Homework 2

1. 3 different protocols: TCP, UDP, ARP

(a) TCP, UDP → transport layer

(pass segments and destination adress to network)

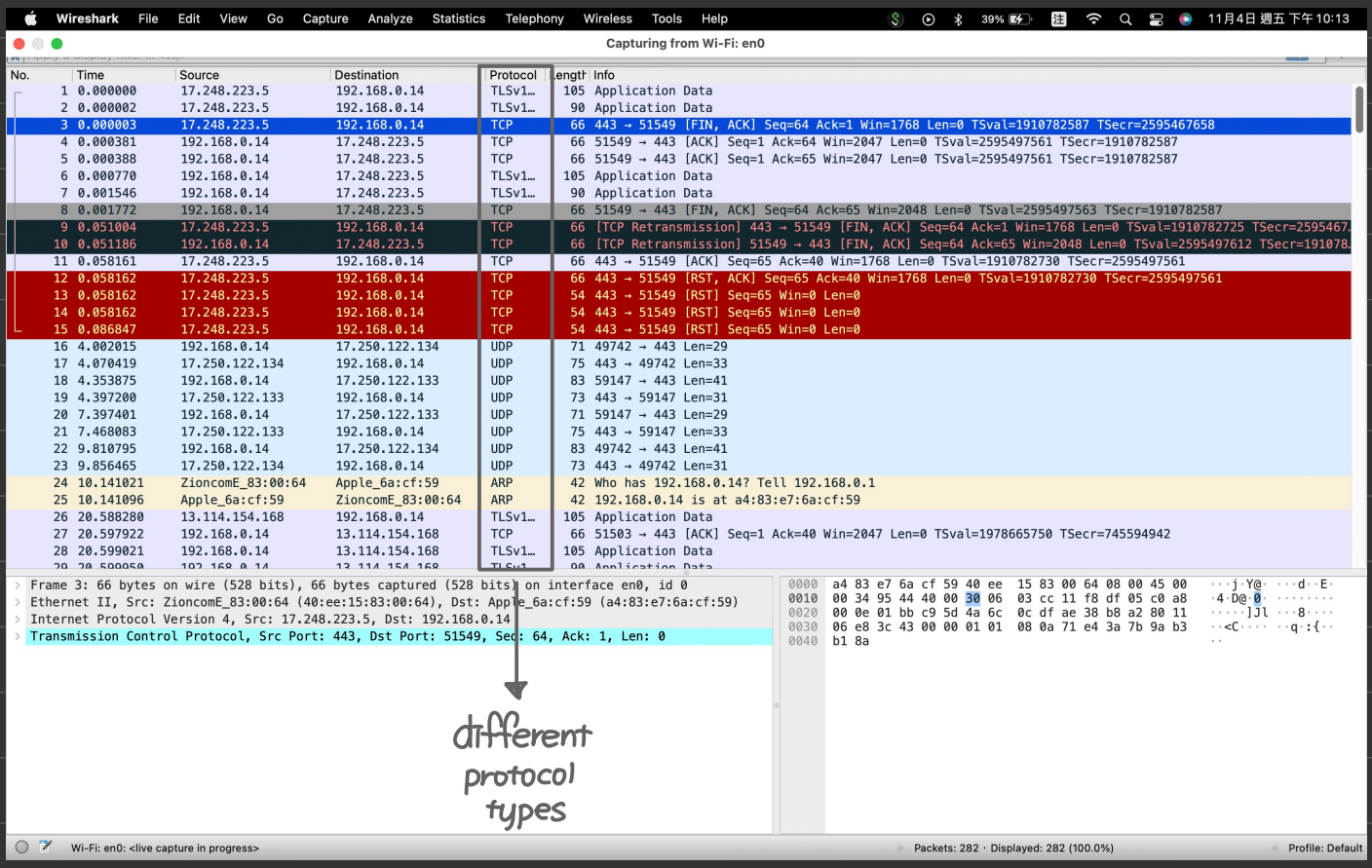
→ TCP

- breaks long message into shorter segments
- guaranteed delivery of application-layer messages

→ UDP

- provides connectionless service to its applications

(b) ARP → network layer

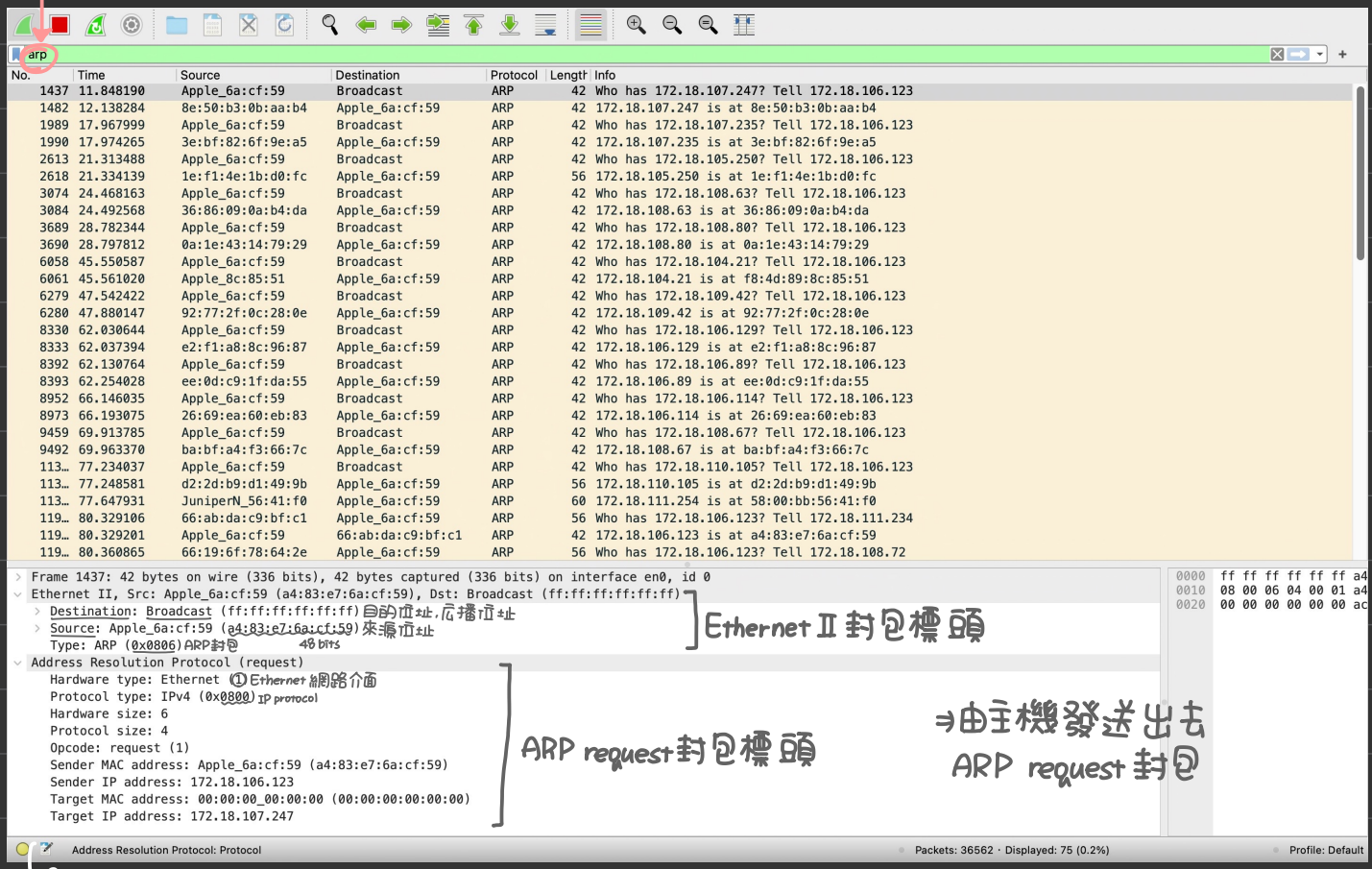


2. ARP protocol - Ethernet 和 IP 位址的轉換

- host 要找另一個 host 時，會用 broadcast 發出一個 ARP query (查詢)，而 ARP query 中包含了想查詢的 IP，又∵是 broadcast，∴網段中所有 host 都會收到，但只有符合 IP 的 host 收到後會回覆，包含它自己的 MAC Adress，而查詢方會把 MAC Adress 紀錄到 ARP Table 中。

