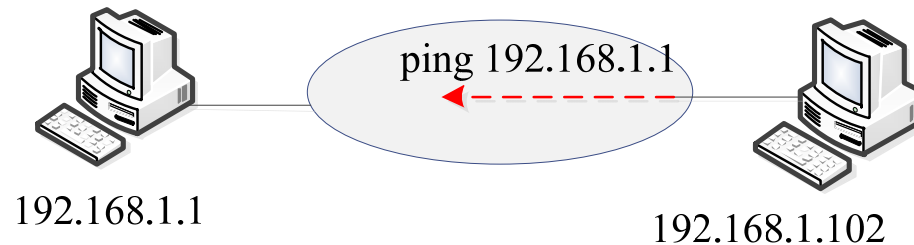


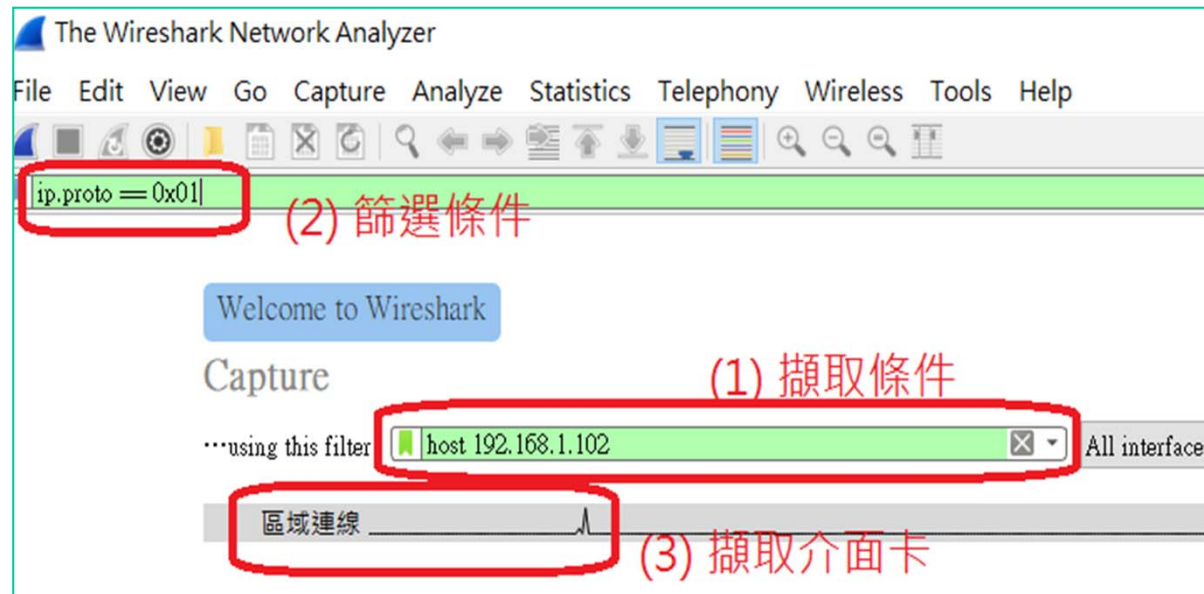
4-4-3 ICMP 封包擷取 – Wireshark (一)



✦ 系統分析



✦ 開啟Wireshark



4-4-3 ICMP 封包擷取 – Wireshark (二)



✦ Echo Request 封包分析

✦ Echo Reply 封包分析

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a packet list with the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	239.255.255.250	IGMPv2	46	Membership Re...
2	0.509172	192.168.1.102	224.0.0.0	IGMPv2	46	Membership Re...
3	4.062838	192.168.1.102	192.168.1.1	ICMP	74	Echo (ping) reques...
4	4.063689	192.168.1.1	192.168.1.102	ICMP	74	Echo (ping) reply
5	5.009414	192.168.1.102	224.0.0.0	IGMPv2	46	Membership Re...

The bottom screenshot shows the detailed view of packet 3, which is an ICMP Echo (ping) request. The details pane shows the following information:

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4d52 [correct] [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence number (BE): 9 (0x0009)
- Sequence number (LE): 2304 (0x0900)
- [Response frame: 4]
- Data (32 bytes)

The top screenshot also shows the detailed view of packet 4, which is an ICMP Echo (ping) reply. The details pane shows the following information:

- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0x5552 [correct] [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence number (BE): 9 (0x0009)
- Sequence number (LE): 2304 (0x0900)
- [Request frame: 3]
- [Response time: 0.851 ms]
- Data (32 bytes)
- Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
- [Length: 32]

