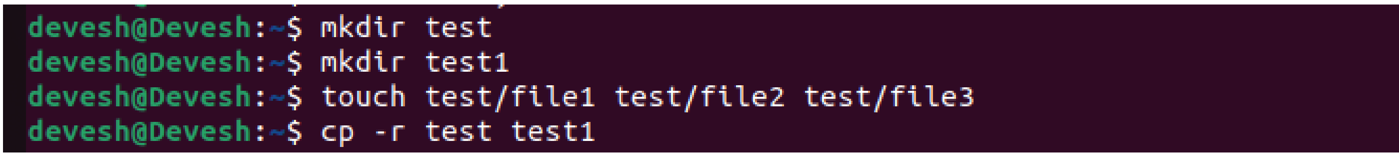
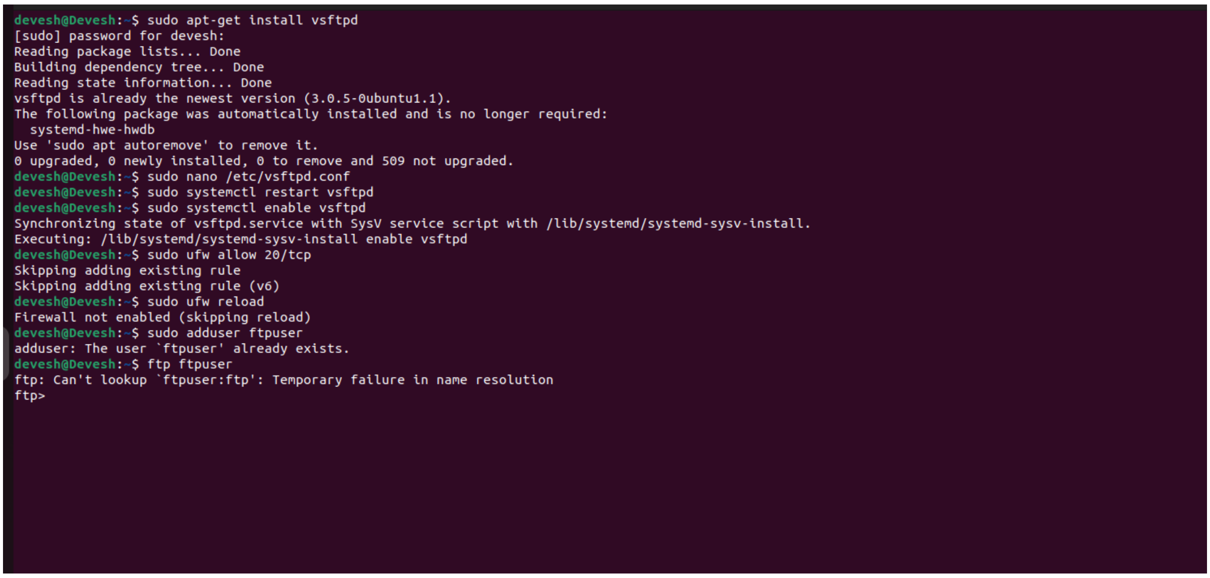
Networking Training Program (Module 1 & 2)

