Ex. No : 3 **Study Basic Commands of Wireshark**

Date:

Aim

To study about installation and the basic commands of Wireshark.

About Wireshark

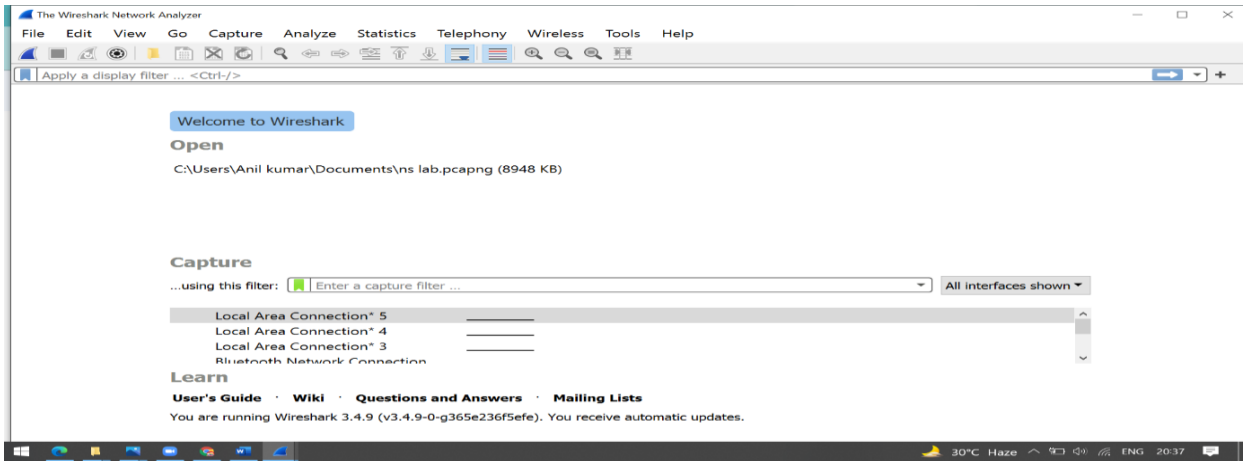
Wireshark is an open-source network protocol analysis tool developed by Gerald Combs in 1998 to review packet captures of network activity Wireshark is a packet sniffer and analysis tool that captures network traffic on the local network and stores that data for offline analysis. Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE 802.11), Token Ring, Frame relay connections, and more.

Installation of Wireshark

https://www.wireshark.org/download.html

When you open you will see list of all network interfaces on your computer. U need to choose which interface u want Wireshark to capture packets on. Select the Wi-Fi option. After this, a new window opens up, which will show the current traffic on the network. Below is the image which tells us about the live capture of packets and our Wireshark will look like:

