Ex: No. 5

Aim: Experiments on packet capture tool: wireshark.

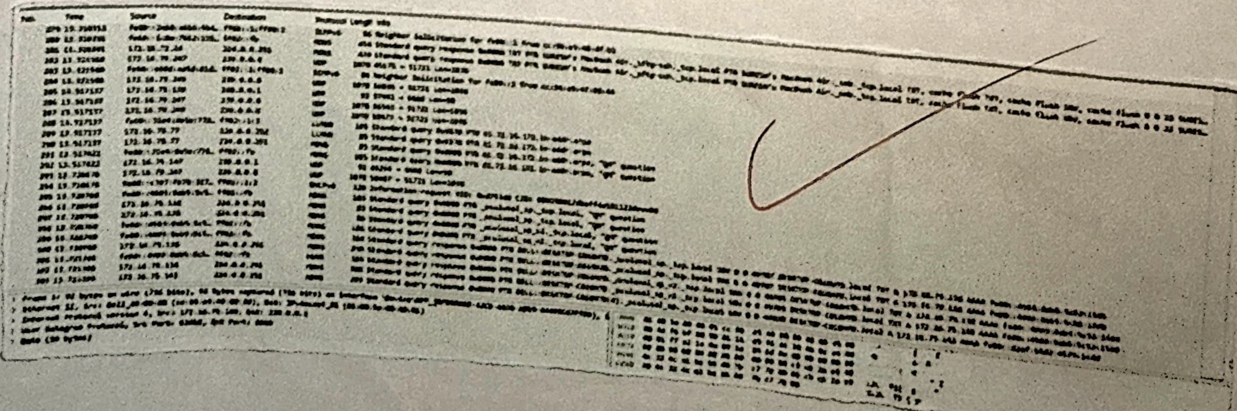
wireshark, a network analysis tool, captures packets in human-readable format. It includes filters, color codin and other features to dig deep into network traffic and chippset individual packets.

What we can do with wire shark

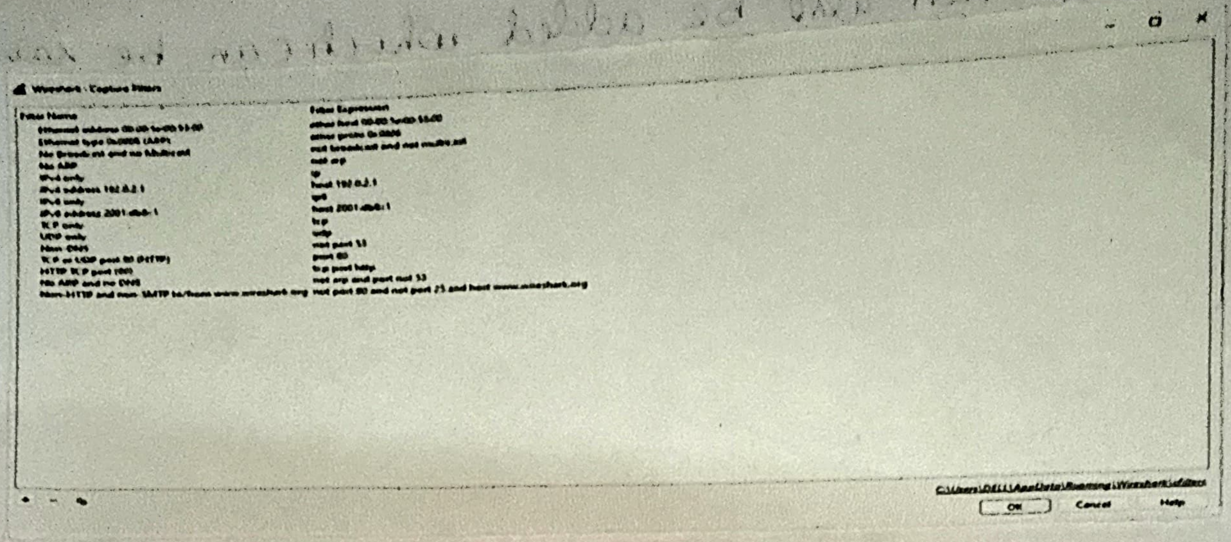
Capture network traffic
Decode packet protocols using dissectors
Define fitters - capture and display
Watch smart statistics
Analyze problems
interactively ~~[illegible]~~ browse the trafic.

