

Homework 2

1. 3 different protocols: TCP, UDP, ARP

(a) TCP, UDP → transport layer

(pass segments and destination address 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

Wireshark Screenshot:

- Protocol: TCP
- Length: 66
- Info: 443 → 51549 [FIN, ACK] Seq=64 Ack=1 Win=1768 Len=0 Tsval=1910782587 TSecr=2595467658
- Source: 17.248.223.5
- Destination: 192.168.0.14
- Sequence Number: 64
- Acknowledgment Number: 1
- Window Size: 1768
- Timestamp: 1910782587
- Timestamp: 2595467658

Hex Dump:

0000	a4 83 e7 6a cf 59 40 ee	15 83 00 64 08 00 45 00	...j.Y@ ...d..E
0010	00 34 95 44 40 00 30 06	03 cc 1f f8 df 05 c0 a8	.4.D@.0 ..JL ..8...
0020	00 0e 01 bb c9 5d 4a 6c	0c df ae 38 b8 02 80 11	..<C... q:{...
0030	06 e8 3c 43 00 00 01 01	08 0a 71 e4 3a 7b 9a b3	..
0040	b1 8a		

different
protocol
types

2. ARP protocol - Ethernet 和 IP 地址的轉換

- 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，所以網段中
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 Address。而查詢方會把 MAC Address 紀錄到
ARP Table 中。

Method to find ARP in wireshark

1. choose 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)

arp

No.	Time	Source	Destination	Protocol	Length	Info
1437	11.848190	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.107.247? Tell 172.18.106.123
1482	12.138284	8e:50:b3:0b:aa:b4	Apple_6a:cf:59	ARP	42	172.18.107.247 is at 8e:50:b3:0b:aa:b4
1989	17.967999	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.107.235? Tell 172.18.106.123
1990	17.974265	3e:bf:82:6f:9e:a5	Apple_6a:cf:59	ARP	42	172.18.107.235 is at 3e:bf:82:6f:9e:a5
2613	21.313488	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.105.250? Tell 172.18.106.123
2618	21.334139	1e:f1:4e:1b:d0:fc	Apple_6a:cf:59	ARP	56	172.18.105.250 is at 1e:f1:4e:1b:d0:fc
3074	24.468163	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.108.63? Tell 172.18.106.123
3084	24.492568	36:86:09:0a:b4:da	Apple_6a:cf:59	ARP	42	172.18.108.63 is at 36:86:09:0a:b4:da
3689	28.782344	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.108.80? Tell 172.18.106.123
3690	28.797812	0a:1e:43:14:79:29	Apple_6a:cf:59	ARP	42	172.18.108.80 is at 0a:1e:43:14:79:29
6058	45.550587	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.104.21? Tell 172.18.106.123
6061	45.561020	Apple_6a:85:51	Apple_6a:cf:59	ARP	42	172.18.104.21 is at f8:4d:89:8c:85:51
6279	47.542422	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.109.42? Tell 172.18.106.123
6280	47.880147	92:77:2f:0c:28:0e	Apple_6a:cf:59	ARP	42	172.18.109.42 is at 92:77:2f:0c:28:0e
8330	62.030644	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.106.129? Tell 172.18.106.123
8333	62.037394	e2:f1:a8:8c:96:87	Apple_6a:cf:59	ARP	42	172.18.106.129 is at e2:f1:a8:8c:96:87
8392	62.130764	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.106.89? Tell 172.18.106.123
8393	62.254028	ee:0d:c9:1f:da:55	Apple_6a:cf:59	ARP	42	172.18.106.89 is at ee:0d:c9:1f:da:55
8952	66.146035	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.106.114? Tell 172.18.106.123
8973	66.193075	26:69:ea:60:eb:83	Apple_6a:cf:59	ARP	42	172.18.106.114 is at 26:69:ea:60:eb:83
9459	69.913785	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.108.67? Tell 172.18.106.123
9492	69.963370	babf:a4:f3:66:7c	Apple_6a:cf:59	ARP	42	172.18.108.67 is at babf:a4:f3:66:7c
113...	77.234037	Apple_6a:cf:59	Broadcast	ARP	42	Who has 172.18.110.105? Tell 172.18.106.123
113...	77.248581	d2:2d:b9:d1:49:9b	Apple_6a:cf:59	ARP	56	172.18.110.105 is at d2:2d:b9:d1:49:9b
113...	77.647931	JuniperN_56:41:f0	Apple_6a:cf:59	ARP	60	172.18.111.254 is at 58:00:bb:56:41:f0
119...	80.329106	66:ab:da:c9:bf:c1	Apple_6a:cf:59	ARP	56	Who has 172.18.106.123? Tell 172.18.111.234
119...	80.329201	Apple_6a:cf:59	66:ab:da:c9:bf:c1	ARP	42	172.18.106.123 is at a4:83:e7:6a:cf:59
119...	80.360865	66:19:f6:78:64:2e	Apple_6a:cf:59	ARP	56	Who has 172.18.106.123? Tell 172.18.108.72

Frame 1437: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0

Ethernet II, Src: Apple_6a:cf:59 (a4:83:e7:6a:cf:59), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff) 目的位址,广播位址

> Source: Apple_6a:cf:59 (a4:83:e7:6a:cf:59) 來源位址

Type: ARP (0x0806) ARP封包 48 bits

Address Resolution Protocol (request)

Hardware type: Ethernet (Ethernet 網路介面)

Protocol type: IPv4 (0x0800) IP protocol

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)

Sender IP address: 172.18.106.123

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 172.18.107.247

ARP request封包標頭

Ethernet II 封包標頭

由主機發送出去 ARP request 封包

Packets: 36562 · Displayed: 75 (0.2%)

Profile: Default

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 (藉由回傳的錯誤訊息分析)

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. choose 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)

The screenshot shows the Wireshark interface capturing from Wi-Fi interface en0. A red circle highlights the 'icmp' display filter in the top bar. A pink box labeled 'terminal (after step 3.)' covers the bottom right of the interface list. The interface list shows many ICMP echo requests and replies between 172.18.106.123 and 8.8.8.8.

