04/8/2025

Practical-V

Wireshark, a network analysis tool, captures packets in real time and displays them in human-readable format. It includes filters, color coding and other features to dig deep into network traffic and inspect individual packets.

What we can do with Wireshark

Capture network traffic

Decode packet protocols using dissectors

Define filters - capture and display

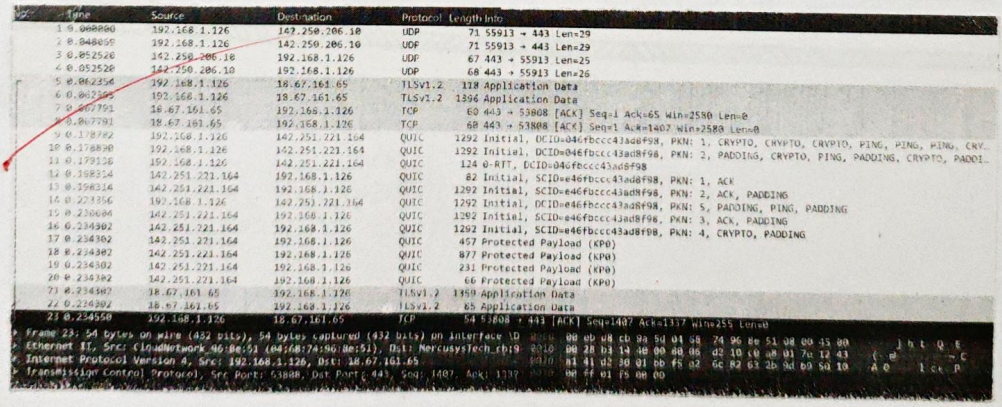
Watch smart statistics

Analyze problems

Interactively browse the traffic

Capturing Packets

Select a network interface under Capture to start capturing packets on that interface. The interface could be Ethernet, Wi-Fi etc. Packets start to appear in real time. Wireshark captures each packet sent to or from your system.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.126	142.250.206.10	UDP	71	55913 → 443 Len=29
2	0.048059	192.168.1.126	142.250.206.10	UDP	71	55913 → 443 Len=29
3	0.052520	142.250.206.10	192.168.1.126	UDP	67	443 → 55913 Len=25
4	0.052520	142.250.206.10	192.168.1.126	UDP	68	443 → 55913 Len=26
5	0.062256	192.168.1.126	18.67.161.65	TLSv1.2	118	Application Data
6	0.063395	192.168.1.126	18.67.161.65	TLSv1.2	1396	Application Data
7	0.067791	18.67.161.65	192.168.1.126	TCP	60	443 → 53808 [ACK] Seq=1 Ack=65 Win=2580 Len=0
8	0.067791	18.67.161.65	192.168.1.126	TCP	68	443 → 53808 [ACK] Seq=1 Ack=1407 Win=2580 Len=0
9	0.178792	192.168.1.126	142.251.221.164	QUIC	1292	Initial, DCID=046fbccc43ad8f98, PKN: 1, CRYPTO, CRYPTO, CRYPTO, PING, PING, PING, CRY…
10	0.178830	192.168.1.126	142.251.221.164	QUIC	1292	Initial, DCID=046fbccc43ad8f98, PKN: 2, PADDING, CRYPTO, PING, PADDING, CRYPTO, PADDI…
11	0.179158	192.168.1.126	142.251.221.164	QUIC	124	0-RTT, DCID=046fbccc43ad8f98
12	0.188314	142.251.221.164	192.168.1.126	QUIC	82	Initial, SCID=e46fbccc43ad8f98, PKN: 1, ACK
13	0.198314	142.251.221.164	192.168.1.126	QUIC	1292	Initial, SCID=e46fbccc43ad8f98, PKN: 2, ACK, PADDING
14	0.223356	192.168.1.126	142.251.221.164	QUIC	1292	Initial, DCID=e46fbccc43ad8f98, PKN: 5, PADDING, PING, PADDING
15	0.230084	142.251.221.164	192.168.1.126	QUIC	1292	Initial, SCID=e46fbccc43ad8f98, PKN: 3, ACK, PADDING
16	0.234302	142.251.221.164	192.168.1.126	QUIC	1292	Initial, SCID=e46fbccc43ad8f98, PKN: 4, CRYPTO, PADDING
17	0.234302	142.251.221.164	192.168.1.126	QUIC	457	Protected Payload (KP0)
18	0.234302	142.251.221.164	192.168.1.126	QUIC	877	Protected Payload (KP0)
19	0.234302	142.251.221.164	192.168.1.126	QUIC	231	Protected Payload (KP0)
20	0.234302	142.251.221.164	192.168.1.126	QUIC	66	Protected Payload (KP0)
21	0.234587	18.67.161.65	192.168.1.126	TLSv1.2	1359	Application Data
22	0.234942	18.67.161.65	192.168.1.126	TLSv1.2	65	Application Data
23	0.234950	192.168.1.126	18.67.161.65	TCP	54	53808 → 443 [ACK] Seq=1407 Ack=1337 Win=255 Len=0

```
▶ Frame 23: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \D
▶ Ethernet II, Src: ClouNetwork_46:8e:51 (04:68:74:96:8e:51), Dst: MercusysTech_cb:9
▶ Internet Protocol Version 4, Src: 192.168.1.126, Dst: 18.67.161.65
▶ Transmission Control Protocol, Src Port: 53808, Dst Port: 443, Seq: 1407, Ack: 1337
```

