IOT & NS-Experiment-6
WireShark

Name :- Sagar Gupta
Roll No. :- 21MCF1R47
Reg. No. :- MC21107
Course :- MCA 3nd year (5th Sem).

Submission Date :- 03-11-2023

Q-1 List at least 4 different protocols that appear in the protocol column on running wireshark.
Ans-1 Various protocols in the "Protocol" column in Wireshark, are:

a) HTTP
b) TCP
c) DNS
d) ARP

Q-2 Do the following:

a) Start the packet capture
b) open a web page: say www.google.com/

Report the time gap between the HTTP GET message and HTTP OK reply (Refer to the time column in Wireshark).

Answer the following questions, based on the contents of the HTTP GET message. Show the selected packet in wireshark to the TA

a) What is the source port, source IP, destination IP, and destination port?

b) What is the 48-bit MAC of your machine?

c) What is the 48 bit destination address in the Ethernet frame? Whose Ethernet address is that?

Answer the above questions based on the contents of the HTTP response message.

Ans-2 :

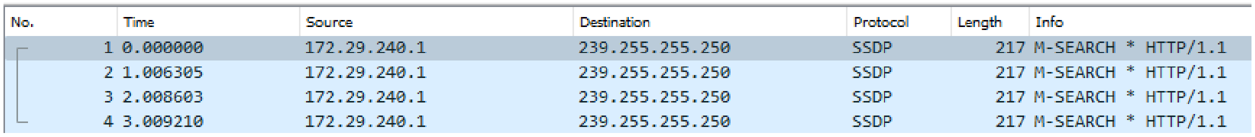
a)

Source Port : 58446

Source IP : 172.29.240.1

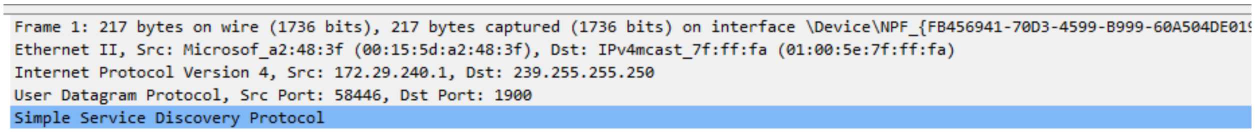
Destination IP : 239.255.255.250

Destination Port : 1900



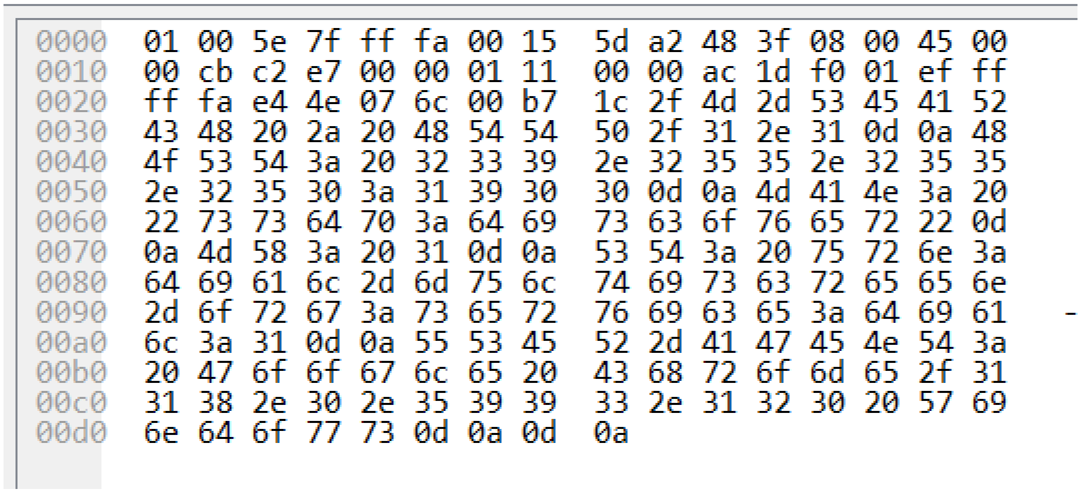
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.29.240.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2	1.006305	172.29.240.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3	2.008603	172.29.240.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4	3.009210	172.29.240.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

b) 00:15:5d:a2:48:3f



```
Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{FB456941-70D3-4599-B999-60A504DE01
Ethernet II, Src: Microsof_a2:48:3f (00:15:5d:a2:48:3f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 172.29.240.1, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 58446, Dst Port: 1900
Simple Service Discovery Protocol
```

c) 01:00:5e:7f:ff:fa and it is the address of college ethernet.



```
0000  01 00 5e 7f ff fa 00 15  5d a2 48 3f 08 00 45 00
0010  00 cb c2 e7 00 00 01 11  00 00 ac 1d f0 01 ef ff
0020  ff fa e4 4e 07 6c 00 b7  1c 2f 4d 2d 53 45 41 52
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61
00a0  6c 3a 31 0d 0a 55 53 45  52 2d 41 47 45 4e 54 3a
00b0  20 47 6f 6f 67 6c 65 20  43 68 72 6f 6d 65 2f 31
00c0  31 38 2e 30 2e 35 39 39  33 2e 31 32 30 20 57 69
00d0  6e 64 6f 77 73 0d 0a 0d  0a
```

