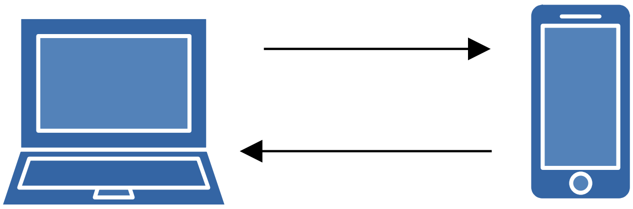
Basic Network Setup and Packet Analysis

1.Introduction:

This presents a basic network setup that i implemented recently. This network consists of a laptop and a mobile phone, with a virtual router hosted using Hostapd. Wireshark is used for monitoring and analyzing network traffic including protocols, packet addresses, and communcation details.



2.Network Setup:

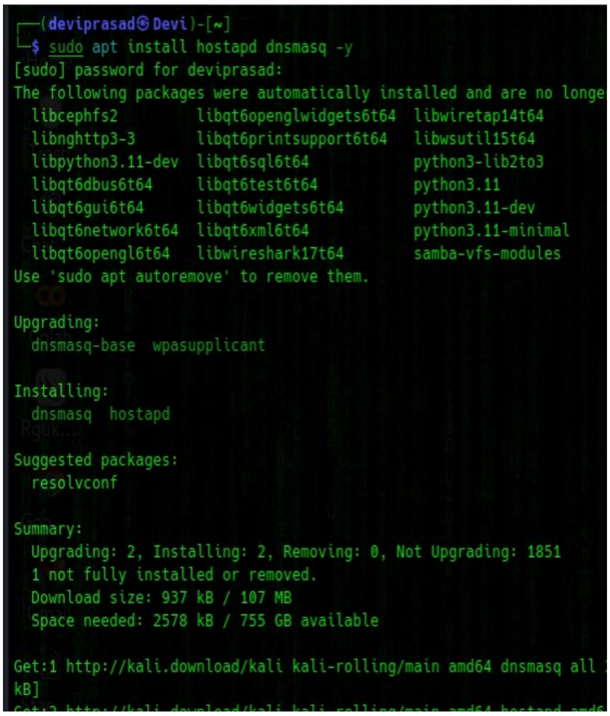
The network Setup using the following devices and tools:

-Laptop : Used as a host and main controller

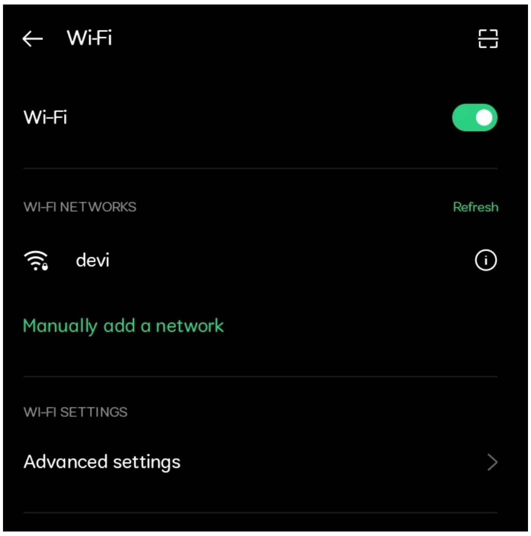
-Mobile Phone: Connected to the network as a client device