No.	Time	Source	Destination	Protocol	Length	Info
39	0.207102	172.18.106.123	8.8.8.8	ICMP	98	Echo (ping) request id=0x372c, seq=60/15360, ttl=64 (reply in 75)
75	0.243796	8.8.8.8	172.18.106.123	ICMP	102	Echo (ping) reply id=0x372c, seq=60/15360, ttl=60 (request in 39)
375	1.207643	172.18.106.123	8.8.8.8	ICMP	98	Echo (ping) request id=0x372c, seq=61/15616, ttl=64 (reply in 376)
376	1.213976	8.8.8.8	172.18.106.123	ICMP	102	Echo (ping) reply id=0x372c, seq=61/15616, ttl=60 (request in 375)
717	2.212986	172.18.106.123	8.8.8.8	ICMP	98	Echo (ping) request id=0x372c, seq=62/15872, ttl=64 (reply in 718)
718	2.222132	8.8.8.8	172.18.106.123	ICMP	102	Echo (ping) reply id=0x372c, seq=62/15872, ttl=60 (request in 717)
1043	3.217730	172.18.106.123	8.8.8.8	ICMP	98	Echo (ping) request id=0x372c, seq=63/16128, ttl=64 (reply in 1044)
1044	3.233996	8.8.8.8	172.18.106.123	ICMP	102	Echo (ping) reply id=0x372c, seq=63/16128, ttl=60 (request in 1043)
1261	4.220751	172.18.106.123	8.8.8.8	ICMP	98	Echo (ping) request id=0x372c, seq=64/16384, ttl=64 (reply in 1276)
1276	4.232400	8.8.8.8	172.18.106.123	ICMP	102	Echo (ping) reply id=0x372c, seq=64/16384, ttl=60 (request in 1261)
1643	5.224141	172.18.106.123	8.8.8.8	ICMP	98	Echo (ping) request id=0x372c, seq=65/16640, ttl=64 (reply in 1677)
1677	5.239529	8.8.8.8	172.18.106.123	ICMP	102	Echo (ping) reply id=0x372c, seq=65/16640, ttl=60 (request in 1643)
1962	6.227701	172.18.106.123	8.8.8.8	ICMP	98	Echo (ping) request id=0x372c, seq=66/16896, ttl=64 (reply in 1968)
1968	6.244628	8.8.8.8	172.18.106.123	ICMP	102	Echo (ping) reply id=0x372c, seq=66/16896, ttl=60 (request in 1962)
2314	7.232205	172.18.106.123	8.8.8.8	ICMP	98	Echo (ping) request id=0x372c, seq=67/17152, ttl=64 (reply in 2315)
2315	7.244792	8.8.8.8	172.18.106.123	ICMP	102	Echo (ping) reply id=0x372c, seq=67/17152, ttl=60 (request in 2314)
2574	8.235484	172.18.106.123	8.8.8.8	ICMP	98	Echo (ping) request id=0x372c, seq=68/17312, ttl=64 (reply in 2575)
2575	8.249761	8.8.8.8	172.18.106.123	ICMP	102	Echo (ping) reply id=0x372c, seq=68/17312, ttl=60 (request in 2574)
2854	9.240468	172.18.106.123	8.8.8.8	ICMP	98	Echo (ping) request id=0x372c, seq=69/17472, ttl=64 (reply in 2855)
2855	9.248096	8.8.8.8	172.18.106.123	ICMP	102	Echo (ping) reply id=0x372c, seq=69/17472, ttl=60 (request in 2854)

terminal (after step 3.)

The terminal window shows the command "candy - ping 8.8.8.8 - 80x24" was run, resulting in 80 ICMP echo requests sent to 8.8.8.8.

The Wireshark interface list shows many ICMP echo requests and replies between 172.18.106.123 and 8.8.8.8.

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

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

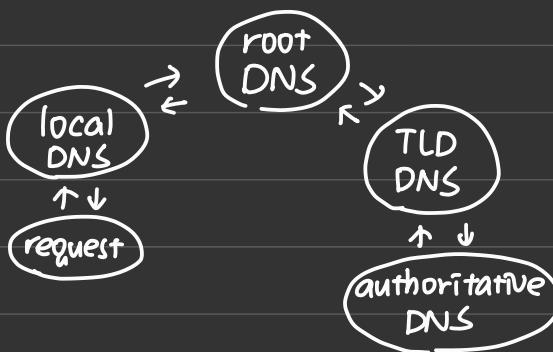
非 application layer process

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

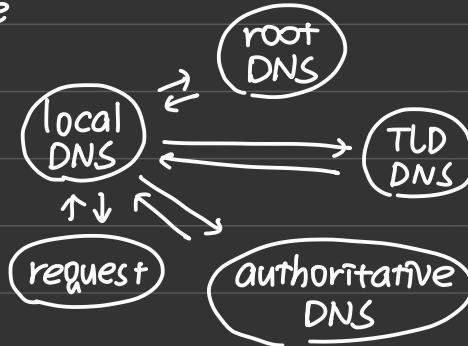
∴ 就不用 port 去指示

4. DNS protocol → 將網址或名稱轉為 IP 地址

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)

A screenshot of the Wireshark application window. The title bar shows 'dns' selected as the display filter. The main pane displays a list of DNS traffic captured on an interface. The columns include Number, Time, Source, Destination, Protocol, Length, and Info. The 'Info' column provides detailed descriptions of each DNS query and response. A red box highlights the 'dns' button in the toolbar.