Wireshark Interface



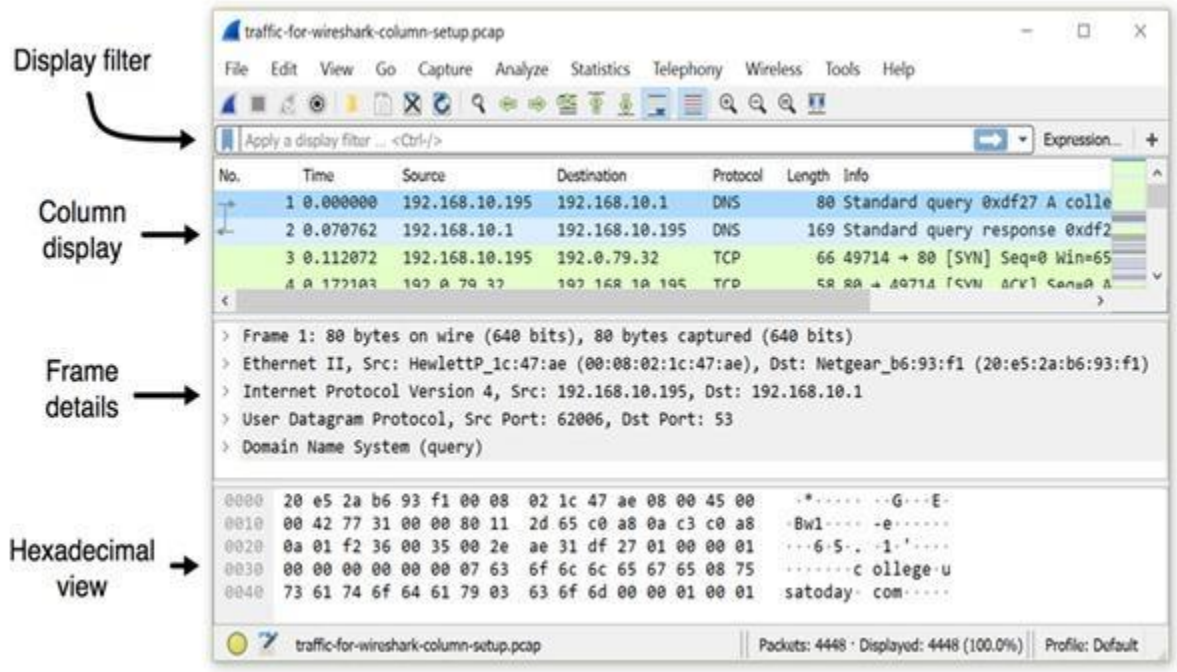
Screen/Interface of the Wireshark

The screen/interface of the Wireshark is divided into five parts:

- First part contains a menu bar and the options displayed below it. This part is at the top of the window. File and the capture menus options are commonly used in Wireshark.

The capture menu allows to start the capturing process. And the File menu is used to open and save a capture file.

- The second part is the packet listing window. It determines the packet flow or the captured packets in the traffic. It includes the packet number, time, source, destination, protocol, length, and info. We can sort the packet list by clicking on the column name.
- Next comes the packet header- detailed window. It contains detailed information about the components of the packets. The protocol info can also be expanded or minimized according to the information required.
- The bottom window called the packet contents window, which displays the content in ASCII and hexadecimal format.
- At last, is the filter field which is at the top of the display. The captured packets on the screen can be filtered based on any component according to your requirements. For example, if we want to see only the packets with the HTTP protocol, we can apply filters to that option. All the packets with HTTP as the protocol will only be displayed on the screen, shown below:



[13:53, 10/19/2021] +91 98408 75382: Figure: Viewing a pcap using Wireshark's default column display.

[13:54, 10/19/2021] +91 98408 75382: Wireshark's default columns are:

- No. -Frame number from the beginning of the pcap. The first frame is always 1.
- Time - Seconds broken down to the nanosecond from the first frame of the pcap. The first frame is always 0.000000.
- Source - Source address, commonly an IPv4, IPv6, or Ethernet address.
- Destination - Destination address, commonly an IPv4, IPv6, or Ethernet address.
- Protocol - Protocol used in the Ethernet frame, IP packet, or TCP segment (ARP, DNS, TCP, HTTP, etc.).

- Length - Length of the frame in bytes

Boolean Expression in Display Filter

Wireshark's display filter uses Boolean expressions, so you can specify values and chain them together. The following expressions are commonly used:

Equals: == or cq.

And: &&or and

Or: || (double pipe) or or

Examples of these filter expressions follow:

- ip addr eq 192.168.10.195 and ip.addr == 192.168.10.1
- http.request && ip.addr == 192.168.10.195
- http.request || http response
- Dns qry name contain Microsoft or qry name contains windows