The "Packet List" Pane

The packet list pane displays all the packets in the current capture file. Each line in the packet list corresponds to one packet in the capture file. Selecting a line in this pane, opens more details in the "Packet Details" and "Packet Bytes" panes.

The "Packet Details" Pane

The packet details pane shows the current selected packet in a more detailed form. This pane shows the protocols and protocol fields of packets selected in "Packet List" pane.

The "Packet Bytes" Pane

The packet bytes pane shows the data of the current packet in a hexdump style.

Color Coding

Wireshark uses colors to help you identify the types of traffic at glance. The colouring rules can also be customized and modified.

Filtering Packets

Wireshark's filters allows to narrow down the traffic to inspect something specific. Basic way to apply filter is by typing it into the filter box. For example, type "tcp" and it will display only TCP packets.

Custom filters can also be added which can be saved for future use.

tcp

No.	Time	Source	Destination	Protocol	Length	Info
5	0.062354	192.168.1.126	18.67.161.65	TLSv1.2	118	Application Data
6	0.062395	192.168.1.126	18.67.161.65	TLSv1.2	1396	Application Data
7	0.067791	18.67.161.65	192.168.1.126	TCP	60	443 → 53808 [ACK] Seq=1 Ack=65 Win=2580 Len=0
8	0.067791	18.67.161.65	192.168.1.126	TCP	60	443 → 53808 [ACK] Seq=1 Ack=1407 Win=2580 Len=0
21	0.234302	18.67.161.65	192.168.1.126	TLSv1.2	1359	Application Data
22	0.234302	18.67.161.65	192.168.1.126	TLSv1.2	85	Application Data
23	0.234550	192.168.1.126	18.67.161.65	TCP	54	53808 → 443 [ACK] Seq=1407 Ack=1337 Win=255 Len=0
28	0.758921	23.202.229.22	192.168.1.126	TLSv1.2	93	Application Data
29	0.758921	23.202.229.22	192.168.1.126	TLSv1.2	78	Application Data
30	0.758921	23.202.229.22	192.168.1.126	TCP	54	443 → 54027 [FIN, ACK] Seq=64 Ack=1 Win=546 Len=0
31	0.758921	23.202.229.22	192.168.1.126	TCP	54	[TCP Retransmission] 443 → 54027 [FIN, ACK] Seq=64
32	0.759033	192.168.1.126	23.202.229.22	TCP	54	54027 → 443 [ACK] Seq=1 Ack=65 Win=253 Len=0
47	2.074206	192.168.1.126	18.67.161.65	TLSv1.2	118	Application Data
48	2.074243	192.168.1.126	18.67.161.65	TLSv1.2	1396	Application Data
49	2.077870	18.67.161.65	192.168.1.126	TCP	60	443 → 53808 [ACK] Seq=1337 Ack=1471 Win=2580 Len=0
50	2.077870	18.67.161.65	192.168.1.126	TCP	60	443 → 53808 [ACK] Seq=1337 Ack=2813 Win=2580 Len=0
51	2.240263	18.67.161.65	192.168.1.126	TLSv1.2	1361	Application Data
52	2.240263	18.67.161.65	192.168.1.126	TLSv1.2	85	Application Data
53	2.240346	192.168.1.126	18.67.161.65	TCP	54	53808 → 443 [ACK] Seq=2813 Ack=2675 Win=250 Len=0
54	4.118098	192.168.1.126	18.67.161.65	TLSv1.2	118	Application Data
55	4.118152	192.168.1.126	18.67.161.65	TLSv1.2	1396	Application Data
56	4.121998	18.67.161.65	192.168.1.126	TCP	60	443 → 53808 [ACK] Seq=2675 Ack=2877 Win=2580 Len=0

CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL

Capture 100 packets from the Wifi Interface and save it.

Procedure

Select Wi-Fi in Wireshark

Go to capture → option

Select stop capture automatically after 100 packets

Then click Start capture.

Save the packets.

1. Create a Filter to display only DNS packets and inspect the packets.

Procedure

Go to capture → option

Select stop capture automatically after 100 packets.

Then click Start capture.

Search DNS packets in search bar.

Save the packets.

dns

No.	Time	Source	Destination	Protocol	Length	Info
564	23.558802	192.168.1.126	192.168.1.1	DNS	74	Standard query 0xb989 A www.google.com
565	23.559012	192.168.1.126	192.168.1.1	DNS	74	Standard query 0xa9fb HTTPS www.google.com
566	23.564615	192.168.1.1	192.168.1.126	DNS	90	Standard query response 0xb989 A www.google.com…
567	23.564615	192.168.1.1	192.168.1.126	DNS	143	Standard query response 0xa9fb HTTPS www.google…
591	23.606837	192.168.1.126	192.168.1.1	DNS	78	Standard query 0x6669 A blockify.b-cdn.net
592	23.607061	192.168.1.126	192.168.1.1	DNS	78	Standard query 0x449b HTTPS blockify.b-cdn.net
601	23.612834	192.168.1.1	192.168.1.126	DNS	94	Standard query response 0x6669 A blockify.b-cdn…
606	23.613704	192.168.1.1	192.168.1.126	DNS	141	Standard query response 0x449b HTTPS blockify.b…
727	23.735902	192.168.1.126	192.168.1.1	DNS	88	Standard query 0xc7ba A ogads-pa.clients6.googl…
728	23.736019	192.168.1.126	192.168.1.1	DNS	88	Standard query 0x4157 HTTPS ogads-pa.clients6.g…
729	23.740616	192.168.1.1	192.168.1.126	DNS	104	Standard query response 0xc7ba A ogads-pa.clien…
730	23.740616	192.168.1.1	192.168.1.126	DNS	138	Standard query response 0x4157 HTTPS ogads-pa.c…
801	24.153654	192.168.1.126	192.168.1.1	DNS	75	Standard query 0xd457 A play.google.com
802	24.153781	192.168.1.126	192.168.1.1	DNS	75	Standard query 0x637f HTTPS play.google.com
803	24.159284	192.168.1.1	192.168.1.126	DNS	91	Standard query response 0xd457 A play.google.co…
804	24.159284	192.168.1.1	192.168.1.126	DNS	125	Standard query response 0x637f HTTPS play.googl…
865	28.609522	192.168.1.126	192.168.1.1	DNS	74	Standard query 0x731e A ogs.google.com
866	28.609626	192.168.1.126	192.168.1.1	DNS	74	Standard query 0xec67 HTTPS ogs.google.com
867	28.614278	192.168.1.1	192.168.1.126	DNS	111	Standard query response 0x731e A ogs.google.com…
868	28.614278	192.168.1.1	192.168.1.126	DNS	145	Standard query response 0xec67 HTTPS ogs.google…
931	28.739450	192.168.1.126	192.168.1.1	DNS	75	Standard query 0x9ebd A www.gstatic.com
932	28.739598	192.168.1.126	192.168.1.1	DNS	75	Standard query 0x3c13 HTTPS www.gstatic.com
933	28.739886	192.168.1.126	192.168.1.1	DNS	75	Standard query 0x0c92 A ssl.gstatic.com
934	28.739947	192.168.1.126	192.168.1.1	DNS	75	Standard query 0xba4a HTTPS ssl.gstatic.com