No.	Time	Source	Destination	Protocol	Length	Info
653	2.962098	172.18.106.123	140.113.1.1	DNS	83	Standard query 0xdd32 A youtube-ui.l.google.com
796	3.962199	172.18.106.123	140.113.1.1	DNS	83	Standard query 0xd62199 A youtube-ui.l.google.com
329	107.355854	172.18.106.123	140.113.1.1	DNS	72	Standard query 0x203d HTTPS sls.weco.net
332	108.357522	172.18.106.123	140.113.1.1	DNS	72	Standard query 0x203d HTTPS sls.weco.net
332	108.397192	172.18.106.123	140.113.1.1	DNS	84	Standard query 0xa4b4 HTTPS www.google-analytics.com
333	108.537549	172.18.106.123	140.113.1.1	DNS	83	Standard query 0x5c09 HTTPS stats.g.doubleclick.net
340	109.397183	172.18.106.123	140.113.1.1	DNS	84	Standard query 0xa4b4 HTTPS www.google-analytics.com
342	109.586825	172.18.106.123	140.113.1.1	DNS	83	Standard query 0x5c09 HTTPS stats.g.doubleclick.net
344	109.778853	172.18.106.123	140.113.1.1	DNS	88	Standard query 0x7aff HTTPS www-alv.google-analytics.com
344	109.779000	172.18.106.123	140.113.1.1	DNS	88	Standard query 0x7f27d A www-alv.google-analytics.com
350	110.314844	172.18.106.123	140.113.1.1	DNS	76	Standard query 0xd464 HTTPS gists.rawgit.com
350	110.315236	172.18.106.123	140.113.1.1	DNS	76	Standard query 0x71da A gists.rawgit.com
352	110.818936	172.18.106.123	140.113.1.1	DNS	88	Standard query 0x7aff HTTPS www-alv.google-analytics.com
352	110.819148	172.18.106.123	140.113.1.1	DNS	88	Standard query 0xf72d A www-alv.google-analytics.com
354	111.314967	172.18.106.123	140.113.1.1	DNS	76	Standard query 0xd464 HTTPS gists.rawgit.com
354	111.363970	172.18.106.123	140.113.1.1	DNS	76	Standard query 0x71da A gists.rawgit.com
355	111.654516	172.18.106.123	140.113.1.1	DNS	83	Standard query 0x5c09 HTTPS stats.g.doubleclick.net
358	112.687441	172.18.106.123	140.113.1.1	DNS	81	Standard query 0xcd58 HTTPS gistsrawgit.b-cdn.net
360	113.687560	172.18.106.123	140.113.1.1	DNS	81	Standard query 0xcd58 HTTPS gistsrawgit.b-cdn.net
361	113.840294	172.18.106.123	140.113.1.1	DNS	83	Standard query 0x5c09 HTTPS stats.g.doubleclick.net
364	114.889184	172.18.106.123	140.113.1.1	DNS	83	Standard query 0x5c09 HTTPS stats.g.doubleclick.net
434	138.005717	172.18.106.123	140.113.1.1	DNS	79	Standard query 0xe6a29 A app-measurement.com
434	138.059877	172.18.106.123	140.113.1.1	DNS	82	Standard query 0xc79d A 3.datadog.pool.ntp.org
434	138.081808	172.18.106.123	140.113.1.1	DNS	87	Standard query 0x2bbd HTTPS inappcheck.itunes.apple.com
434	138.081912	172.18.106.123	140.113.1.1	DNS	87	Standard query 0xb6c8 A inappcheck.itunes.apple.com
437	139.005711	172.18.106.123	140.113.1.1	DNS	79	Standard query 0xe6a29 A app-measurement.com
438	139.087438	172.18.106.123	140.113.1.1	DNS	82	Standard query 0xc79d A 3.datadog.pool.ntp.org
438	139.087563	172.18.106.123	140.113.1.1	DNS	87	Standard query 0x2bbd HTTPS inappcheck.itunes.apple.com
438	139.087623	172.18.106.123	140.113.1.1	DNS	87	Standard query 0xb6c8 A inappcheck.itunes.apple.com
440	140.226446	172.18.106.123	140.113.1.1	DNS	120	Standard query 0x938a HTTPS mysterious-silverfish-marz868fhkcodflxxs2k4xhi.herokuapp.com
442	140.935096	172.18.106.123	140.113.1.1	DNS	106	Standard query 0x0110 HTTPS in1-gw-01-ce7dd027.eastus2.cloudapp.azure.com
443	141.252761	172.18.106.123	140.113.1.1	DNS	120	Standard query 0x938a HTTPS mysterious-silverfish-marz868fhkcodflxxs2k4xhi.herokuapp.com
445	141.983444	172.18.106.123	140.113.1.1	DNS	106	Standard query 0x0110 HTTPS in1-gw-01-ce7dd027.eastus2.cloudapp.azure.com
863	278.611065	172.18.106.123	140.113.1.1	DNS	75	Standard query 0xa6ec HTTPS play.google.com
867	279.611145	172.18.106.123	140.113.1.1	DNS	75	Standard query 0xa6ec HTTPS play.google.com
1273	6.105350	8.8.8.8	172.18.106.123	DNS	167	Standard query response 0xdd32 A youtube-ui.l.google.com A 172.217.160.110 A 142.251.43.14 A 172.2:
6078	28.114200	8.8.8.8	172.18.106.123	DNS	150	Standard query response 0x5449 HTTPS cdnco.spotify.map.fastly.net SOA ns1.fastly.net
6324	28.755992	8.8.8.8	172.18.106.123	DNS	111	Standard query response 0x0453 HTTPS kknews.cc HTTPS
6325	28.759432	8.8.8.8	172.18.106.123	DNS	117	Standard query response 0x9925 A kknews.cc A 104.22.27.227 A 172.67.26.195 A 104.22.26.227
6650	29.349551	8.8.8.8	172.18.106.123	DNS	119	Standard query response 0x570b A a.kknews.cc A 104.22.27.227 A 104.22.26.227 A 172.67.26.195

Frame 6655: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface en0, id 0 0000 a4 83 e7 6a cf 59 58 00 bb 56 41 f0 08 04 05 00 ...j-YX-·VA··E·
 > Ethernet II, Src: Juniper_N_56:41:f0 (58:00:bb:56:41:f0), Dst: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
 > Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.18.106.123
 > User Datagram Protocol, Src Port: 53, Dst Port: 64947
 0 2 Frame (frame), 124 bytes