1. Copying a Folder with Multiple Files:



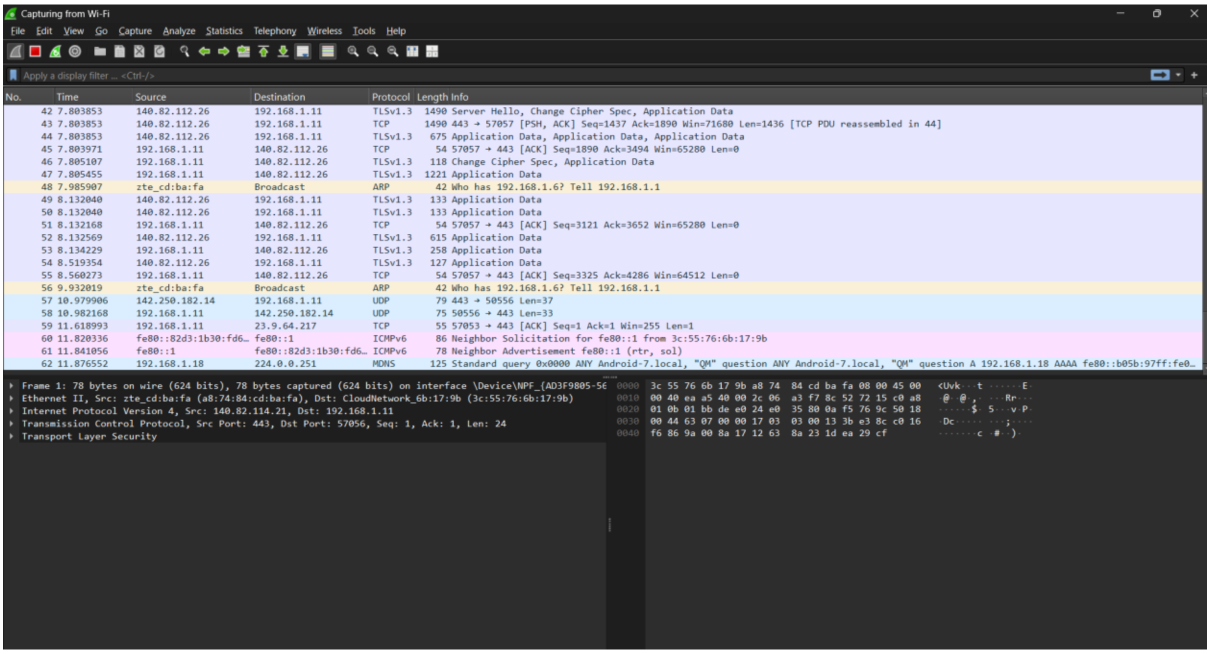
```
devesh@Devesh:~$ mkdir test
devesh@Devesh:~$ mkdir test1
devesh@Devesh:~$ touch test/file1 test/file2 test/file3
devesh@Devesh:~$ cp -r test test1
```

2. Hosting an FTP and SFTP Server; Performing PUT and GET Operations



```
devesh@Devesh:~$ sudo apt-get install vsftpd
[sudo] password for devesh:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.5-0ubuntu1.1).
The following package was automatically installed and is no longer required:
  systemd-hwe-hwdb
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 509 not upgraded.
devesh@Devesh:~$ sudo nano /etc/vsftpd.conf
devesh@Devesh:~$ sudo systemctl restart vsftpd
devesh@Devesh:~$ sudo systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
devesh@Devesh:~$ sudo ufw allow 20/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
devesh@Devesh:~$ sudo ufw reload
Firewall not enabled (skipping reload)
devesh@Devesh:~$ sudo adduser ftpuser
adduser: The user `ftpuser' already exists.
devesh@Devesh:~$ ftp ftpuser
ftp: Can't lookup `ftpuser:ftp': Temporary failure in name resolution
ftp>
```