Method to find ARP in wireshark

1. chose the interface(s) you want to capture
2. type "arp" in the display filter
3. you can find out ARP packets of the interface(s)



點開想分析的 packet，即可看到它的內容

ex. 點開 No. 1437 packet

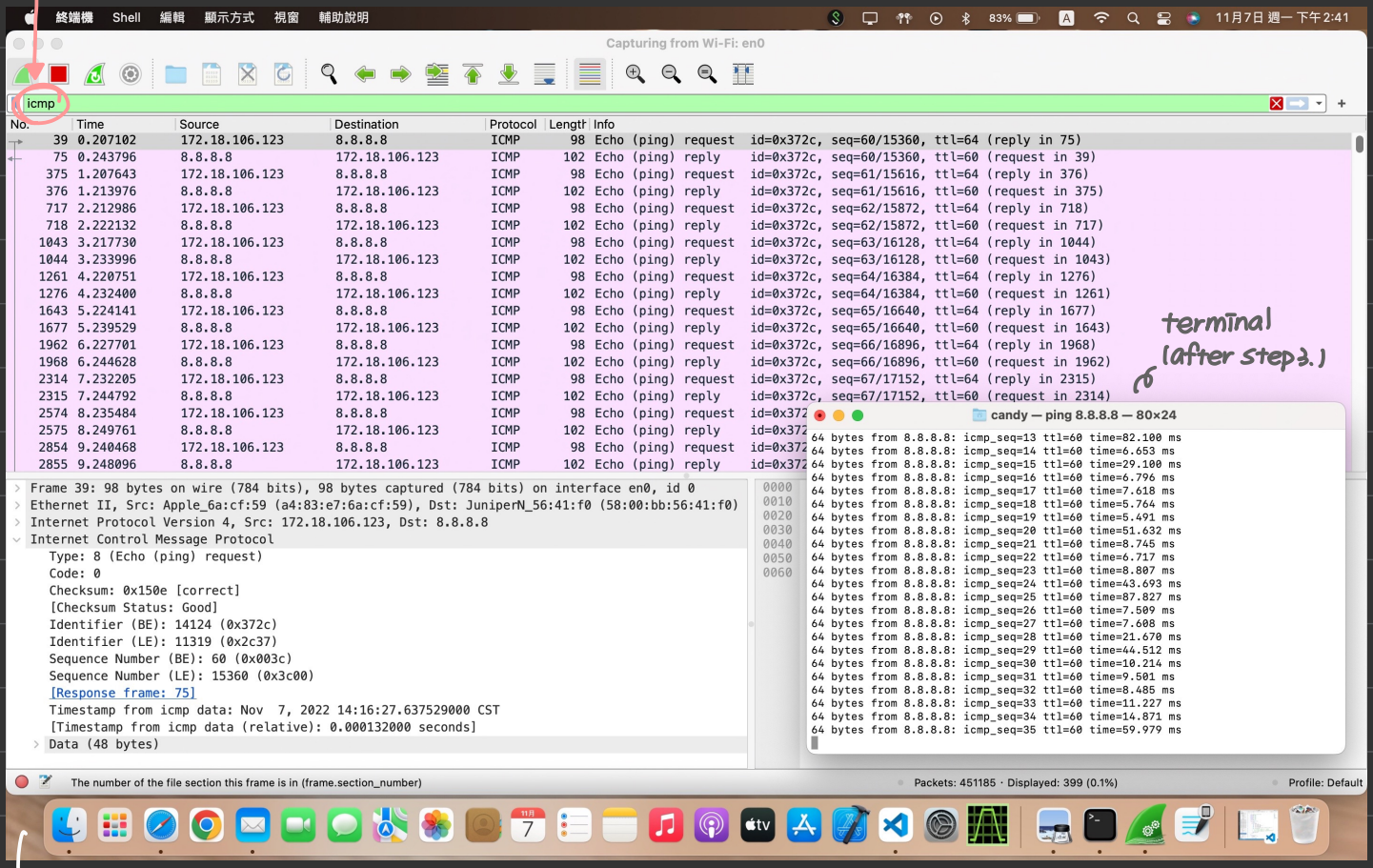
3. ICMP protocol → 解析封包或分析路由(藉由D傳的錯誤訊息分析)

① generate errors to share with the sending device in the event that any of the data didn't get to the destination.

② perform network diagnostic

Method to find ICMP in wireshark

1. chose the interface(s) you want to capture
2. open the terminal in your computer
3. type "ping 8.8.8.8" in command line
4. go back to wireshark and type "icmp" in the display filter
5. you can find out ICMP packets of the interface(s)



