

# Wireshark 基礎教學

助教：陳哲安  
授課老師：張宏慶 老師



# AGENDA

- Wireshark安裝
- 基礎操作流程

# Wireshark安裝(官網)

[NEWS](#)[Get Acquainted ▼](#)[Get Help ▼](#)[Develop ▼](#)[Our Sponsor](#)[SharkFest](#)

## Download Wireshark

The current stable release of Wireshark is 2.4.0. It supersedes all previous releases. You can also download the latest development release (2.4.0rc2) and documentation.

### Stable Release (2.4.0)

Windows Installer (64-bit)  
Windows Installer (32-bit)  
Windows PortableApps® (32-bit)  
📁 macOS 10.6 and later Intel 64-bit .dmg  
Source Code

### Old Stable Release (2.2.8)

### Documentation

Having Problems?

Explore our [download area](#) or look in our [third party package list](#) below.

<https://www.wireshark.org/download.html>

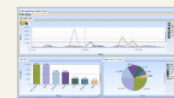
## Go Beyond with Riverbed Technology

Riverbed is Wireshark's primary sponsor and provides our funding. They also make great products that fully integrate with Wireshark.

### *I have a lot of traffic...*

**ANSWER:** [SteelCentral™ Packet Analyzer PE](#)

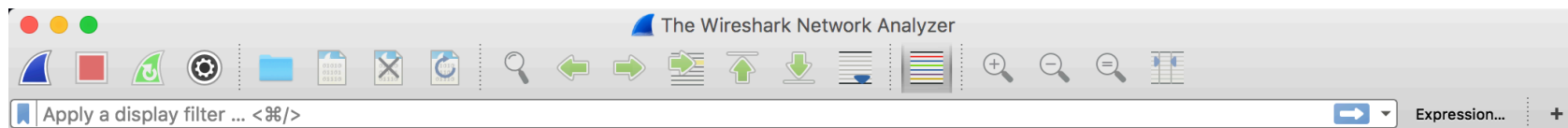
- Visually rich, powerful LAN analyzer
- Quickly access very large pcap files
- Professional, customizable reports
- Advanced triggers and alerts
- Fully integrated with Wireshark and AirPcap™

[Learn More](#)[Buy Now](#)

### *No, really, I have a LOT of traffic...*

**ANSWER:** [SteelCentral™ NetShark appliance](#)

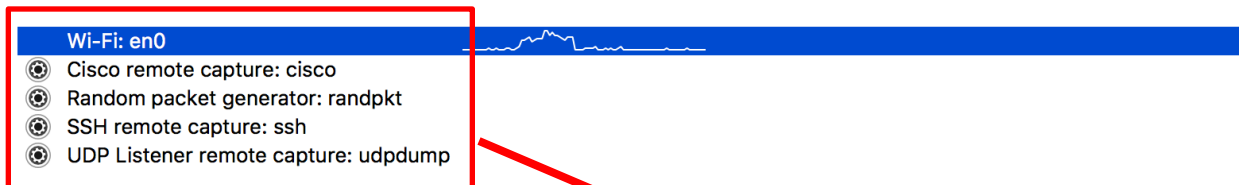
# 操作流程 - 挑選網路介面卡



Welcome to Wireshark

## Capture

...using this filter:  5 interface(s) shown, 9 hidden



選擇一個

## Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 2.4.0 (v2.4.0-0-g9be0fa5).

停止擷取

## Packet List

| No. | Time     | Source                | Destination     | Protocol | Length | Info                                                    |
|-----|----------|-----------------------|-----------------|----------|--------|---------------------------------------------------------|
| 1   | 0.000000 | 2001::9d38:90d7:34... | ff02::1         | IPv6     | 82     | IPv6 no next header                                     |
| 2   | 0.205001 | 2001::9d38:90d7:41... | ff02::1         | IPv6     | 82     | IPv6 no next header                                     |
| 3   | 0.205005 | 2001::9d38:90d7:10... | ff02::1         | IPv6     | 82     | IPv6 no next header                                     |
| 4   | 0.205257 | 10.232.238.114        | 224.0.0.251     | MDNS     | 82     | Standard query 0x0000 PTR _googlecast._tcp.local, "Q... |
| 5   | 0.205261 | 2001::9d38:90d7:38... | ff02::1         | IPv6     | 82     | IPv6 no next header                                     |
| 6   | 0.205993 | 10.232.238.114        | 239.255.255.250 | SSDP     | 215    | M-SEARCH * HTTP/1.1                                     |
|     |          | 10.232.237.70         | 224.0.0.251     | MDNS     | 54     | Standard query response 0x0000                          |
|     |          | 10.232.238.123        | 224.0.0.251     | MDNS     | 103    | Standard query 0x0003 PTR _805741C9._sub._googlecast... |
| 9   | 0.206166 | 10.232.237.70         | 224.0.0.251     | MDNS     | 54     | Standard query response 0x0000                          |
| 10  | 0.307658 | 10.232.228.94         | 224.0.0.251     | MDNS     | 217    | Standard query response 0x0000 PTR cc:08:8d:5f:f8:68... |
| 11  | 0.307662 | 2001::9d38:90d7:b2... | ff02::1         | IPv6     | 82     | IPv6 no next header                                     |
| 12  | 0.307664 | 2001::9d38:90d7:38... | ff02::1         | IPv6     | 82     | IPv6 no next header                                     |
| 13  | 0.409916 | 10.232.233.230        | 239.255.255.250 | SSDP     | 169    | M-SEARCH * HTTP/1.1                                     |
| 14  | 0.409921 | 10.232.237.246        | 224.0.0.252     | LLMNR    | 68     | Standard query 0x530d ANY kelly-pc                      |

