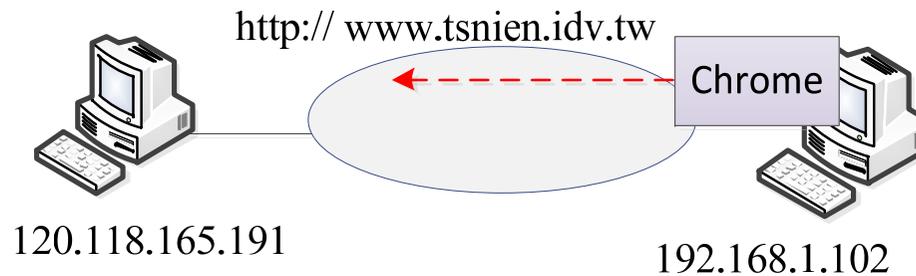


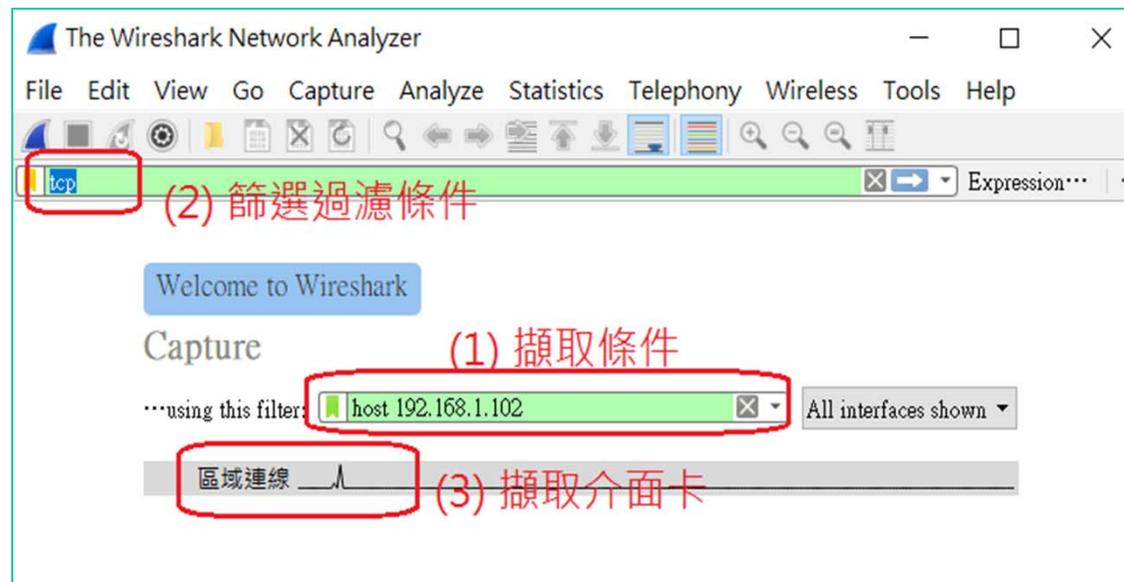
4-5-4 TCP 擷取與分析 – Wireshark (一)



✦ 系統分析



✦ 開啟Wireshark



4-5-4 TCP 擷取與分析 – Wireshark (二)



✧ 客戶端建立連線封包

The screenshot shows the Wireshark interface with a packet capture of a TCP SYN packet. The packet list table is highlighted with a red box, and the packet details pane for the selected packet is also highlighted with a red box.

No.	Time	Source	Destination	Protocol	Length
13	0.001525	192.168.1.102	120.118.165.191	TCP	66
41	0.085946	120.118.165.191	192.168.1.102	TCP	66
43	0.086021	192.168.1.102	120.118.165.191	TCP	54
44	0.086233	192.168.1.102	120.118.165.191	HTTP	574

Frame 13: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface
> Ethernet II, Src: AsustekC_83:d1:c3 (34:97:f6:83:d1:c3), Dst: D-LinkIn_e6:af:
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 120.118.165.191
Transmission Control Protocol, Src Port: 50699, Dst Port: 80, Seq: 0, Len: 0
Source Port: 50699
Destination Port: 80
[Stream index: 9]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1000 = Header Length: 32 bytes (8)
> Flags: 0x002 (SYN)
Window size value: 64240
[Calculated window size: 64240]
Checksum: 0xe06a [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scal
> [Timestamps]



4-5-4 TCP 擷取與分析 – Wireshark (三)



✪ 伺服器回應同意連線封包

The screenshot displays the Wireshark interface with a packet capture of a TCP SYN-ACK response. The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
13	0.001525	192.168.1.102	120.118.165.191	TCP	66	50699 →
41	0.085946	120.118.165.191	192.168.1.102	TCP	66	80 → 50699
43	0.086021	192.168.1.102	120.118.165.191	TCP	54	50699 →
44	0.086233	192.168.1.102	120.118.165.191	HTTP	574	GFT /

The packet details pane for packet 41 shows the following information:

- Ethernet II, Src: D-LinkIn_e6:af:0c (78:54:2e:e6:af:0c), Dst: AsustekC_83:d1:c3 (34:86:e6:83:d1:c3)
- Internet Protocol Version 4, Src: 120.118.165.191, Dst: 192.168.1.102
- Transmission Control Protocol, Src Port: 80, Dst Port: 50699, Seq: 0, Ack: 1, Len: 0
 - Source Port: 80
 - Destination Port: 50699
 - [Stream index: 9]
 - [TCP Segment Len: 0]
 - Sequence number: 0 (relative sequence number)
 - [Next sequence number: 0 (relative sequence number)]
 - Acknowledgment number: 1 (relative ack number)
 - 1000 = Header Length: 32 bytes (8)
 - Flags: 0x012 (SYN, ACK)
 - Window size value: 29200
 - [Calculated window size: 29200]
 - Checksum: 0x0488 [unverified]
 - [Checksum Status: Unverified]
 - Urgent pointer: 0
 - Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP)
 - [SEQ/ACK analysis]



4-5-4 TCP 擷取與分析 – Wireshark (四)



✦ 客戶端確認連線成功

The screenshot shows the Wireshark interface with a packet capture for TCP. The packet list pane shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
13	0.001525	192.168.1.102	120.118.165.191	TCP	66	50699 →
41	0.085946	120.118.165.191	192.168.1.102	TCP	66	80 → 50
43	0.086021	192.168.1.102	120.118.165.191	TCP	54	50699 →
44	0.086233	192.168.1.102	120.118.165.191	HTTP	574	GFT / H

The details pane for packet 43 (Transmission Control Protocol) is expanded and highlighted with a red box:

- Transmission Control Protocol, Src Port: 50699, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
- Source Port: 50699
- Destination Port: 80
- [Stream index: 9]
- [TCP Segment Len: 0]
- Sequence number: 1 (relative sequence number)
- [Next sequence number: 1 (relative sequence number)]
- Acknowledgment number: 1 (relative ack number)
- 0101 = Header Length: 20 bytes (5)
- > Flags: 0x010 (ACK)
- Window size value: 257
- [Calculated window size: 65792]
- [Window size scaling factor: 256]
- Checksum: 0xe05e [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- > [SEQ/ACK analysis]

