

Exp. 5

Experiment on Packet Capture tool:

Wireshark.

Objectives:

Aim:

Object at Experiment on packet capture tool:
Wireshark.

Wireshark:

A network analysis tool that captures real time network packets and displays them in human readable format.

Key features:

1) Real time packet capture

2) Filtering

3) Protocol decoding using selector

4) Traffic browsing and smart statistics.

Uses of Wireshark:

1. Network Admin: Trouble shoot network issue.

2. Analysis security incidents

3. Debug network protocol implementation

4. Understand step by step protocols interactions.

~~Windows~~: Download wireshark from official website.

a) Capturing packets:

Launch Wireshark and double click a network interface to begin capturing packets.

Packets appear in real time and include all traffic of previous mode is enabled (Capture options > enable promiscuous mode).

b) Coding colour:

Using of light green for TCP.

Light blue for UDP

Black for error packets

Customize colour; view

Colouring rule.

c) Sample capture:-

Load sample capture from Wireshark, wifi via file > open.

Save in your own capture using

file > save as dialog.

d) Filtering packets:

a) Use the filter bar to isolate traffic.

Press enter (or) click Apply

Access default listen file via analyse > display filter.

e) Following TCP streams:

Right click a packet > follow TCP stream.

Close window auto apply a filter for that connection.

Inputting packets:

Click a packet to see its details.

Right click protocol fields > apply a filter based on it.

Flow graph:

Use statistics.

Visually traffic flow between devices flow graph.

Capturing and analyzing using Wireshark tool.

Procedure:

Select Local Area Selection.

Capture > options > set stop after 100 packets.

click start

save packets

Filter: Display TCP/UDP packets and show flow graph.

procedure:

* Start capture as above

* In filter bar, search TCP or UDP.

* Statistics > Flow Graph to view.

* Type two way packets

* Save packets

Filter: Display only ARP packets:

* Start capture as above

* In filter bar, type UDP

* Save packets

Filter: Display only DNS packets and show flow graph.

* Start capture as above

* In filter bar, type dns

* Statistics > Flow Graph to view

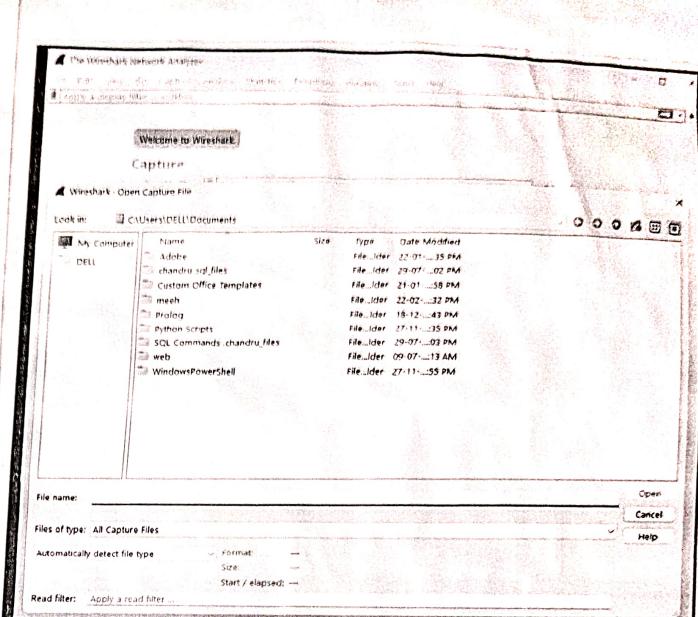
* Save packets

Filter: Display only HTTPS packets:

* Start capture as above

* In filter bar, type HTTP

* Save packets



No.	Time	Source	Destination	Protocol	Length	Info
369	5.122991	fe80::a95a:b1ff:429...ff02::fb		NDNS	319	Standard query response 0x0000 PTR DEL
370	5.122991	172.16.75.134	224.0.0.251	NDNS	299	Standard query response 0x0000 PTR DEL
371	5.122991	fe80::4903:8ab5:5c5...ff02::fb		NDNS	328	Standard query response 0x0000 PTR DEL
372	5.124455	172.16.75.149	224.0.0.251	NDNS	368	Standard query response 0x0000 PTR DEL
374	5.126749	172.16.75.150	224.0.0.251	NDNS	1177	Standard query response 0x0000 PTR DEL
375	5.126749	172.16.75.138	224.0.0.251	NDNS	308	Standard query response 0x0000 PTR DEL
376	5.126749	172.16.75.151	224.0.0.251	NDNS	969	Standard query response 0x0000 PTR DEL
377	5.128353	172.16.75.134	224.0.0.251	NDNS	304	Standard query response 0x0000 PTR DEL
379	5.128353	fe80::ecf5:1acf:3cb...ff02::fb		NDNS	319	Standard query response 0x0000 PTR DEL
380	5.129733	172.16.75.142	224.0.0.251	NDNS	1471	Standard query response 0x0000 PTR DEL
381	5.131317	fe80::51cd:5857:155...ff02::fb		NDNS	1237	Standard query response 0x0000 PTR DEL
382	5.131317	fe80::3c3a:1528:bb4...ff02::fb		NDNS	929	Standard query response 0x0000 PTR DEL
383	5.131317	fe80::f22c:a4d1:846...ff02::1:1:2		DHCPv6	121	Information-request XID: 0x5c2df0 CID:
384	5.147739	172.16.75.17	142.251.220.110	UDP	71	63949 - 443 Len=29
385	5.156756	142.251.220.110	172.16.75.17	UDP	68	443 - 200 Len=26
386	5.157188	172.16.75.17	142.251.220.106	UDP	71	52994 - 443 Len=29
387	5.165145	142.251.220.106	172.16.75.17	UDP	68	443 - 52994 Len=26
388	5.380561	172.16.75.17	142.251.220.106	UDP	71	52994 - 443 Len=29

> Frame 1: 86 bytes on wire (688 bits), 86 bytes captured
> Ethernet II, Src: GigabyteTech_53:a5:a8 (e0:d5:5e:53:a5:a8), Dst: 00:00:00:20:3a:ff
> Internet Protocol Version 6, Src: fe80::e2d5:5eff:fe53:a8
> Internet Control Message Protocol v6

0000 33 33 ff 49 84 b2 e0 d5 5e 53 a5 a8 86 dd 60 00
0010 00 00 00 20 3a ff fe 80 00 00 00 00 00 00 e2 d5
0020 5e ff fe 53 a5 b2 e0 00 00 00 00 00 00 00 00 00
0030 00 01 ff 49 84 b2 87 00 cc 47 00 00 00 00 fe 80
0040 00 00 00 00 00 00 00 00 ba d6 ff fe 49 84 b2 01 01
0050 e0 d5 5e 53 a5 a8

Student Observations

- 1) What is promiscous mode?
It allows a network device to capture all packets on the network, not just those addressed to it.
- 2) Does ARP packets has transport layer header? explain?
No, ARP operates at data link layer and does not have a transport layer header.
- 3) Which transport layer protocol is used by DNS?
DNS uses UDP by default and TCP for large queries like zone transfer.
- 4) What is the port number used by http protocol?
Port 80 is used by http protocol.
- 5) What is broadcast ip address?
It is 255.255.255.255 used to send data to all hosts on a local network.

Result:

Thus the above experiment was completed and executed.