

6/8/24

Exercise: 5

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.

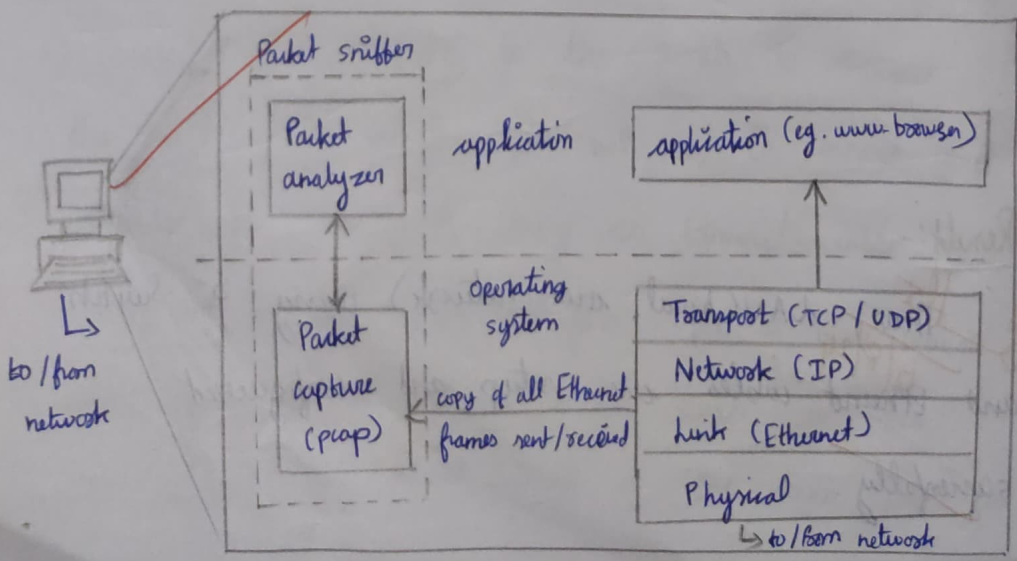
Packet Sniffer Structure Diagnostic Tools:-

* Tcpdump

- Eg: `tcpdump -enx host 10.129.41.2 -w exe3.out`

* Wireshark

- `wireshark -o exe3.out`



Capturing network traffic:-

After downloading and installing Wireshark, launch it and double-click the name of a network interface to capture.

Procedure:-

- 1) Select local Area connection in Wireshark
- 2) Go to capture \rightarrow options
- 3) Select stop capture automatically after 100 packets
- 4) Save the packets.

Output :-

[illegible]

Filtering Pockets :-

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). We can also apply filters by selecting the packet \rightarrow Apply as Filter \rightarrow Selected.

Output:-

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.101.41	192.168.101.84	DNS	90	Standard query 0xc3ef AAAA ss-prod-anl-ns.aws.adobee.com
2	0.028851	48.218.107.40	192.168.101.41	TLSv1.2	1153	Application Data
3	0.028851	52.123.178.24	192.168.101.41	TLSv1.2	482	Application Data
4	0.028851	52.123.178.24	192.168.101.41	TLSv1.2	92	Application Data
5	0.028874	192.168.101.41	52.123.178.24	TCP	54	56207 → 443 [ACK] Seq=1 Acl=467 Win=252 Len=0
6	0.029213	192.168.101.41	48.218.107.40	TLSv1.2	319	Application Data
7	0.029243	192.168.101.41	48.218.107.40	TLSv1.2	110	Application Data
8	0.030276	64.ffff:00b:300	2400:400d:304:33cb::	TLSv1.2	293	Application Data
9	0.030441	192.168.101.41	Mark/Unmark Packet	CBT-M	273	Application Data
10	0.030541	192.168.101.41	Ignore/Unignore Packet	CBT-D	242	Application Data
11	0.030535	2400:400d:304:33cb::	Set/Unset Time Reference	CBT-T	74	56202 → 443 [ACK] Seq=1 Acl=220 Win=254 Len=0
12	0.030551	192.168.101.9	Time Shift	CBT-Shift-T	374	Standard query response 0xc3ef AAAA ss-prod-anl-ns.aws.adobee.com
13	0.030551	2400:400d:304:33cb::	Packet Comments		86	56208 → 443 [SYN] Seq=0 Win=64512 Len=0 MSS=1412 WS=256
14	0.030551	52.123.178.24	192.168.101.41	TCP	54	443 → 56207 [ACK] Seq=467 Acl=100 Win=16384 Len=0
15	0.031311	48.218.107.40	192.168.101.41	TCP	54	443 → 56199 [ACK] Seq=1100 Acl=322 Win=2049 Len=0

Frame 8: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface [Device]NPF_{A0B0F00F-D005} (0.0.0.0) on interface [Device]NPF_{A0B0F00F-D005}

Ethernet II, Src: c6:c0:2e:56:23:41 (c6:c0:2e:56:23:41), Dst: 48:218:107:40:00:00 (48:218:107:40:00:00)