## Packet Details

- Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
- Ethernet II, Src: LiteonTe\_91:a3:d3 (94:e9:79:91:a3:d3), Dst: IPv4mcast\_fd (01:00:5e:00:00:fd)
- Internet Protocol Version 4, Src: 10.232.234.138, Dst: 224.0.0.253
- Internet Protocol Version 6, Src Port: 65264, Dst Port: 3544
- Internet Protocol Version 6, Src: 2001::9d38:90d7:3467:10f:7388:86f9, Dst: ff02::1

```
0000  01 00 5e 00 00 fd 94 e9 79 91 a3 d3 08 00 45 00  ..^....y....E.
0010  00 44 27 ed 00 00 01 11 bb 4c 0a e8 ea 8a e0 00  .D'....L.....
0020  00 fd fe f0 0d d8 00 30 04 32 60 00 00 00 00 00  .....0.2`.....
0030  3b 15 20 01 00 00 9d 38 90 d7 34 67 01 0f 73 88  ;. ....8 ..4g..s.
0040  86 f9 ff 02 00 00 00 00 00 00 00 00 00 00 00 00  .....
0050  00 01  ..
```

## Packet Bytes

Wi-Fi: en0: <live capture in progress>

Packets: 903 · Displayed: 903 (100.0%)

Profile: Default



# 操作流程 - 封包篩選器

- 擷取篩選器 (Capture filter)
- 顯示篩選器 (Display filter)

# 擷取篩選器

The image shows the Wireshark network protocol analyzer interface. The 'Capture' menu is open, highlighting the 'Options...' option. The main packet list shows a series of IPv6 and MDNS packets. The packet details pane shows the structure of the first packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Internet Protocol Version 6. The packet bytes pane shows the raw data in hexadecimal and ASCII.

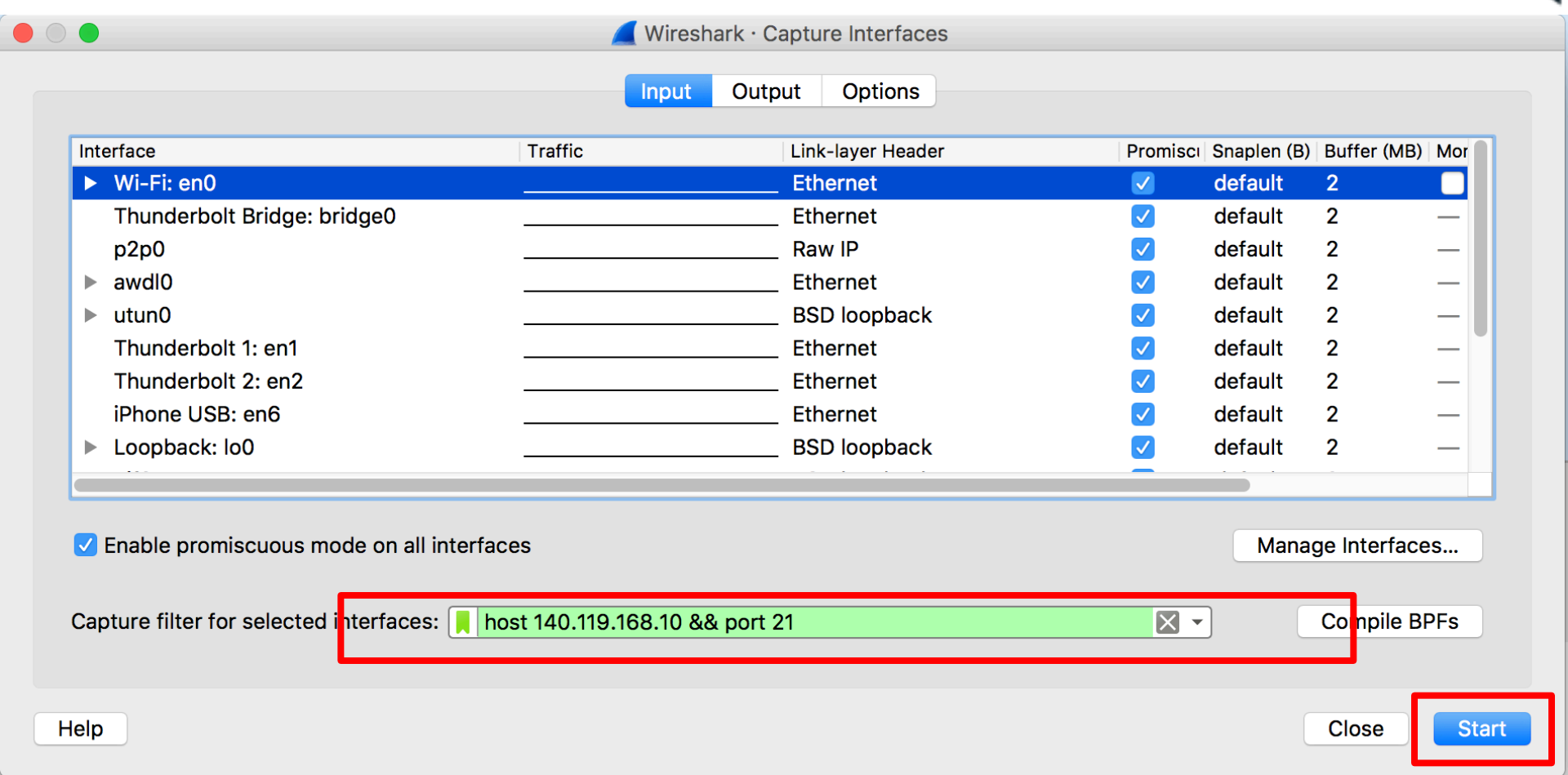
**Wireshark Interface Components:**

- Menu Bar:** File, Edit, View, Go, **Capture**, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Start, Stop, Restart, Capture Filters..., Refresh Interfaces.
- Packet List:**