3. Capturing packets using wireshark

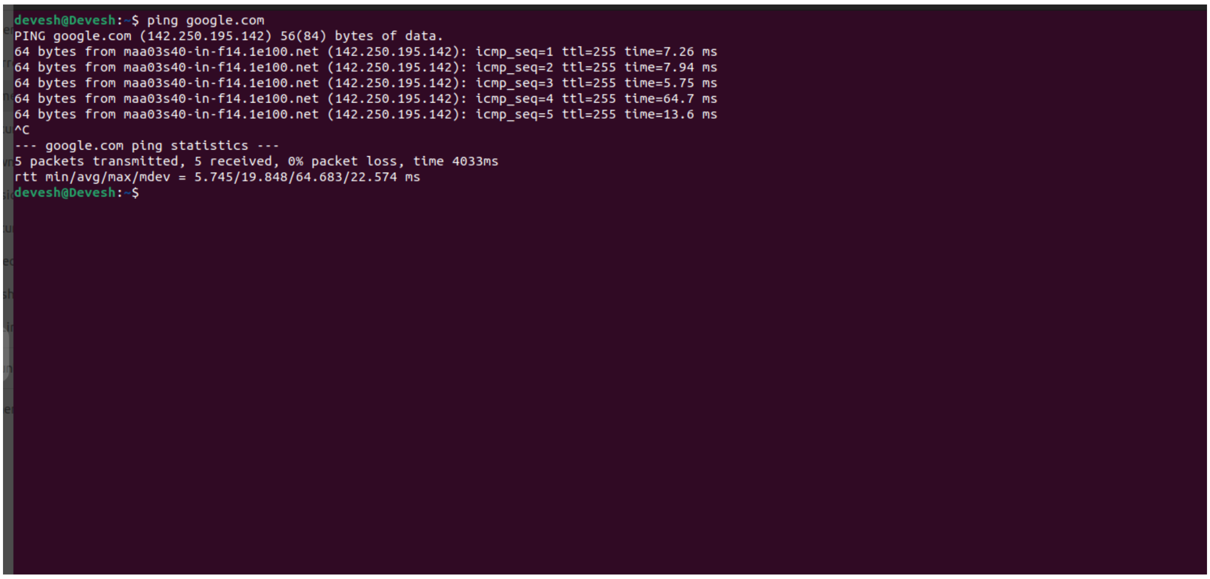

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
42	7.803853	140.82.112.26	192.168.1.11	TLSv1.3	1490	Server Hello, Change Cipher Spec, Application Data
43	7.803853	140.82.112.26	192.168.1.11	TCP	1490	443 → 57057 [PSH, ACK] Seq=1437 Ack=1890 Win=71680 Len=1436 [TCP PDU reassembled in 44]
44	7.803853	140.82.112.26	192.168.1.11	TLSv1.3	675	Application Data, Application Data, Application Data
45	7.803971	192.168.1.11	140.82.112.26	TCP	54	57057 → 443 [ACK] Seq=1890 Ack=3494 Win=65280 Len=0
46	7.805107	192.168.1.11	140.82.112.26	TLSv1.3	118	Change Cipher Spec, Application Data
47	7.805455	192.168.1.11	140.82.112.26	TLSv1.3	1221	Application Data
48	7.985907	zte_cd:ba:fa	Broadcast	ARP	42	Who has 192.168.1.6? Tell 192.168.1.1
49	8.132040	140.82.112.26	192.168.1.11	TLSv1.3	133	Application Data
50	8.132040	140.82.112.26	192.168.1.11	TLSv1.3	133	Application Data
51	8.132168	192.168.1.11	140.82.112.26	TCP	54	57057 → 443 [ACK] Seq=3121 Ack=3652 Win=65280 Len=0
52	8.132569	140.82.112.26	192.168.1.11	TLSv1.3	615	Application Data
53	8.134229	192.168.1.11	140.82.112.26	TLSv1.3	258	Application Data
54	8.519354	140.82.112.26	192.168.1.11	TLSv1.3	127	Application Data
55	8.560273	192.168.1.11	140.82.112.26	TCP	54	57057 → 443 [ACK] Seq=3325 Ack=4286 Win=64512 Len=0
56	9.932019	zte_cd:ba:fa	Broadcast	ARP	42	Who has 192.168.1.6? Tell 192.168.1.1
57	10.979906	142.250.182.14	192.168.1.11	UDP	79	443 → 50556 Len=37
58	10.982168	192.168.1.11	142.250.182.14	UDP	75	50556 → 443 Len=33
59	11.618993	192.168.1.11	23.9.64.217	TCP	55	57053 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
60	11.820336	fe80::82d3:1b30:fd6…	fe80::1	ICMPv6	86	Neighbor Solicitation for fe80::1 from 3c:55:76:6b:17:9b
61	11.841056	fe80::1	fe80::82d3:1b30:fd6…	ICMPv6	78	Neighbor Advertisement fe80::1 (rtr, sol)
62	11.876552	192.168.1.18	224.0.0.251	MDNS	125	Standard query 0x0000 ANY Android-7.local, "QM" question ANY Android-7.local, "QM" question A 192.168.1.18 AAAA fe80::b05b:97ff:fe0…