和ARP相比沒有"source"及"destination"的 port numbers

① ICMP是用來交換 network layer 中 host 和 router 間的訊息

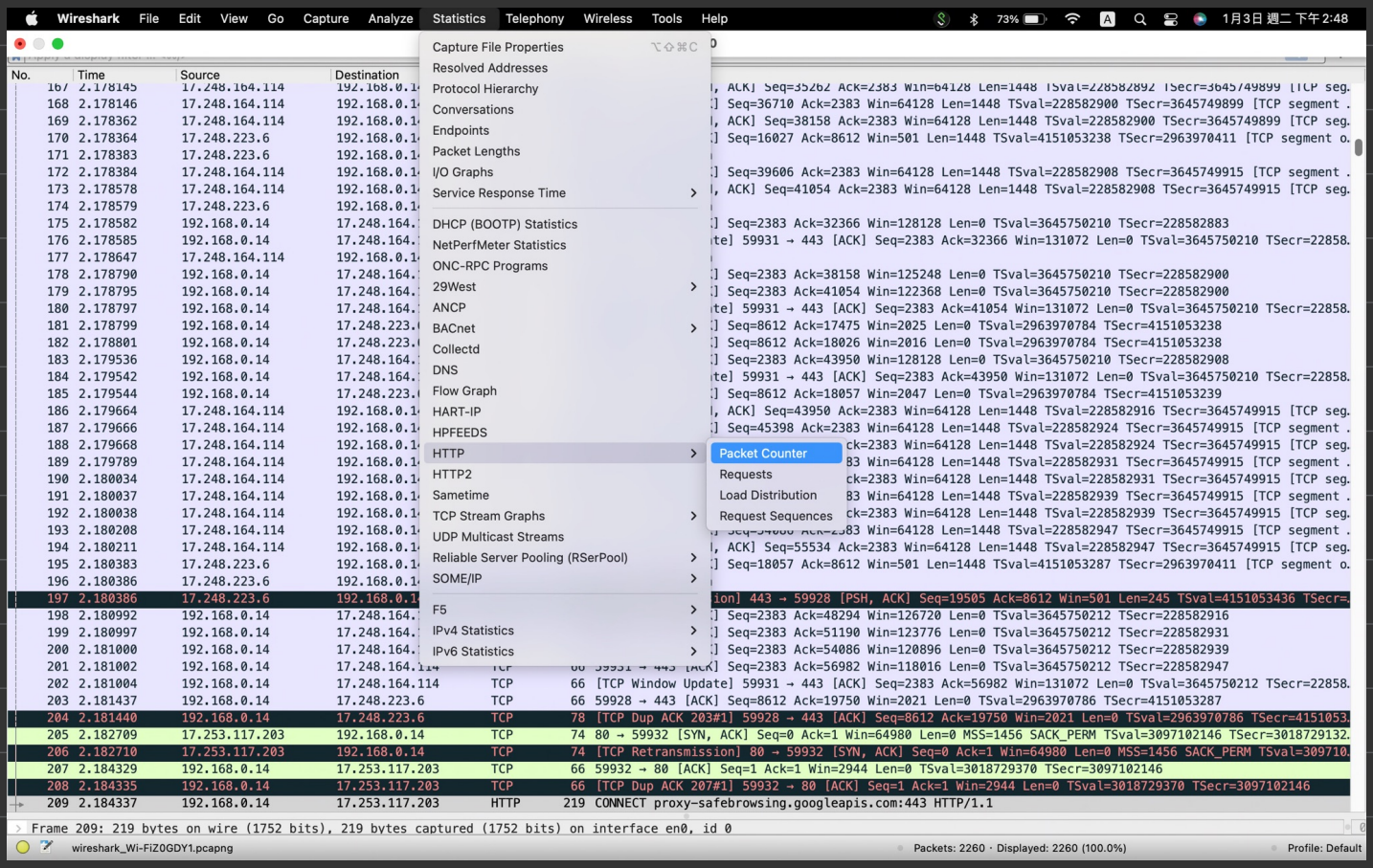
非 application layer process

② 每一個 ICMP 封包都有"type"和"code",結合這兩者就可識別訊息

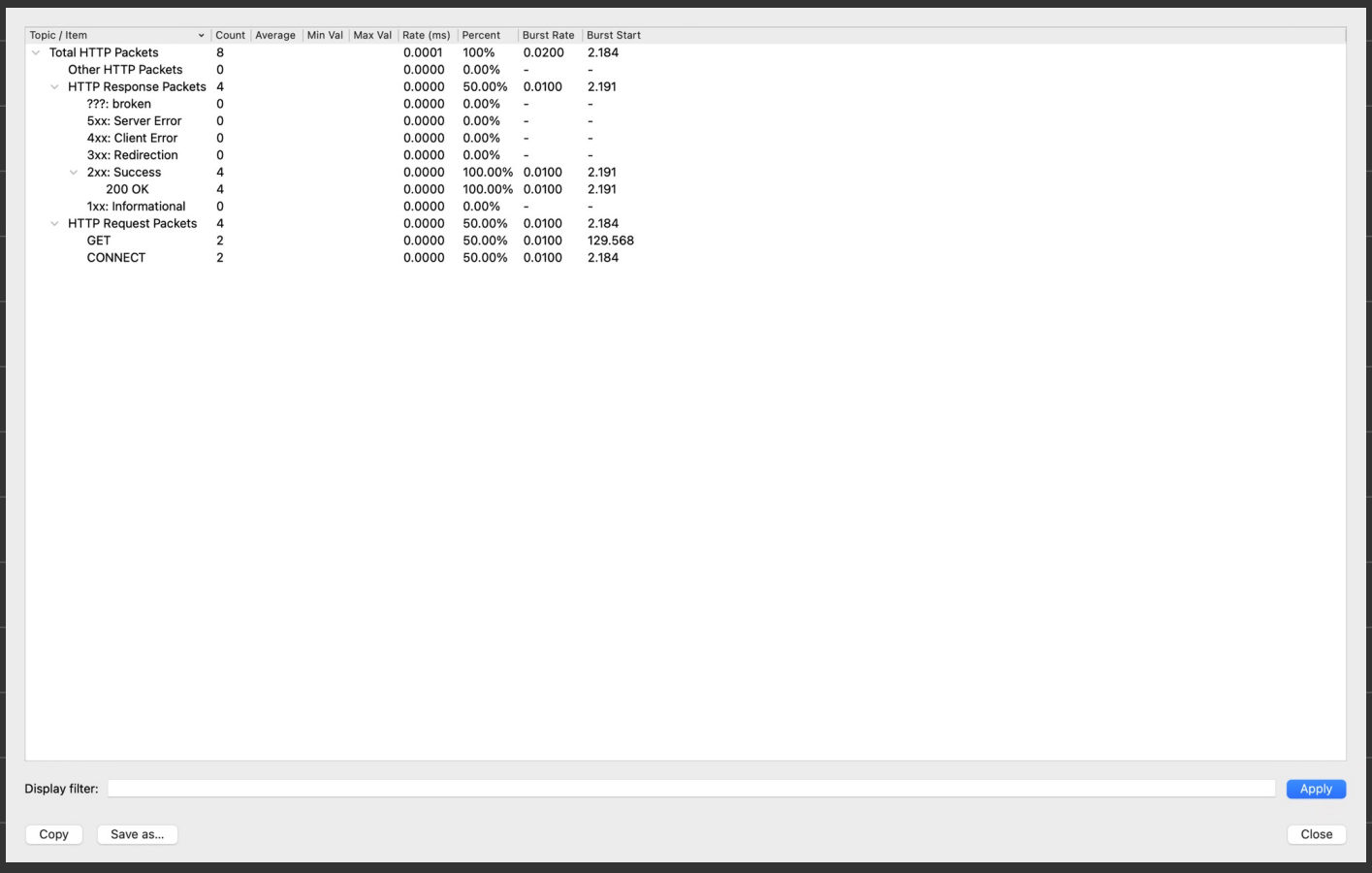
∴就不用 port 去指示

Homework 3

1. HTTP Packet Counter statistics



Choose statistics → HTTP → Packet Counter



2. 2 benefits

(1) Reduce connection establishment latency

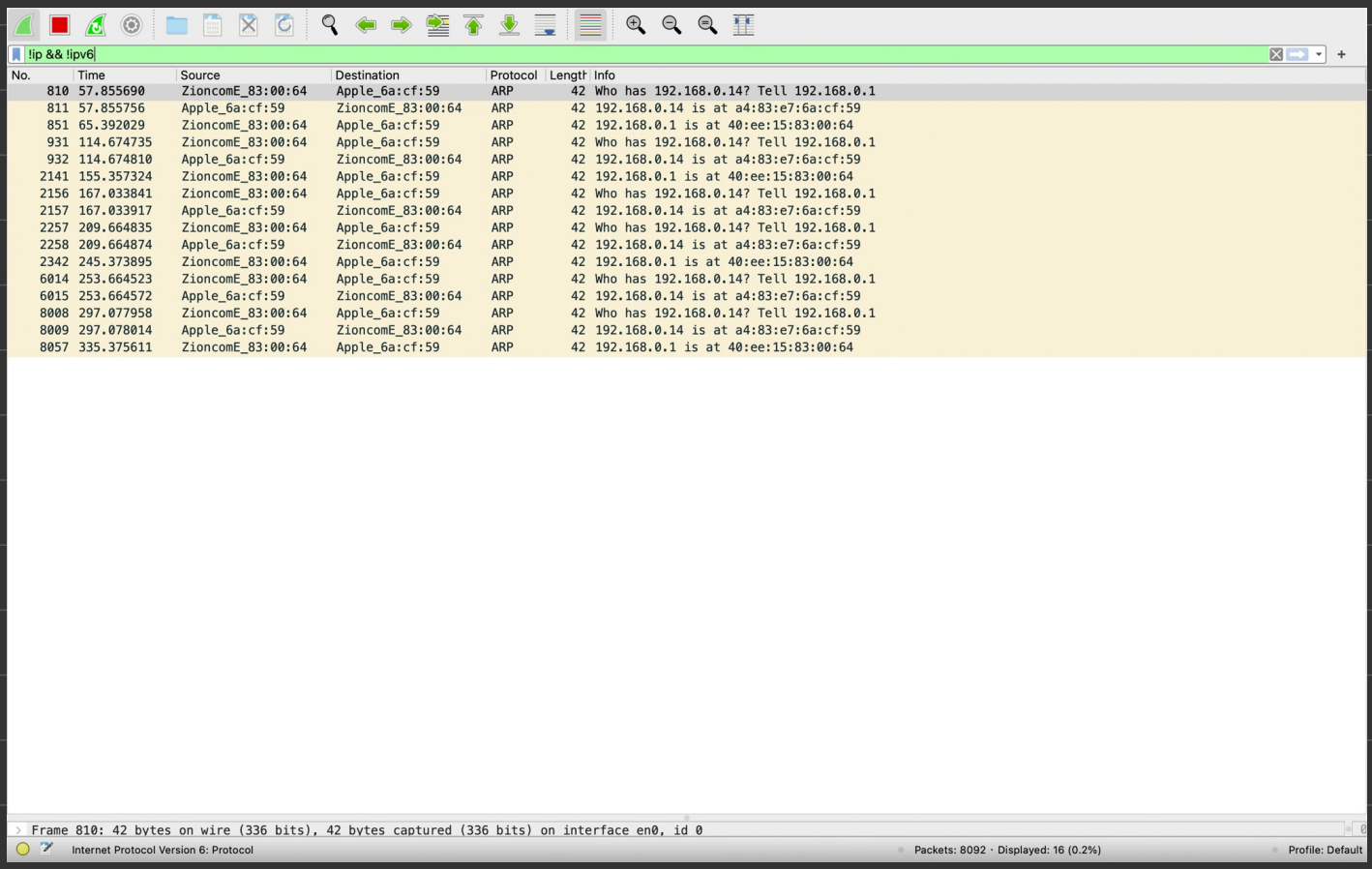
QUIC: a single handshake to establish a secure session

(2) Multiplexing without head-of-line blocking

QUIC: 多路複用

(在同一個連線中進行多個 stream 的傳輸，∴某一個 stream 中的 packet 遺失時，其他 stream 仍可正常傳輸)