| No. | Time     | Source                | Destination     | Protocol | Length | Info                                                                            |
|-----|----------|-----------------------|-----------------|----------|--------|---------------------------------------------------------------------------------|
| 1   | 0.000000 | 2001::9d38:90d7       | ff02::1         | IPv6     | 82     | IPv6 no next header                                                             |
| 2   | 0.205001 | 2001::9d38:90d7       | 239.255.255.250 | IPv6     | 82     | IPv6 no next header                                                             |
| 3   | 0.205005 | 2001::9d38:90d7       | 224.0.0.251     | IPv6     | 82     | IPv6 no next header                                                             |
| 4   | 0.205257 | 10.232.238.114        | 224.0.0.251     | MDNS     | 82     | Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question                 |
| 5   | 0.205261 | 2001::9d38:90d7:38... | ff02::1         | IPv6     | 82     | IPv6 no next header                                                             |
| 6   | 0.205993 | 10.232.238.114        | 239.255.255.250 | SSDP     | 215    | M-SEARCH * HTTP/1.1                                                             |
| 7   | 0.205998 | 10.232.237.70         | 224.0.0.251     | MDNS     | 54     | Standard query response 0x0000                                                  |
| 8   | 0.206164 | 10.232.238.123        | 224.0.0.251     | MDNS     | 103    | Standard query 0x0003 PTR _805741C9._sub._googlecast._tcp.local, "QM" questi... |
| 9   | 0.206166 | 10.232.237.70         | 224.0.0.251     | MDNS     | 54     | Standard query response 0x0000                                                  |
| 10  | 0.307658 | 10.232.228.94         | 224.0.0.251     | MDNS     | 217    | Standard query response 0x0000 PTR cc:08:8d:5f:f8:68@fe80::ce08:8dff:fe5f:f8... |
| 11  | 0.307662 | 2001::9d38:90d7:b2... | ff02::1         | IPv6     | 82     | IPv6 no next header                                                             |
| 12  | 0.307664 | 2001::9d38:90d7:38... | ff02::1         | IPv6     | 82     | IPv6 no next header                                                             |
| 13  | 0.409916 | 10.232.233.230        | 239.255.255.250 | SSDP     | 169    | M-SEARCH * HTTP/1.1                                                             |
| 14  | 0.409921 | 10.232.237.246        | 224.0.0.252     | LLMNR    | 68     | Standard query 0x530d ANY kelly-pc                                              |
| 15  | 0.410375 | 10.232.224.214        | 239.255.255.250 | SSDP     | 175    | M-SEARCH * HTTP/1.1                                                             |
| 16  | 0.492740 | 10.232.239.109        | 216.58.200.238  | QUIC     | 293    | Payload (Encrypted), PKN: 7, CID: 971701462731095760                            |
| 17  | 0.493701 | 10.232.239.109        | 216.58.200.238  | QUIC     | 1392   | Payload (Encrypted), PKN: 8, CID: 971701462731095760                            |
| 18  | 0.493702 | 10.232.239.109        | 216.58.200.238  | QUIC     | 102    | Payload (Encrypted), PKN: 9, CID: 971701462731095760                            |
| 19  | 0.499337 | 216.58.200.238        | 10.232.239.109  | QUIC     | 81     | Payload (Encrypted), PKN: 7                                                     |
- Packet Details:**
  - Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
  - Ethernet II, Src: LiteonTe\_91:a3:d3 (94:e9:79:91:a3:d3), Dst: IPv4mcast\_fd (01:00:5e:00:00:fd)
  - Internet Protocol Version 4, Src: 10.232.234.138, Dst: 224.0.0.253
  - User Datagram Protocol, Src Port: 65264, Dst Port: 3544
  - Teredo IPv6 over UDP tunneling
  - Internet Protocol Version 6, Src: 2001::9d38:90d7:3467:10f:7388:86f9, Dst: ff02::1
- Packet Bytes:**

| Offset | Hex                                             | ASCII            |
|--------|-------------------------------------------------|------------------|
| 0000   | 01 00 5e 00 00 fd 94 e9 79 91 a3 d3 08 00 45 00 | ..^.... y....E.  |
| 0010   | 00 44 27 ed 00 00 01 11 bb 4c 0a e8 ea 8a e0 00 | .D'.... .L.....  |
| 0020   | 00 fd fe f0 0d d8 00 30 04 32 60 00 00 00 00 00 | .....0 .2`....   |
| 0030   | 3b 15 20 01 00 00 9d 38 90 d7 34 67 01 0f 73 88 | ;.....8 ..4g..s. |
| 0040   | 86 f9 ff 02 00 00 00 00 00 00 00 00 00 00 00 00 | .....            |
| 0050   | 00 01                                           | ..               |





## Wireshark - Capture Interfaces

Input

Output

Options

| Interface                   | Traffic | Link-layer Header | Promisc                             | Snaplen (B) | Buffer (MB) | More                     |
|-----------------------------|---------|-------------------|-------------------------------------|-------------|-------------|--------------------------|
| ▶ Wi-Fi: en0                |         | Ethernet          | <input checked="" type="checkbox"/> | default     | 2           | <input type="checkbox"/> |
| Thunderbolt Bridge: bridge0 |         | Ethernet          | <input checked="" type="checkbox"/> | default     | 2           | —                        |
| p2p0                        |         | Raw IP            | <input checked="" type="checkbox"/> | default     | 2           | —                        |
| ▶ awdl0                     |         | Ethernet          | <input checked="" type="checkbox"/> | default     | 2           | —                        |
| ▶ utun0                     |         | BSD loopback      | <input checked="" type="checkbox"/> | default     | 2           | —                        |
| Thunderbolt 1: en1          |         | Ethernet          | <input checked="" type="checkbox"/> | default     | 2           | —                        |
| Thunderbolt 2: en2          |         | Ethernet          | <input checked="" type="checkbox"/> | default     | 2           | —                        |
| iPhone USB: en6             |         | Ethernet          | <input checked="" type="checkbox"/> | default     | 2           | —                        |
| ▶ Loopback: lo0             |         | BSD loopback      | <input checked="" type="checkbox"/> | default     | 2           | —                        |

☒ Enable promiscuous mode on all interfaces

Manage Interfaces...

Capture filter for selected interfaces:

Compile BPFs

Help

Close

Start



# 篩選語法

| 限定詞   | 說明                | 舉例                      |
|-------|-------------------|-------------------------|
| Type  | 識別ID名稱或代號         | host, port              |
| Dir   | 指定ID名稱或代號之轉換或來的方向 | src , dst               |
| Proto | 限制對特定協定的比對        | ip, tcp, udp, http, ftp |

## 邏輯運算子

- AND 運算子 (&&)
- OR 運算子 (||)
- NOT 運算子 (!)