Packets: 89615 · Displayed: 169 (0.2%) · Dropped: 0 (0.0%) · Profile: Default

① query packet

```

Frame 653: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface en0, id 0
Ethernet II, Src: Apple_6a:cf:59 (a4:83:e7:6a:cf:59), Dst: Juniper_N_56:41:f0 (58:00:bb:56:41:f0)
Internet Protocol Version 4, Src: 172.18.106.123, Dst: 140.113.1.1
User Datagram Protocol, Src Port: 58023, Dst Port: 53
    Source Port: 58023
    Destination Port: 53
    Length: 49
    Checksum: 0x8f28 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 272]
    > [Timestamps]
        UDP payload (41 bytes)
    Domain Name System (query)
        Transaction ID: 0xd32 標誌 (query-response)
        Flags: 0x0100 Standard query
        [Flags]
            0... .0. .... .... = Response: Message is a query
            .000 0. .... .... = Opcode: Standard query (0)
        标誌位 .....0. .... .... = Truncated: Message is not truncated
        .....1 .... .... = Recursion desired: Do query recursively
        .....0. .... .... = Z: reserved (0)
        .....0. .... .... = Non-authenticated data: Unacceptable
        Questions: 1
            Answer RRs: 0
            Authority RRs: 0
            Additional RRs: 0
        < Queries
            youtube-ui.l.google.com: type A, class IN
        域名   Name: youtube-ui.l.google.com
                [Name Length: 23]
                [Label Count: 4]
                Type: A (Host Address) (1)
                Class: IN (0x0001)
    0000 58 00 bb 56 41 f0 a4 83 e7 6a cf 59 08 00 45 00 X-VA-... j Y- E-
    0010 00 45 23 84 00 00 40 11 b3 24 ac 12 6a 7b 8c 71 EF-@-S- -j- q
    0020 01 01 c2 a7 00 35 00 31 8f 28 dd 32 01 00 00 01 .....51 -(2- ...
    0030 00 00 00 00 00 00 00 79 6f 75 74 75 62 65 2d 75 .....y outube-u
    0040 69 61 6c 06 67 6f 67 6c 65 03 63 6f 6d 00 00 01 i-t-goog le-com-
    0050 01 00 01 ...

```

首部區域

查詢問題區域

Show packet bytes [Help](#) [Close](#)

② response packet

```

Length: 129
Checksum: 0x6220 [unverified]
[Checksum Status: Unverified]
[Stream index: 409]
> [Timestamps]
    UDP payload (121 bytes)
Domain Name System (response)
    Transaction ID: 0xd32
    Flags: 0x0100 Standard query response, No error
        1... .... .... = Response: Message is a response
        .000 0. .... .... = Opcode: Standard query (0)
        .....0. .... .... = Authoritative: Server is not an authority for domain
        .....0. .... .... = Truncated: Message is not truncated
        .....1 .... .... = Recursion desired: Do query recursively
        .....1. .... .... = Recursion available: Server can do recursive queries
        .....0. .... .... = Z: reserved (0)
        .....0. .... .... = Answer authenticated: Answer/authority portion was not authenticated by the server
        .....0. .... .... = Non-authenticated data: Unacceptable
        .....0. .... .... = Reply code: No error (0)
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
    < Queries
        youtube-ui.l.google.com: type A, class IN
            Name: youtube-ui.l.google.com
            [Name Length: 23]
            [Label Count: 4]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    答案   < Answers
        youtube-ui.l.google.com: type A, class IN, addr 172.217.160.110
    域名   Name: youtube-ui.l.google.com
            Type: A (Host Address) (1)
            Class: IN (0x0001) 請別 Internet, 這 =)
            Time to live: 22 (22 seconds)
            Data length: 4
            Address: 172.217.160.110 (DNS 解析 IP 位置)
        > youtube-ui.l.google.com: type A, class IN, addr 142.251.43.14
        > youtube-ui.l.google.com: type A, class IN, addr 172.217.160.78
        > youtube-ui.l.google.com: type A, class IN, addr 142.251.42.238
        > youtube-ui.l.google.com: type A, class IN, addr 172.217.163.46

```

首部區域

查詢問題區域

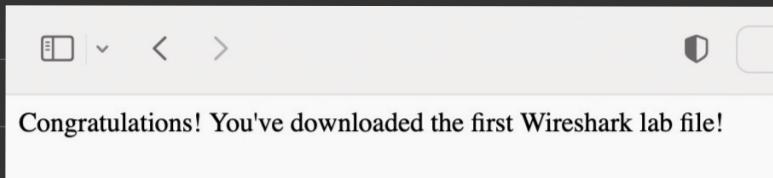
回答區域

Show packet bytes [Help](#) [Close](#)

* Flags → 查詢/響應 → 截斷 → 返回碼



5. Enter the URL



② HTTP packets information

點進去可以看到詳細資料

No.	Time	Source	Destination	Protocol	Length	Info
442	144.550135	192.168.0.14	128.119.245.12	HTTP	478	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
444	144.756873	128.119.245.12	192.168.0.14	HTTP	504	HTTP/1.1 200 OK (text/html)
461	145.373180	192.168.0.14	128.119.245.12	HTTP	435	GET /favicon.ico HTTP/1.1
463	145.579564	128.119.245.12	192.168.0.14	HTTP	551	HTTP/1.1 404 Not Found (text/html)

```

Frame 442: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface en0, id 0
Ethernet II, Src: Apple_6acf:59 (a4:83:e7:6acf:59), Dst: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
  Destination: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
    Address: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
      .... .0. .... .... .... = L6 bit: Globally unique address (factory default)
      .... .0. .... .... .... = IG bit: Individual address (unicast)
  Source: Apple_6acf:59 (a4:83:e7:6acf:59)
    Address: Apple_6acf:59 (a4:83:e7:6acf:59)
      .... .0. .... .... .... = L6 bit: Globally unique address (factory default)
      .... .0. .... .... .... = IG bit: Individual address (unicast)
  Type: IP4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.0.14, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51585, Dst Port: 80, Seq: 1, Ack: 1, Len: 412
> Hypertext Transfer Protocol