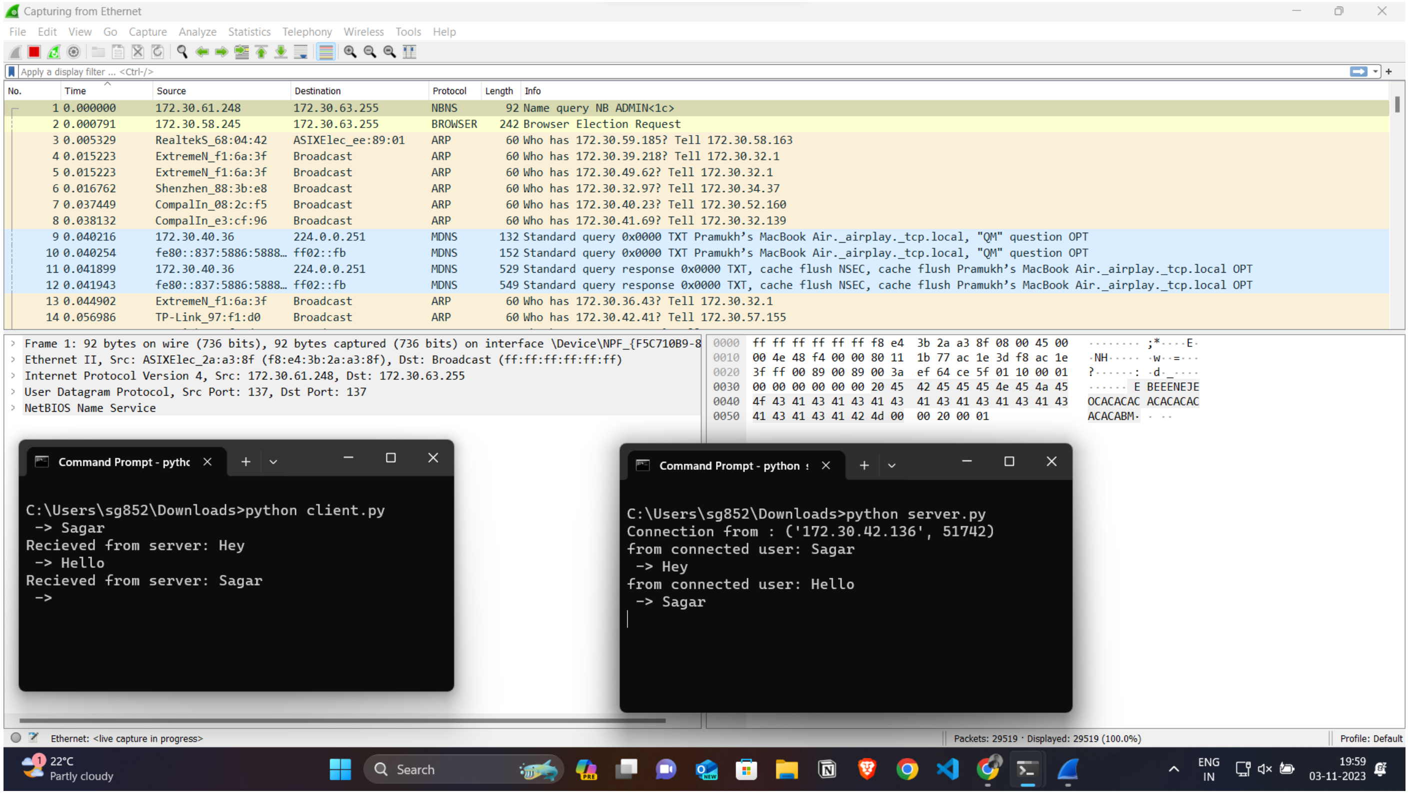
Q-3 Download the client server program that you built in the CN course. Close all other applications that may introduce network traffic and then start wireshark. Run the server, and the client.

Focus on the connection setup phase. Identify the packets corresponding to the 3-way handshake of TCP.

a) write down which port number is used by the client and the server?

b) which Seq number is used by the client and the server during the handshake? Verify whether the same is present in the corresponding ACK.

