Post-Lab 1: Wireshark and your local network

What to submit?

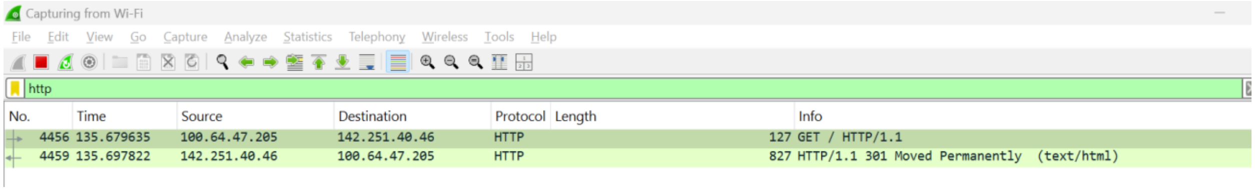
Please use this document as a template, add your responses directly, and export it as a PDF to Gradescope. For this lab, each student should submit their own report.

Name: Rajan Verma

Student ID:A69028626

C: Wireshark Practice

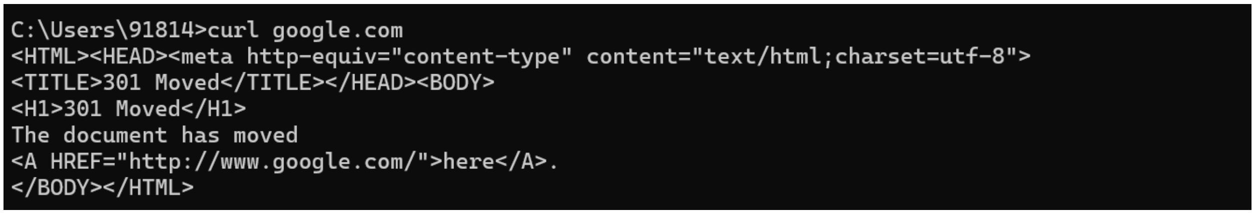
Show a screenshot of your captured HTTP request/response:


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

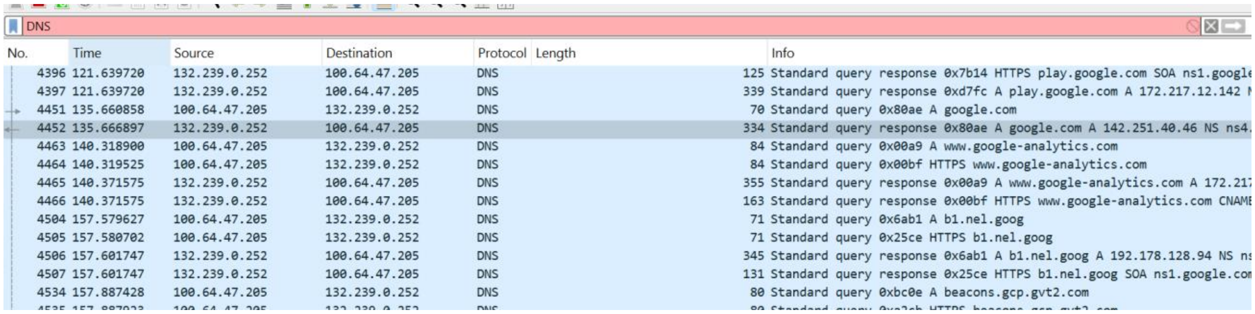
No.	Time	Source	Destination	Protocol	Length	Info
4456	135.679635	100.64.47.205	142.251.40.46	HTTP	127	GET / HTTP/1.1
4459	135.697822	142.251.40.46	100.64.47.205	HTTP	827	HTTP/1.1 301 Moved Permanently (text/html)

from cmd prompt :



```
C:\Users\91814>curl google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
```

Show a screenshot of your captured DNS request/response:

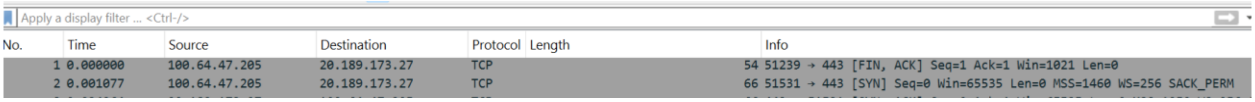


DNS

No.	Time	Source	Destination	Protocol	Length	Info
4396	121.639720	132.239.0.252	100.64.47.205	DNS	125	Standard query response 0x7b14 HTTPS play.google.com SOA ns1.google
4397	121.639720	132.239.0.252	100.64.47.205	DNS	339	Standard query response 0xd7fc A play.google.com A 172.217.12.142
4451	135.660858	100.64.47.205	132.239.0.252	DNS	70	Standard query 0x80ae A google.com
4452	135.666897	132.239.0.252	100.64.47.205	DNS	334	Standard query response 0x80ae A google.com A 142.251.40.46 NS ns4.
4463	140.318900	100.64.47.205	132.239.0.252	DNS	84	Standard query 0x00a9 A www.google-analytics.com
4464	140.319525	100.64.47.205	132.239.0.252	DNS	84	Standard query 0x00bf HTTPS www.google-analytics.com
4465	140.371575	132.239.0.252	100.64.47.205	DNS	355	Standard query response 0x00a9 A www.google-analytics.com A 172.217
4466	140.371575	132.239.0.252	100.64.47.205	DNS	163	Standard query response 0x00bf HTTPS www.google-analytics.com CNAME
4504	157.579627	100.64.47.205	132.239.0.252	DNS	71	Standard query 0x6ab1 A b1.nel.goog
4505	157.580702	100.64.47.205	132.239.0.252	DNS	71	Standard query 0x25ce HTTPS b1.nel.goog
4506	157.601747	132.239.0.252	100.64.47.205	DNS	345	Standard query response 0x6ab1 A b1.nel.goog A 192.178.128.94 NS ns
4507	157.601747	132.239.0.252	100.64.47.205	DNS	131	Standard query response 0x25ce HTTPS b1.nel.goog SOA ns1.google.com
4534	157.887428	100.64.47.205	132.239.0.252	DNS	80	Standard query 0xbc0e A beacons.gcp.gvt2.com
4535	157.887923	100.64.47.205	132.239.0.252	DNS	80	Standard query 0xa2cb HTTPS beacons.gcp.gvt2.com

D: Inspect Ping Traffic

Show a screenshot of your captured *ping* traffic:



```
No.   Time        Source          Destination     Protocol Length   Info
    1 0.000000    100.64.47.205   20.189.173.27   TCP          54 51239 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1021 Len=0
    2 0.001077    100.64.47.205   20.189.173.27   TCP          66 51531 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
```

What does “ICMP” stand for?

Internet Control Message Protocol : sends error messages when data transmission fails

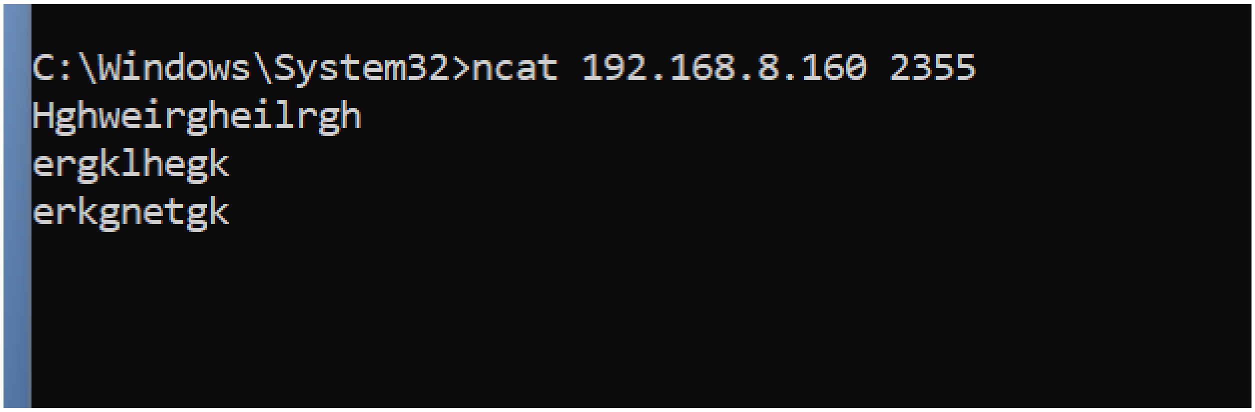
For one of your ping packets, start from the PHY and list each of the layers that were used to send the packet, and which technology was used.

