Homework 2

1. 3 different protocols: TCP, UDP, ARP

(a) TCP, UDP → transport layer

(pass segments and destination adress to network)

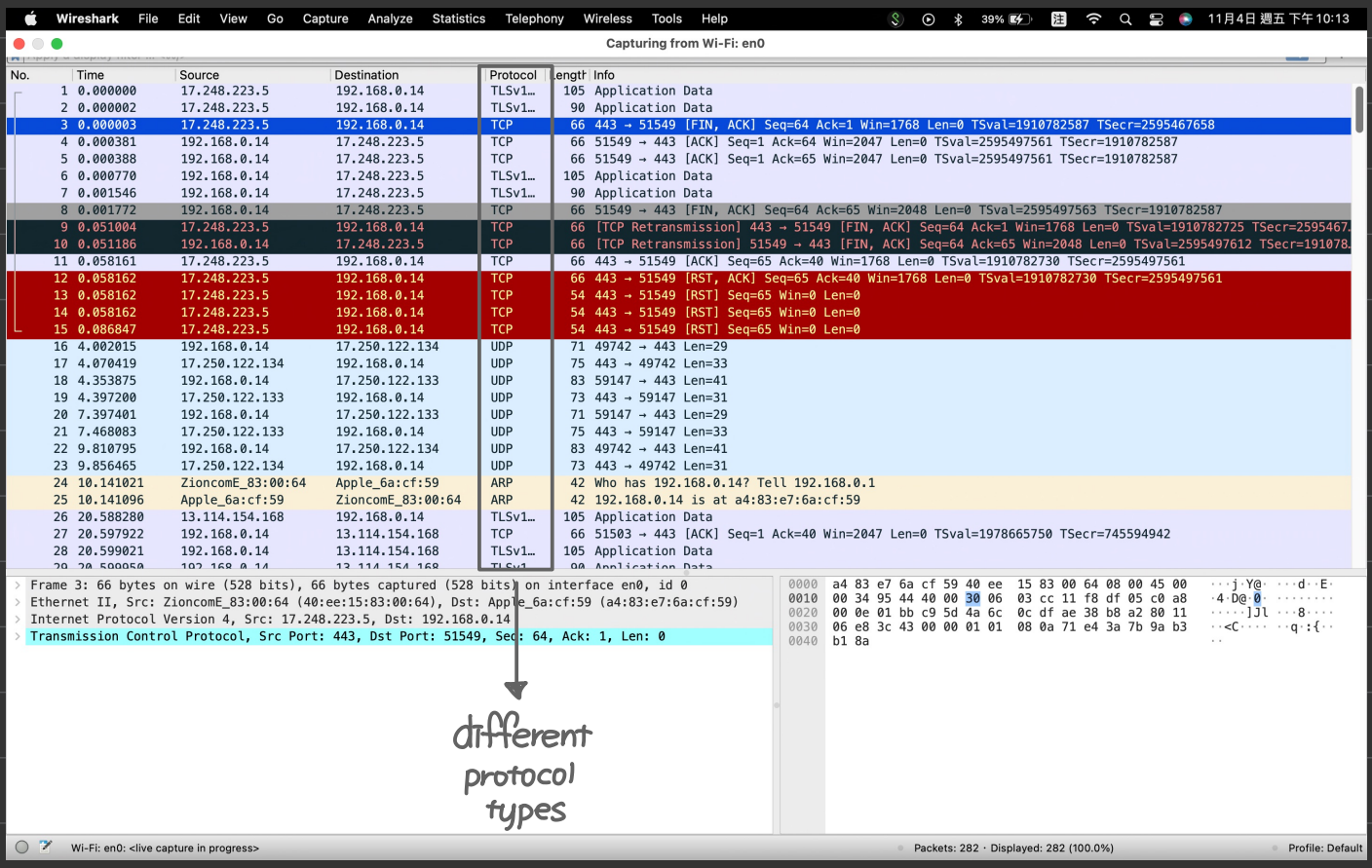
→ TCP

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

→ UDP

- provides connectionless service to its applications