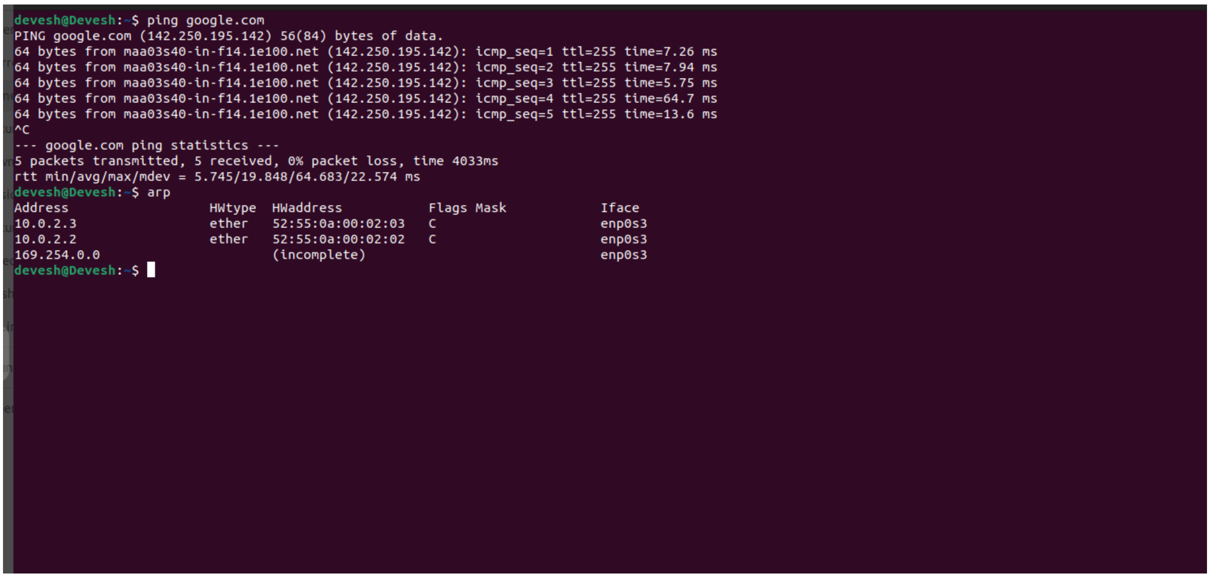
```
▸ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{AD3F9805-5E
▸ Ethernet II, Src: zte_cd:ba:fa (a8:74:84:cd:ba:fa), Dst: CloudNetwork_6b:17:9b (3c:55:76:6b:17:9b)
▸ Internet Protocol Version 4, Src: 140.82.114.21, Dst: 192.168.1.11
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 57056, Seq: 1, Ack: 1, Len: 24
▸ Transport Layer Security
```

```
0000  3c 55 76 6b 17 9b a8 74  84 cd ba fa 08 00 45 00   <Uvk···t ······E·
0010  00 40 ea a5 40 00 2c 06  a3 f7 8c 52 72 15 c0 a8   ·@··@·,· ···Rr···
0020  01 0b 01 bb de e0 24 e0  35 80 0a f5 76 9c 50 18   ······$· 5···v·P·
0030  00 44 63 07 00 00 17 03  03 00 13 3b e3 8c c0 16   ·Dc····· ···;····
0040  f6 86 9a 00 8a 17 12 63  8a 23 1d ea 29 cf         ·······c ·#··)·
```

4. Understanding Linux Utility Commands (ping, arp)



```
devesh@Devesh:~$ ping google.com
PING google.com (142.250.195.142) 56(84) bytes of data.
64 bytes from maa03s40-in-f14.1e100.net (142.250.195.142): icmp_seq=1 ttl=255 time=7.26 ms
64 bytes from maa03s40-in-f14.1e100.net (142.250.195.142): icmp_seq=2 ttl=255 time=7.94 ms
64 bytes from maa03s40-in-f14.1e100.net (142.250.195.142): icmp_seq=3 ttl=255 time=5.75 ms
64 bytes from maa03s40-in-f14.1e100.net (142.250.195.142): icmp_seq=4 ttl=255 time=64.7 ms
64 bytes from maa03s40-in-f14.1e100.net (142.250.195.142): icmp_seq=5 ttl=255 time=13.6 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4033ms
rtt min/avg/max/mdev = 5.745/19.848/64.683/22.574 ms
devesh@Devesh:~$
```



```
devesh@Devesh:~$ ping google.com
PING google.com (142.250.195.142) 56(84) bytes of data.
64 bytes from maa03s40-in-f14.1e100.net (142.250.195.142): icmp_seq=1 ttl=255 time=7.26 ms
64 bytes from maa03s40-in-f14.1e100.net (142.250.195.142): icmp_seq=2 ttl=255 time=7.94 ms
64 bytes from maa03s40-in-f14.1e100.net (142.250.195.142): icmp_seq=3 ttl=255 time=5.75 ms
64 bytes from maa03s40-in-f14.1e100.net (142.250.195.142): icmp_seq=4 ttl=255 time=64.7 ms
64 bytes from maa03s40-in-f14.1e100.net (142.250.195.142): icmp_seq=5 ttl=255 time=13.6 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4033ms
rtt min/avg/max/mdev = 5.745/19.848/64.683/22.574 ms
devesh@Devesh:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                 ether   52:55:0a:00:02:03   C                     enp0s3
10.0.2.2                 ether   52:55:0a:00:02:02   C                     enp0s3
169.254.0.0                      (incomplete)                              enp0s3
devesh@Devesh:~$ 
```