EX :

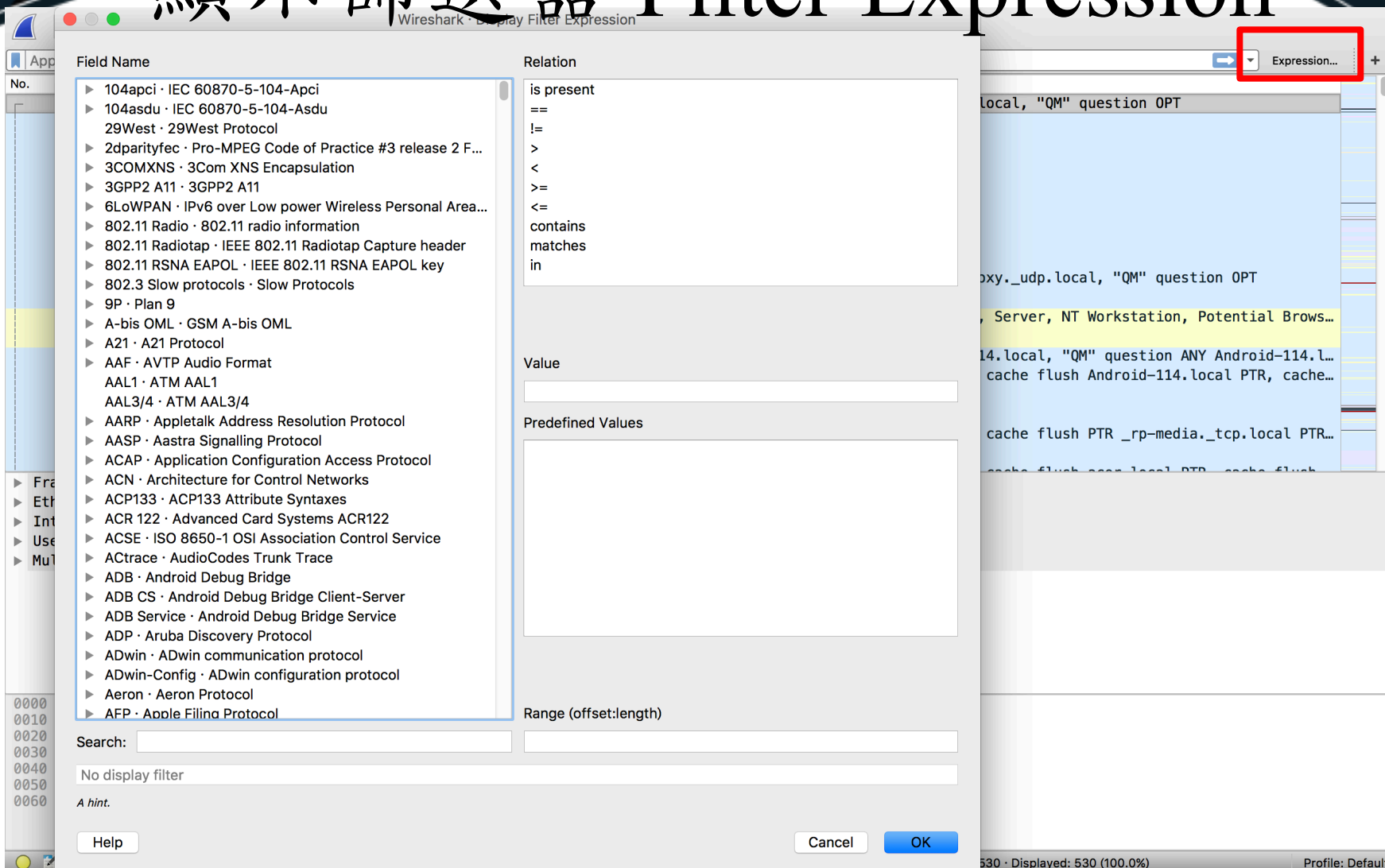
運算子

dst host 140.119.168.10 && port 21

└─┬─┘ └──────────┘ └─┬─┘ └─┬─┘

限定詞 ID 限定詞 ID

# 顯示篩選器 Filter Expression



The image shows the Wireshark Filter Expression dialog box, which is used to create and apply display filters. The dialog is titled "Wireshark - Display Filter Expression". It features a list of field names on the left, a list of relations in the center, and a text area for the value on the right. A red box highlights the "Expression..." button in the top right corner of the dialog.

**Field Name**

- 104apci · IEC 60870-5-104-Apci
- 104asdu · IEC 60870-5-104-Asdu
- 29West · 29West Protocol
- 2dparityfec · Pro-MPEG Code of Practice #3 release 2 F...
- 3COMXNS · 3Com XNS Encapsulation
- 3GPP2 A11 · 3GPP2 A11
- 6LoWPAN · IPv6 over Low power Wireless Personal Area...
- 802.11 Radio · 802.11 radio information
- 802.11 Radiotap · IEEE 802.11 Radiotap Capture header
- 802.11 RSNA EAPOL · IEEE 802.11 RSNA EAPOL key
- 802.3 Slow protocols · Slow Protocols
- 9P · Plan 9
- A-bis OML · GSM A-bis OML
- A21 · A21 Protocol
- AAF · AVTP Audio Format
- AAL1 · ATM AAL1
- AAL3/4 · ATM AAL3/4
- AARP · Appletalk Address Resolution Protocol
- AASP · Aastra Signalling Protocol
- ACAP · Application Configuration Access Protocol
- ACN · Architecture for Control Networks
- ACP133 · ACP133 Attribute Syntaxes
- ACR 122 · Advanced Card Systems ACR122
- ACSE · ISO 8650-1 OSI Association Control Service
- ACtrace · AudioCodes Trunk Trace
- ADB · Android Debug Bridge
- ADB CS · Android Debug Bridge Client-Server
- ADB Service · Android Debug Bridge Service
- ADP · Aruba Discovery Protocol
- ADwin · ADwin communication protocol
- ADwin-Config · ADwin configuration protocol
- Aeron · Aeron Protocol
- AFP · Apple Filing Protocol

**Relation**

- is present
- ==
- !=
- >
- <
- >=
- <=
- contains
- matches
- in

**Value**

**Predefined Values**

**Range (offset:length)**

**Search:**

No display filter

*A hint.*

Help Cancel OK

Wireshark · Display Filter Expression

Field Name

▶ INITSHUTDOWN · Init shutdown service

▶ Interlink · Interlink Protocol

▶ IO-RAW · TwinCAT IO-RAW

▶ IOXIDResolver · DCOM OXID Resolver

▶ IP/IEEE1394 · Apple IP-over-IEEE 1394

▶ IPA · GSM over IP ip.access CCM sub-protocol

▶ IPARS · International Passenger Airline Reservation System...

