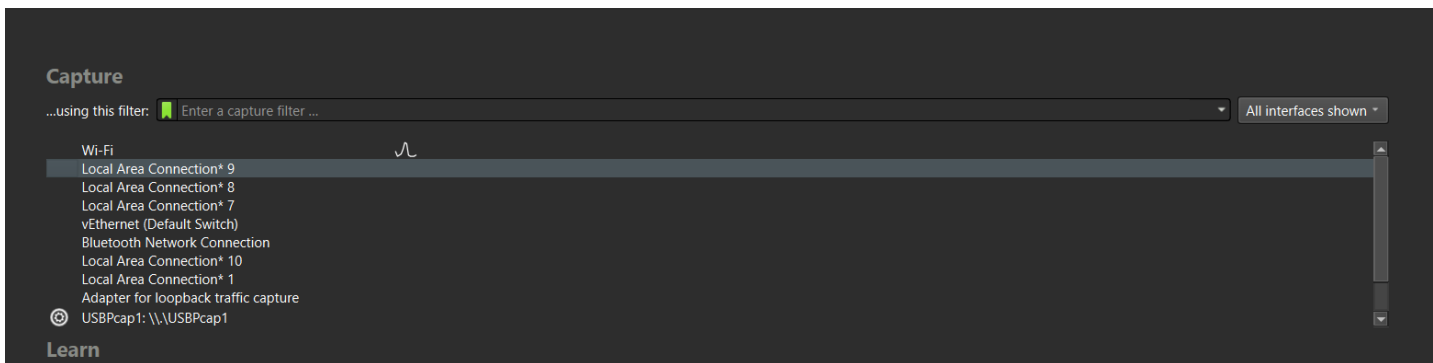
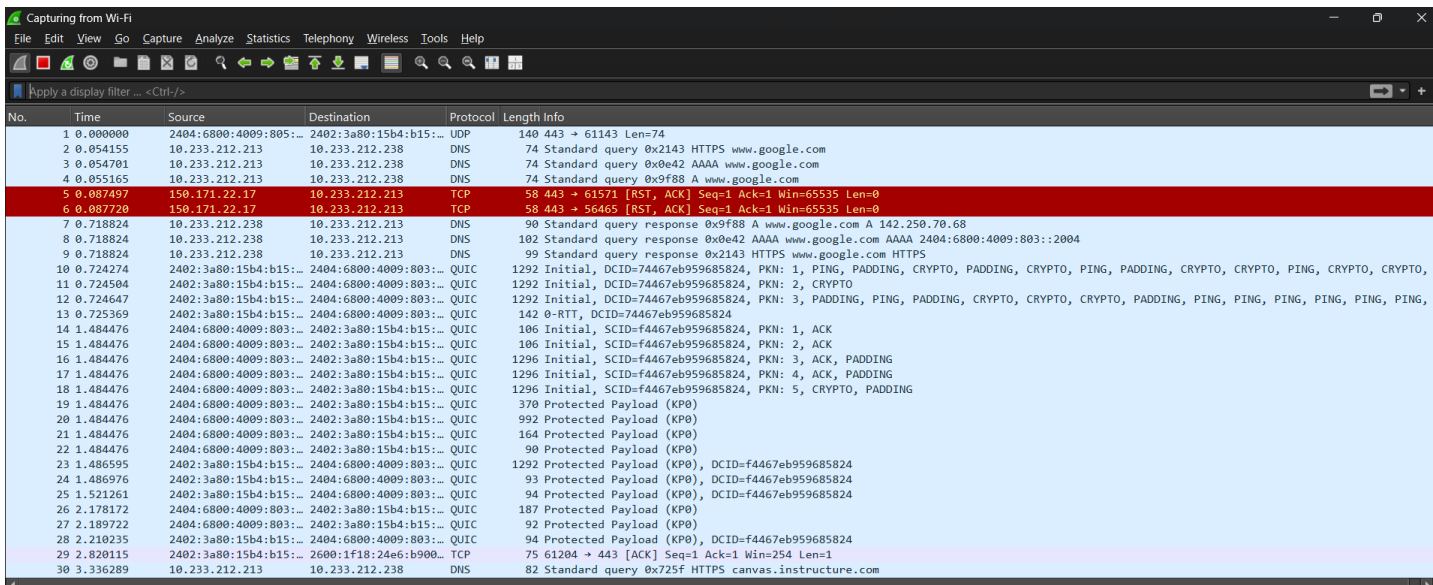
 Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology		
Subject: Computer Networks (01CT0503)	Aim: Experiment 12 - Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.	
Experiment No: 12	Date:	Enrolment No: 92301733041

Aim: Experiment 12 - Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.