(b) ARP → network layer

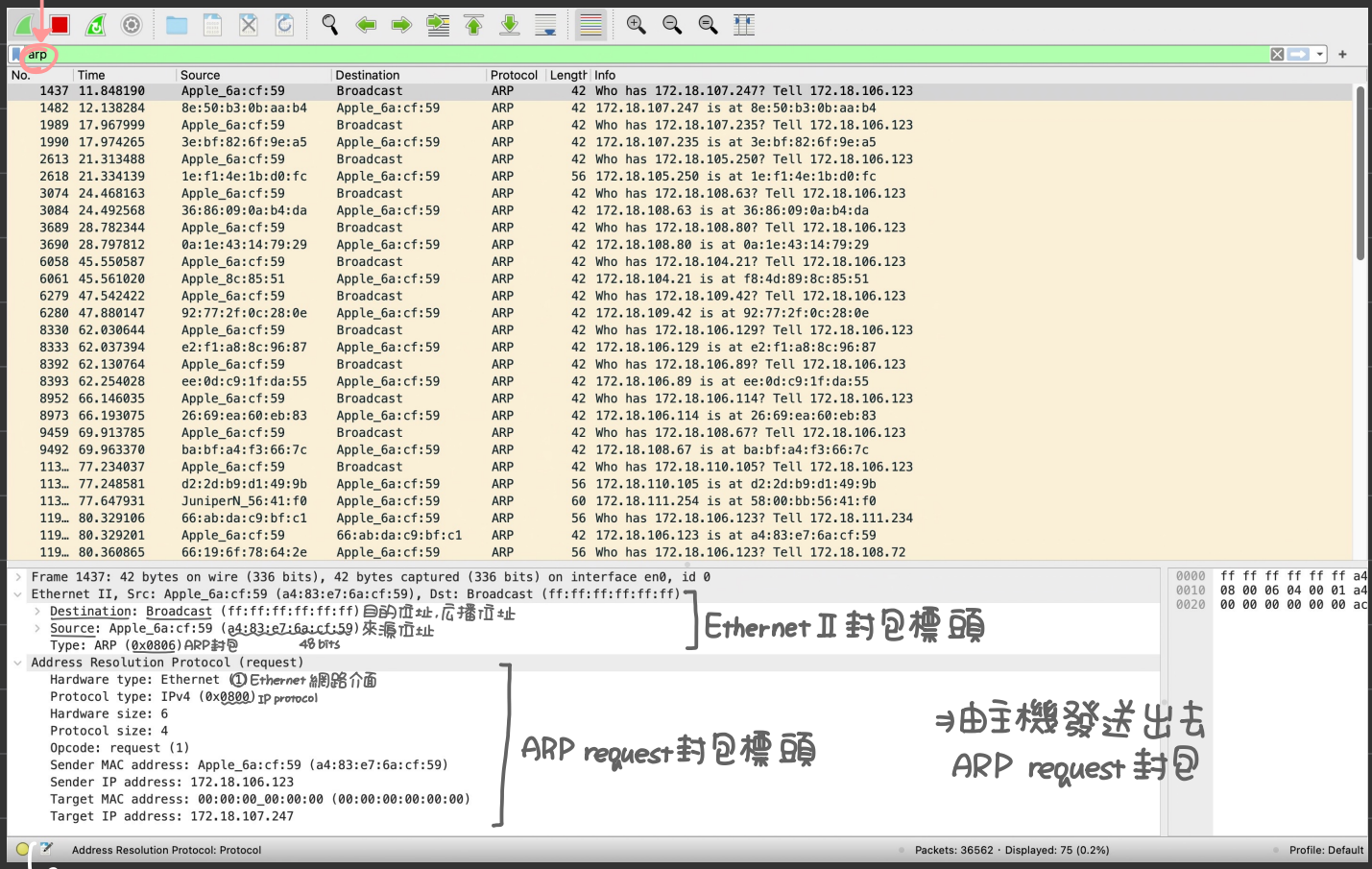


2. ARP protocol - Ethernet 和 IP 位址的轉換

- 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

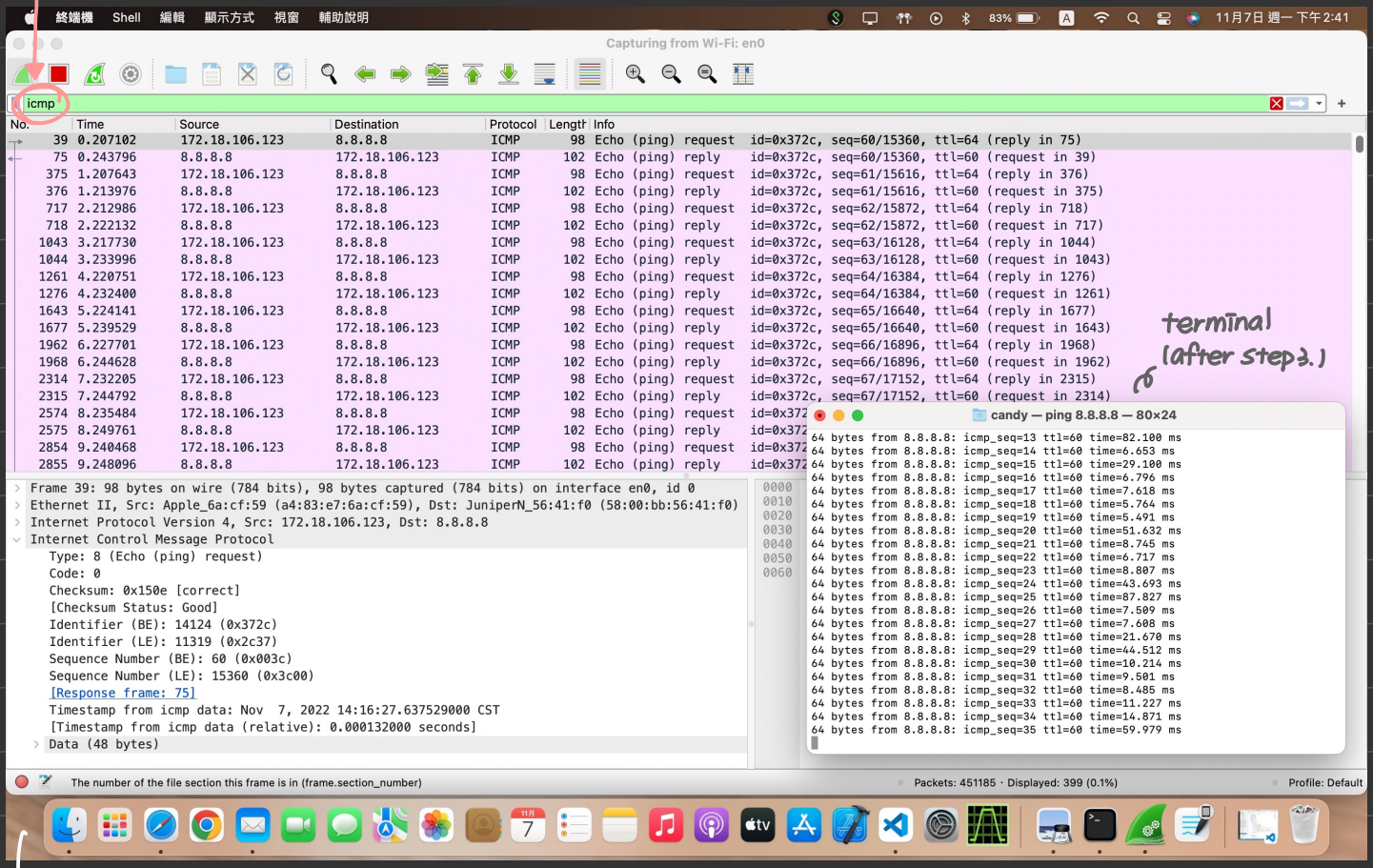
3. ICMP protocol → 解析封包或分析路由(藉由D傳的錯誤訊息分析)