Arp -a :-

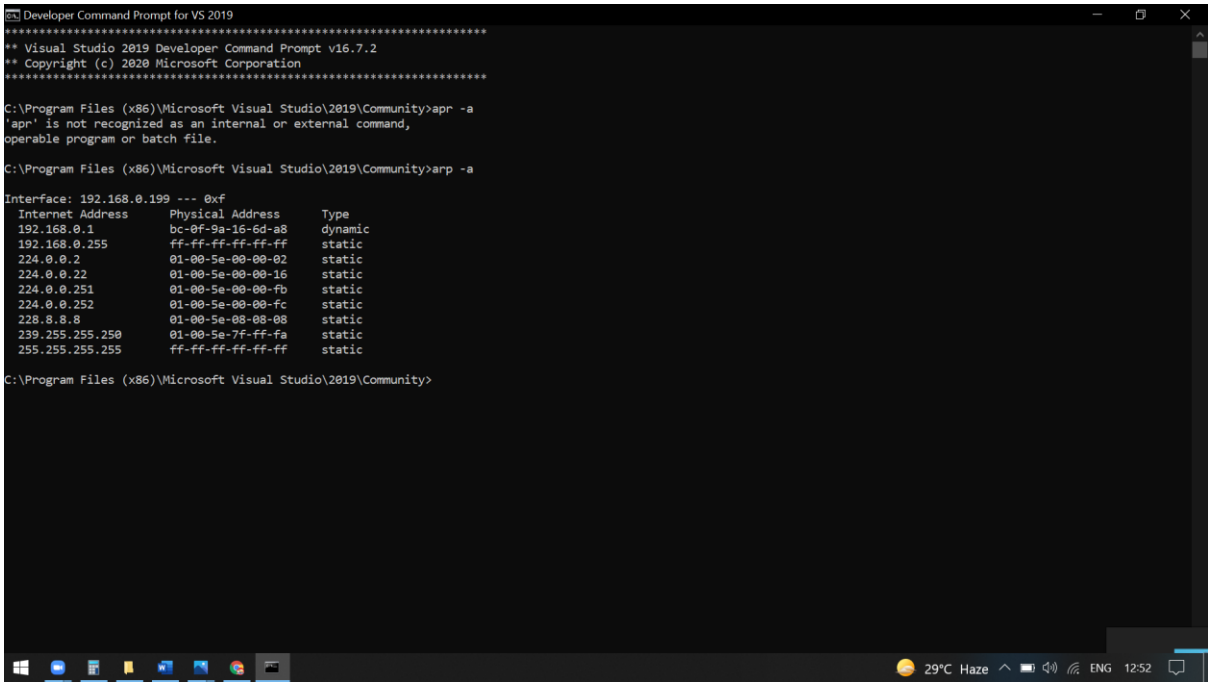
The Address Resolution Protocol (ARP) maps internet addresses to hardware addresses. TCP/IP uses ARP to collect and distribute the information for mapping

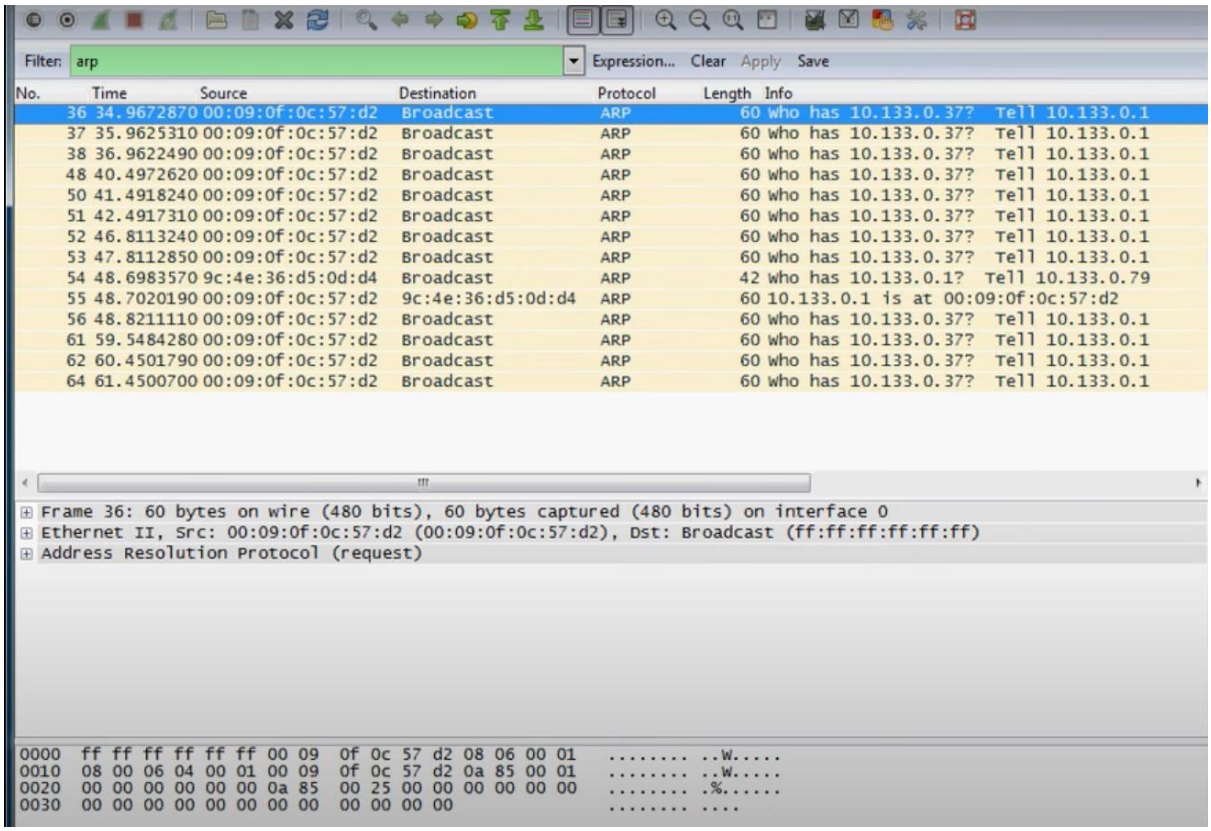
Start a Wireshark capture. Use arp -d to clear the ARP cache. Use ping <default gateway address> to ping the default gateway address. Use arp -a to view the ARP cache and confirm an entry has been added for the default gateway address.

```
arp -a
```