```

```

0000 40 ee 15 83 00 64 aa 83 e7 6a cf 59 08 00 45 00 @...d...j.Y..E.
0010 01 d0 00 00 40 00 40 00 02 ee c0 a8 00 0e 80 77 ...@.....w
0020 f5 0c c9 81 00 50 e6 47 6f c8 71 35 7e 0d 80 18 .....P.G.o.q5~...
0030 08 0a 4a cc 00 00 01 01 08 0a b9 98 8d 33 50 f2 ..J...3P.
0040 bb b6 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b ..GET /w ireshark
0050 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d 77 69 72 65 -labs/IN TRO-wire
0060 73 68 61 72 6b 2d 66 69 66 65 31 2e 68 74 6d 6c shark-fi le1.html
0070 20 48 54 54 58 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1.1 -Host:
0080 20 67 61 69 61 2e 63 73 21 75 6d 61 73 73 2a 65
0090 64 75 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65
00a0 63 75 72 65 2d 52 65 71 75 65 73 73 3a 20 31
00b0 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68
00c0 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 66 2f
00d0 78 68 74 6d 6c 2b 78 6d 66 2c 61 70 70 6c 69 63
00e0 61 74 69 6f 6e 2f 78 6d 63 3b 71 3d 30 2e 39 2c
00f0 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 55 73 65 72 2d
0100 41 67 65 66 74 3a 20 4d 6f 7a 69 6c 66 61 2f 35
0110 2e 30 20 28 4d 61 63 69 6e 74 6f 73 68 3b 20 49

```

Packets: 810 • Displayed: 4 (0.5%) • Profile: Default

(a) 128.119.245.12

```

Frame 442: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface en0, id 0
Ethernet II, Src: Apple_6acf:59 (a4:83:e7:6acf:59), Dst: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
  Destination: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
    Address: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
      .... .0. .... .... .... = L6 bit: Globally unique address (factory default)
      .... .0. .... .... .... = IG bit: Individual address (unicast)
  Source: Apple_6acf:59 (a4:83:e7:6acf:59)
    Address: Apple_6acf:59 (a4:83:e7:6acf:59)
      .... .0. .... .... .... = L6 bit: Globally unique address (factory default)
      .... .0. .... .... .... = IG bit: Individual address (unicast)
  Type: IP4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.0.14, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51585, Dst Port: 80, Seq: 1, Ack: 1, Len: 412
> Hypertext Transfer Protocol

```

```

0000 40 ee 15 83 00 64 aa 83 e7 6a cf 59 08 00 45 00 @...d...j.Y..E.
0010 01 d0 00 00 40 00 40 00 02 ee c0 a8 00 0e 80 77 ...@.....w
0020 f5 0c c9 81 00 50 e6 47 6f c8 71 35 7e 0d 80 18 .....P.G.o.q5~...
0030 08 0a 4a cc 00 00 01 01 08 0a b9 98 8d 33 50 f2 ..J...3P.
0040 bb b6 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b ..GET /w ireshark
0050 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d 77 69 72 65 -labs/IN TRO-wire
0060 73 68 61 72 6b 2d 66 69 66 65 31 2e 68 74 6d 6c shark-fi le1.html
0070 20 48 54 54 58 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1.1 -Host:
0080 20 67 61 69 61 2e 63 73 21 75 6d 61 73 73 2a 65
0090 64 75 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65
00a0 63 75 72 65 2d 52 65 71 75 65 73 73 3a 20 31
00b0 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68
00c0 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 66 2f
00d0 78 68 74 6d 6c 2b 78 6d 66 2c 61 70 70 6c 69 63
00e0 61 74 69 6f 6e 2f 78 6d 63 3b 71 3d 30 2e 39 2c
00f0 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 55 73 65 72 2d
0100 41 67 65 66 74 3a 20 4d 6f 7a 69 6c 66 61 2f 35
0110 2e 30 20 28 4d 61 63 69 6e 74 6f 73 68 3b 20 49

```

Show packet bytes Help Close

(b) 192.168.0.14

```
> Frame 444: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface en0, id 0
Ethernet II, Src: ZlioniCore_E8:00:64 (40:ee:c1:58:63:00), Dst: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
  Destination: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
    Address: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
      ...0....0....0....0....0....0 = LG bit: Globally unique address (factory default)
      ...0....0....0....0....0....0 = IG bit: Individual address (unicast)
  Source: ZlioniCore_E8:00:64 (40:ee:c1:58:63:00)
    Address: ZlioniCore_E8:00:64 (40:ee:c1:58:63:00) = LG bit: Globally unique address (factory default)
    ...0....0....0....0....0....0 = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.14
  Transmission Control Protocol, Src Port: 51585, Seq: 1, Ack: 413, Len: 438
  Hypertext Transfer Protocol
  Line-based text data: text/html (3 lines)

0000  a4 83 c7 6a cf 59 40 ee 15 83 00 64 88 00 45 00  ..j Y@ d-E-
0010  01 e9 c2 8d 40 00 2a 06 56 48 80 77 f5 0c c9 a8  ..@* Vh w...
0020  00 0e 00 50 c9 81 71 35 7e 0d e6 47 71 5c 88 18  ..P q5 ~ Gq...
0030  00 eb 1e c2 00 01 01 08 50 f2 bc 87 b9 98  .....P...
0040  89 33 00 54 54 74 65 31 26 20 30 20 28 44 10 00  ..P. .....
0050  20 4e 6f 76 20 32 32 32 20 31 34 3a 32 32 3a  K- Date: Fri, 04
0060  20 4e 6f 76 20 32 32 32 20 31 34 3a 32 32 3a  Nov 20 2012 20:24:22
0070  30 35 20 47 4d 54 0d 0a 53 65 72 79 65 72 3a 20  35 GMT-- Server:
0080  41 70 61 63 68 65 2f 32 26 34 2e 3b 28 28 43 65 Apache/2.4.6 (Ce
0090  62 74 63 53 2b 65 2f 32 26 34 2e 3b 28 28 43 65 Apache/2.4.6 (Ce
00a0  30 32 30 6d 64 66 70 70 73 20 33 53 52 31 26 0.2K-IP: PHP/7.0.1
00b0  34 2e 33 20 6d 64 66 5f 76 65 72 6c 2f 32 26 4.30 mod perl/2.2
00c0  34 2e 31 31 20 58 65 72 6c 2f 76 35 2e 31 36 26 0.11 Per l/v5.16.
00d0  33 0d 04 6c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3 -Last-Modified
00e0  33 0d 04 6c 61 73 74 2d 4d 6f 64 69 66 69 65 64  : Fri, 04 Nov 20
00f0  32 32 30 36 35 2b 35 39 3a 30 32 20 47 4d 54 0d 12:00:00 +02 GM
0100  09 45 54 61 67 3a 20 22 35 31 24 35 65 63 39 65 Etag: "51-secde
0110  63 35 34 34 65 34 38 39 22 0d 0a 41 63 65 70 c54de489 " Accep
0120  74 2d 52 61 66 67 65 73 3a 26 62 79 74 65 73 0d c-Ranges bytes
0130  64 65 66 67 65 70 73 3d 20 4c 65 68 66 68 3d Content-length:
0140  20 38 31 30 0d 0a 4b 65 70 73 20 4c 65 68 66 3d Content-type: application/x-htm
0150  20 74 69 65 65 75 74 3d 35 2c 20 6d 61 78 3d timeout=5, max=
0160  31 30 30 0d 0a 43 6f 66 6e 65 63 74 69 6f 6e 3d 100 - Connection:
0170  20 4b 65 65 70 2d 41 6c 69 76 65 0a 43 6f 6e Keep-Alive: Con
0180  74 64 66 65 70 2d 41 6c 69 76 65 0a 43 6f 6e Content-Type: text/html; charset=UTF-8
0190  64 74 66 65 70 2d 63 68 61 72 73 64 7d 55 54 html; charset=UTF-8
01a0  46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c 3e 0a 43 6f F-8 -< html> Co
```

