Exp No: 5

Practical - 5

Date: 9/8/24

Aim:

Experiments on packet capture tool: Wireshark

Packet Sniffer

- Sniffs messages being sent / received from / by your computer
- Store and display the contents of the various protocol fields in the messages.
- Passive program
  - never sends packets itself
  - no packets addressed to it
  - receives a copy of all packets

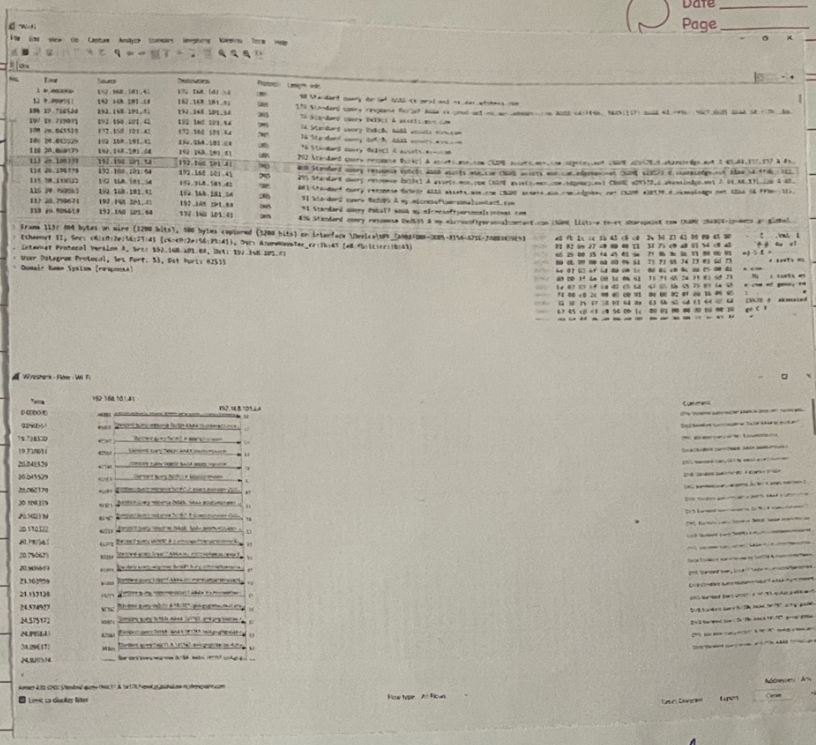
Packet Sniffer Structure Diagnostic Tools

- tcp dump
  - E.g. tcp dump -ew host 10.129.41.2 -w exe3.out
- Wireshark
  - wireshark -r exe3.out.

Procedure:

Select Local Area Connection in wireshark Go to capture - options

Select stop capture automatically after 100 packets



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 → graph
Save the packets.

For DNS:

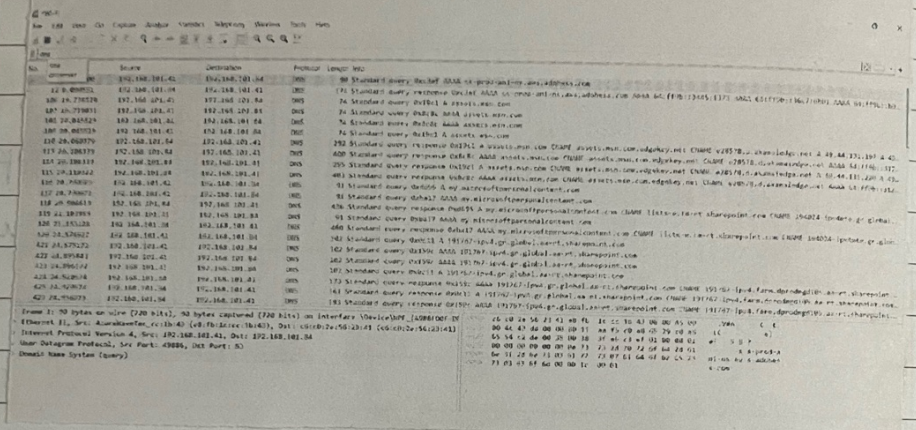
*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

dns
dnsserver

No.		Source	Destination	Protocol	Length	Info
	00	192.168.101.41	192.168.101.84	DNS	90	Sta
2	0.028851	48.218.107.40	192.168.101.41	TLSv1.2	1153	App
3	0.028851	52.123.178.24	192.168.101.41	TLSv1.2	482	App
4	0.028851	52.123.178.24	192.168.101.41	TLSv1.2	92	App
5	0.028974	192.168.101.41	52.123.178.24	TCP	54	562
6	0.032513	192.168.101.41	48.218.107.40	TLSv1.2	319	App
7	0.032843	192.168.101.41	48.218.107.40	TLSv1.2	110	App
8	0.038276	64:ff9b::d6b:380	2409:408d:384:33cb:...	TLSv1.2	293	App
9	0.039494	192.168.101.41	52.123.178.24	TLSv1.2	173	App



Student observations:

1) What is promiscuous mode?

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

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

No, ARP layer has no transport layer head

3) Which transport layer is used by DNS?

VDP (virtual station interface discovery protocol)

4) What is the port number used by https 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.

RESULT:

Thus the packet capturing, observing flow graph are done using wireshark.