

PG LAB assignment 2a

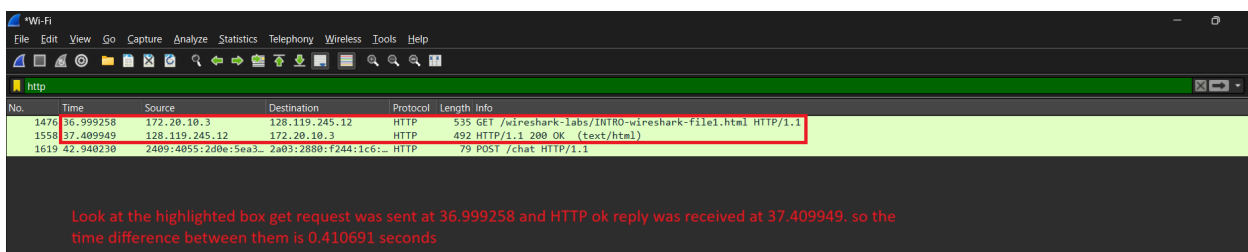
1) Answer -

No.	Time	Source	Destination	Protocol	Length	Info
51	4.020132	Intel_5d:7c:30	Broadcast	ARP	42	Who has 172.20.10.1? Tell 172.20.10.3
54	4.131593	c2:b6:58:a7:58:64	Intel_5d:7c:30	ARP	42	172.20.10.1 is at c2:b6:58:a7:58:64
5091	80.478857	172.30.4.170	172.26.15.77	DNS	127	Standard query response 0x008c A accounts.youtube.com CNAME www3.l.google.com A 142.250.193.78
5092	80.478857	172.30.4.170	172.26.15.77	DNS	171	Standard query response 0x1247 HTTPS accounts.youtube.com CNAME www3.l.google.com SOA ns1.google.com
40	3.517942	152.195.38.76	172.20.10.3	OCSP	791	Response
90	5.361910	172.20.10.3	49.44.179.225	HTTP	208	GET /connecttest.txt HTTP/1.1
271	14.093191	2409:4055:2d0e:5ea3...	2409:4055:2d0e:5ea3...	ICMPv6	78	Neighbor Advertisement 2409:4055:2d0e:5ea3:dec:96b8:a7f0:8928 (rtr, sol)
515	16.993362	fe80::c0b6:58ff:fea...	fe80::7825:bed4:229...	ICMPv6	86	Neighbor Solicitation for fe80::7825:bed4:229c:43ab from c2:b6:58:a7:58:64
7677	143.256794	172.20.10.3	224.0.0.252	LLMNR	65	Standard query 0x0caa A https
7732	143.855784	fe80::7825:bed4:229...	ff02::1:3	LLMNR	85	Standard query 0xf87a A https
4276	105.158348	172.20.10.3	224.0.0.251	MDNS	500	Standard query response 0x0000 PTR, cache flush Yash.local PTR, cache flush Yash.local PTR, cache flush Yash.local PTR, cache f...
7625	142.832513	172.20.10.3	224.0.0.251	MDNS	71	Standard query 0x0000 A https.local, "QM" question
245	13.834428	2404:6800:4002:80c...	2409:4055:2d0e:5ea3...	QUIC	1292	Initial, SCID=efd7666e73913039, PKN: 1, ACK, PADDING
246	13.834428	2404:6800:4002:80c...	2409:4055:2d0e:5ea3...	QUIC	1292	Initial, SCID=efd7666e73913039, PKN: 1, ACK, PADDING
3009	91.856461	172.20.10.3	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3350	98.229961	172.20.10.3	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
242	9.422093	172.26.15.77	180.149.52.210	TCP	54	53377 → 443 [ACK] Seq=4664 Ack=29826 Win=262144 Len=0
243	9.424575	172.26.15.77	180.149.52.210	TLSv1.3	420	Application Data
339	9.663753	172.26.15.77	142.250.194.42	UDP	75	65237 → 443 Len=33
340	9.671091	142.250.194.42	172.26.15.77	UDP	361	443 → 65237 Len=319

The different protocols that I captured by applying the respective filter are:

1. ARP
2. DNS
3. HTTP
4. ICMPV6
5. LLMNR
6. MDNS
7. QUIC
8. SSDP
9. TCP
10. UDP

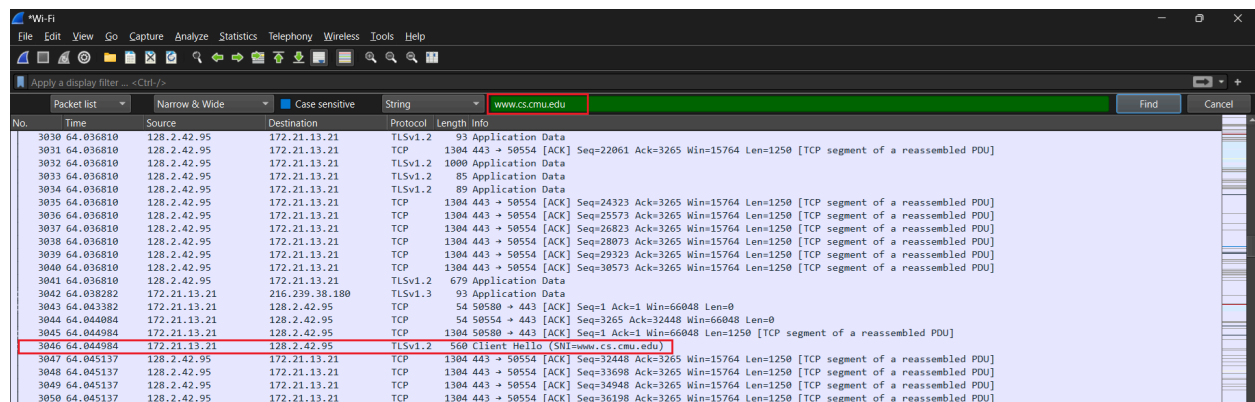
2) Answer -



Look at the highlighted box get request was sent at 36.999258 and HTTP ok reply was received at 37.409949, so the time difference between them is 0.410691 seconds

In the time column, look at the time of the GET request, which is at 36.999258 seconds after I started recording, and then look at the time column of ok HTTP, which is 37.409949, so the time difference between them is 0.410691 seconds.