Capturing packets:

Select the network interface under capture to start capturing packet on that interface. The interface could be EThernet, wIFI-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
```



Wireshark · Capture Filters

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org

C:\Users\DELL\AppData\Roaming\Wireshark\cfilters

~~CAP~~ The "Packet List" Pane

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

The "Packet Details" Pane

The packet details pane shows the current selected packet is in more detaited form. This pane shows the protocols and protocol feild of packets selected in "Packet List" pane

The "Packet Bytes" pane

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

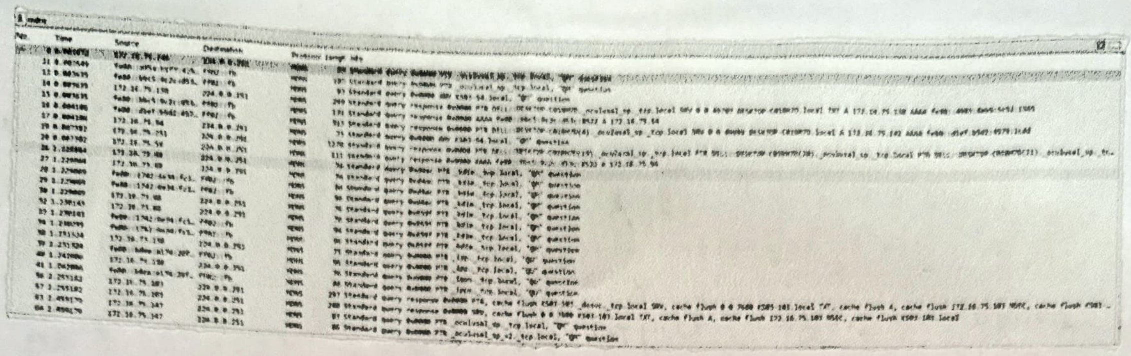
color coding:

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

Filtering Packets;

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

custom filter can also be added which can be saved for future life.



No. Time Source Destination Protocol Length Info

CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL

Capture, 100 packets from the wifi Interface and save it.

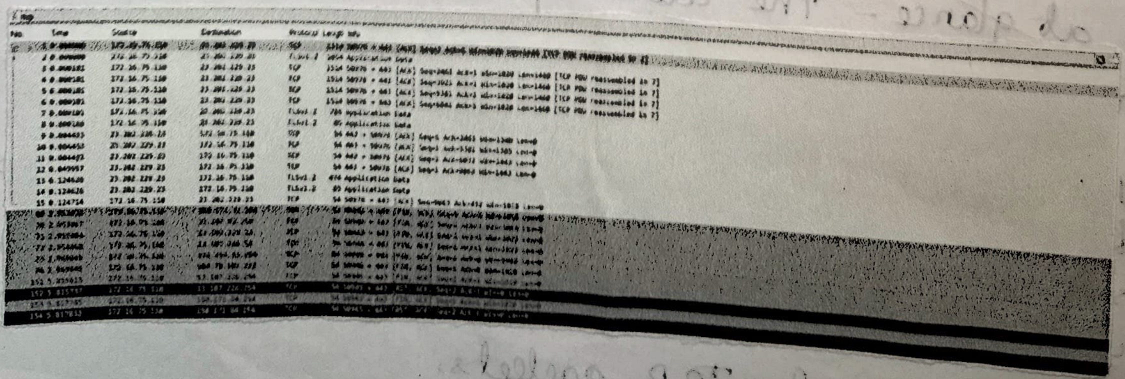
procedure:

Select WIFI in wireshark
Go to Capture → option
Select stop capture automatically after 100 packets
Then, click start capture
Save the packets.

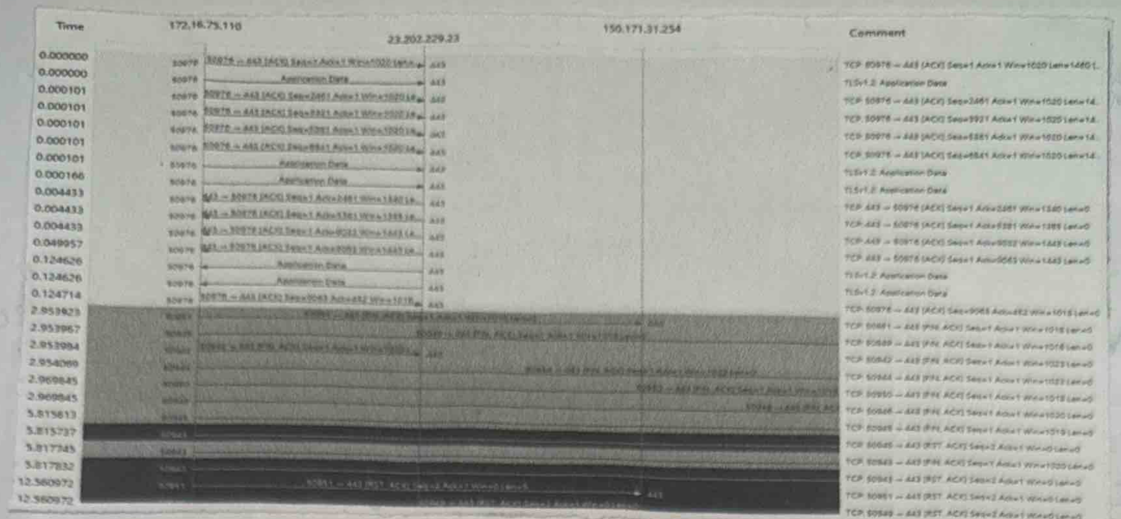
1. Create a Filter to display only TCP packets

Procedure:

Go to capture → option
Select stop capture automatically after 100 packets
Then click start capture
Search TCP, packets in search bar
Save the packets



No. Time Source Destination Protocol Length Info