Internet Protocol Version 4, Src: 192.168.101.41, Dst: 48.218.107.40

Transmission Control Protocol, Src Port: 56207, Dst Port: 443, Seq: 1, Len: 219

Transport Layer Security

No.	Time	Source	Destination	Protocol	Length	Info
1	0.028851	48.218.107.40	192.168.101.41	TLSv1.2	1153	Application Data
2	0.028851	52.123.178.24	192.168.101.41	TLSv1.2	482	Application Data
3	0.028851	52.123.178.24	192.168.101.41	TLSv1.2	92	Application Data
4	0.029213	192.168.101.41	48.218.107.40	TLSv1.2	319	Application Data
5	0.029243	192.168.101.41	48.218.107.40	TLSv1.2	110	Application Data
6	0.030276	64.ffff:00b:300	2400:400d:304:33cb::	TLSv1.2	293	Application Data
7	0.030441	192.168.101.41	52.123.178.24	TLSv1.2	173	Application Data
8	0.030541	48.218.107.40	192.168.101.41	TLSv1.2	342	Application Data
9	0.030551	52.123.178.24	192.168.101.41	TLSv1.2	99	Application Data
10	0.030551	52.123.178.24	192.168.101.41	TLSv1.2	180	Application Data
11	0.030551	2400:400d:304:33cb::	64.ffff:00b:300	TLSv1.2	269	Client Hello (SHA-256)
12	0.030551	64.ffff:00b:300	2400:400d:304:33cb::	TLSv1.2	4124	Server Hello
13	0.030551	64.ffff:00b:300	2400:400d:304:33cb::	TLSv1.2	120	Certificate
14	0.030551	64.ffff:00b:300	2400:400d:304:33cb::	TLSv1.2	375	Server Key Exchange, Server Hello Done
15	0.030551	2400:400d:304:33cb::	64.ffff:00b:300	TLSv1.2	167	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

Frame 9: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface [Device]NPF_{A0B0F00F-D005} (0.0.0.0) on interface [Device]NPF_{A0B0F00F-D005}

Ethernet II, Src: c6:c0:2e:56:23:41 (c6:c0:2e:56:23:41), Dst: 48:218:107:40:00:00 (48:218:107:40:00:00)

Internet Protocol Version 4, Src: 192.168.101.41, Dst: 48.218.107.40

Transmission Control Protocol, Src Port: 443, Dst Port: 56202, Seq: 1, Len: 219

Transport Layer Security

Inspecting Packets:-

Click a packet to select it and you can dig down to view its details.

Output:-

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.101.41	192.168.101.84	DNS	90	Standard query 0xc3ef AAAA ss-prod-anl-ns.aws.adobee.com
2	0.028851	48.218.107.40	192.168.101.41	TLSv1.2	1153	Application Data
3	0.028851	52.123.178.24	192.168.101.41	TLSv1.2	482	Application Data
4	0.028851	52.123.178.24	192.168.101.41	TLSv1.2	92	Application Data
5	0.028874	192.168.101.41	52.123.178.24	TCP	54	56207 → 443 [ACK] Seq=1 Acl=467 Win=252 Len=0
6	0.029213	192.168.101.41	48.218.107.40	TLSv1.2	319	Application Data
7	0.029243	192.168.101.41	48.218.107.40	TLSv1.2	110	Application Data
8	0.030276	64.ffff:00b:300	2400:400d:304:33cb::	TLSv1.2	293	Application Data
9	0.030441	192.168.101.41	52.123.178.24	TLSv1.2	173	Application Data
10	0.030541	48.218.107.40	192.168.101.41	TLSv1.2	342	Application Data
11	0.030551	52.123.178.24	192.168.101.41	TLSv1.2	99	Application Data
12	0.030551	52.123.178.24	192.168.101.41	TLSv1.2	180	Application Data
13	0.030551	2400:400d:304:33cb::	64.ffff:00b:300	TLSv1.2	269	Client Hello (SHA-256)
14	0.030551	64.ffff:00b:300	2400:400d:304:33cb::	TLSv1.2	4124	Server Hello
15	0.030551	64.ffff:00b:300	2400:400d:304:33cb::	TLSv1.2	120	Certificate
16	0.030551	64.ffff:00b:300	2400:400d:304:33cb::	TLSv1.2	375	Server Key Exchange, Server Hello Done
17	0.030551	2400:400d:304:33cb::	64.ffff:00b:300	TLSv1.2	167	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

Frame 9: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface [Device]NPF_{A0B0F00F-D005} (0.0.0.0) on interface [Device]NPF_{A0B0F00F-D005}

Ethernet II, Src: AzureWaveNet.cc:1b:43 (c6:c0:2e:56:23:41), Dst: c6:c0:2e:56:23:41 (c6:c0:2e:56:23:41)

