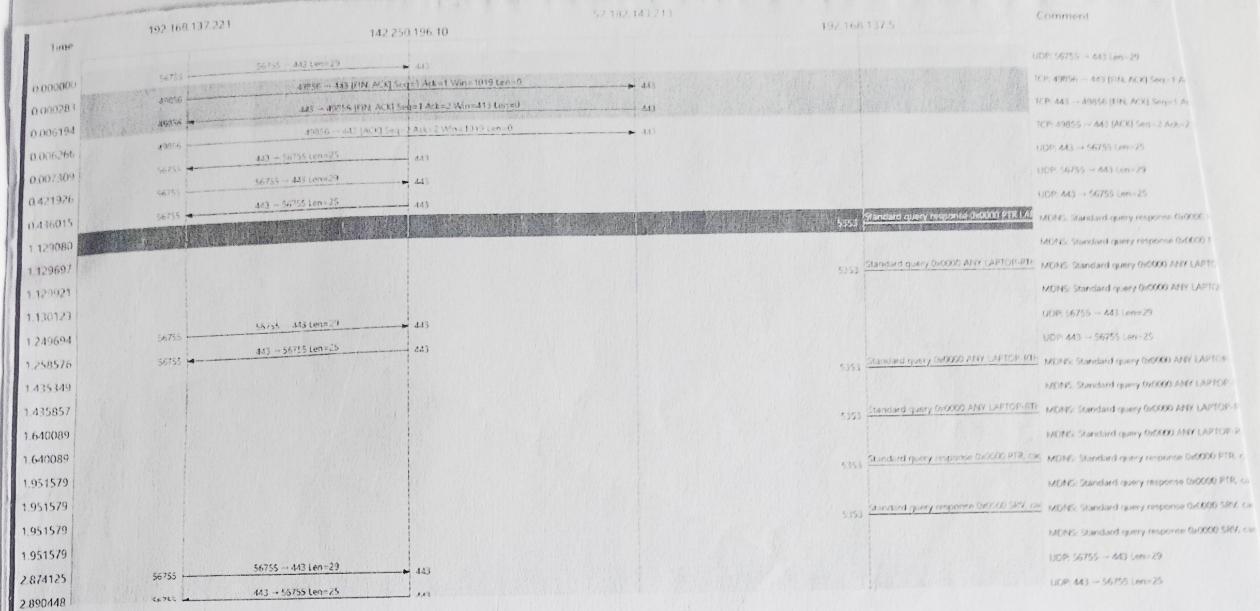
Search TCP packets in search bar

To see flow graph click statistics - flow graph.

Save the packets.

No.	Time	Source	Destination	Protocol	Length	Info
37515	1869.497608	192.168.137.221	20.210.166.59	TCP	55	[TCP Keep-Alive] 50157 → 443 [ACK] Seq=27303 Ack=210 Win=0
37516	1870.371824	192.168.137.221	142.250.195.78	TCP	55	[TCP Keep-Alive] 50183 → 443 [ACK] Seq=45934 Ack=210 Win=0
37517	1870.395697	142.250.195.78	192.168.137.221	TCP	66	[TCP Keep-Alive ACK] 443 → 50183 [ACK] Seq=15344 Ack=210 Win=0
37518	1870.727307	192.168.137.221	142.251.175.188	TCP	55	[TCP Keep-Alive] 49760 → 5228 [ACK] Seq=27 Ack=210 Win=0
37519	1870.811259	192.168.137.5	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
37520	1870.914747	192.168.137.5	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
37521	1871.938972	192.168.137.5	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
37522	1872.043462	192.168.137.221	52.113.194.132	TCP	54	50176 → 443 [RST, ACK] Seq=2152 Ack=7388 Win=0
37523	1872.263802	192.168.137.221	204.79.197.239	TCP	55	[TCP Keep-Alive] 50154 → 443 [ACK] Seq=3083 Ack=210 Win=0
37524	1872.962275	192.168.137.5	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
37525	1874.323988	192.168.137.221	20.198.119.143	TLSv1.2	155	Application Data
37526	1874.590713	192.168.137.221	20.198.119.143	TCP	155	[TCP Retransmission] 53929 → 443 [PSH, ACK] Seq=155 Ack=155 Win=0
37527	1874.687225	192.168.137.221	142.250.196.10	QUIC	71	Protected Payload (KPB), DCID=fef08d52bba2f2af
37528	1874.722665	142.250.196.10	192.168.137.221	QUIC	67	Protected Payload (KPB)
37529	1874.985646	192.168.137.221	20.198.119.143	TCP	155	[TCP Retransmission] 53929 → 443 [PSH, ACK] Seq=155 Ack=155 Win=0
37530	1875.517315	192.168.137.221	20.198.119.143	TCP	155	[TCP Retransmission] 53929 → 443 [PSH, ACK] Seq=155 Ack=155 Win=0
37531	1876.737173	192.168.137.221	20.198.119.143	TCP	155	[TCP Retransmission] 53929 → 443 [PSH, ACK] Seq=155 Ack=155 Win=0
37532	1877.937572	192.158.137.221	20.198.119.143	TCP	155	[TCP Retransmission] 53929 → 443 [PSH, ACK] Seq=155 Ack=155 Win=0

# FLOW GRAPH is a graphical display with a chain of flows along edges



student observation :

1) What is promiscuous mode?

Promiscuous mode is a network interface card setting that allows card to intercept and read all network packets on network segments.

2) Does ARP layer has transport layer headers? Explain?

No, ARP layer has no transport layer headers.

3) Which transport layer is used by DNS?

VDP (virtual station Interface proto discovery protocol)

4) What is the port number used by http protocol?

Port 443.

5) What is a broadcast IP address?  
It is a broadcast IP address which is used to send packets to all devices on a specific network segment.

8/8  
9/8/24

### RESULT:

Thus the packet capturing, filtering and flow graph are observed using airshark