(C) 128.119.245.12

```
> Frame 461: 435 bytes on wire (3480 bits), 435 bytes captured (3480 bits) on interface en0, id 0
-+ EtherType [Dest: 00:00:00:00:00:00 Src: Apple_6a:c1:59 (4d:83:e7:6a:c1:59) Dst: Zioncom_E_83:00:64 (40:ee:15:83:00:64)]
  + Destination: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
    Address: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
      .... .0 .. = LG bit: Globally unique address (factory default)
      .... 0 .. = IG bit: Individual address (unicast)
  + Source: Apple_6a:c1:59 (4d:83:e7:6a:c1:59)
    Address: Apple_6a:c1:59 (4d:83:e7:6a:c1:59)
      .... .0 .. = LG bit: Globally unique address (factory default)
      .... 0 .. = IG bit: Individual address (unicast)
  + Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.0.14, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 5186, Dst Port: 80, Seq: 1, Ack: 1, Len: 369
> Hypertext Transfer Protocol

0000  40 ee 15 83 00 64 a4 83 e7 6a cf 59 08 00 45 00 @... d... j-Y-E.
0010  01 a5 00 08 40 00 40 00 00 00 00 00 00 00 80 77 @...@. ....w
0020  f5 0c c9 82 00 50 a7 48 15 1b 2f 75 e7 0f 80 18 P-H ..u...
0030  08 0a a4 1b 00 00 01 01 08 0a f9 e1 eb 15 50 f2 .....p...
0040  09 0a 64 54 20 21 00 00 60 76 69 63 6b 0e 26 60 GE HTTP avicci.1
0050  0a 64 54 20 21 00 00 00 60 76 69 63 6b 0e 26 60 co /favicon.ico
0060  74 3a 20 67 61 69 61 6e 63 73 2e 75 6d 61 73 73 t: gaias.cs.umass.edu - Co nnection
0070  2e 65 64 75 0d 0a 43 6f 6e 65 65 63 74 69 6f 6a .edu - Co nnection
0080  3a 20 6b 65 78 20 61 6c 69 6f 65 68 0a 01 41 63 .keep-a live Ac cept: */* User-Agent: Mozilla/5.0
0090  41 65 78 20 61 6c 69 6f 65 68 0a 01 41 63 Accept: Macintosh; I
00a0  2e 30 20 28 4d 61 63 69 6e 74 6f 73 68 2b 49 49 0 (Mac) Macintosh; I
00b0  6e 74 65 6c 20 4d 61 63 20 4f 53 28 58 2b 31 30 tel Mac OS X 10
00c0  5f 31 35 5f 37 29 20 41 70 78 6c 65 57 65 62 40 15.7) AppleWebkit
00d0  44 4c 21 36 38 35 26 2e 26 35 28 2b 48 54 17/1.1.1 (KHTML like Gecko)
00e0  4d 4c 21 36 38 35 26 2e 26 35 28 2b 48 54 17/1.1.1 (KHTML like Gecko)
0100  56 65 72 73 69 6f 2f 31 35 3e 24 30 53 61 66 Version/ 15.4 Safari/605.1.15 - Ac cept: Lan guage: z
0110  61 72 69 2f 36 38 35 3e 21 31 35 0a 01 63 ari/605.1.15 - Ac cept: Lan guage: z
0120  63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 7a cept-Lan guage: z
0130  68 2d 54 2c 7c 78 61 2d 48 66 65 66 30 71 3d 30 h-TM Refe rer: http://gaias.cs.umass.edu
0140  39 65 72 73 69 6f 2e 63 73 2e 75 6d 61 73 pi/gaias.cs.umass.edu
0150  79 3a 2f 67 61 69 61 2e 63 73 2e 75 6d 61 73 s.edu/wi reshark-
0160  73 2e 65 64 75 2f 77 69 72 65 73 68 6f 72 66 20 labs/INT RO-wires
0170  6c 61 62 73 2f 49 4f 54 52 4f 27 77 62 72 65 73 hark-fil e.html
0180  68 61 72 5b 2d 66 69 6c 6d 31 2e 68 74 6d 6c 0d :Accept- Encoding
0190  0a 41 63 63 65 78 74 2d 45 68 63 61 64 69 6e 67 :gzip, deflate
01a0  3a 20 67 78 79 2c 2d 46 65 66 6c 01 74 65 0d : Close
```