▶ IPComp · IP Payload Compression

▶ IPDC · IP Device Control (SS7 over IP)

▶ IPDR/SP · IPDR

▶ iPerf2 · iPerf2 Packet Data

▶ IPFC · IP Over FC

▶ IPMB · Intelligent Platform Management Bus

▶ IPMI · Intelligent Platform Management Interface

▶ IPMI Session · Intelligent Platform Management Interface...

▶ ipmi-trace · IPMI Trace Data Collection

▶ IPNET · Solaris IPNET

▶ IPoIB · IP over Infiniband

▶ IPOS · IPOS Kernel Packet Protocol

▶ IPP · Internet Printing Protocol

▶ IPSec/IKE · IPSec/IKE

▶ IPv4 · Internet Protocol Version 4

▶ ip.addr · Source or Destination Address

▶ ip.bogus · Expert Info

▶ ip.bogus\_ip\_version · Expert Info

▶ ip.checksum · Header checksum

▶ ip.checksum\_bad.expert · Expert Info

▶ ip.checksum\_calculated · Calculated Checksum

▶ ip.checksum.status · Header checksum status

▶ ip.cipso.categories · Categories

▶ ip.cipso.doi · DOI

▶ ip.cipso.malformed · Expert Info

▶ ip.cipso.sensitivity\_level · Sensitivity Level

Relation

is present

==

!=

>

<

>=

<=

in

Value (IPv4 address)

140.119.168.10

Predefined match against this value.

Range (offset:length)

Search:

ip.addr == 140.119.168.10

Click OK to insert this filter

Help

Cancel

OK



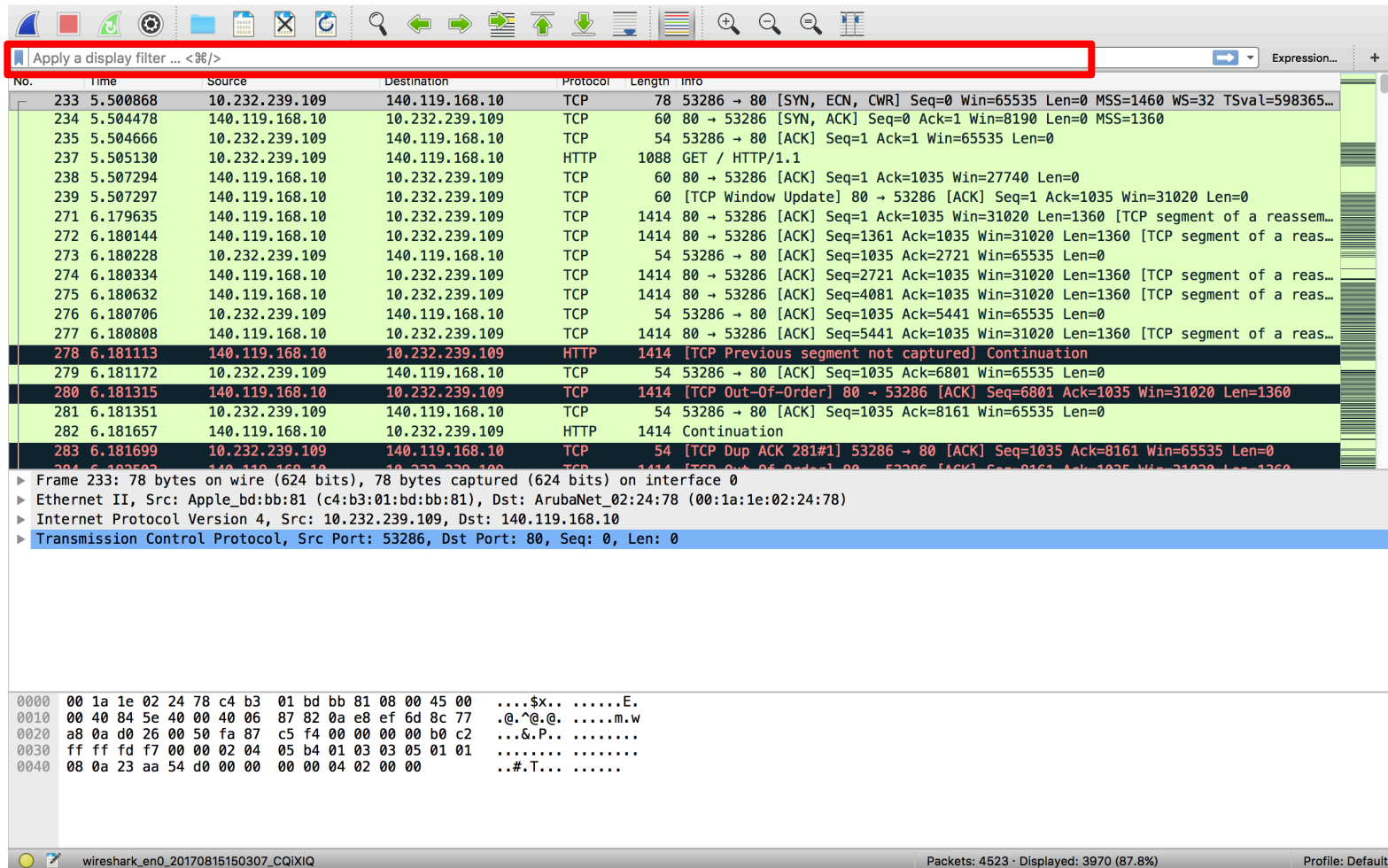
ip.addr == 140.119.168.10

| No. | Time     | Source         | Destination    | Protocol | Length | Info                                                                            |
|-----|----------|----------------|----------------|----------|--------|---------------------------------------------------------------------------------|
| 233 | 5.500868 | 10.232.239.109 | 140.119.168.10 | TCP      | 78     | 53286 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=598365... |
| 234 | 5.504478 | 140.119.168.10 | 10.232.239.109 | TCP      | 60     | 80 → 53286 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360                       |
| 235 | 5.504666 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | 53286 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0                                    |
| 237 | 5.505130 | 10.232.239.109 | 140.119.168.10 | HTTP     | 1088   | GET / HTTP/1.1                                                                  |
| 238 | 5.507294 | 140.119.168.10 | 10.232.239.109 | TCP      | 60     | 80 → 53286 [ACK] Seq=1 Ack=1035 Win=27740 Len=0                                 |
| 239 | 5.507297 | 140.119.168.10 | 10.232.239.109 | TCP      | 60     | [TCP Window Update] 80 → 53286 [ACK] Seq=1 Ack=1035 Win=31020 Len=0             |
| 271 | 6.179635 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | 80 → 53286 [ACK] Seq=1 Ack=1035 Win=31020 Len=1360 [TCP segment of a reassem... |
| 272 | 6.180144 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | 80 → 53286 [ACK] Seq=1361 Ack=1035 Win=31020 Len=1360 [TCP segment of a reas... |
| 273 | 6.180228 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | 53286 → 80 [ACK] Seq=1035 Ack=2721 Win=65535 Len=0                              |
| 274 | 6.180334 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | 80 → 53286 [ACK] Seq=2721 Ack=1035 Win=31020 Len=1360 [TCP segment of a reas... |
| 275 | 6.180632 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | 80 → 53286 [ACK] Seq=4081 Ack=1035 Win=31020 Len=1360 [TCP segment of a reas... |
| 276 | 6.180706 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | 53286 → 80 [ACK] Seq=1035 Ack=5441 Win=65535 Len=0                              |
| 277 | 6.180808 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | 80 → 53286 [ACK] Seq=5441 Ack=1035 Win=31020 Len=1360 [TCP segment of a reas... |
| 278 | 6.181113 | 140.119.168.10 | 10.232.239.109 | HTTP     | 1414   | [TCP Previous segment not captured] Continuation                                |
| 279 | 6.181172 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | 53286 → 80 [ACK] Seq=1035 Ack=6801 Win=65535 Len=0                              |
| 280 | 6.181315 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | [TCP Out-Of-Order] 80 → 53286 [ACK] Seq=6801 Ack=1035 Win=31020 Len=1360        |
| 281 | 6.181351 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | 53286 → 80 [ACK] Seq=1035 Ack=8161 Win=65535 Len=0                              |
| 282 | 6.181657 | 140.119.168.10 | 10.232.239.109 | HTTP     | 1414   | Continuation                                                                    |
| 283 | 6.181699 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | [TCP Dup ACK 281#1] 53286 → 80 [ACK] Seq=1035 Ack=8161 Win=65535 Len=0          |
| 284 | 6.182503 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | [TCP Out-Of-Order] 80 → 53286 [ACK] Seq=8161 Ack=1035 Win=31020 Len=1360        |

- ▶ Frame 233: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
- ▶ Ethernet II, Src: Apple\_bd:bb:81 (c4:b3:01:bd:bb:81), Dst: ArubaNet\_02:24:78 (00:1a:1e:02:24:78)
- ▶ Internet Protocol Version 4, Src: 10.232.239.109, Dst: 140.119.168.10
- ▶ Transmission Control Protocol, Src Port: 53286, Dst Port: 80, Seq: 0, Len: 0

```
0000  00 1a 1e 02 24 78 c4 b3 01 bd bb 81 08 00 45 00  ....$x.. .....E.
0010  00 40 84 5e 40 00 40 06 87 82 0a e8 ef 6d 8c 77  .@.^@.@. ....m.w
0020  a8 0a d0 26 00 50 fa 87 c5 f4 00 00 00 00 b0 c2  ...&.P. ....
0030  ff ff fd f7 00 00 02 04 05 b4 01 03 03 05 01 01  ....
0040  08 0a 23 aa 54 d0 00 00 00 00 04 02 00 00  ..#.T... .....
```

# 顯示篩選器



The image shows the Wireshark network traffic analysis interface. A red box highlights the display filter field, which contains the filter `<*>`. The packet list shows various network packets, including TCP and HTTP traffic. The bottom pane displays the raw packet data in hexadecimal and ASCII format.