- **Ping is initiated.**
- **Phy Layer : Wifi handles physical layer.**
- **Datalink Layer : Wifi and Ethernet.**
- **Network Layer : Ipv4-v6, TCP IP Protocol.**
- **Transport Layer : ICMP**

E: Investigate Intentional Traffic

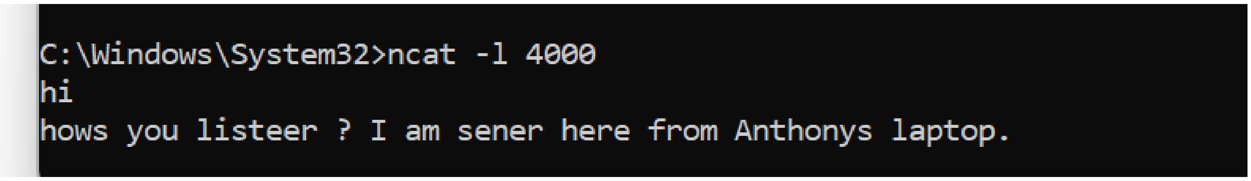
Show a screenshot of your captured *netcat* traffic from both you as a listener and as a sender. Clearly document which case is which.

As a Sender :

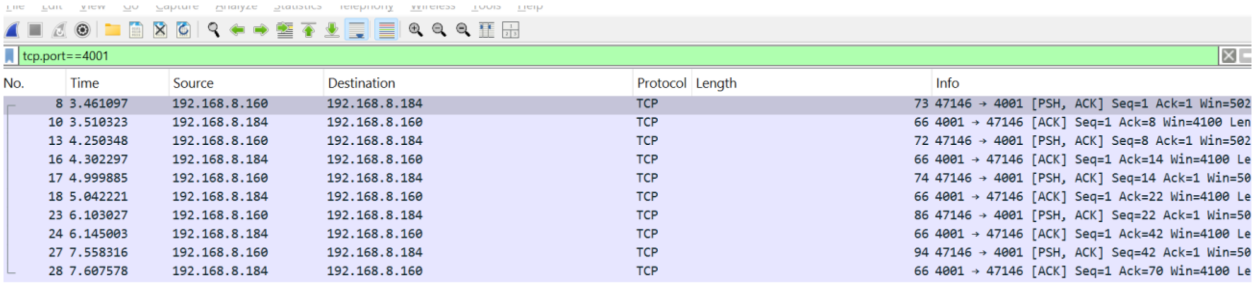


```
C:\Windows\System32>ncat 192.168.8.160 2355
Hghweirgheilrgh
ergklhegk
erkgnetgk
```

As a Reciever :



```
C:\Windows\System32>ncat -l 4000
hi
hows you listeer ? I am sener here from Anthonys laptop.
```



```
tcp.port==4001
```