(d) 192.168.0.14

```

> Frame 463: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface en0, id 0
  Ethernet II, Src: Zioncom_E_83:00:64 (40:ee:15:83:00:64), Dst: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
    Address: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
      .... ..0..... .... = LG bit: Globally unique address (factory default)
      .... ..0..... .... = IG bit: Individual address (unicast)
  > Destination: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
    Address: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
      .... ..0..... .... = LG bit: Globally unique address (factory default)
      .... ..0..... .... = IG bit: Individual address (unicast)
  > Source: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
    Address: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
      .... ..0..... .... = LG bit: Globally unique address (factory default)
      .... ..0..... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.14
> Transmission Control Protocol, Src Port: 80, Dst Port: 51586, Seq: 1, Ack: 370, Len: 485
> Hypertext Transfer Protocol
> Line-based text data: text/html (7 lines)

0000 a4 83 e7 6a cf 59 40 ee 15 83 00 64 08 00 45 00 ... j Y@... d-E
0010 02 19 58 b4 40 00 29 06 c0 f0 80 77 15 0c c0 a8 ... X@... w...
0020 00 0e 00 58 c9 82 2f 75 e7 0f a7 48 16 8c 80 18 ... P@... u... H...
0030 00 eb 57 f0 00 01 01 08 01 50 2f bd f9 e1 ... W.... P....
0040 eb 15 48 54 54 50 2f 31 2e 31 20 34 30 34 20 44 ... HTTP/1.1 404 N
0050 67 74 69 2c 20 39 34 20 36 20 47 44 54 0d 08 53 ... Date: Fri, 04 Nov 2022
0060 20 31 34 3a 32 32 3a 33 36 20 47 44 54 0d 08 53 ... 14:22:23 6 GMT-S
0070 00 65 72 76 65 72 3a 20 41 70 61 63 68 65 2f 32 2e ... erver: Apache/2.4.46 (CentOS) OpenSSL/1.1.1k FIPS PHP/7.4.30 mod...
0080 34 2e 36 20 28 43 65 66 74 4f 53 29 20 4f 70 65 ... 4.6 (CentOS) OpenSSL/1.0.2k-fips
0090 6e 53 53 4c 2f 31 2e 2e 32 6b 2d 66 69 70 73 ... nSSL/1.0.2k-fips
00a0 20 50 48 58 2f 37 2e 34 2e 33 30 20 6f 64 5f ... PHP/7.4.30 mod...
00b0 70 65 72 6c 2f 32 2e 30 2e 31 31 20 50 65 72 60 ... perl/2.0.11 Perl
00c0 21 76 65 64 3d 30 58 68 64 0d 61 60 65 64 50 ... /v1.16.1 Content-Type: ...
00d0 74 54 45 66 67 74 48 60 32 33 34 35 39 69 0d 0a ... t-length: 209 K
00e0 65 65 70 2d 41 6c 69 76 65 3a 20 74 69 65 66 ... eop-Aliv e: timo
0100 75 74 3d 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 ... ut=5, ma=x=100 C
0110 6f 6e 65 63 74 69 6f 66 3a 20 4b 65 65 70 2d ... onnection: Keep-Alive: C content-T
0120 41 6c 65 76 65 0d 0a 43 6f 66 74 65 66 74 2d 54 ... ope: text/t/html;
0130 79 70 65 3a 20 76 65 78 74 2f 68 74 66 6c 3b 20 ... charset: iso-8859-1
0140 63 68 65 72 73 65 74 3d 69 73 2d 38 38 35 39 ... Content-Type: ...
0150 20 48 54 4d 4c 20 50 55 42 49 43 20 42 2d 4c 20 3f ... HTML PUB LIC "-//I
0160 48 54 4d 4c 20 50 55 42 49 43 20 42 2d 4c 20 3f ... IETF//DTD HTML 2
0170 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 ... .0//EN"> <html><
0180 2e 30 2f 2f 45 46 22 3e 0a 3c 68 74 6d 6c 3e 3c ... heads> <title>404</t
0190 68 65 61 64 3e 0c 74 69 74 6c 65 34 30 34 ... head> <title>404</t
01a0 20 4e 6f 74 28 46 75 6e 64 3c 2f 74 69 74 66 ... Not Found</title>

```

No.: 463 · Time: 145.579564 · Source: 128.119.245.12 · Destination: 192.168.0.14 · Protocol: HTTP · Length: 551 · Info: HTTP/1.1 404 Not Found (text/html)

Show packet bytes

Help

Close

6.

No.	Time	Source	Destination	Protocol	Length	Info
442	144.550135	192.168.0.14	128.119.245.12	HTTP	478	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
444	144.756873	128.119.245.12	192.168.0.14	HTTP	504	HTTP/1.1 200 OK (text/html)
461	145.373180	192.168.0.14	128.119.245.12	HTTP	435	GET /favicon.ico HTTP/1.1
463	145.579564	128.119.245.12	192.168.0.14	HTTP	551	HTTP/1.1 404 Not Found (text/html)