The output will look something like this:

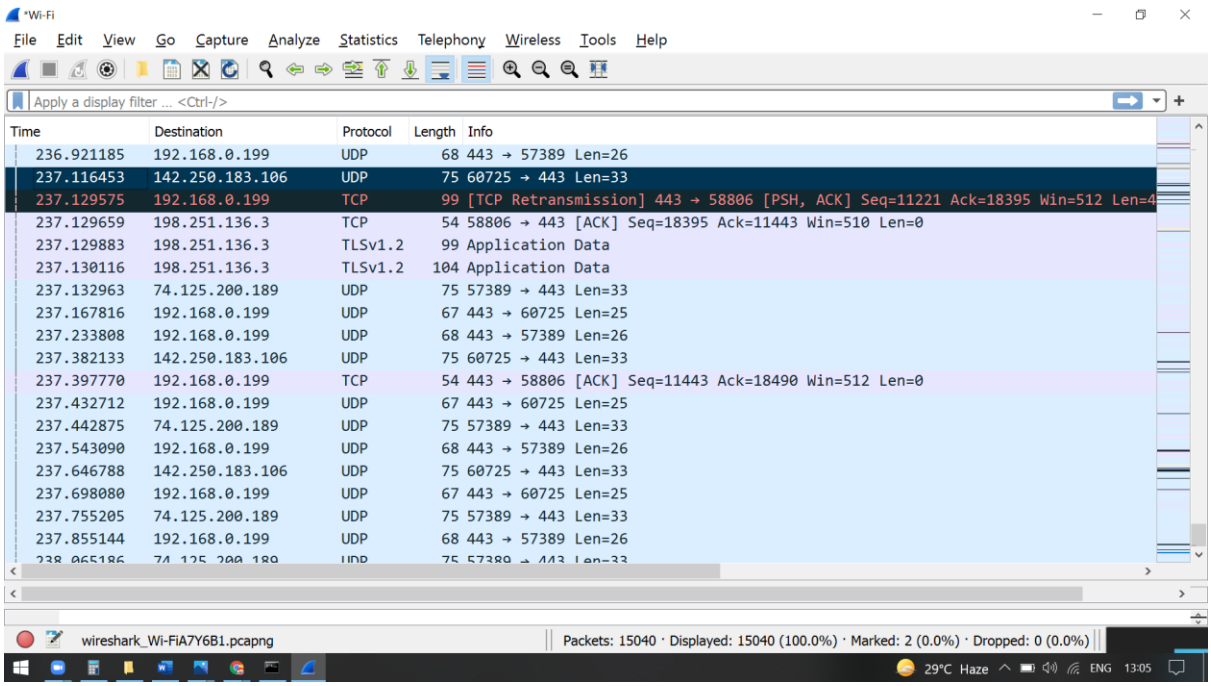
```
Internet Address      Physical Address

192.168.5.1           00-14-22-01-23-45
192.168.5.201         40-d4-48-cr-55-b8
192.168.5.202         00-14-22-01-23-45
```