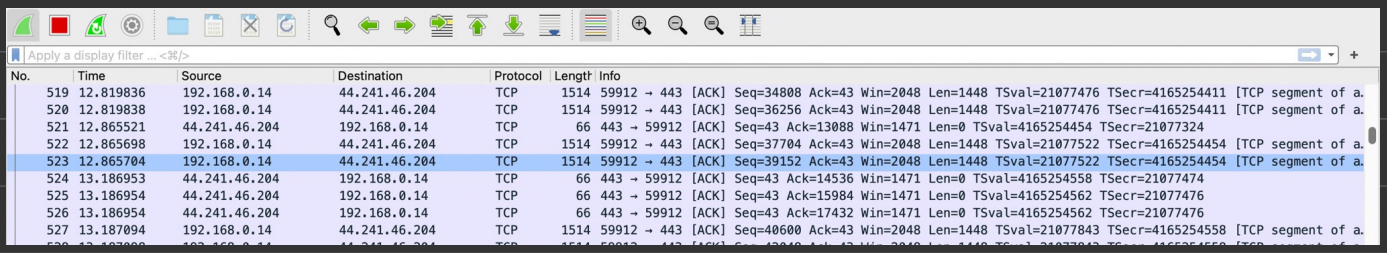
3. add constrain to filter (!ip && !ipv6)



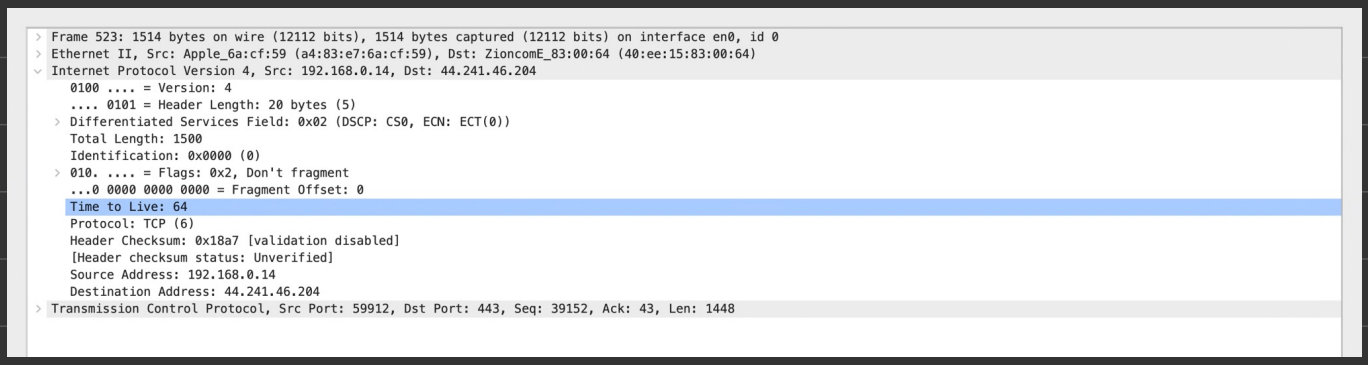
4. (1) TTL:

represents the amount of time when the packet is floating on a network

(2)



No.	Time	Source	Destination	Protocol	Length	Info
519	12.819836	192.168.0.14	44.241.46.204	TCP	1514	59912 → 443 [ACK] Seq=34808 Ack=43 Win=2048 Len=1448 TSval=21077476 TSecr=4165254411 [TCP segment of a.
520	12.819838	192.168.0.14	44.241.46.204	TCP	1514	59912 → 443 [ACK] Seq=36256 Ack=43 Win=2048 Len=1448 TSval=21077476 TSecr=4165254411 [TCP segment of a.
521	12.865521	44.241.46.204	192.168.0.14	TCP	66	443 → 59912 [ACK] Seq=43 Ack=13088 Win=1471 Len=0 TSval=4165254454 TSecr=21077324
522	12.865698	192.168.0.14	44.241.46.204	TCP	1514	59912 → 443 [ACK] Seq=37704 Ack=43 Win=2048 Len=1448 TSval=21077522 TSecr=4165254454 [TCP segment of a.
523	12.865704	192.168.0.14	44.241.46.204	TCP	1514	59912 → 443 [ACK] Seq=39152 Ack=43 Win=2048 Len=1448 TSval=21077522 TSecr=4165254454 [TCP segment of a.
524	13.186953	44.241.46.204	192.168.0.14	TCP	66	443 → 59912 [ACK] Seq=43 Ack=14536 Win=1471 Len=0 TSval=4165254558 TSecr=21077474
525	13.186954	44.241.46.204	192.168.0.14	TCP	66	443 → 59912 [ACK] Seq=43 Ack=15984 Win=1471 Len=0 TSval=4165254562 TSecr=21077476
526	13.186954	44.241.46.204	192.168.0.14	TCP	66	443 → 59912 [ACK] Seq=43 Ack=17432 Win=1471 Len=0 TSval=4165254562 TSecr=21077476
527	13.187094	192.168.0.14	44.241.46.204	TCP	1514	59912 → 443 [ACK] Seq=40600 Ack=43 Win=2048 Len=1448 TSval=21077843 TSecr=4165254558 [TCP segment of a.

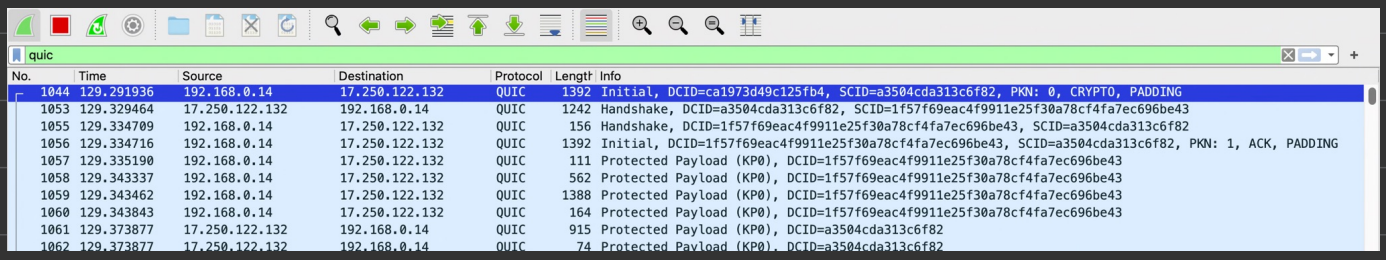


```
> Frame 523: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
> Ethernet II, Src: Apple_6a:cf:59 (a4:83:e7:6a:cf:59), Dst: ZioncomE_83:00:64 (40:ee:15:83:00:64)
v Internet Protocol Version 4, Src: 192.168.0.14, Dst: 44.241.46.204
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))
    Total Length: 1500
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x18a7 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.14
    Destination Address: 44.241.46.204
> Transmission Control Protocol, Src Port: 59912, Dst Port: 443, Seq: 39152, Ack: 43, Len: 1448
```

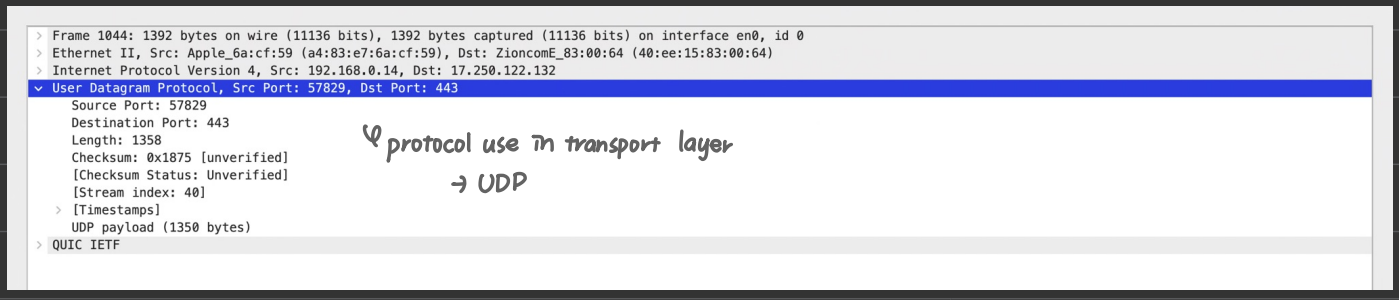
↳ Choose No. 523 → Internet Protocol Version 4

