LAB 9

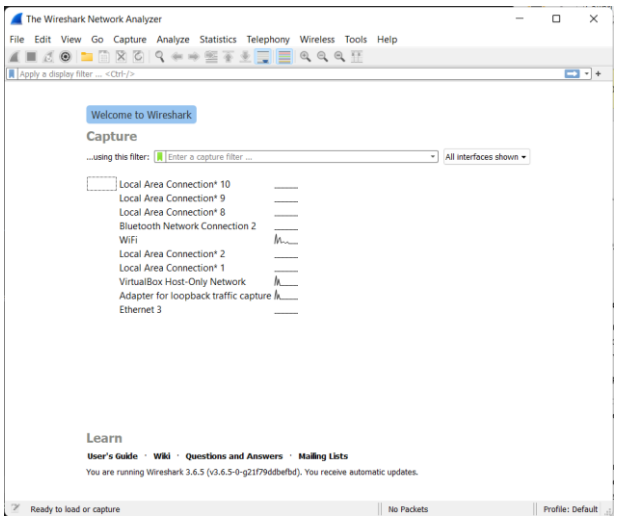
Packet capture and header analysis by Wire-Shark (TCP, UDP, IP)

Objective:

- To understand the packet analysis tool.
- Understand TCP/UDP/IP header.

Background:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.



Capturing Packets:

After downloading and installing Wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface.

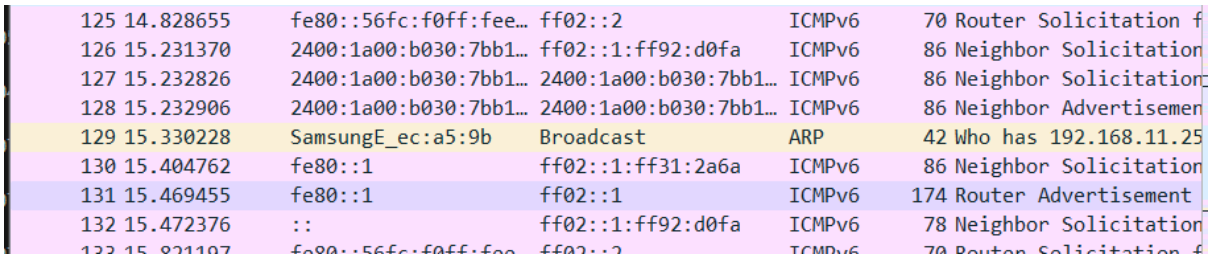
As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system. If you're capturing on a wireless interface and have promiscuous mode enabled in your capture options, you'll also see other the other packets on the network.

No.	Time	Source	Destination	Protocol	Length	Info
312	16.514693	2400:1a00:b030:7bb1…	2400:1a00:b030:7bb1…	ICMPv6	86	Neighbor Solicitation for
313	16.514865	2400:1a00:b030:7bb1…	2400:1a00:b030:7bb1…	ICMPv6	86	Neighbor Advertisement 24
314	16.526276	2400:1a00:b030:7bb1…	2400:1a00:b030:7bb1…	ICMPv6	86	Neighbor Solicitation for
315	16.526364	2400:1a00:b030:7bb1…	2400:1a00:b030:7bb1…	ICMPv6	86	Neighbor Advertisement 24
316	16.984591	fe80::1	ff02::1:ff31:2a6a	ICMPv6	86	Neighbor Solicitation for
317	17.492796	2400:1a00:b030:7bb1…	ff02::1:fff6:9c97	ICMPv6	86	Neighbor Solicitation for

```
> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{90E3C1F3-F
> Ethernet II, Src: SamsungE_ec:a5:9b (54:fc:f0:ec:a5:9b), Dst: MegaWell_19:f4:71 (a4:fc:77:19:f4:71)
> Internet Protocol Version 6, Src: ::, Dst: ff02::1:ffec:a59b
> Internet Control Message Protocol v6
```

Color Coding:

You'll probably see packets highlighted in green, blue, and black. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.



125	14.828655	fe80::56fc:f0ff:fee…	ff02::2	ICMPv6	70	Router Solicitation f
126	15.231370	2400:1a00:b030:7bb1…	ff02::1:ff92:d0fa	ICMPv6	86	Neighbor Solicitation
127	15.232826	2400:1a00:b030:7bb1…	2400:1a00:b030:7bb1…	ICMPv6	86	Neighbor Solicitation
128	15.232906	2400:1a00:b030:7bb1…	2400:1a00:b030:7bb1…	ICMPv6	86	Neighbor Advertisemen
129	15.330228	SamsungE_ec:a5:9b	Broadcast	ARP	42	Who has 192.168.11.25
130	15.404762	fe80::1	ff02::1:ff31:2a6a	ICMPv6	86	Neighbor Solicitation
131	15.469455	fe80::1	ff02::1	ICMPv6	174	Router Advertisement
132	15.472376	::	ff02::1:ff92:d0fa	ICMPv6	78	Neighbor Solicitation

Filtering Packets:

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through.