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

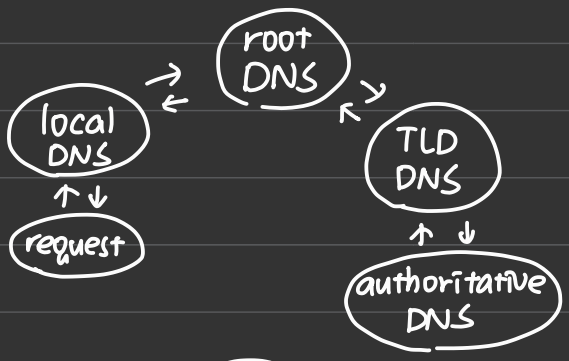
非 application layer process

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

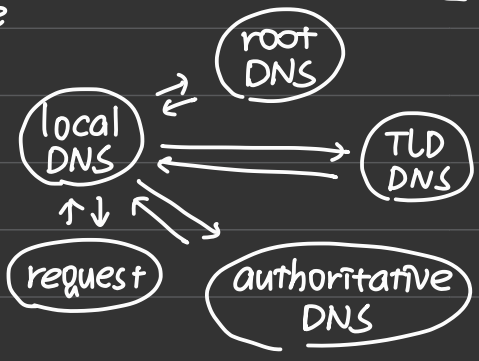
∴就不用 port 去指示

4. DNS protocol → 將網域名稱轉為 IP 位址

① Recursive