Then we'll get No. 523's Time to Live = 64

5. UDP



No.	Time	Source	Destination	Protocol	Length	Info
1044	129.291936	192.168.0.14	17.250.122.132	QUIC	1392	Initial, DCID=ca1973d49c125fb4, SCID=a3504cda313c6f82, PKN: 0, CRYPTO, PADDING
1053	129.329464	17.250.122.132	192.168.0.14	QUIC	1242	Handshake, DCID=a3504cda313c6f82, SCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43
1055	129.334709	192.168.0.14	17.250.122.132	QUIC	156	Handshake, DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43, SCID=a3504cda313c6f82
1056	129.334716	192.168.0.14	17.250.122.132	QUIC	1392	Initial, DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43, SCID=a3504cda313c6f82, PKN: 1, ACK, PADDING
1057	129.335190	192.168.0.14	17.250.122.132	QUIC	111	Protected Payload (KP0), DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43
1058	129.343337	192.168.0.14	17.250.122.132	QUIC	562	Protected Payload (KP0), DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43
1059	129.343462	192.168.0.14	17.250.122.132	QUIC	1388	Protected Payload (KP0), DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43
1060	129.343843	192.168.0.14	17.250.122.132	QUIC	164	Protected Payload (KP0), DCID=1f57f69eac4f9911e25f30a78cf4fa7ec696be43
1061	129.373877	17.250.122.132	192.168.0.14	QUIC	915	Protected Payload (KP0), DCID=a3504cda313c6f82
1062	129.373877	17.250.122.132	192.168.0.14	QUIC	74	Protected Payload (KP0), DCID=a3504cda313c6f82



```
> Frame 1044: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface en0, id 0
> Ethernet II, Src: Apple_6a:cf:59 (a4:83:e7:6a:cf:59), Dst: ZioncomE_83:00:64 (40:ee:15:83:00:64)
> Internet Protocol Version 4, Src: 192.168.0.14, Dst: 17.250.122.132
v User Datagram Protocol, Src Port: 57829, Dst Port: 443
    Source Port: 57829
    Destination Port: 443
    Length: 1358
    Checksum: 0x1875 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 40]
  > [Timestamps]
    UDP payload (1350 bytes)
> QUIC IETF
```

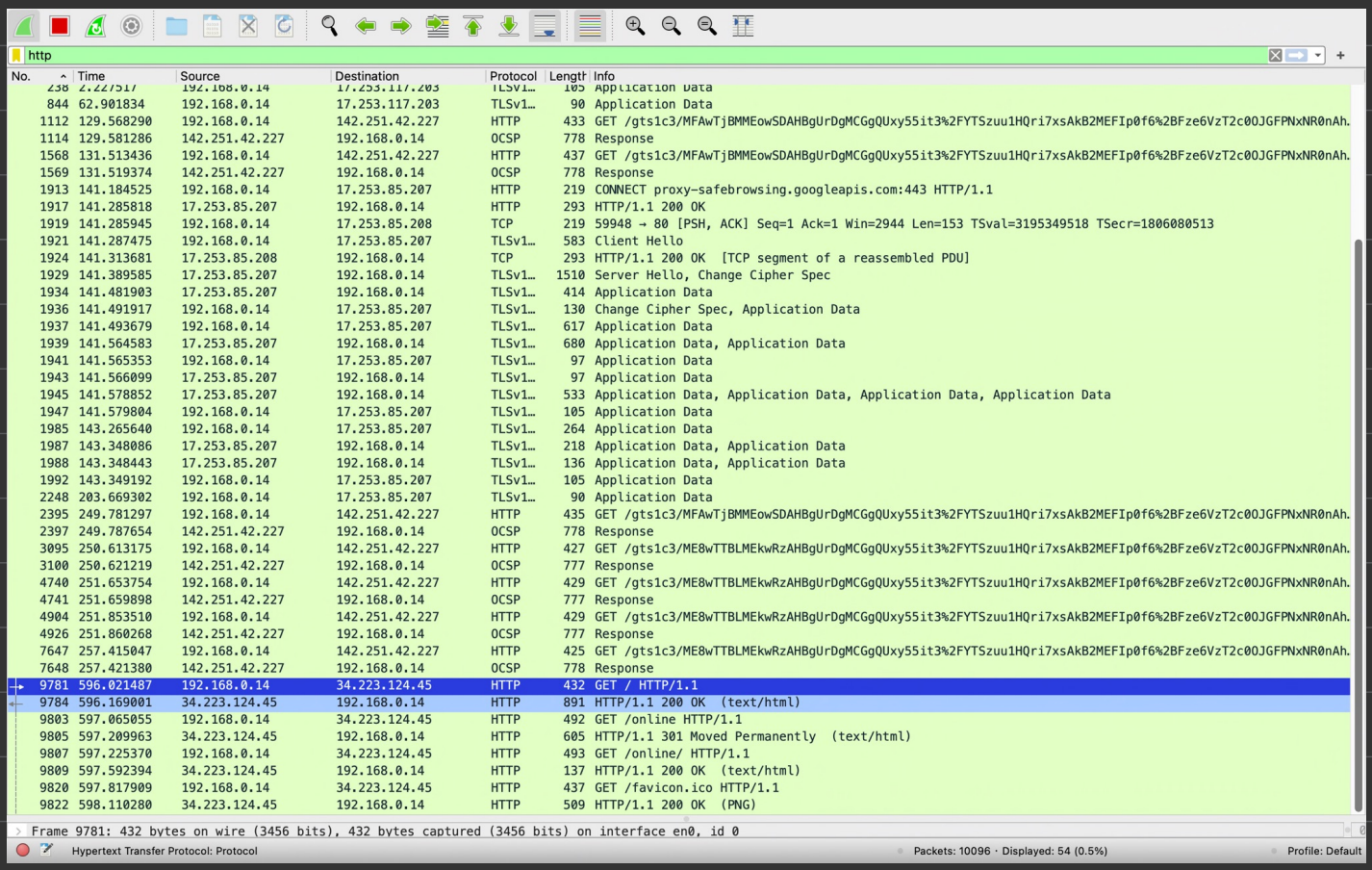
↳ protocol use in transport layer → UDP

Type "quic" in the display filter → choose anyone you like

for example choose No. 1044

→ it shows "User Datagram Protocol

6.