5. Effects of Duplicate IP Addresses in a Network

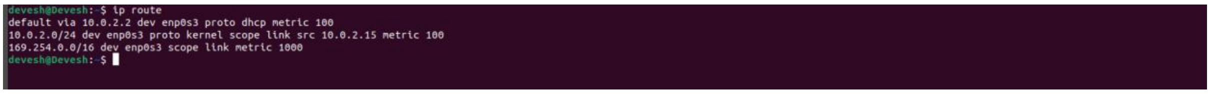
- Leads to highly unstable network.
- Packet flow is disrupted. Some packets may be delivered to one machine and other packets maybe delivered to others.
- It leads to the collapse of the network infrastructure.

6. Remote connections

- Remote desktop is a windows feature that allows us to remotely access a device and perform anything on it.
- SSH is a technique using which we can remotely log on to a computer and execute commands on it.

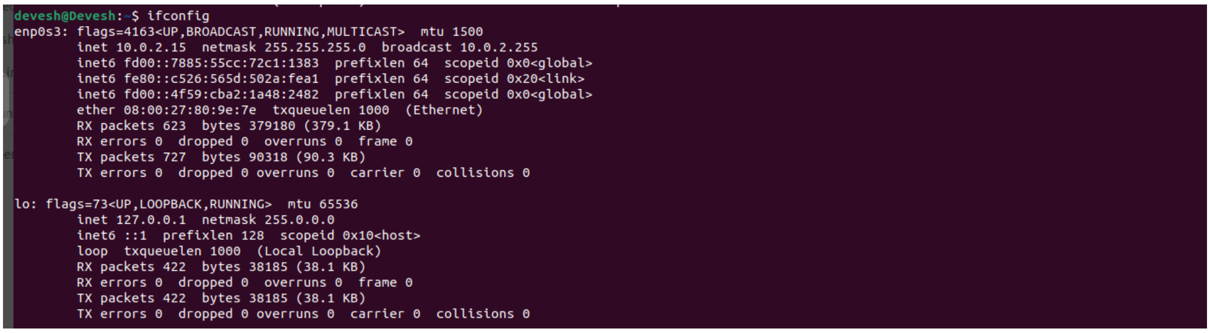
7. Default Gateway Reachable or not.

- Try pinging the default gateway
- Otherwise use ip route to find the default gateway if it is unknown.
- Check if a default gateway is properly configured to the device.



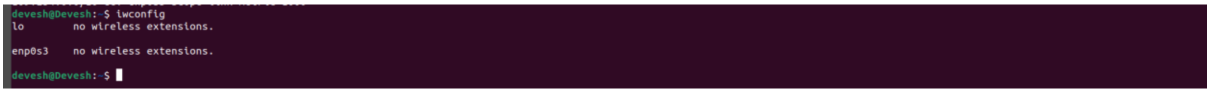
```
devesh@Devesh:~$ ip route
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
devesh@Devesh:~$ 
```

8. ifconfig iwconfig.



```
devesh@Devesh:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd00::7885:55cc:72c1:1383  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::c526:565d:502a:fea1  prefixlen 64  scopeid 0x20<link>
        inet6 fd00::4f59:cba2:1a48:2482  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:80:9e:7e  txqueuelen 1000  (Ethernet)
        RX packets 623  bytes 379180 (379.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 727  bytes 90318 (90.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 422  bytes 38185 (38.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 422  bytes 38185 (38.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
devesh@Devesh:~$ iwconfig
lo        no wireless extensions.

enp0s3    no wireless extensions.

devesh@Devesh:~$ 
```

9. Logging into a Home Router and Checking Connected Devices

- Go into the given ip address
- Provide proper user name and password
- Inside the LAN, we can see the no. of devices connected and the ip address assigned to them.

10. How a DHCP Server Assigns IP Addresses

DHCP Server used DORA process

- Discover
- Offer
- Request
- Acknowledgement

First the device broadcasts it's request to find DHCP server

Then the server offers it's services.

Device requests the DHCP for an available IP

Ip address is given and acknowledged.

11. Connecting to a Remote Machine via SSH and Telnet

- SSH stand for secure shell and it's a secure way to log on remotely to a system and execute commands.
- Telnet is an unsecure way of doing the same.