No.	Time	Source	Destination	Protocol	Length	Info
8	3.461097	192.168.8.160	192.168.8.184	TCP	73	47146 → 4001 [PSH, ACK] Seq=1 Ack=1 Win=502
10	3.510323	192.168.8.184	192.168.8.160	TCP	66	4001 → 47146 [ACK] Seq=1 Ack=8 Win=4100 Len
13	4.250348	192.168.8.160	192.168.8.184	TCP	72	47146 → 4001 [PSH, ACK] Seq=8 Ack=1 Win=502
16	4.302297	192.168.8.184	192.168.8.160	TCP	66	4001 → 47146 [ACK] Seq=1 Ack=14 Win=4100 Le
17	4.999885	192.168.8.160	192.168.8.184	TCP	74	47146 → 4001 [PSH, ACK] Seq=14 Ack=1 Win=50
18	5.042221	192.168.8.184	192.168.8.160	TCP	66	4001 → 47146 [ACK] Seq=1 Ack=22 Win=4100 Le
23	6.103027	192.168.8.160	192.168.8.184	TCP	86	47146 → 4001 [PSH, ACK] Seq=22 Ack=1 Win=50
24	6.145003	192.168.8.184	192.168.8.160	TCP	66	4001 → 47146 [ACK] Seq=1 Ack=42 Win=4100 Le
27	7.558316	192.168.8.160	192.168.8.184	TCP	94	47146 → 4001 [PSH, ACK] Seq=42 Ack=1 Win=50
28	7.607578	192.168.8.184	192.168.8.160	TCP	66	4001 → 47146 [ACK] Seq=1 Ack=70 Win=4100 Le

Can you see other *netcat* traffic from other students in the class? Why or why not?

I cant see from other students apart from Anthony since they have left. If others students were here and connected then it would show up on the wireshark.

Imagine you were having a *netcat* conversation with a friend at George Mason. Besides you and your friend, who else could see the contents of your conversation?

Yes the packets are visible as a TCP protocol data. Then we need to convert the ASCII codes to make it human readable. Netcat doesnt encrypt so spying or snooping or hearing is easily possible.