Internet Protocol Version 4, Src: 192.168.101.41, Dst: 52.123.178.24

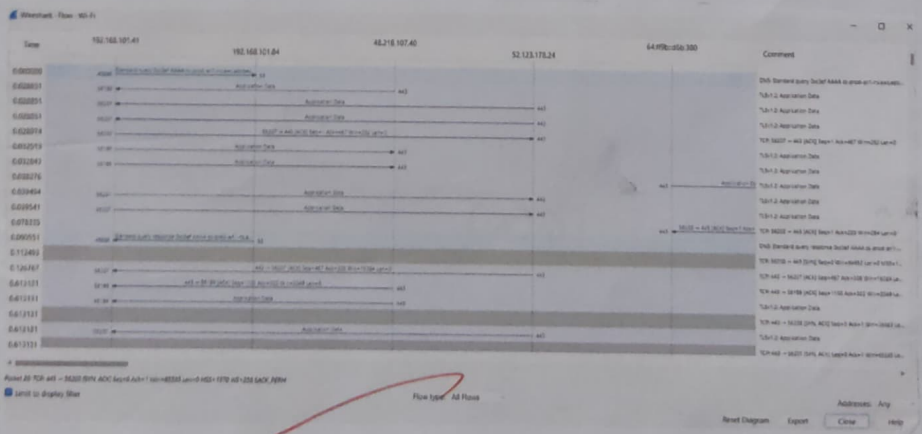
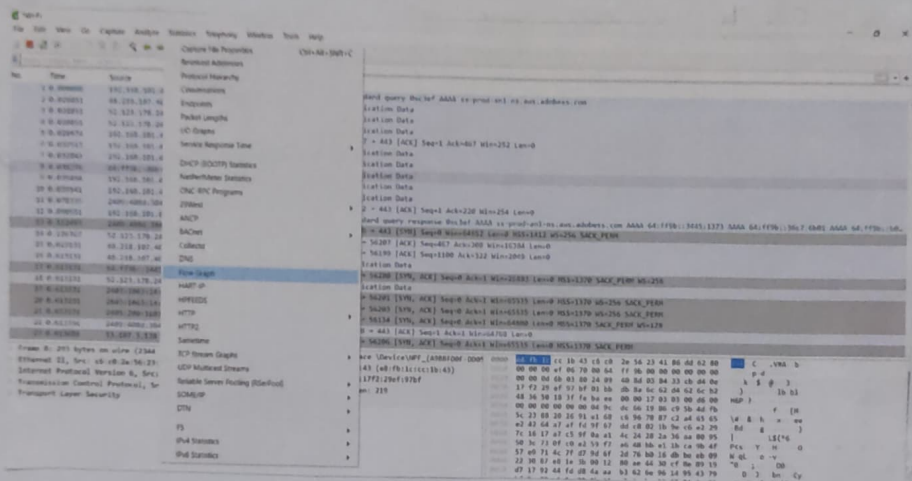
Transmission Control Protocol, Src Port: 56207, Dst Port: 443, Seq: 1, Len: 119

Transport Layer Security

Flow Graph:-

We can see the flow graph of the packets. by clicking on the statistics and selecting the flow graph and it displays the flow graph of the packets.

Output:-



Create a Filter to display only DNS packets and provide the flow graph.

Procedure :-

- Go to capture → option.
- Select stop capture automatically after 100 packets.
- Then click start capture.
- Search DNS packets in search bar.
- To see flow graph click Statistics → Flow graph.
- Save the packets.

Capturing and Filtering :-

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Source	Destination	Protocol	Length	Info
1	192.168.101.41	192.168.101.84	DNS	90	Standard query request 192.168.101.41 to 192.168.101.84
2	192.168.101.41	192.168.101.84	DNS	1153	Standard query response 192.168.101.84 to 192.168.101.41
3	192.168.101.41	192.168.101.84	TLSv1.2	482	Standard query request 192.168.101.41 to 192.168.101.84
4	192.168.101.41	192.168.101.84	TLSv1.2	92	Standard query response 192.168.101.84 to 192.168.101.41
5	192.168.101.41	48.218.107.40	TLSv1.2	54	Standard query request 192.168.101.41 to 48.218.107.40
6	192.168.101.41	48.218.107.40	TLSv1.2	319	Standard query response 48.218.107.40 to 192.168.101.41
7	192.168.101.41	48.218.107.40	TLSv1.2	110	Standard query request 192.168.101.41 to 48.218.107.40
8	192.168.101.41	2409:408d:384:33cb:...	TLSv1.2	293	Standard query request 192.168.101.41 to 2409:408d:384:33cb:...
9	192.168.101.41	52.123.178.24	TLSv1.2	173	Standard query request 192.168.101.41 to 52.123.178.24

Frame 3: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface vti0-eth0 (en0) ...
 Internet Protocol Version 4, Src: 192.168.101.41, Dest: 192.168.101.84
 User Datagram Protocol, Src Port: 49080, Dest Port: 53
 Domain Name System (Query)