3) Answer -

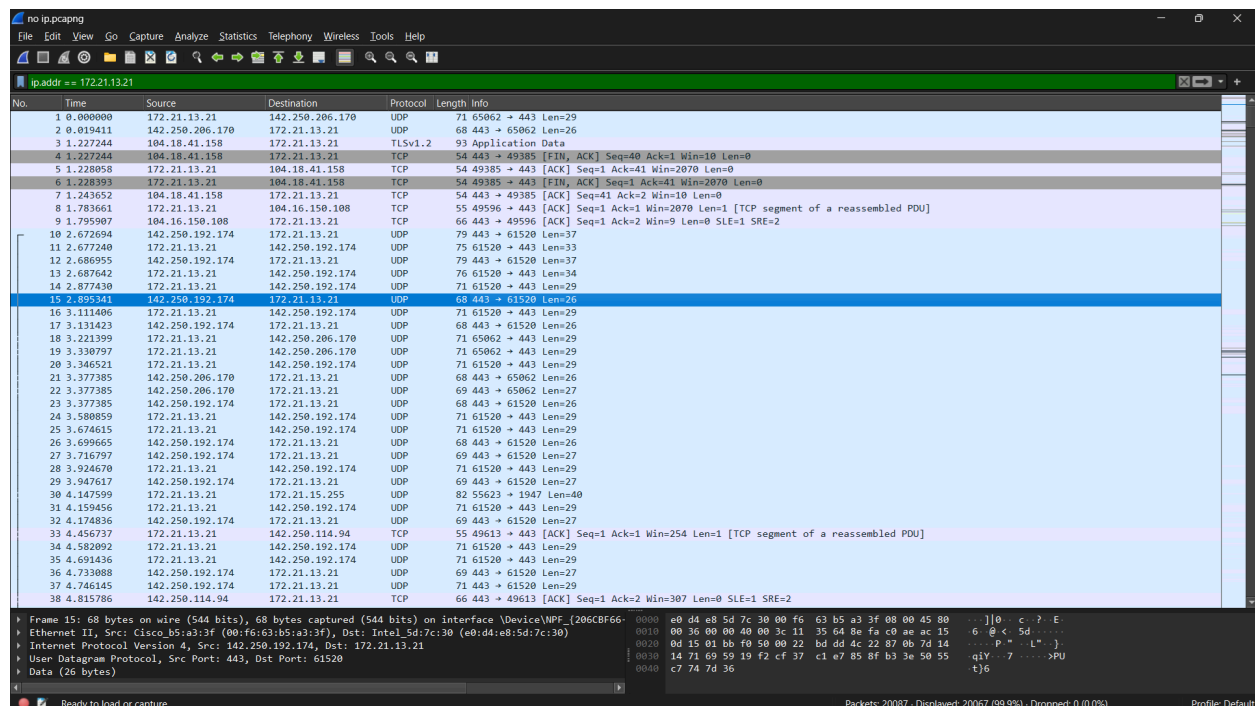


No.	Time	Source	Destination	Protocol	Length	Info
3030	64.036810	128.2.42.95	172.21.13.21	TLSv1.2	93	Application Data
3031	64.036810	128.2.42.95	172.21.13.21	TCP	1304	443 → 50554 [ACK] Seq=22061 Ack=3265 Win=15764 Len=1250 [TCP segment of a reassembled PDU]
3032	64.036810	128.2.42.95	172.21.13.21	TLSv1.2	1000	Application Data
3033	64.036810	128.2.42.95	172.21.13.21	TLSv1.2	85	Application Data
3034	64.036810	128.2.42.95	172.21.13.21	TLSv1.2	89	Application Data
3035	64.036810	128.2.42.95	172.21.13.21	TCP	1304	443 → 50554 [ACK] Seq=24323 Ack=3265 Win=15764 Len=1250 [TCP segment of a reassembled PDU]
3036	64.036810	128.2.42.95	172.21.13.21	TCP	1304	443 → 50554 [ACK] Seq=25573 Ack=3265 Win=15764 Len=1250 [TCP segment of a reassembled PDU]
3037	64.036810	128.2.42.95	172.21.13.21	TCP	1304	443 → 50554 [ACK] Seq=26823 Ack=3265 Win=15764 Len=1250 [TCP segment of a reassembled PDU]
3038	64.036810	128.2.42.95	172.21.13.21	TCP	1304	443 → 50554 [ACK] Seq=28073 Ack=3265 Win=15764 Len=1250 [TCP segment of a reassembled PDU]
3039	64.036810	128.2.42.95	172.21.13.21	TCP	1304	443 → 50554 [ACK] Seq=29323 Ack=3265 Win=15764 Len=1250 [TCP segment of a reassembled PDU]
3040	64.036810	128.2.42.95	172.21.13.21	TCP	1304	443 → 50554 [ACK] Seq=30573 Ack=3265 Win=15764 Len=1250 [TCP segment of a reassembled PDU]
3041	64.036810	128.2.42.95	172.21.13.21	TLSv1.2	679	Application Data
3042	64.038282	172.21.13.21	216.239.38.100	TLSv1.3	93	Application Data
3043	64.043382	172.21.13.21	128.2.42.95	TCP	54	50580 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
3044	64.044084	172.21.13.21	128.2.42.95	TCP	54	50554 → 443 [ACK] Seq=3265 Ack=32448 Win=66048 Len=0
3045	64.044984	172.21.13.21	128.2.42.95	TCP	1304	50580 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=1250 [TCP segment of a reassembled PDU]
3046	64.044984	172.21.13.21	128.2.42.95	TLSv1.2	560	Client Hello [SHA=www.cs.cmu.edu]
3047	64.045137	128.2.42.95	172.21.13.21	TCP	1304	443 → 50554 [ACK] Seq=32448 Ack=3265 Win=15764 Len=1250 [TCP segment of a reassembled PDU]
3048	64.045137	128.2.42.95	172.21.13.21	TCP	1304	443 → 50554 [ACK] Seq=33698 Ack=3265 Win=15764 Len=1250 [TCP segment of a reassembled PDU]
3049	64.045137	128.2.42.95	172.21.13.21	TCP	1304	443 → 50554 [ACK] Seq=34948 Ack=3265 Win=15764 Len=1250 [TCP segment of a reassembled PDU]
3050	64.045137	128.2.42.95	172.21.13.21	TCP	1304	443 → 50554 [ACK] Seq=36198 Ack=3265 Win=15764 Len=1250 [TCP segment of a reassembled PDU]

Look at the info column of the highlighted row. HTTP requests were not showing for www.cs.cmu.edu, so I used the “Ctrl + F” key to find the string “www.cs.cmu.edu” to find packets that contain this website name. In the destination column IP address of the website is mentioned, which is 128.2.42.95, and my network IP is in the source column, which is 172.21.13.21