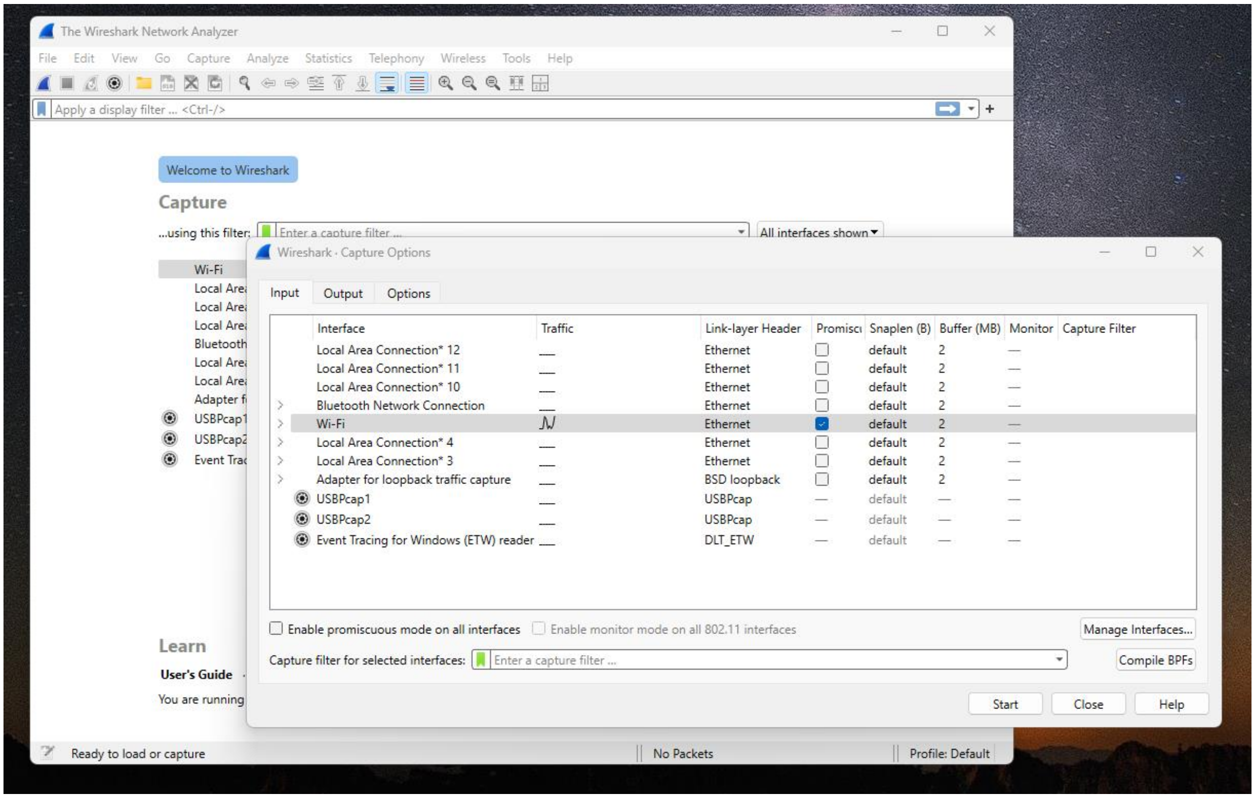
F: Discover WiFi Networks Around You

What is the name of the WiFi network we set up?

tock_tutorial

What are the types of probe packets that you see?

I tried to install npcap and with monitor mode enabled but somehow in wireshark even in administer mode I get greyed out at monitor mode for the Wifi :



	Interface	Traffic	Link-layer Header	Promiscı	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
	Local Area Connection* 12	___	Ethernet	☐	default	2	—	
	Local Area Connection* 11	___	Ethernet	☐	default	2	—	
	Local Area Connection* 10	___	Ethernet	☐	default	2	—	
>	Bluetooth Network Connection	___	Ethernet	☐	default	2	—	
>	Wi-Fi		Ethernet	☑	default	2	—	
>	Local Area Connection* 4	___	Ethernet	☐	default	2	—	
>	Local Area Connection* 3	___	Ethernet	☐	default	2	—	
>	Adapter for loopback traffic capture	___	BSD loopback	☐	default	2	—	
	USBPcap1	___	USBPcap	—	default	—	—	
	USBPcap2	___	USBPcap	—	default	—	—	
	Event Tracing for Windows (ETW) reader	___	DLT_ETW	—	default	—	—	

☐ Enable promiscuous mode on all interfaces ☐ Enable monitor mode on all 802.11 interfaces

Capture filter for selected interfaces: Enter a capture filter ...