$\bar{P}_H = 144.550135 - 144.756873 = 0.206738(s)$

```

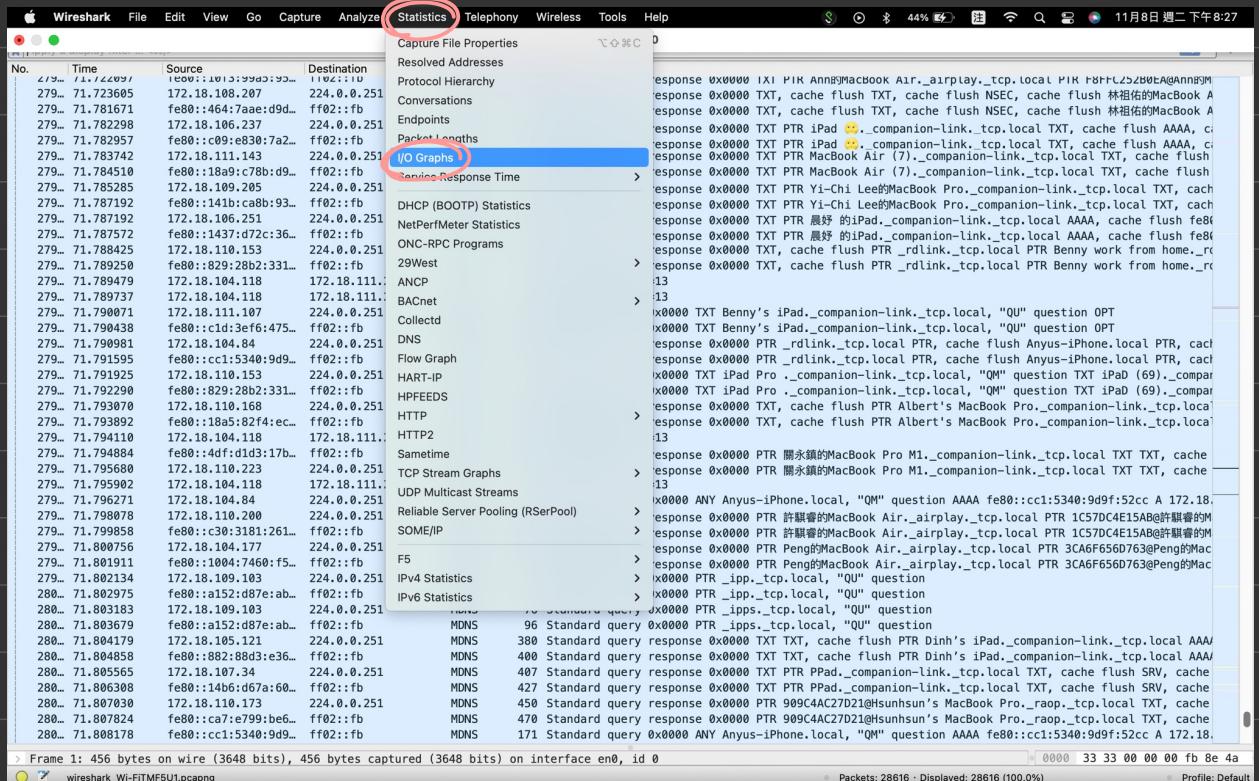
> Frame 442: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface en0, id 0
  Ethernet II, Src: Apple_6a:cf:59 (a4:83:e7:6a:cf:59), Dst: Zioncom_E_83:00:64 (40:ee:15:83:00:64)
    Address: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
      .... ..0..... .... = LG bit: Globally unique address (factory default)
      .... ..0..... .... = IG bit: Individual address (unicast)
  > Destination: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
    Address: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
      .... ..0..... .... = LG bit: Globally unique address (factory default)
      .... ..0..... .... = IG bit: Individual address (unicast)
  > Source: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
    Address: Apple_6a:cf:59 (a4:83:e7:6a:cf:59)
      .... ..0..... .... = LG bit: Globally unique address (factory default)
      .... ..0..... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.0.14, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 478, Dst Port: 80, Seq: 1, Ack: 1, Len: 412
> Hypertext Transfer Protocol

```

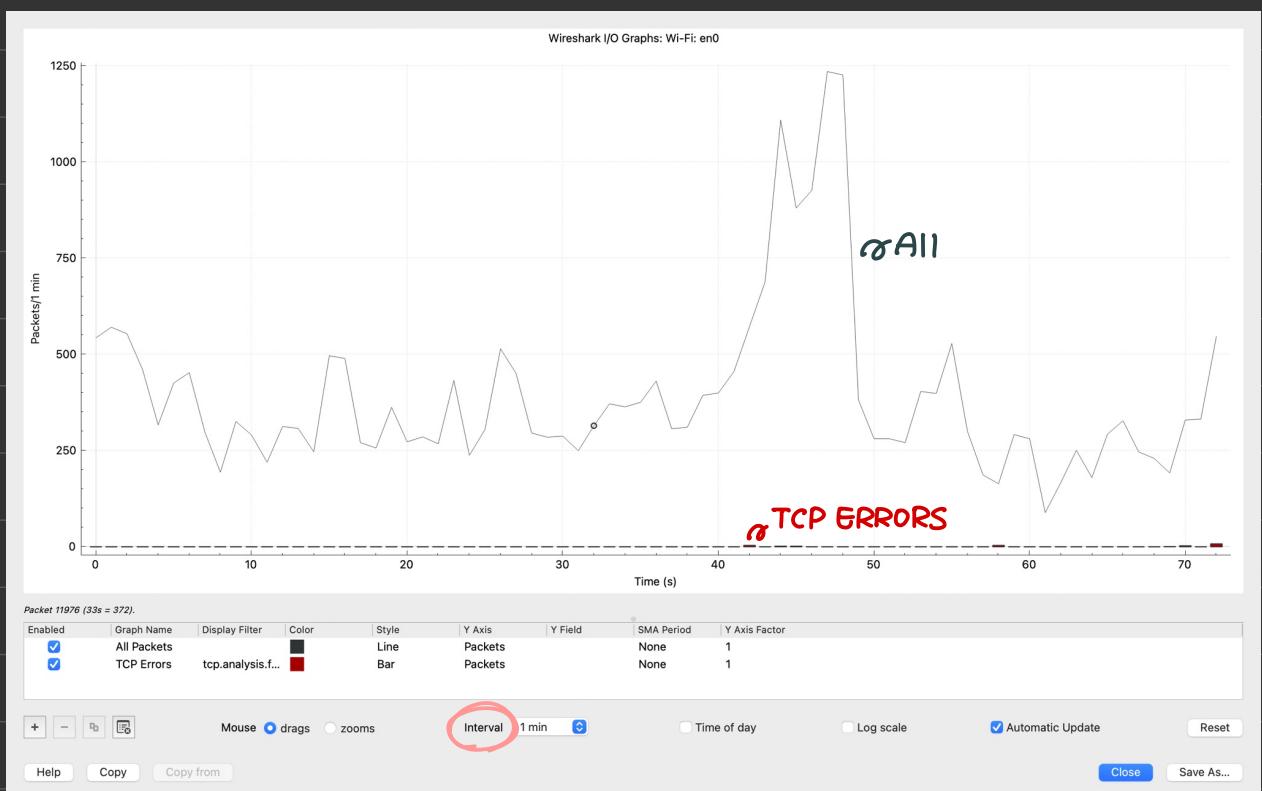
Packets: 810 · Displayed: 4 (0.5%) · Profile: Default

1. Method to get the number of income packets

1. Choose "Statistics" → "I/O Graphs"



2. Select "interval" to 1 min



8.① TLS protocol → 提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、重改

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 address and deliver
but MAC address 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)