-Hostapd: A virtual router software usd for Creating the wifi network

-Wireshark: A packet analyzer tool used to capture network traffic



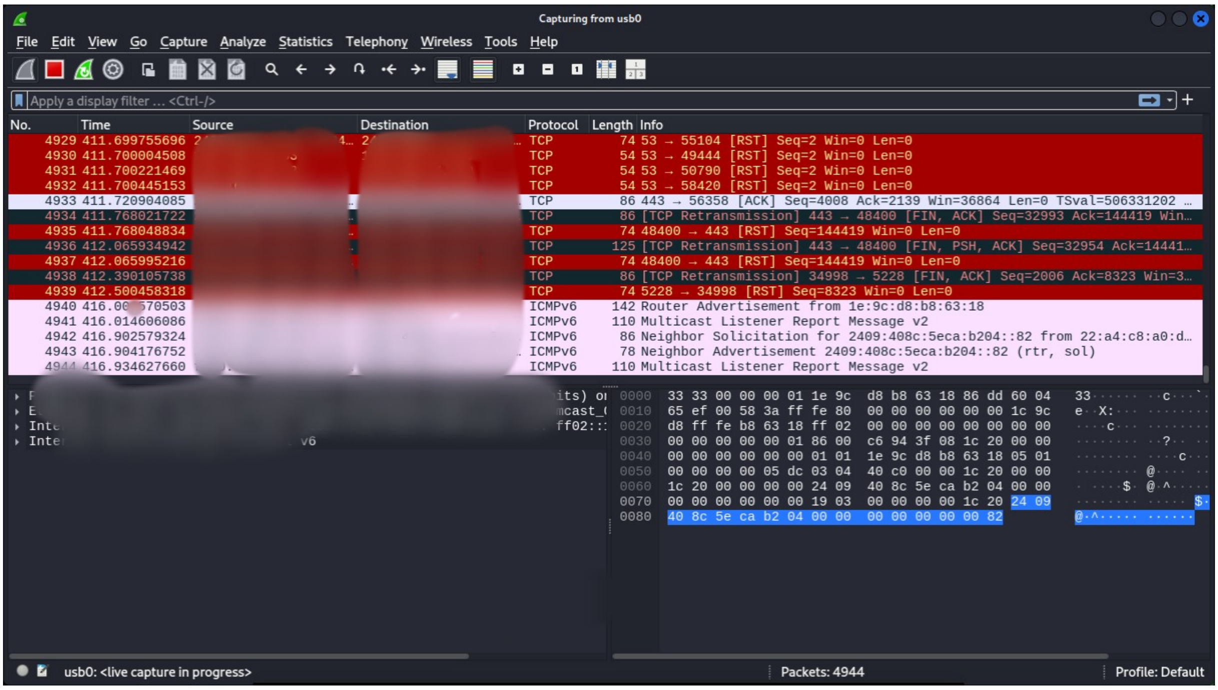
```
┌──(deviprasad㉿Devi)-[~]
└─$ sudo apt install hostapd dnsmasq -y
[sudo] password for deviprasad:
The following packages were automatically installed and are no longe
  libcephfs2          libqt6openglwidgets6t64  libwiretap14t64
  libnghttp3-3        libqt6printsupport6t64   libwsutil15t64
  libpython3.11-dev   libqt6sql6t64            python3-lib2to3
  libqt6dbus6t64      libqt6test6t64           python3.11
  libqt6gui6t64       libqt6widgets6t64        python3.11-dev
  libqt6network6t64   libqt6xml6t64            python3.11-minimal
  libqt6opengl6t64    libwireshark17t64        samba-vfs-modules
Use 'sudo apt autoremove' to remove them.

Upgrading:
  dnsmasq-base  wpasupplicant

Installing:
  dnsmasq  hostapd

Suggested packages:
  resolvconf

Summary:
  Upgrading: 2, Installing: 2, Removing: 0, Not Upgrading: 1851
  1 not fully installed or removed.
  Download size: 937 kB / 107 MB
  Space needed: 2578 kB / 755 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 dnsmasq all
kB]
```



The network was configured with the laptop hosting the virtual router , allowing the mobile connect it via Wi-Fi. This setup facilitated the monitoring of communication between the devices

Packet Analysis:

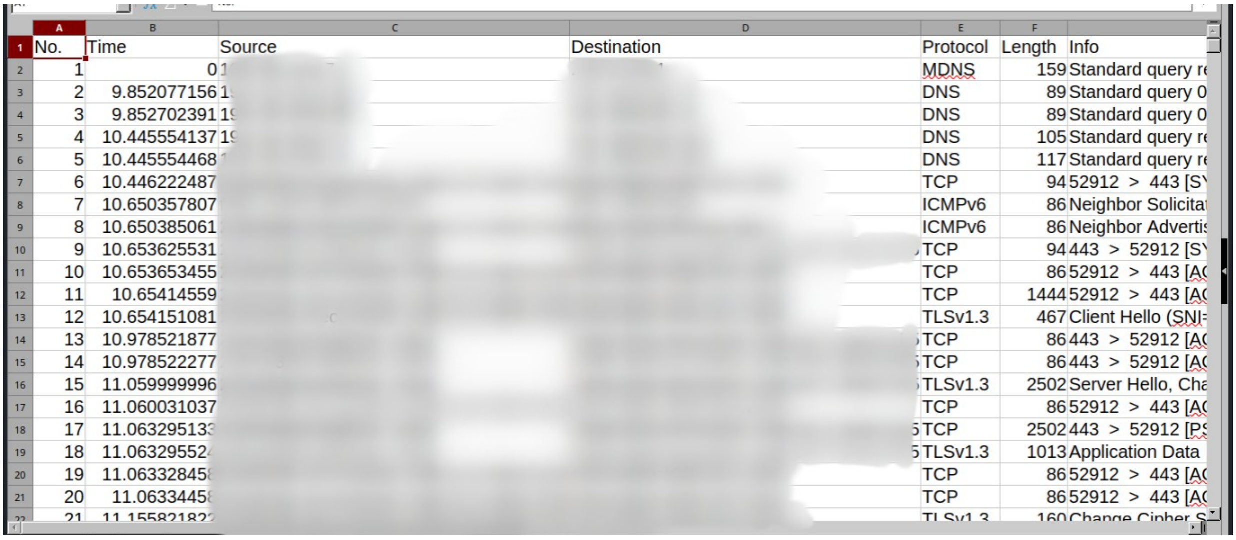
Wireshark was used to capture and analyze packets from the network. The analysis provided insights into the following aspects:
-Source and destination ip address
-Protocols being used (e.g.,TCP , UDP)
-Packet sizes and timing
-Network performance and any detected issues


Capturing from usb0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source      Destination  Protocol Length Info
4929 411.699755696 [redacted]               TCP       74 53 → 55104 [RST] Seq=2 Win=0 Len=0
4930 411.700004508                          TCP       54 53 → 49444 [RST] Seq=2 Win=0 Len=0
4931 411.700221469                          TCP       54 53 → 50790 [RST] Seq=2 Win=0 Len=0
4932 411.700445153                          TCP       54 53 → 58420 [RST] Seq=2 Win=0 Len=0
4933 411.720904085                          TCP       86 443 → 56358 [ACK] Seq=4008 Ack=2139 Win=36864 Len=0 TSval=506331202 …
4934 411.768021722                          TCP       86 [TCP Retransmission] 443 → 48400 [FIN, ACK] Seq=32993 Ack=144419 Win…
4935 411.768048834                          TCP       74 48400 → 443 [RST] Seq=144419 Win=0 Len=0
4936 412.065934942                          TCP      125 [TCP Retransmission] 443 → 48400 [FIN, PSH, ACK] Seq=32954 Ack=14441…
4937 412.065995216                          TCP       74 48400 → 443 [RST] Seq=144419 Win=0 Len=0
4938 412.390105738                          TCP       86 [TCP Retransmission] 34998 → 5228 [FIN, ACK] Seq=2006 Ack=8323 Win=3…
4939 412.500458318                          TCP       74 5228 → 34998 [RST] Seq=8323 Win=0 Len=0
4940 416.00 570503                          ICMPv6   142 Router Advertisement from 1e:9c:d8:b8:63:18
4941 416.014606086                          ICMPv6   110 Multicast Listener Report Message v2
4942 416.902579324                          ICMPv6    86 Neighbor Solicitation for 2409:408c:5eca:b204::82 from 22:a4:c8:a0:d…
4943 416.904176752                          ICMPv6    78 Neighbor Advertisement 2409:408c:5eca:b204::82 (rtr, sol)
4944 416.934627660                          ICMPv6   110 Multicast Listener Report Message v2
```