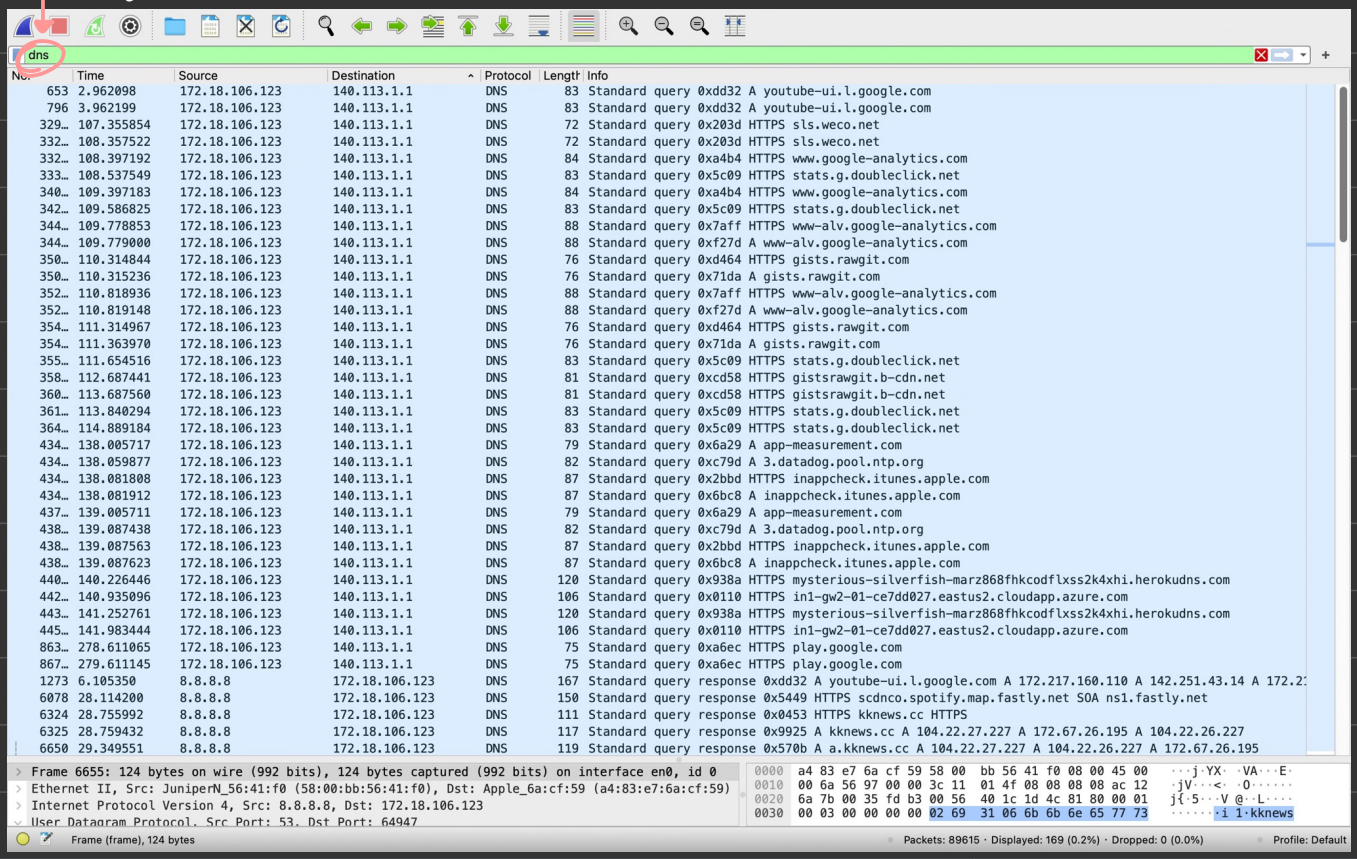


② Iterative

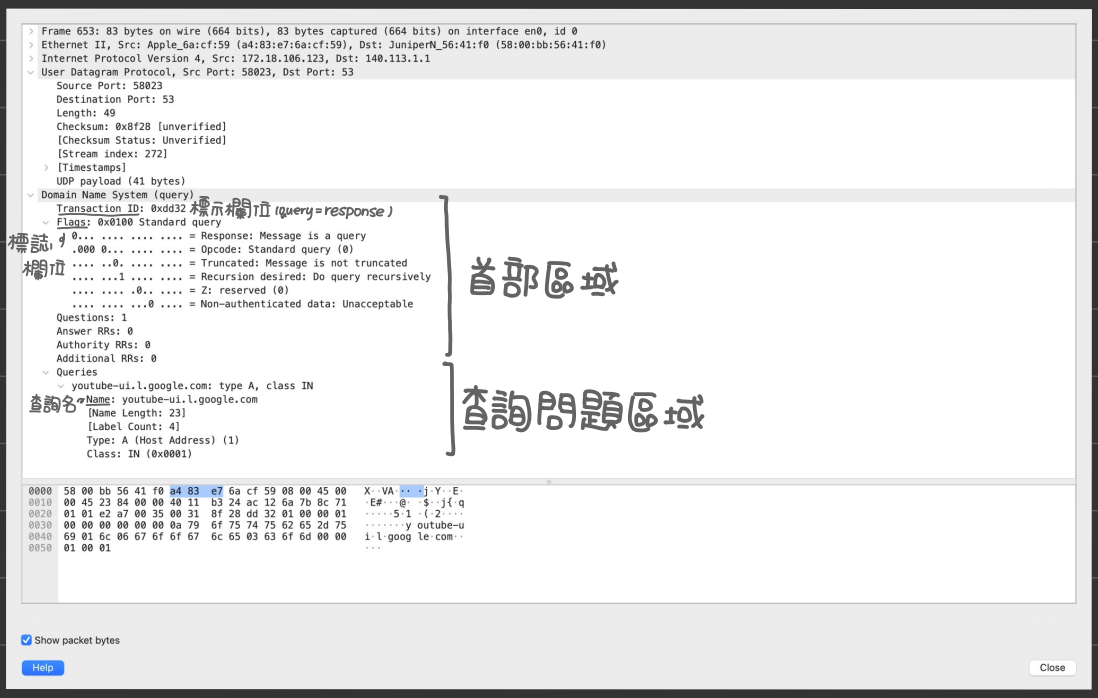


Method to find DNS in wireshark

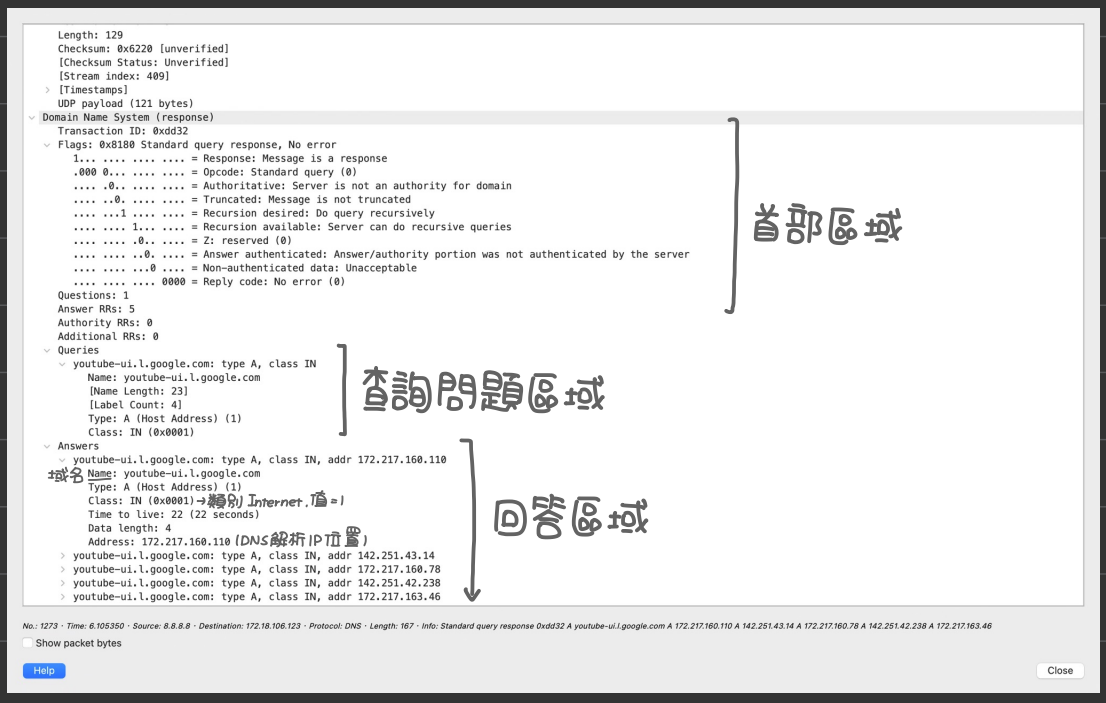
1. chose the interface(s) you want to capture
2. type "dns" in the display filter
3. you can find out DNS packets of the interface(s)