What I see is

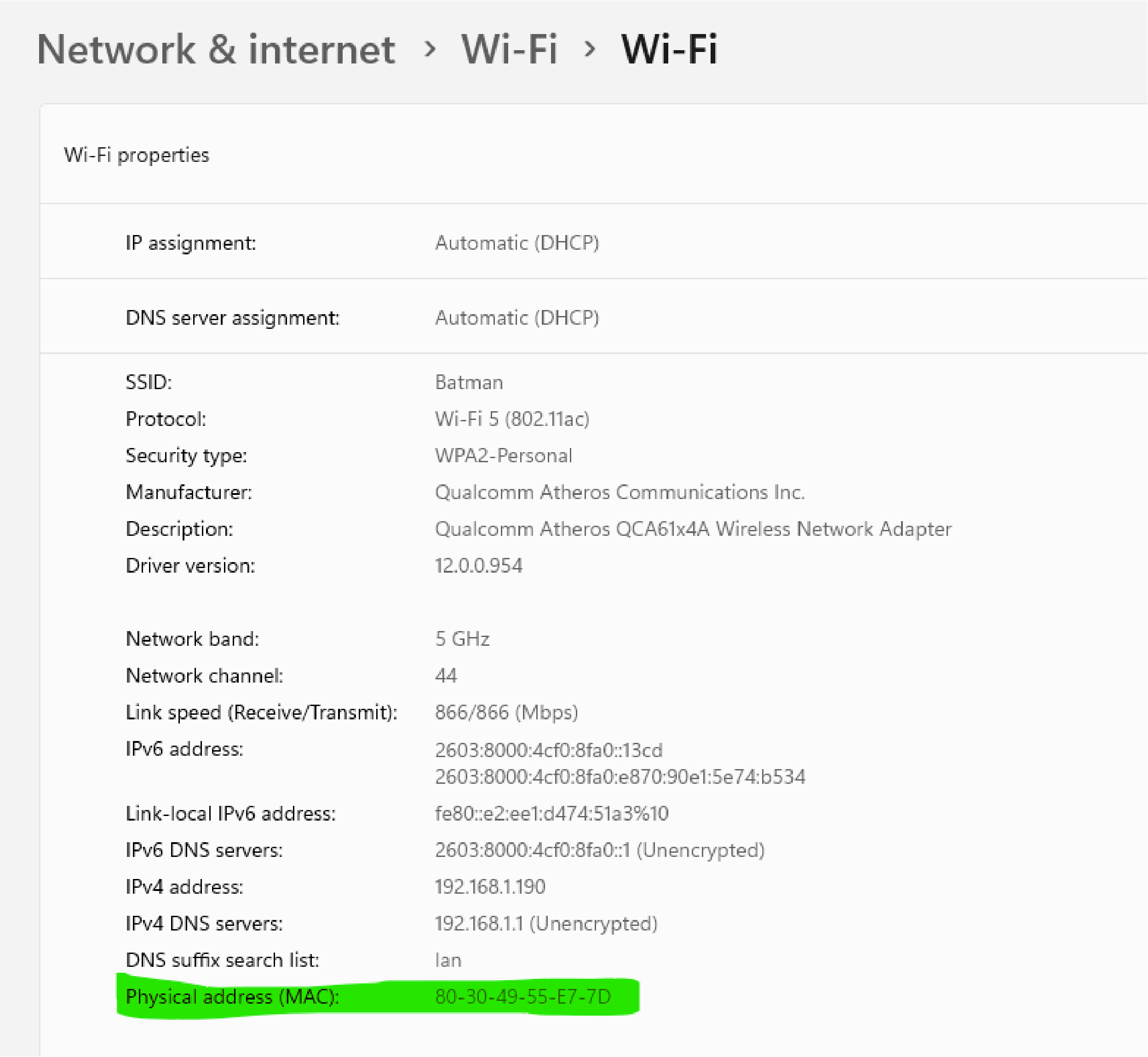
What filter did you use to see only packets from our test network?

to see probe packet I would have used this:

wlan.fc.type_subtype == 0x5 | | wlan.fc.subtype ==0x4

What is the MAC address of the router for the test network?

Since I am doing this from home now, my hoime wifi is , please see the green highlighted.



Network & internet › Wi-Fi › Wi-Fi

Wi-Fi properties

IP assignment:	Automatic (DHCP)
DNS server assignment:	Automatic (DHCP)
SSID:	Batman
Protocol:	Wi-Fi 5 (802.11ac)
Security type:	WPA2-Personal
Manufacturer:	Qualcomm Atheros Communications Inc.
Description:	Qualcomm Atheros QCA61x4A Wireless Network Adapter
Driver version:	12.0.0.954
Network band:	5 GHz
Network channel:	44
Link speed (Receive/Transmit):	866/866 (Mbps)
IPv6 address:	2603:8000:4cf0:8fa0::13cd 2603:8000:4cf0:8fa0:e870:90e1:5e74:b534
Link-local IPv6 address:	fe80::e2:ee1:d474:51a3%10
IPv6 DNS servers:	2603:8000:4cf0:8fa0::1 (Unencrypted)
IPv4 address:	192.168.1.190
IPv4 DNS servers:	192.168.1.1 (Unencrypted)
DNS suffix search list:	lan
Physical address (MAC):	80-30-49-55-E7-7D