Apply a display filter ... `<*>`

| No. | Time     | Source         | Destination    | Protocol | Length | Info                                                                            |
|-----|----------|----------------|----------------|----------|--------|---------------------------------------------------------------------------------|
| 233 | 5.500868 | 10.232.239.109 | 140.119.168.10 | TCP      | 78     | 53286 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=598365... |
| 234 | 5.504478 | 140.119.168.10 | 10.232.239.109 | TCP      | 60     | 80 → 53286 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360                       |
| 235 | 5.504666 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | 53286 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0                                    |
| 237 | 5.505130 | 10.232.239.109 | 140.119.168.10 | HTTP     | 1088   | GET / HTTP/1.1                                                                  |
| 238 | 5.507294 | 140.119.168.10 | 10.232.239.109 | TCP      | 60     | 80 → 53286 [ACK] Seq=1 Ack=1035 Win=27740 Len=0                                 |
| 239 | 5.507297 | 140.119.168.10 | 10.232.239.109 | TCP      | 60     | [TCP Window Update] 80 → 53286 [ACK] Seq=1 Ack=1035 Win=31020 Len=0             |
| 271 | 6.179635 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | 80 → 53286 [ACK] Seq=1 Ack=1035 Win=31020 Len=1360 [TCP segment of a reassem... |
| 272 | 6.180144 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | 80 → 53286 [ACK] Seq=1361 Ack=1035 Win=31020 Len=1360 [TCP segment of a reas... |
| 273 | 6.180228 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | 53286 → 80 [ACK] Seq=1035 Ack=2721 Win=65535 Len=0                              |
| 274 | 6.180334 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | 80 → 53286 [ACK] Seq=2721 Ack=1035 Win=31020 Len=1360 [TCP segment of a reas... |
| 275 | 6.180632 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | 80 → 53286 [ACK] Seq=4081 Ack=1035 Win=31020 Len=1360 [TCP segment of a reas... |
| 276 | 6.180706 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | 53286 → 80 [ACK] Seq=1035 Ack=5441 Win=65535 Len=0                              |
| 277 | 6.180808 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | 80 → 53286 [ACK] Seq=5441 Ack=1035 Win=31020 Len=1360 [TCP segment of a reas... |
| 278 | 6.181113 | 140.119.168.10 | 10.232.239.109 | HTTP     | 1414   | [TCP Previous segment not captured] Continuation                                |
| 279 | 6.181172 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | 53286 → 80 [ACK] Seq=1035 Ack=6801 Win=65535 Len=0                              |
| 280 | 6.181315 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | [TCP Out-Of-Order] 80 → 53286 [ACK] Seq=6801 Ack=1035 Win=31020 Len=1360        |
| 281 | 6.181351 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | 53286 → 80 [ACK] Seq=1035 Ack=8161 Win=65535 Len=0                              |
| 282 | 6.181657 | 140.119.168.10 | 10.232.239.109 | HTTP     | 1414   | Continuation                                                                    |
| 283 | 6.181699 | 10.232.239.109 | 140.119.168.10 | TCP      | 54     | [TCP Dup ACK 281#1] 53286 → 80 [ACK] Seq=1035 Ack=8161 Win=65535 Len=0          |
| 284 | 6.182502 | 140.119.168.10 | 10.232.239.109 | TCP      | 1414   | [TCP Out-Of-Order] 80 → 53286 [ACK] Seq=8161 Ack=1035 Win=31020 Len=1360        |

▶ Frame 233: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0  
▶ Ethernet II, Src: Apple\_bd:bb:81 (c4:b3:01:bd:bb:81), Dst: ArubaNet\_02:24:78 (00:1a:1e:02:24:78)  
▶ Internet Protocol Version 4, Src: 10.232.239.109, Dst: 140.119.168.10  
▶ Transmission Control Protocol, Src Port: 53286, Dst Port: 80, Seq: 0, Len: 0

```
0000  00 1a 1e 02 24 78 c4 b3 01 bd bb 81 08 00 45 00  ....$.x.. ..E.
0010  00 40 84 5e 40 00 00 06 87 82 0a e8 ef 6d 8c 77  .@.^@.@. ....m.w
0020  a8 0a d0 26 00 50 fa 87 c5 f4 00 00 00 00 b0 c2  ..&.P.....
0030  ff ff fd f7 00 00 02 04 05 b4 01 03 03 05 01 01  .....
0040  08 0a 23 aa 54 d0 00 00 00 00 04 02 00 00 00  ..#.T.....
```

wireshark\_en0\_20170815150307\_CQIXIQ Packets: 4523 · Displayed: 3970 (87.8%) Profile: Default



# 顯示篩選器

Wireshark interface showing a packet capture filter 'http' applied to the capture. The filter is highlighted with a red box. The packet list shows various HTTP packets, including GET requests and continuations. The packet details pane shows the structure of a selected packet.

| No. | Time     | Source         | Destination    | Protocol | Length | Info                                                                            |
|-----|----------|----------------|----------------|----------|--------|---------------------------------------------------------------------------------|
| 237 | 5.505130 | 10.232.239.109 | 140.119.168.10 | HTTP     | 088    | GET / HTTP/1.1                                                                  |
| 278 | 6.181113 | 140.119.168.10 | 10.232.239.109 | HTTP     | 414    | [TCP Previous segment not captured] Continuation                                |
| 282 | 6.181657 | 140.119.168.10 | 10.232.239.109 | HTTP     | 414    | Continuation                                                                    |
| 288 | 6.183975 | 140.119.168.10 | 10.232.239.109 | HTTP     | 414    | Continuation                                                                    |
| 289 | 6.184947 | 140.119.168.10 | 10.232.239.109 | HTTP     | 324    | Continuation                                                                    |
| 295 | 6.216772 | 10.232.239.109 | 140.119.168.10 | HTTP     | 048    | GET /assets/template/template-a513007afa2e79671a9d85528834a355.css HTTP/1.1     |
| 319 | 6.229527 | 140.119.168.10 | 10.232.239.109 | HTTP     | 481    | HTTP/1.1 200 OK (text/css)                                                      |
| 328 | 6.233750 | 10.232.239.109 | 140.119.168.10 | HTTP     | 004    | GET /assets/basic/icon HTTP/1.1                                                 |
| 329 | 6.233818 | 10.232.239.109 | 140.119.168.10 | HTTP     | 017    | GET /assets/lib/orbit_bar/orbit_bar HTTP/1.1                                    |
| 337 | 6.240102 | 10.232.239.109 | 140.119.168.10 | HTTP     | 023    | GET /assets/frontend-8338adc0c5e32b6d28215ca591059bb9.js HTTP/1.1               |
| 340 | 6.242584 | 140.119.168.10 | 10.232.239.109 | HTTP     | 145    | HTTP/1.1 200 OK (text/css)                                                      |
| 349 | 6.247516 | 140.119.168.10 | 10.232.239.109 | HTTP     | 664    | HTTP/1.1 200 OK (application/x-javascript)                                      |
| 352 | 6.247813 | 140.119.168.10 | 10.232.239.109 | HTTP     | 866    | HTTP/1.1 200 OK (text/css)                                                      |
| 354 | 6.265928 | 10.232.239.109 | 140.119.168.10 | HTTP     | 073    | GET /uploads/site/default_image/542e45757470001ec1170000/nccu_logo.png HTTP/1.1 |
| 356 | 6.269066 | 140.119.168.10 | 10.232.239.109 | HTTP     | 298    | HTTP/1.1 200 OK (PNG)                                                           |
| 358 | 6.272918 | 10.232.239.109 | 140.119.168.10 | HTTP     | 104    | GET /uploads/ad_image/file/598aec83e78fe14ca50068c7/%E5%AD%B8%E6%A0%A1%E5%AE... |
| 454 | 6.347320 | 10.232.239.109 | 140.119.168.10 | HTTP     | 063    | GET /uploads/ad_image/file/598ae69be78fe1354100692d/0011.png HTTP/1.1           |
| 592 | 6.420641 | 10.232.239.109 | 140.119.168.10 | HTTP     | 082    | GET /assets/bg.png HTTP/1.1                                                     |
| 611 | 6.434269 | 10.232.239.109 | 140.119.168.10 | HTTP     | 069    | GET /uploads/ad_image/file/5982e2efe78fe1306600536f/0008banner.png HTTP/1.1     |