http

No.	Time	Source	Destination	Protocol	Length	Info
844	62.901834	192.168.0.14	17.253.117.203	TLSv1…	90	Application Data
1112	129.568290	192.168.0.14	142.251.42.227	HTTP	433	GET /gts1c3/MFAwTjBMMEowSDAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAh…
1114	129.581286	142.251.42.227	192.168.0.14	OCSP	778	Response
1568	131.513436	192.168.0.14	142.251.42.227	HTTP	437	GET /gts1c3/MFAwTjBMMEowSDAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAh…
1569	131.519374	142.251.42.227	192.168.0.14	OCSP	778	Response
1913	141.184525	192.168.0.14	17.253.85.207	HTTP	219	CONNECT proxy-safebrowsing.googleapis.com:443 HTTP/1.1
1917	141.285818	17.253.85.207	192.168.0.14	HTTP	293	HTTP/1.1 200 OK
1919	141.285945	192.168.0.14	17.253.85.208	TCP	219	59948 → 80 [PSH, ACK] Seq=1 Ack=1 Win=2944 Len=153 TSval=3195349518 TSecr=1806080513
1921	141.287475	192.168.0.14	17.253.85.207	TLSv1…	583	Client Hello
1924	141.313681	17.253.85.208	192.168.0.14	TCP	293	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]
1929	141.389585	17.253.85.207	192.168.0.14	TLSv1…	1510	Server Hello, Change Cipher Spec
1934	141.481903	17.253.85.207	192.168.0.14	TLSv1…	414	Application Data
1936	141.491917	192.168.0.14	17.253.85.207	TLSv1…	130	Change Cipher Spec, Application Data
1937	141.493679	192.168.0.14	17.253.85.207	TLSv1…	617	Application Data
1939	141.564583	17.253.85.207	192.168.0.14	TLSv1…	680	Application Data, Application Data
1941	141.565353	192.168.0.14	17.253.85.207	TLSv1…	97	Application Data
1943	141.566099	17.253.85.207	192.168.0.14	TLSv1…	97	Application Data
1945	141.578852	17.253.85.207	192.168.0.14	TLSv1…	533	Application Data, Application Data, Application Data, Application Data
1947	141.579804	192.168.0.14	17.253.85.207	TLSv1…	105	Application Data
1985	143.265640	192.168.0.14	17.253.85.207	TLSv1…	264	Application Data
1987	143.348086	17.253.85.207	192.168.0.14	TLSv1…	218	Application Data, Application Data
1988	143.348443	17.253.85.207	192.168.0.14	TLSv1…	136	Application Data, Application Data
1992	143.349192	192.168.0.14	17.253.85.207	TLSv1…	105	Application Data
2248	203.669302	192.168.0.14	17.253.85.207	TLSv1…	90	Application Data
2395	249.781297	192.168.0.14	142.251.42.227	HTTP	435	GET /gts1c3/MFAwTjBMMEowSDAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAh…
2397	249.787654	142.251.42.227	192.168.0.14	OCSP	778	Response
3095	250.613175	192.168.0.14	142.251.42.227	HTTP	427	GET /gts1c3/ME8wTTBLMEkwRzAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAh…
3100	250.621219	142.251.42.227	192.168.0.14	OCSP	777	Response
4740	251.653754	192.168.0.14	142.251.42.227	HTTP	429	GET /gts1c3/ME8wTTBLMEkwRzAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAh…
4741	251.659898	142.251.42.227	192.168.0.14	OCSP	777	Response
4904	251.853510	192.168.0.14	142.251.42.227	HTTP	429	GET /gts1c3/ME8wTTBLMEkwRzAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAh…
4926	251.860268	142.251.42.227	192.168.0.14	OCSP	777	Response
7647	257.415047	192.168.0.14	142.251.42.227	HTTP	425	GET /gts1c3/ME8wTTBLMEkwRzAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c0OJGFPNxNR0nAh…
7648	257.421380	142.251.42.227	192.168.0.14	OCSP	778	Response
9781	596.021487	192.168.0.14	34.223.124.45	HTTP	432	GET / HTTP/1.1
9784	596.169001	34.223.124.45	192.168.0.14	HTTP	891	HTTP/1.1 200 OK (text/html)
9803	597.065055	192.168.0.14	34.223.124.45	HTTP	492	GET /online HTTP/1.1
9805	597.209963	34.223.124.45	192.168.0.14	HTTP	605	HTTP/1.1 301 Moved Permanently (text/html)
9807	597.225370	192.168.0.14	34.223.124.45	HTTP	493	GET /online/ HTTP/1.1
9809	597.592394	34.223.124.45	192.168.0.14	HTTP	137	HTTP/1.1 200 OK (text/html)
9820	597.817909	192.168.0.14	34.223.124.45	HTTP	437	GET /favicon.ico HTTP/1.1
9822	598.110280	34.223.124.45	192.168.0.14	HTTP	509	HTTP/1.1 200 OK (PNG)

Frame 9781: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface en0, id 0

Hypertext Transfer Protocol: Protocol

Packets: 10096 · Displayed: 54 (0.5%)

Profile: Default

Info time

GET 596.021487

OK 596.169001

Δt = 596.169001 - 596.021487

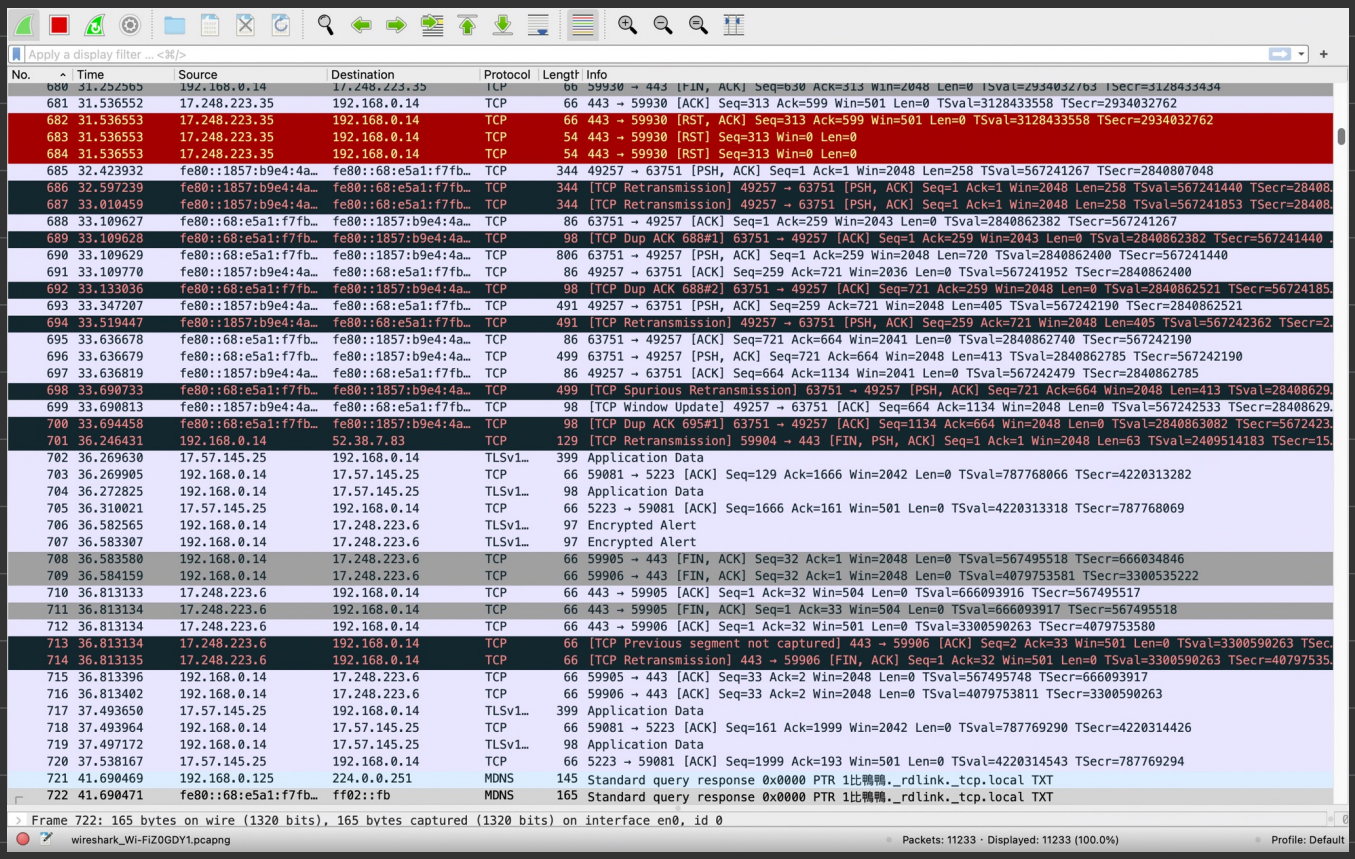
= 0.147514 (s) #

Type "http" in the display filter

→ find two packets which Info says GET and OK with the opposite source and destination

→ calculate the time difference

7.