Developer Command Prompt for VS 2019
** Visual Studio 2019 Developer Command Prompt v16.7.2
** Copyright (c) 2020 Microsoft Corporation
C:\Program Files (x86)\Microsoft Visual Studio\2019\Community>apr -a
'apr' is not recognized as an internal or external command,
operable program or batch file.
C:\Program Files (x86)\Microsoft Visual Studio\2019\Community>arp -a
Interface: 192.168.0.199 --- 0xf
Internet Address Physical Address Type
192.168.0.1 bc-0f-9a-16-6d-a8 dynamic
192.168.0.255 ff-ff-ff-ff-ff-ff static
224.0.0.2 01-00-5e-00-00-02 static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
228.8.8.8 01-00-5e-08-08-08 static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Program Files (x86)\Microsoft Visual Studio\2019\Community>
29°C Haze ENG 12:52


Filter: arp
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
36 34.9672870 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
37 35.9625310 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
38 36.9622490 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
48 40.4972620 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
50 41.4918240 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
51 42.4917310 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
52 46.8113240 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
53 47.8112850 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
54 48.6983570 9c:4e:36:d5:0d:d4 Broadcast ARP 42 Who has 10.133.0.1? Tell 10.133.0.79
55 48.7020190 00:09:0f:0c:57:d2 9c:4e:36:d5:0d:d4 ARP 60 10.133.0.1 is at 00:09:0f:0c:57:d2
56 48.8211110 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
61 59.5484280 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
62 60.4501790 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
64 61.4500700 00:09:0f:0c:57:d2 Broadcast ARP 60 Who has 10.133.0.37? Tell 10.133.0.1
Frame 36: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: 00:09:0f:0c:57:d2 (00:09:0f:0c:57:d2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 09 0f 0c 57 d2 08 06 00 01 ....W.....
0010 08 00 06 04 00 01 00 09 0f 0c 57 d2 0a 85 00 01 ....W.....
0020 00 00 00 00 00 00 0a 85 00 25 00 00 00 00 00 00 ..... .%.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 ....

There are several ways to mark and unmark packets. From the Edit menu you can select from the following:

- Mark/Unmark Packet toggles the marked state of a single packet. This option is also available in the packet list context menu.
- Mark All Displayed set the mark state of all displayed packets.
- Unmark All Displayed reset the mark state of all packets.