```
Time        Comment
0.000000    TCP: 50976 → 443 [ACK] Seq=1 Ack=1 Win=1020 Len=1460 [...
0.000000    TLSv1.2: Application Data
0.000101    TCP: 50976 → 443 [ACK] Seq=2461 Ack=1 Win=1020 Len=14...
0.000101    TCP: 50976 → 443 [ACK] Seq=3921 Ack=1 Win=1020 Len=14...
0.000101    TCP: 50976 → 443 [ACK] Seq=5381 Ack=1 Win=1020 Len=14...
0.000101    TCP: 50976 → 443 [ACK] Seq=6841 Ack=1 Win=1020 Len=14...
0.000101    TLSv1.2: Application Data
0.000166    TLSv1.2: Application Data
0.004433    TCP: 443 → 50976 [ACK] Seq=1 Ack=2461 Win=1340 Len=0
0.004433    TCP: 443 → 50976 [ACK] Seq=1 Ack=5381 Win=1389 Len=0
0.004433    TCP: 443 → 50976 [ACK] Seq=1 Ack=9032 Win=1443 Len=0
0.049957    TCP: 443 → 50976 [ACK] Seq=1 Ack=9065 Win=1443 Len=0
0.124626    TLSv1.2: Application Data
0.124626    TLSv1.2: Application Data
0.124714    TCP: 50976 → 443 [ACK] Seq=9065 Ack=482 Win=1018 Len=0
2.953823    TCP: 50881 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1018 Len=0
2.953967    TCP: 50589 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1018 Len=0
2.953984    TCP: 50842 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
2.954060    TCP: 50944 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
2.969845    TCP: 50950 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1018 Len=0
2.969845    TCP: 50868 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
5.815613    TCP: 50948 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1019 Len=0
5.815737    TCP: 50645 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
5.817745    TCP: 50843 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
5.817832    TCP: 50943 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
12.560972   TCP: 50861 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
12.560972   TCP: 50549 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
```

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

1. What is premiscuous mode?
A node 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 doesn't contain; ARP works at the data link layer.

3. which transport layer protocol is user by DNS?
DNS primarily uses UDP test uses TCP for large queries

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

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

8|9|25

Result: Hence the wireshark experiment was successful