No.	Time	Source	Destination	Protocol	Length	Info
680	31.252565	192.168.0.14	17.248.223.35	TCP	66	59930 → 443 [FIN, ACK] Seq=630 Ack=313 Win=2048 Len=0 TSval=2934032763 TSecr=3128433434
681	31.536552	17.248.223.35	192.168.0.14	TCP	66	443 → 59930 [ACK] Seq=313 Ack=599 Win=501 Len=0 TSval=3128433558 TSecr=2934032762
682	31.536553	17.248.223.35	192.168.0.14	TCP	66	443 → 59930 [RST, ACK] Seq=313 Ack=599 Win=501 Len=0 TSval=3128433558 TSecr=2934032762
683	31.536553	17.248.223.35	192.168.0.14	TCP	54	443 → 59930 [RST] Seq=313 Win=0 Len=0
684	31.536553	17.248.223.35	192.168.0.14	TCP	54	443 → 59930 [RST] Seq=313 Win=0 Len=0
685	32.423932	fe80::1857:b9e4:4a…	fe80::68:e5a1:f7fb…	TCP	344	49257 → 63751 [PSH, ACK] Seq=1 Ack=1 Win=2048 Len=258 TSval=567241267 TSecr=2840807048
686	32.597239	fe80::1857:b9e4:4a…	fe80::68:e5a1:f7fb…	TCP	344	[TCP Retransmission] 49257 → 63751 [PSH, ACK] Seq=1 Ack=1 Win=2048 Len=258 TSval=567241440 TSecr=28408.
687	33.010459	fe80::1857:b9e4:4a…	fe80::68:e5a1:f7fb…	TCP	344	[TCP Retransmission] 49257 → 63751 [PSH, ACK] Seq=1 Ack=1 Win=2048 Len=258 TSval=567241853 TSecr=28408.
688	33.109627	fe80::68:e5a1:f7fb…	fe80::1857:b9e4:4a…	TCP	86	63751 → 49257 [ACK] Seq=1 Ack=259 Win=2043 Len=0 TSval=2840862382 TSecr=567241267
689	33.109628	fe80::68:e5a1:f7fb…	fe80::1857:b9e4:4a…	TCP	98	[TCP Dup ACK 688#1] 63751 → 49257 [ACK] Seq=1 Ack=259 Win=2043 Len=0 TSval=2840862382 TSecr=567241440 .
690	33.109629	fe80::68:e5a1:f7fb…	fe80::1857:b9e4:4a…	TCP	806	63751 → 49257 [PSH, ACK] Seq=1 Ack=259 Win=2048 Len=720 TSval=2840862400 TSecr=567241440
691	33.109770	fe80::1857:b9e4:4a…	fe80::68:e5a1:f7fb…	TCP	86	49257 → 63751 [ACK] Seq=259 Ack=721 Win=2036 Len=0 TSval=567241952 TSecr=2840862400
692	33.133036	fe80::68:e5a1:f7fb…	fe80::1857:b9e4:4a…	TCP	98	[TCP Dup ACK 688#2] 63751 → 49257 [ACK] Seq=721 Ack=259 Win=2048 Len=0 TSval=2840862521 TSecr=56724185.
693	33.347207	fe80::1857:b9e4:4a…	fe80::68:e5a1:f7fb…	TCP	491	49257 → 63751 [PSH, ACK] Seq=259 Ack=721 Win=2048 Len=405 TSval=567242190 TSecr=2840862521
694	33.519447	fe80::1857:b9e4:4a…	fe80::68:e5a1:f7fb…	TCP	491	[TCP Retransmission] 49257 → 63751 [PSH, ACK] Seq=259 Ack=721 Win=2048 Len=405 TSval=567242362 TSecr=2.
695	33.636678	fe80::68:e5a1:f7fb…	fe80::1857:b9e4:4a…	TCP	86	63751 → 49257 [ACK] Seq=721 Ack=664 Win=2041 Len=0 TSval=2840862740 TSecr=567242190
696	33.636679	fe80::68:e5a1:f7fb…	fe80::1857:b9e4:4a…	TCP	499	63751 → 49257 [PSH, ACK] Seq=721 Ack=664 Win=2048 Len=413 TSval=2840862785 TSecr=567242190
697	33.636819	fe80::1857:b9e4:4a…	fe80::68:e5a1:f7fb…	TCP	86	49257 → 63751 [ACK] Seq=664 Ack=1134 Win=2041 Len=0 TSval=567242479 TSecr=2840862785
698	33.690733	fe80::68:e5a1:f7fb…	fe80::1857:b9e4:4a…	TCP	499	[TCP Spurious Retransmission] 63751 → 49257 [PSH, ACK] Seq=721 Ack=664 Win=2048 Len=413 TSval=28408629.
699	33.690813	fe80::1857:b9e4:4a…	fe80::68:e5a1:f7fb…	TCP	98	[TCP Window Update] 49257 → 63751 [ACK] Seq=664 Ack=1134 Win=2048 Len=0 TSval=567242533 TSecr=28408629.
700	33.694458	fe80::68:e5a1:f7fb…	fe80::1857:b9e4:4a…	TCP	98	[TCP Dup ACK 695#1] 63751 → 49257 [ACK] Seq=1134 Ack=664 Win=2048 Len=0 TSval=2840863082 TSecr=5672423.
701	36.246431	192.168.0.14	52.38.7.83	TCP	129	[TCP Retransmission] 59904 → 443 [FIN, PSH, ACK] Seq=1 Ack=1 Win=2048 Len=63 TSval=2409514183 TSecr=15.
702	36.269630	17.57.145.25	192.168.0.14	TLSv1…	399	Application Data
703	36.269905	192.168.0.14	17.57.145.25	TCP	66	59081 → 5223 [ACK] Seq=129 Ack=1666 Win=2042 Len=0 TSval=787768066 TSecr=4220313282
704	36.272825	192.168.0.14	17.57.145.25	TLSv1…	98	Application Data
705	36.310021	17.57.145.25	192.168.0.14	TCP	66	5223 → 59081 [ACK] Seq=1666 Ack=161 Win=501 Len=0 TSval=4220313318 TSecr=787768069
706	36.582565	192.168.0.14	17.248.223.6	TLSv1…	97	Encrypted Alert
707	36.583307	192.168.0.14	17.248.223.6	TLSv1…	97	Encrypted Alert
708	36.583580	192.168.0.14	17.248.223.6	TCP	66	59905 → 443 [FIN, ACK] Seq=32 Ack=1 Win=2048 Len=0 TSval=567495518 TSecr=666034846
709	36.584159	192.168.0.14	17.248.223.6	TCP	66	59906 → 443 [FIN, ACK] Seq=32 Ack=1 Win=2048 Len=0 TSval=4079753581 TSecr=3300535222
710	36.813133	17.248.223.6	192.168.0.14	TCP	66	443 → 59905 [ACK] Seq=1 Ack=32 Win=504 Len=0 TSval=666093916 TSecr=567495517
711	36.813134	17.248.223.6	192.168.0.14	TCP	66	443 → 59905 [FIN, ACK] Seq=1 Ack=33 Win=504 Len=0 TSval=666093917 TSecr=567495518
712	36.813134	17.248.223.6	192.168.0.14	TCP	66	443 → 59906 [ACK] Seq=1 Ack=32 Win=501 Len=0 TSval=3300590263 TSecr=4079753580
713	36.813134	17.248.223.6	192.168.0.14	TCP	66	[TCP Previous segment not captured] 443 → 59906 [ACK] Seq=2 Ack=33 Win=501 Len=0 TSval=3300590263 TSec.
714	36.813135	17.248.223.6	192.168.0.14	TCP	66	[TCP Retransmission] 443 → 59906 [FIN, ACK] Seq=1 Ack=32 Win=501 Len=0 TSval=3300590263 TSecr=40797535.
715	36.813396	192.168.0.14	17.248.223.6	TCP	66	59905 → 443 [ACK] Seq=33 Ack=2 Win=2048 Len=0 TSval=567495748 TSecr=666093917
716	36.813402	192.168.0.14	17.248.223.6	TCP	66	59906 → 443 [ACK] Seq=33 Ack=2 Win=2048 Len=0 TSval=4079753811 TSecr=3300590263
717	37.493650	17.57.145.25	192.168.0.14	TLSv1…	399	Application Data
718	37.493964	192.168.0.14	17.57.145.25	TCP	66	59081 → 5223 [ACK] Seq=161 Ack=1999 Win=2042 Len=0 TSval=787769290 TSecr=4220314426
719	37.497172	192.168.0.14	17.57.145.25	TLSv1…	98	Application Data
720	37.538167	17.57.145.25	192.168.0.14	TCP	66	5223 → 59081 [ACK] Seq=1999 Ack=193 Win=501 Len=0 TSval=4220314543 TSecr=787769294
721	41.690469	192.168.0.125	224.0.0.251	MDNS	145	Standard query response 0x0000 PTR 1比鴨鴨._rdlink._tcp.local TXT
722	41.690471	fe80::68:e5a1:f7fb…	ff02::fb	MDNS	165	Standard query response 0x0000 PTR 1比鴨鴨._rdlink._tcp.local TXT

Frame 722: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface en0, id 0

wireshark_Wi-FiZ0GDY1.pcapng — Packets: 11233 · Displayed: 11233 (100.0%) — Profile: Default