4) Answer -

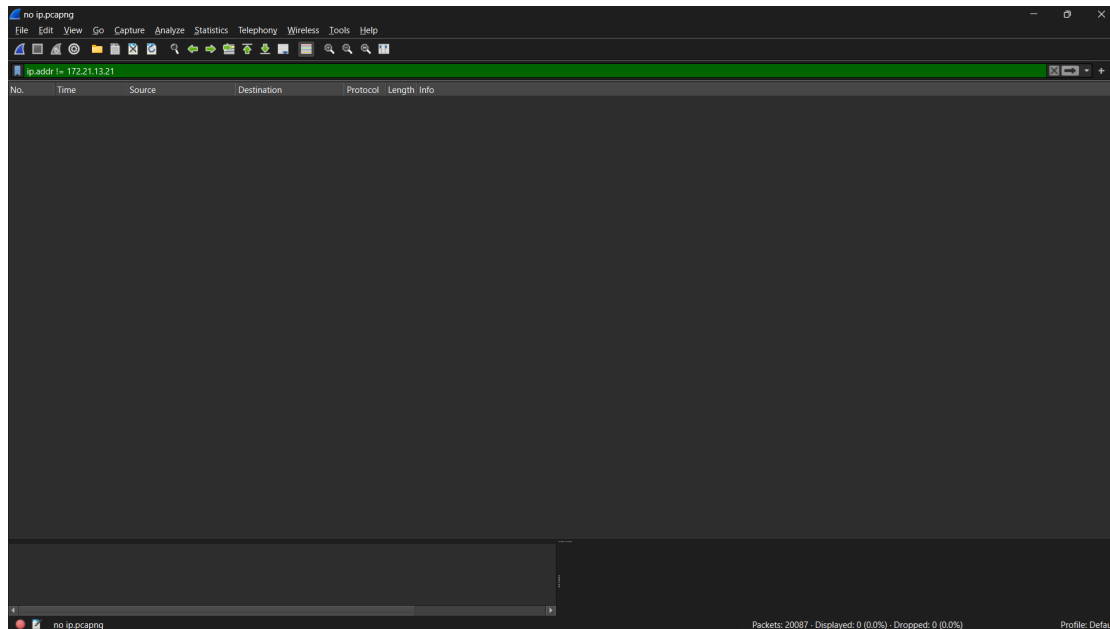
Wireshark captured 20087 packets. 20067 packets contain my IP address which I found out by using the filter `ip.addr == 172.21.13.21`, and at the bottom left corner, it shows the total number of packets after applying the filter(Displayed). 0 packets do not contain my IP. I used `ip.addr != 172.21.13.21` this filter to see it.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.21.13.21	142.250.206.170	UDP	71	65062 → 443 Len=29
2	0.019411	142.250.206.170	172.21.13.21	UDP	68	443 → 65062 Len=26
3	1.227244	104.18.41.158	172.21.13.21	TLSv1.2	93	Application Data
4	1.227244	104.18.41.158	172.21.13.21	TCP	54	443 → 49385 [FIN, ACK] Seq=40 Ack=1 Win=0 Len=0
5	1.228058	172.21.13.21	104.18.41.158	TCP	54	49385 → 443 [ACK] Seq=1 Ack=41 Win=2070 Len=0
6	1.228058	172.21.13.21	104.18.41.158	TCP	54	49385 → 443 [FIN, ACK] Seq=1 Ack=41 Win=2070 Len=0
7	1.243652	104.18.41.158	172.21.13.21	TCP	54	443 → 49385 [ACK] Seq=41 Ack=2 Win=0 Len=0
8	1.783661	172.21.13.21	104.16.150.108	TCP	55	49596 → 443 [ACK] Seq=1 Ack=1 Win=2070 Len=1 [TCP segment of a reassembled PDU]
9	1.795907	104.16.150.108	172.21.13.21	TCP	66	443 → 49596 [ACK] Seq=1 Ack=2 Win=9 Len=0 SLE=1 SRE=2
10	2.672694	142.250.192.174	172.21.13.21	UDP	79	443 → 61520 Len=37
11	2.677240	172.21.13.21	142.250.192.174	UDP	75	61520 → 443 Len=33
12	2.686955	142.250.192.174	172.21.13.21	UDP	79	443 → 61520 Len=37
13	2.687642	172.21.13.21	142.250.192.174	UDP	76	61520 → 443 Len=34
14	2.877430	172.21.13.21	142.250.192.174	UDP	71	61520 → 443 Len=29
15	2.895341	142.250.192.174	172.21.13.21	UDP	68	443 → 61520 Len=26
16	3.111486	172.21.13.21	142.250.192.174	UDP	71	61520 → 443 Len=29
17	3.131423	142.250.192.174	172.21.13.21	UDP	68	443 → 61520 Len=26
18	3.221399	172.21.13.21	142.250.206.170	UDP	71	65062 → 443 Len=29
19	3.330797	172.21.13.21	142.250.206.170	UDP	71	65062 → 443 Len=29
20	3.346521	172.21.13.21	142.250.192.174	UDP	71	61520 → 443 Len=29
21	3.377385	142.250.206.170	172.21.13.21	UDP	68	443 → 65062 Len=26
22	3.377385	142.250.206.170	172.21.13.21	UDP	69	443 → 65062 Len=27
23	3.377385	142.250.192.174	172.21.13.21	UDP	68	443 → 61520 Len=26
24	3.588859	172.21.13.21	142.250.192.174	UDP	71	61520 → 443 Len=29
25	3.674615	172.21.13.21	142.250.192.174	UDP	71	61520 → 443 Len=29
26	3.699665	142.250.192.174	172.21.13.21	UDP	68	443 → 61520 Len=26
27	3.716797	142.250.192.174	172.21.13.21	UDP	69	443 → 61520 Len=27
28	3.924670	172.21.13.21	142.250.192.174	UDP	71	61520 → 443 Len=29
29	3.947617	142.250.192.174	172.21.13.21	UDP	69	443 → 61520 Len=27
30	4.147599	172.21.13.21	172.21.15.255	UDP	82	55623 → 1947 Len=40
31	4.159456	172.21.13.21	142.250.192.174	UDP	71	61520 → 443 Len=29
32	4.174836	142.250.192.174	172.21.13.21	UDP	69	443 → 61520 Len=27
33	4.456737	172.21.13.21	142.250.114.94	TCP	55	49613 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP segment of a reassembled PDU]
34	4.582092	172.21.13.21	142.250.192.174	UDP	71	61520 → 443 Len=29
35	4.691436	172.21.13.21	142.250.192.174	UDP	71	61520 → 443 Len=29
36	4.733088	142.250.192.174	172.21.13.21	UDP	69	443 → 61520 Len=27
37	4.746145	142.250.192.174	172.21.13.21	UDP	71	443 → 61520 Len=29
38	4.815786	142.250.114.94	172.21.13.21	TCP	66	443 → 49613 [ACK] Seq=1 Ack=2 Win=307 Len=0 SLE=1 SRE=2