① query packet



② response packet

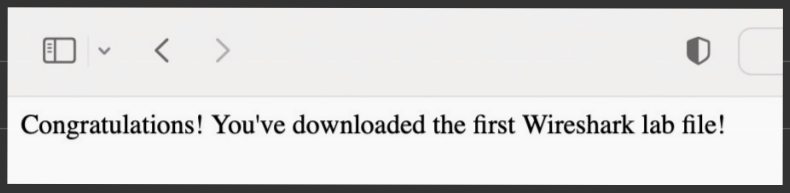


* Flags → 查詢/響應 → 截斷 → 返回碼

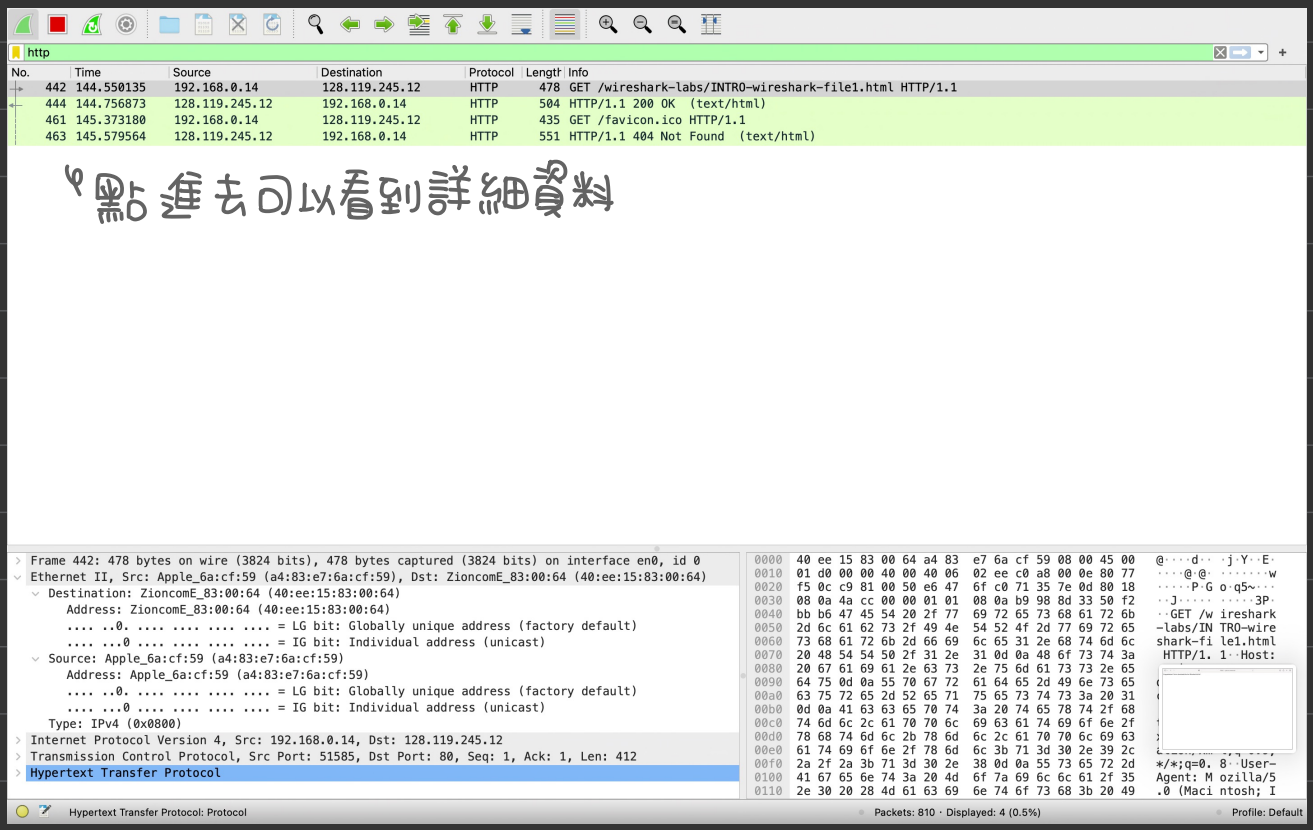
QR	opcode	AA	TC	RD	RA	(zero)	rcode
1	4	1	1	1	1	3	4