Wireshark · Flow · Wi-Fi

Time	192.168.1.126		192.168.1.1	Comment
23.558802	52117	Standard query 0xb989 A www.google.com →	53	DNS: Standard query 0xb989 A www.google.com
23.559012	59226	Standard query 0xa9fb HTTPS www.google.c →	53	DNS: Standard query 0xa9fb HTTPS www.google.com
23.564615	52117	← Standard query response 0xb989 A www.go...	53	DNS: Standard query response 0xb989 A www.google.com A ...
23.564615	59226	← Standard query response 0xa9fb HTTPS ww...	53	DNS: Standard query response 0xa9fb HTTPS www.google.co...
23.606837	56678	Standard query 0x6669 A blockify.b-cdn.net →	53	DNS: Standard query 0x6669 A blockify.b-cdn.net
23.607061	59687	Standard query 0x449b HTTPS blockify.b-cd... →	53	DNS: Standard query 0x449b HTTPS blockify.b-cdn.net
23.612834	56678	← Standard query response 0x6669 A blockify....	53	DNS: Standard query response 0x6669 A blockify.b-cdn.net A ...
23.613704	59687	← Standard query response 0x449b HTTPS blo...	53	DNS: Standard query response 0x449b HTTPS blockify.b-cdn...
23.735902	61879	Standard query 0xc7ba A ogads-pa.clients6... →	53	DNS: Standard query 0xc7ba A ogads-pa.clients6.google.com
23.736019	50139	Standard query 0x4157 HTTPS ogads-pa.clie... →	53	DNS: Standard query 0x4157 HTTPS ogads-pa.clients6.google
23.740616	61879	← Standard query response 0xc7ba A ogads-p...	53	DNS: Standard query response 0xc7ba A ogads-pa.clients6.go...
23.740616	50139	← Standard query response 0x4157 HTTPS oga...	53	DNS: Standard query response 0x4157 HTTPS ogads-pa.client...
24.153654	51152	Standard query 0xd457 A play.google.com →	53	DNS: Standard query 0xd457 A play.google.com
24.153781	55731	Standard query 0x637f HTTPS play.google.c... →	53	DNS: Standard query 0x637f HTTPS play.google.com

We can follow the same strategy for displaying and inspecting other packets like TCP/UDP, ARP, HTTP, IP/ICMP, DHCP, etc.

1. What is promiscuous mode?
   A mode where it captures all packets on the network, instead of only the ones addressed in the network adapter.

2. Does ARP packets has transport layer header? Explain.
   No, ARP packets don't contain. ARP works at the data link layer.

3. Which transport layer protocol is used by DNS?
   DNS primarily uses UDP, but uses TCP for large queries.

4. What is the port number used by http protocol?
   HTTP uses port number 80.

4/4

5. What is a broadcast ip address?
   An ip address used to send data to all hosts in a network.

Result:
Hence, the experiment in Wireshark was successfully implemented.