Frame 15: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface DeviceWPF {206CBF66-0000-0000-0000-000000000000} on 0:15:5d:7c:30:00:f6:63:b5:a3:3f:08:00:45:80
Ethernet II, Src: Cisco B5:a3:3f:08:00:45:80, Dst: Intel 5d:7c:30:00:f6:63:b5:a3:3f:08:00:45:80
Internet Protocol Version 4, Src: 142.250.192.174, Dst: 172.21.13.21
User Datagram Protocol, Src Port: 443, Dst Port: 61520
Data (26 bytes)
0000 e0 d4 e8 5d 7c 30 00 f6 63 b5 a3 3f 08 00 45 80 ... 0
0010 00 36 00 00 40 00 3e 11 35 64 be f6 00 00 15 ... 6
0020 0d 15 01 b6 f0 50 00 22 b4 dd dc 22 87 0b 7d 14 ... p " " L " }
0030 14 71 69 59 19 f2 cf 37 c1 e7 85 8f b3 3e 50 55 ... q i Y 7 - - - - - P U
0040 c7 74 7d 36 ... t j 6

Packets: 20087 - Displayed: 20067 (99.9%) - Dropped: 0 (0.0%) Profile: Default



5) Answer -

I set up a local FTP server on my Windows PC and tried to log in to the FTP server using a terminal while capturing packets on Wireshark(I selected an adapter for loopback traffic capture for capturing the packets since we have a local FTP server). I entered the username CS509-student, and the terminal asked me for a password I entered “IITRPR-cs509”, and I logged in. In Wireshark, I filtered the packets to show only ftp protocols, and there I saw the FTP protocol packet requesting the password and giving the response packet User logged in after I entered the password “IITRPR-cs509”, which concludes it is the correct password.