```
▸ F [redacted] its) o
▸ E                     mcast_(
▸ Inte                  ff02:::
▸ Inte              v6

0000  33 33 00 00 00 01 1e 9c  d8 b8 63 18 86 dd 60 04   33······ ··c···`·
0010  65 ef 00 58 3a ff fe 80  00 00 00 00 00 00 1c 9c   e··X:··· ········
0020  d8 ff fe b8 63 18 ff 02  00 00 00 00 00 00 00 00   ····c··· ········
0030  00 00 00 00 00 01 86 00  c6 94 3f 08 1c 20 00 00   ········ ··?·· ··
0040  00 00 00 00 00 00 01 01  1e 9c d8 b8 63 18 05 01   ········ ····c···
0050  00 00 00 00 05 dc 03 04  40 c0 00 00 1c 20 00 00   ········ @····· ··
0060  1c 20 00 00 00 00 24 09  40 8c 5e ca b2 04 00 00   · ····$· @·^·····
0070  00 00 00 00 00 00 19 03  00 00 00 00 1c 20 24 09   ········ ······$·
0080  40 8c 5e ca b2 04 00 00  00 00 00 00 00 82         @·^····· ······
```

usb0: <live capture in progress>
Packets: 4944
Profile: Default



No.	Time	Source	Destination	Protocol	Length	Info
1	0	[redacted]	[redacted]	MDNS	159	Standard query re
2	9.852077156	[redacted]	[redacted]	DNS	89	Standard query 0
3	9.852702391	[redacted]	[redacted]	DNS	89	Standard query 0
4	10.445554137	[redacted]	[redacted]	DNS	105	Standard query re
5	10.445554468	[redacted]	[redacted]	DNS	117	Standard query re
6	10.446222487	[redacted]	[redacted]	TCP	94	52912 > 443 [SY
7	10.650357807	[redacted]	[redacted]	ICMPv6	86	Neighbor Solicitat
8	10.650385061	[redacted]	[redacted]	ICMPv6	86	Neighbor Advertis
9	10.653625531	[redacted]	[redacted]	TCP	94	443 > 52912 [SY
10	10.653653455	[redacted]	[redacted]	TCP	86	52912 > 443 [AC
11	10.65414559	[redacted]	[redacted]	TCP	1444	52912 > 443 [AC
12	10.654151081	[redacted]	[redacted]	TLSv1.3	467	Client Hello (SNI=
13	10.978521877	[redacted]	[redacted]	TCP	86	443 > 52912 [AC
14	10.978522277	[redacted]	[redacted]	TCP	86	443 > 52912 [AC
15	11.059999996	[redacted]	[redacted]	TLSv1.3	2502	Server Hello, Cha
16	11.060031037	[redacted]	[redacted]	TCP	86	52912 > 443 [AC
17	11.06329513	[redacted]	[redacted]	TCP	2502	443 > 52912 [PS
18	11.06329552	[redacted]	[redacted]	TLSv1.3	1013	Application Data
19	11.06332845	[redacted]	[redacted]	TCP	86	52912 > 443 [AC
20	11.0633445	[redacted]	[redacted]	TCP	86	52912 > 443 [AC
21	11.15582182	[redacted]	[redacted]	TLSv1.3	160	Change Cipher S

4. Conclusion:

The project successfully demonstrated the setup of a basic network using a laptop and mobile phone, with the use of hostapd to create a virtual router. Wireshark provided valuable insights into packet-level details and network traffic analysis. This experiment contributes to a deeper understanding of networking concepts and packet analysis, which are essential skills in the field of cybersecurity.

If I made any mistakes or if you want to suggest something regarding this please feel free to contact me.
-Deviprasad