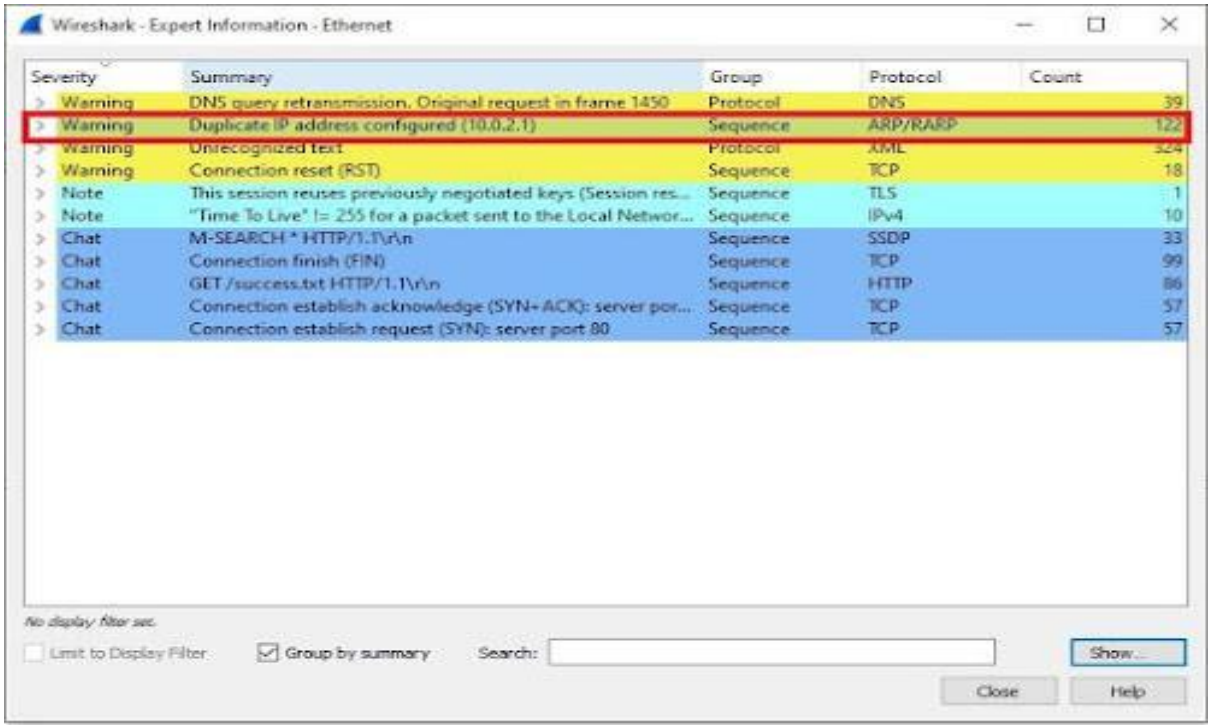


ARP Spoofing

- The ARP protocol was not designed for security, so it does not verify that a response to an ARP request really comes from an authorized party.
- It also lets hosts accept ARP responses even if they never sent out a request. This is a weak point in the ARP protocol, which opens the door to ARP spoofing attacks.
- An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices.

Detection:

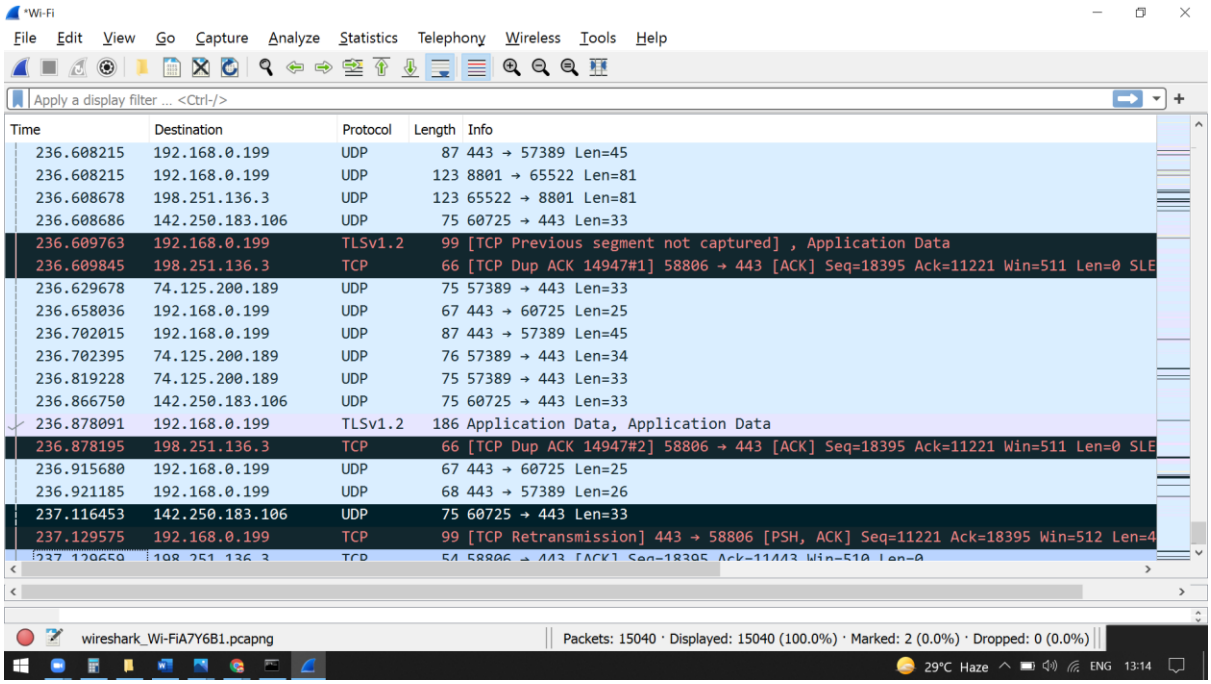
- Go to Analyze > Expert Information (Last Option as per v3.2.5).
- Sort the Protocol in ascending order, and you will see ARP/RARP if any ARP Attacks.
- You will see Warning as Severity, Duplicate IP Address... as Summary, and so on.