Step 1: firstly connect to router/wifi and start wireshark



Step 2: double click on wifi and live capture will start




Step 3: On filter bar , search for any filter what ever you want to do

1.ARP

No.	Time	Source	Destination	Protocol	Length	Info
70	5.311635	da:39:fb:57:7f:9e	Intel_d8:40:a5	ARP	42	Who has 10.233.212.213? Tell 10.233.212.238
71	5.311653	Intel_d8:40:a5	da:39:fb:57:7f:9e	ARP	42	10.233.212.213 is at 14:85:7f:d8:40:a5
274	26.283223	da:39:fb:57:7f:9e	Intel_d8:40:a5	ARP	42	Who has 10.233.212.213? Tell 10.233.212.238
275	26.283272	Intel_d8:40:a5	da:39:fb:57:7f:9e	ARP	42	10.233.212.213 is at 14:85:7f:d8:40:a5
326	42.161768	da:39:fb:57:7f:9e	Intel_d8:40:a5	ARP	42	Who has 10.233.212.213? Tell 10.233.212.238
327	42.161827	Intel_d8:40:a5	da:39:fb:57:7f:9e	ARP	42	10.233.212.213 is at 14:85:7f:d8:40:a5
399	67.004315	da:39:fb:57:7f:9e	Intel_d8:40:a5	ARP	42	Who has 10.233.212.213? Tell 10.233.212.238
400	67.004368	Intel_d8:40:a5	da:39:fb:57:7f:9e	ARP	42	10.233.212.213 is at 14:85:7f:d8:40:a5

Understanding: Here Arp (address resolution protocol) works like this device broadcasting this Ip and asking which device has this Ip tell me, because directly device can't get the mac using Ip that's why ARP used, first packet is **broadcasting** in network that why color is

 Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology	
Subject: Computer Networks (01CT0503)	Aim: Experiment 12 - Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.	
Experiment No: 12	Date:	Enrolment No: 92301733041

yellow, and in second packet the reply came from that device that “it is my Ip and this is my mac address” so reply will be **unicast** so it is in grey color. This process keeps continuing after every time out occurs

2. RARP

RARP (Reverse Address Resolution Protocol) is an obsolete protocol used to map MAC addresses to IP addresses. Modern networks no longer use RARP because DHCP performs this function. Therefore, no RARP packets were captured during the experiment.

3. DHCP

dhcp					
No.	Time	Source	Destination	Protocol	Length Info
5	17.936941	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Transaction ID 0x1b65c54c
10	17.975559	10.233.212.238	10.233.212.213	DHCP	352 DHCP ACK - Transaction ID 0x1b65c54c

When my laptop is already known to WIFI that why is showing only 2 packets, just client requesting for the old Ip and dhcp allocating that Ip. Then I release that ip and again check then I got 4 packets
 D= discover

O= Offer

R=request

A= acknowledgement


379	20.986465	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x2c8f457d
390	21.041372	10.233.212.238	10.233.212.213	DHCP	352 DHCP Offer - Transaction ID 0x2c8f457d
391	21.042688	0.0.0.0	255.255.255.255	DHCP	344 DHCP Request - Transaction ID 0x2c8f457d
397	21.065096	10.233.212.238	10.233.212.213	DHCP	352 DHCP ACK - Transaction ID 0x2c8f457d

Here first client will say I want Ip (broadcast packet)

Then dhcp will offer him Ip

Client will confirm

And last dhcp will ack it that Ip confirm

 Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology	
Subject: Computer Networks (01CT0503)	Aim: Experiment 12 - Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.	
Experiment No: 12	Date:	Enrolment No: 92301733041

4. HTTP

No.	Time	Source	Destination	Protocol	Length	Info
→ 95	3.649211	2402:3a80:15b4:b15::...	2600:1f13:37c:1400::...	HTTP	685	GET /online/ HTTP/1.1
← 106	5.178301	2600:1f13:37c:1400::...	2402:3a80:15b4:b15::...	HTTP	324	HTTP/1.1 200 OK (text/html)

Here analysis is client is sending http request to server side in first packet, in second packet response came from server status 200 ok, And type html/text means html page is successfully fetched

Conclusion: In this exp, I show the live traffic of network using Wireshark, where I show the Ip to mac accessing by ARP, how DHCP were assigning the Ip to any new or already connected client/device, also some http side request.