- AA → 授權回答
- RD → 是否希望得到 recursive 的回答
- opcode → 查詢/響應類型

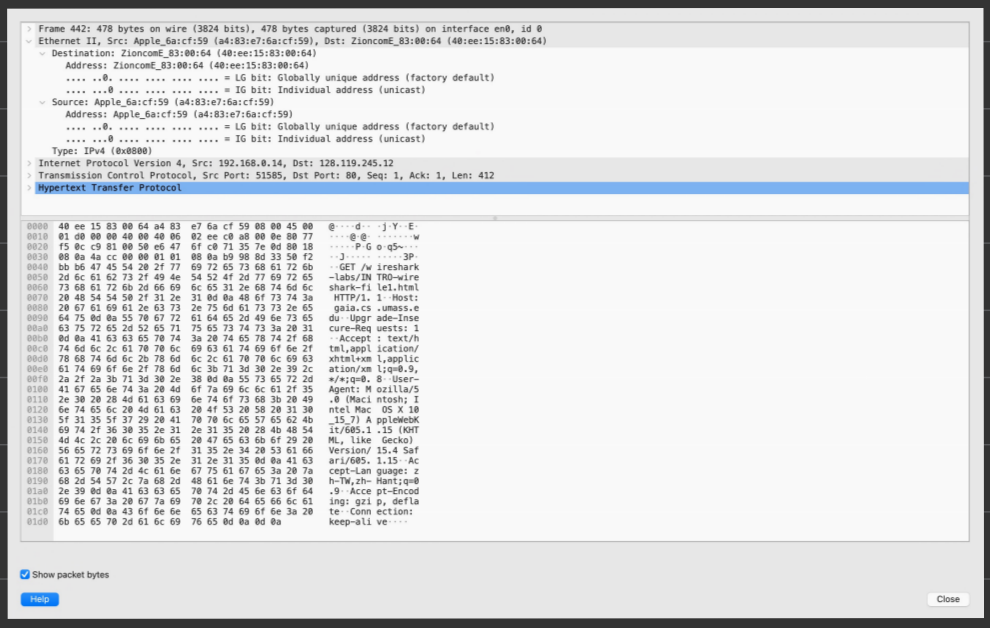
5. ① enter the URL



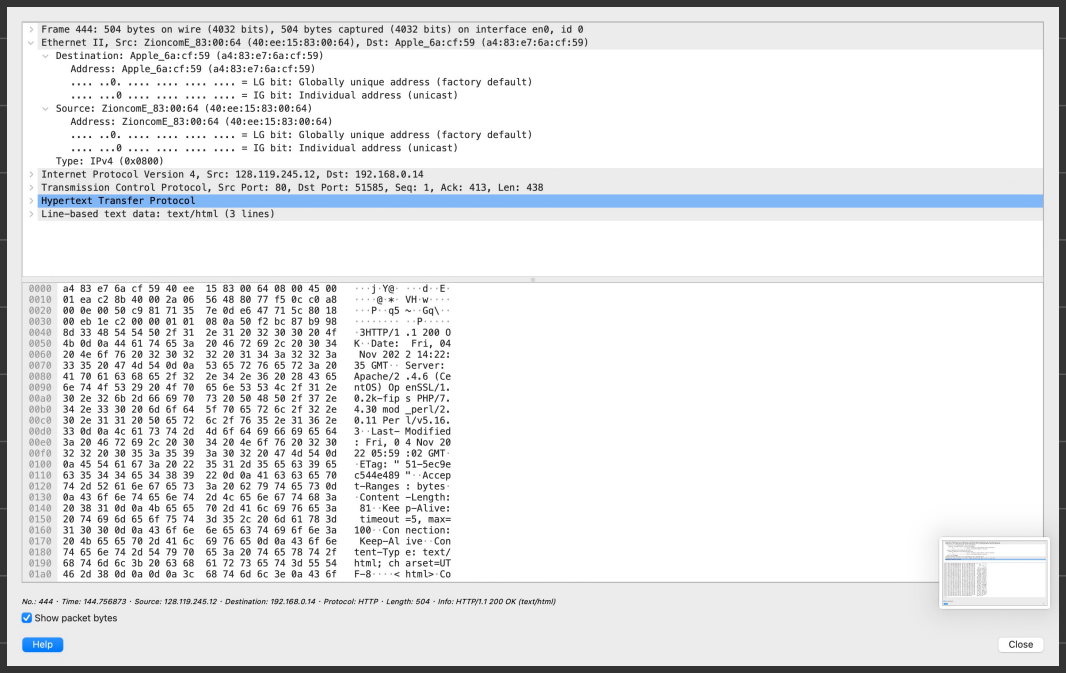
② HTTP packets information



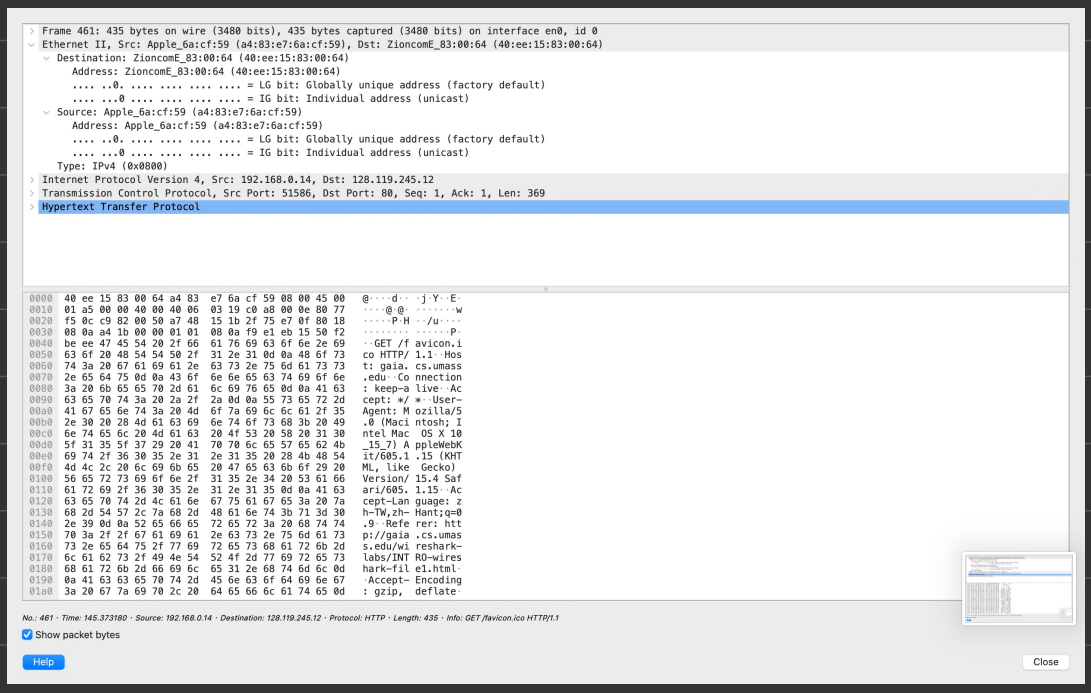
(a) 128.119.245.12



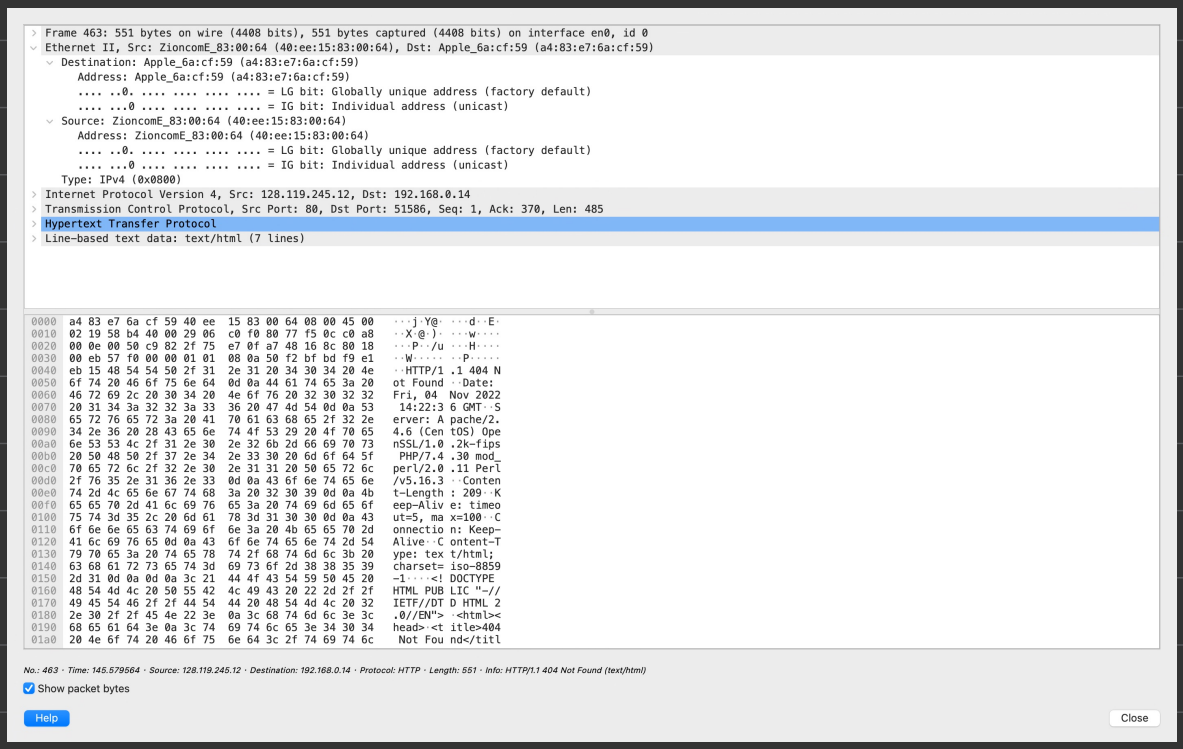
(b) 192.168.0.14