Frame 237: 1088 bytes on wire (8704 bits), 1088 bytes captured (8704 bits) on interface 0

Ethernet II, Src: Apple\_bd:bb:81 (c4:b3:01:bd:bb:81), Dst: ArubaNet\_02:24:78 (00:1a:1e:02:24:78)

Internet Protocol Version 4, Src: 10.232.239.109, Dst: 140.119.168.10

Transmission Control Protocol, Src Port: 53286, Dst Port: 80, Seq: 1, Ack: 1, Len: 1034

Hypertext Transfer Protocol

```
0000 00 1a 1e 02 24 78 c4 b3 01 bd bb 81 08 00 45 00 ....$x.. ..E.
0010 04 32 4a 1f 40 00 40 06 bd cf 0a e8 ef 6d 8c 77 .2J.@. ....m.w
0020 a8 0a d0 26 00 50 fa 87 c5 f5 31 04 c8 d0 50 18 ...&.P.. !...P.
0030 ff ff 97 c8 00 00 47 45 54 20 2f 20 48 54 54 50 .....GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 34 30 2e /1.1..Ho st: 140.
0050 31 31 39 2e 31 36 38 2e 31 30 0d 0a 43 6f 6e 6e 119.168. 10..Conn
0060 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 ection: keep-ali
0070 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 ve..Upgr ade-Inse
0080 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 cure-Req uests: 1
```

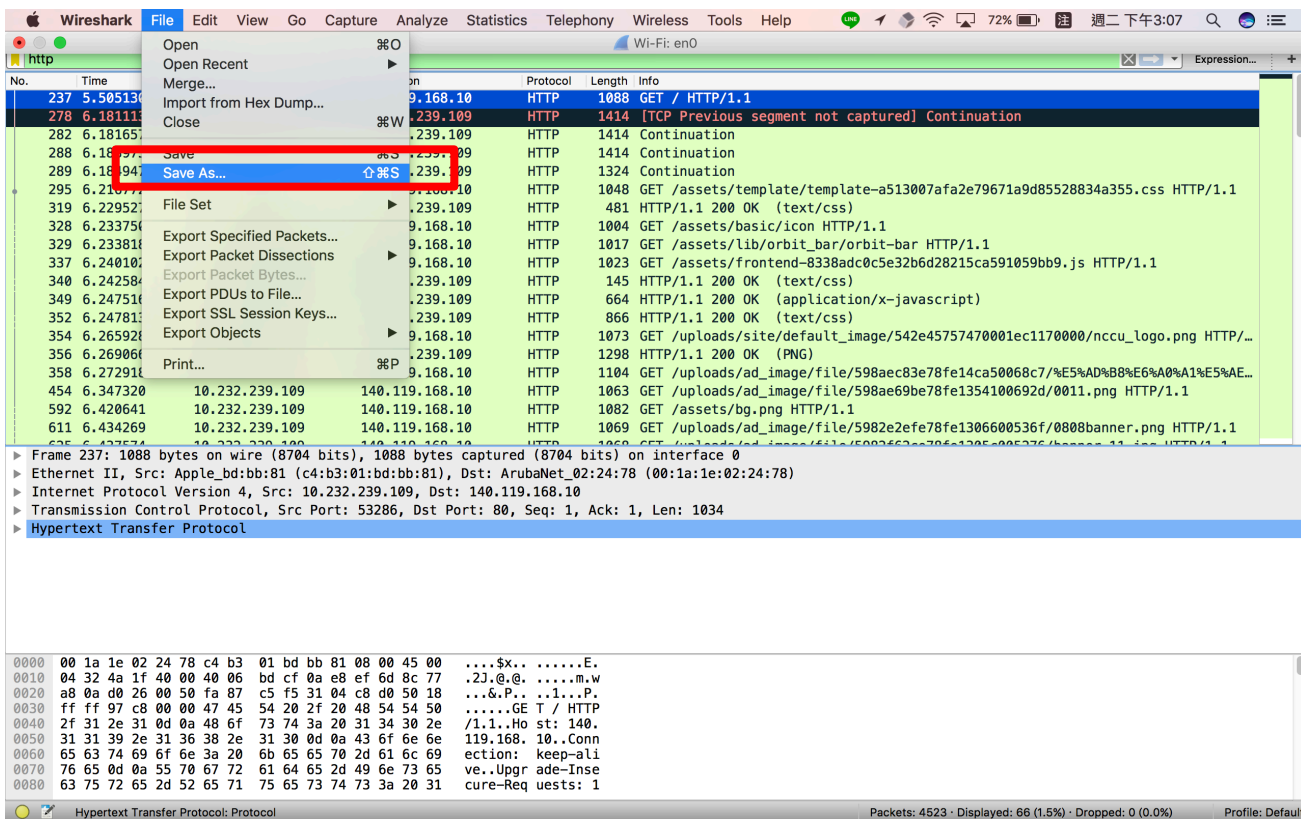
Hypertext Transfer Protocol: Protocol

Packets: 4523 · Displayed: 66 (1.5%) · Dropped: 0 (0.0%)

Profile: Default

# 封包儲存

需中斷抓取封包，才能儲存







End