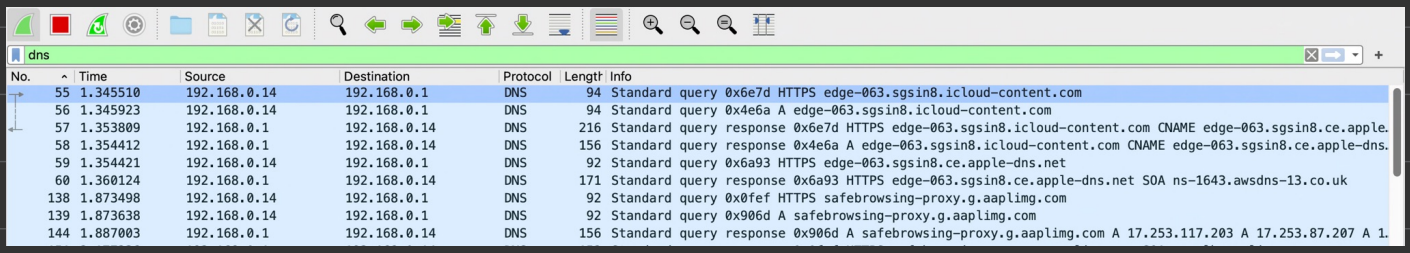
No.702 → IPV4

```
> Frame 702: 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface en0, id 0
> Ethernet II, Src: ZioncomE_83:00:64 (40:ee:15:83:00:64), Dst: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
> Internet Protocol Version 4 Src: 17.57.145.25, Dst: 192.168.0.14
> Transmission Control Protocol, Src Port: 5223, Dst Port: 59081, Seq: 1333, Ack: 129, Len: 333
> Transport Layer Security
```

No.700 → IPV6

```
> Frame 700: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: c6:18:84:a0:da:39 (c6:18:84:a0:da:39), Dst: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
> Internet Protocol Version 6 Src: fe80::68:e5a1:f7fb:f907, Dst: fe80::1857:b9e4:4a0a:5a4b
> Transmission Control Protocol, Src Port: 63751, Dst Port: 49257, Seq: 1134, Ack: 664, Len: 0
```

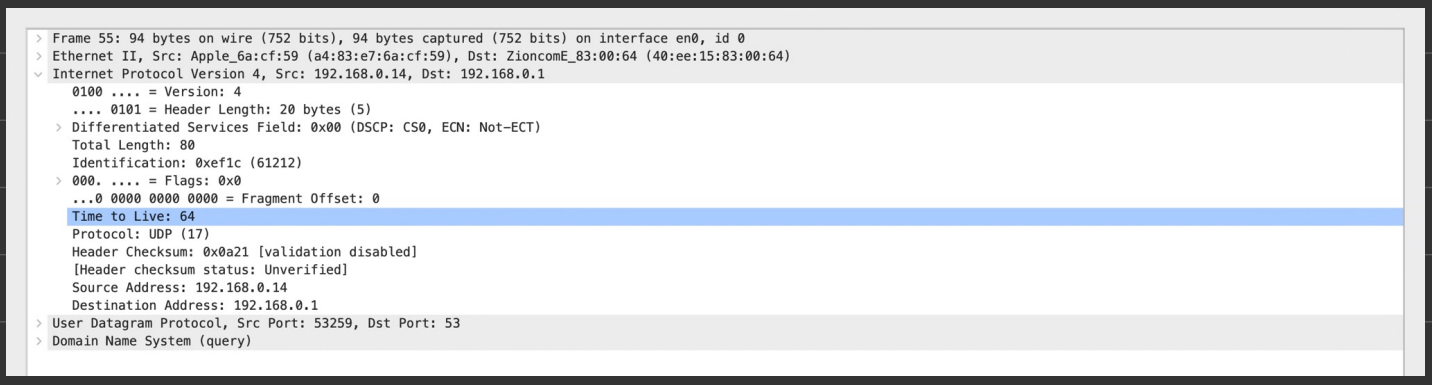
8.



dns

No.	Time	Source	Destination	Protocol	Length	Info
55	1.345510	192.168.0.14	192.168.0.1	DNS	94	Standard query 0x6e7d HTTPS edge-063.sgsin8.icloud-content.com
56	1.345923	192.168.0.14	192.168.0.1	DNS	94	Standard query 0x4e6a A edge-063.sgsin8.icloud-content.com
57	1.353809	192.168.0.1	192.168.0.14	DNS	216	Standard query response 0x6e7d HTTPS edge-063.sgsin8.icloud-content.com CNAME edge-063.sgsin8.ce.apple.
58	1.354412	192.168.0.1	192.168.0.14	DNS	156	Standard query response 0x4e6a A edge-063.sgsin8.icloud-content.com CNAME edge-063.sgsin8.ce.apple-dns.
59	1.354421	192.168.0.14	192.168.0.1	DNS	92	Standard query 0x6a93 HTTPS edge-063.sgsin8.ce.apple-dns.net
60	1.360124	192.168.0.1	192.168.0.14	DNS	171	Standard query response 0x6a93 HTTPS edge-063.sgsin8.ce.apple-dns.net SOA ns-1643.awsdns-13.co.uk
138	1.873498	192.168.0.14	192.168.0.1	DNS	92	Standard query 0x0fef HTTPS safebrowsing-proxy.g.aaplimg.com
139	1.873638	192.168.0.14	192.168.0.1	DNS	92	Standard query 0x906d A safebrowsing-proxy.g.aaplimg.com
144	1.887003	192.168.0.1	192.168.0.14	DNS	156	Standard query response 0x906d A safebrowsing-proxy.g.aaplimg.com A 17.253.117.203 A 17.253.87.207 A 1.

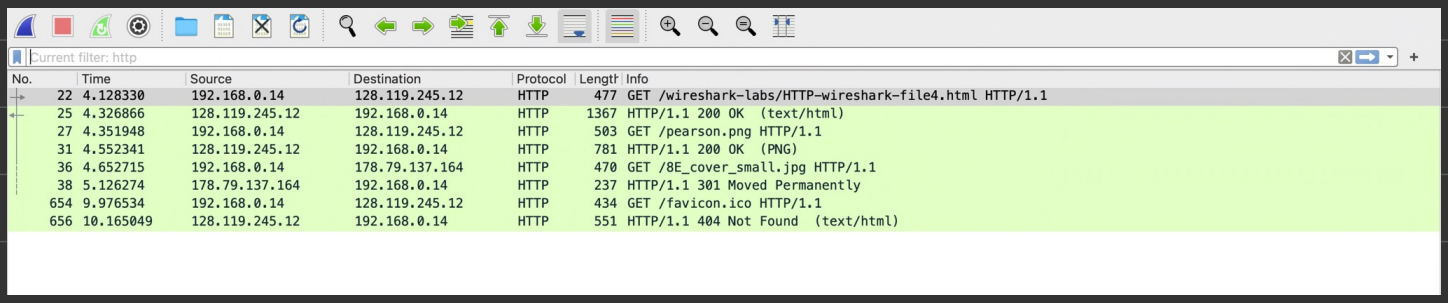
No. 55



```
Frame 55: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface en0, id 0
Ethernet II, Src: Apple_6a:cf:59 (a4:83:e7:6a:cf:59), Dst: ZioncomE_83:00:64 (40:ee:15:83:00:64)
Internet Protocol Version 4, Src: 192.168.0.14, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 80
    Identification: 0xef1c (61212)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x0a21 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.14
    Destination Address: 192.168.0.1
User Datagram Protocol, Src Port: 53259, Dst Port: 53
Domain Name System (query)
```

(9 Type "DNS" in display filter → choose any one you like
for example choose No.55
→ Internet Protocol Version 4
→ You'll get No.55's TTL = 54

9.



Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
22	4.128330	192.168.0.14	128.119.245.12	HTTP	477	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
25	4.326866	128.119.245.12	192.168.0.14	HTTP	1367	HTTP/1.1 200 OK (text/html)
27	4.351948	192.168.0.14	128.119.245.12	HTTP	503	GET /pearson.png HTTP/1.1
31	4.552341	128.119.245.12	192.168.0.14	HTTP	781	HTTP/1.1 200 OK (PNG)
36	4.652715	192.168.0.14	178.79.137.164	HTTP	470	GET /8E_cover_small.jpg HTTP/1.1
38	5.126274	178.79.137.164	192.168.0.14	HTTP	237	HTTP/1.1 301 Moved Permanently
654	9.976534	192.168.0.14	128.119.245.12	HTTP	434	GET /favicon.ico HTTP/1.1
656	10.165049	128.119.245.12	192.168.0.14	HTTP	551	HTTP/1.1 404 Not Found (text/html)

(a) ① 4

② 128.119.245.12

128.119.245.12

178.79.137.164

128.119.245.12

(b) ① Serially

② because second image's "GET" is sent after receiving first image