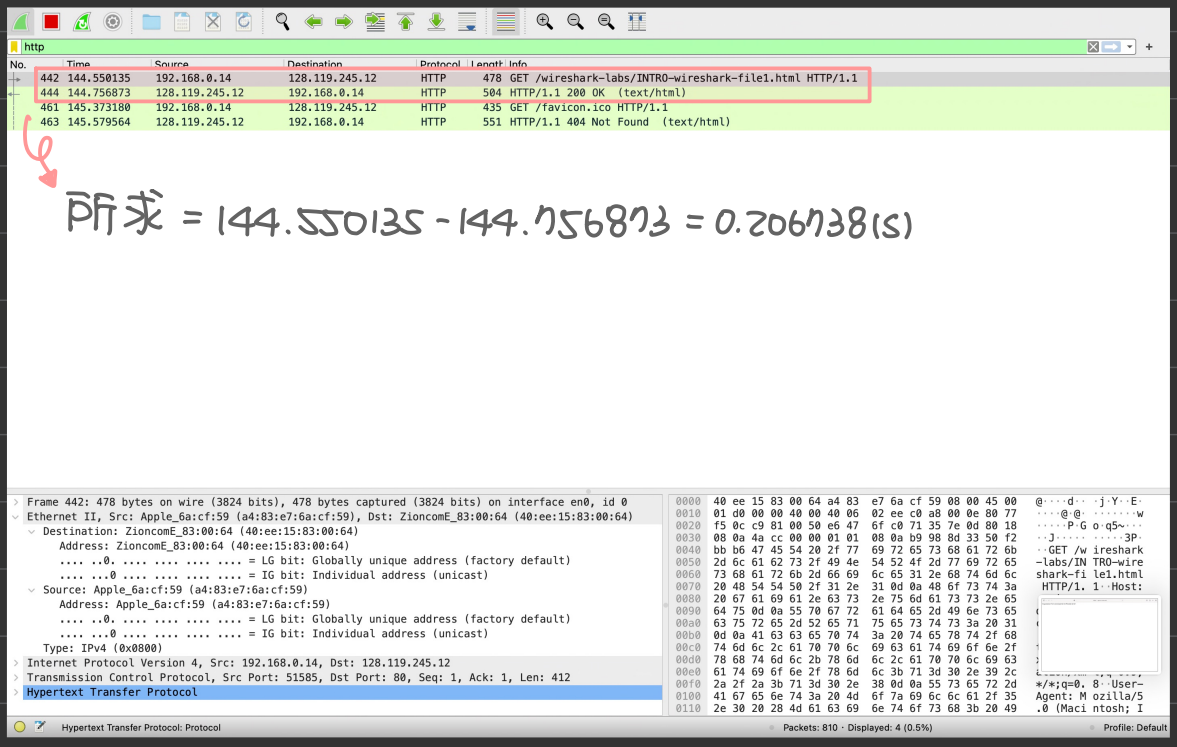
(c) 128.119.245.12



(d) 192.168.0.14

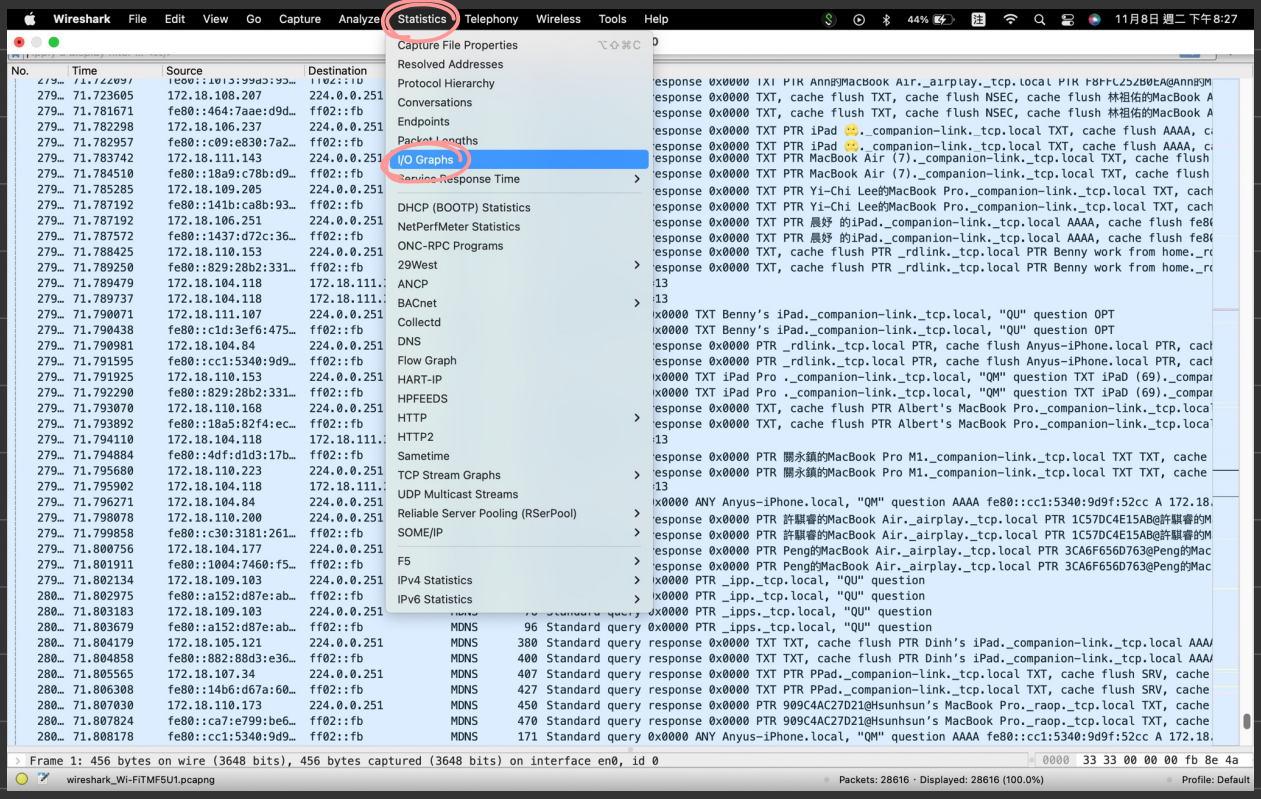


6.



1. Method to get the number of income packets

1. Chose "Statistics" → "I/O Graphs"



2. Select "Interval" to 1 min

8. ① TLS protocol → 促進網際網路通信的私密性和資料安全
(加密通信)
→ 分為 (a) 加密：隱藏從第三方傳輸的資料
(b) 身份驗証：確保交換資訊的兩方
是它們所稱的身份
(c) 完整性：驗証資料沒有被偽造、更改
② 因為 TLS packet 的資料是經過加密的，
要有相對應的密鑰才可以看到 packet 的內容

9. ∵ wireshark is using layer 3 protocol to adress and deliver
but MAC adress for remote host is in layer 2.

10. ① Capture filter → 只保留符合條件的 packets
(i.e. 在抓包時捨棄不符合條件的 packets)
② Display filter → 在已抓到的 packets 中對對應的 packets 進行過濾，
只顯示符合條件的 packets
(i.e. 隱藏不符合的 packets)