Ans-3


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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.30.61.248	172.30.63.255	NBNS	92	Name query NB ADMIN<1c>
2	0.000791	172.30.58.245	172.30.63.255	BROWSER	242	Browser Election Request
3	0.005329	RealtekS_68:04:42	ASIXElec_ee:89:01	ARP	60	Who has 172.30.59.185? Tell 172.30.58.163
4	0.015223	ExtremeN_f1:6a:3f	Broadcast	ARP	60	Who has 172.30.39.218? Tell 172.30.32.1
5	0.015223	ExtremeN_f1:6a:3f	Broadcast	ARP	60	Who has 172.30.49.62? Tell 172.30.32.1
6	0.016762	Shenzhen_88:3b:e8	Broadcast	ARP	60	Who has 172.30.32.97? Tell 172.30.34.37
7	0.037449	CompalIn_08:2c:f5	Broadcast	ARP	60	Who has 172.30.40.23? Tell 172.30.52.160
8	0.038132	CompalIn_e3:cf:96	Broadcast	ARP	60	Who has 172.30.41.69? Tell 172.30.32.139
9	0.040216	172.30.40.36	224.0.0.251	MDNS	132	Standard query 0x0000 TXT Pramukh’s MacBook Air._airplay._tcp.local, "QM" question OPT
10	0.040254	fe80::837:5886:5888…	ff02::fb	MDNS	152	Standard query 0x0000 TXT Pramukh’s MacBook Air._airplay._tcp.local, "QM" question OPT
11	0.041899	172.30.40.36	224.0.0.251	MDNS	529	Standard query response 0x0000 TXT, cache flush NSEC, cache flush Pramukh’s MacBook Air._airplay._tcp.local OPT
12	0.041943	fe80::837:5886:5888…	ff02::fb	MDNS	549	Standard query response 0x0000 TXT, cache flush NSEC, cache flush Pramukh’s MacBook Air._airplay._tcp.local OPT
13	0.044902	ExtremeN_f1:6a:3f	Broadcast	ARP	60	Who has 172.30.36.43? Tell 172.30.32.1
14	0.056986	TP-Link_97:f1:d0	Broadcast	ARP	60	Who has 172.30.42.41? Tell 172.30.57.155

```
> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{F5C710B9-8
> Ethernet II, Src: ASIXElec_2a:a3:8f (f8:e4:3b:2a:a3:8f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.30.61.248, Dst: 172.30.63.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff f8 e4  3b 2a a3 8f 08 00 45 00   ········ ;*····E·
0010  00 4e 48 f4 00 00 80 11  1b 77 ac 1e 3d f8 ac 1e   ·NH····· ·w··=···
0020  3f ff 00 89 00 89 00 3a  ef 64 ce 5f 01 10 00 01   ?······: ·d·_····
0030  00 00 00 00 00 00 20 45  42 45 45 45 4e 45 4a 45   ······ E BEEENEJE
0040  4f 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   OCACACAC ACACACAC
0050  41 43 41 43 41 42 4d 00  00 20 00 01               ACACABM· · ··
```

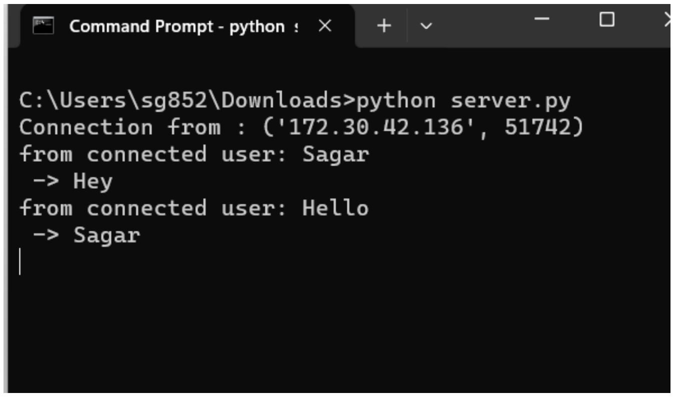
```
C:\Users\sg852\Downloads>python client.py
 -> Sagar
Recieved from server: Hey
 -> Hello
Recieved from server: Sagar
 ->
```

```
C:\Users\sg852\Downloads>python server.py
Connection from : ('172.30.42.136', 51742)
from connected user: Sagar
 -> Hey
from connected user: Hello
 -> Sagar
```

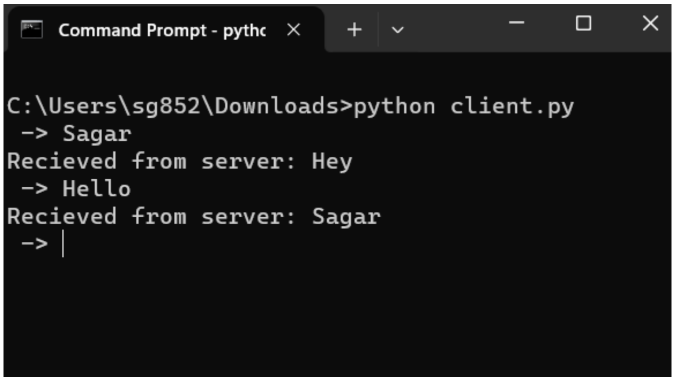
Ethernet: <live capture in progress>
Packets: 29519 · Displayed: 29519 (100.0%)
Profile: Default
22°C
Partly cloudy
Search
ENG
IN
19:59
03-11-2023

a) Port Used by Client and Server is 137

b)



```
C:\Users\sg852\Downloads>python server.py
Connection from : ('172.30.42.136', 51742)
from connected user: Sagar
 -> Hey
from connected user: Hello
 -> Sagar
```



```
C:\Users\sg852\Downloads>python client.py
 -> Sagar
Recieved from server: Hey
 -> Hello
Recieved from server: Sagar
 ->
```