Delta Times :-

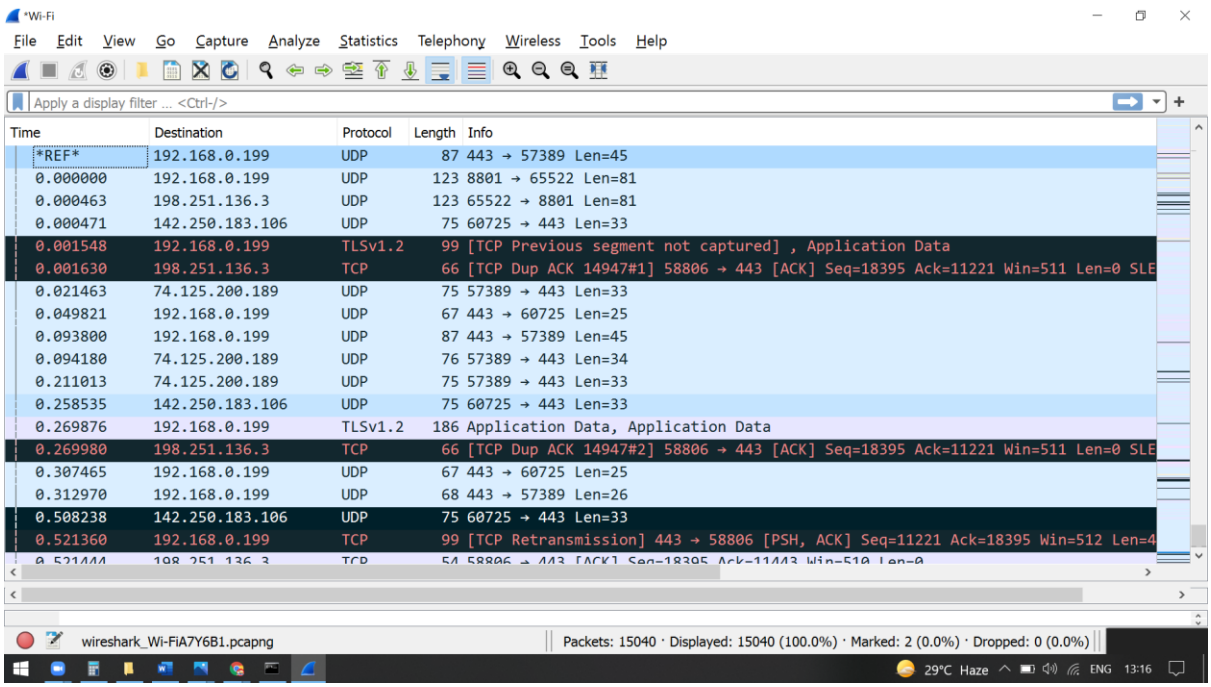
There is significant TCP Delta Times, and most of the packets are going to 192.168.0.136. In this example, it would be good to identify the remote systems that are serving packets to 192.168.0.136, in an attempt to understand why there is latency in the transmission of data

1. In Wireshark, press Ctrl + Shift + P (or select Edit > Preferences).
2. In the left panel, expand Protocols and select TCP.
3. Ensure Calculate conversation timestamps is checked.



Time references

To work with time references, choose one of the Time Reference items in the menu:[Edit] menu or from the pop-up menu of the “Packet List” pane. See Section 3.6, “The “Edit” Menu”. Set Time Reference (toggle) Toggles the time reference state of the currently selected packet to on or off.



Result:

Hence the study about installation and the basic commands of Wireshark is done.