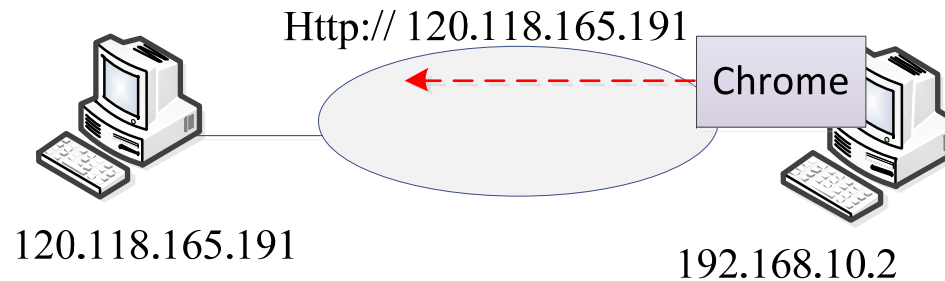


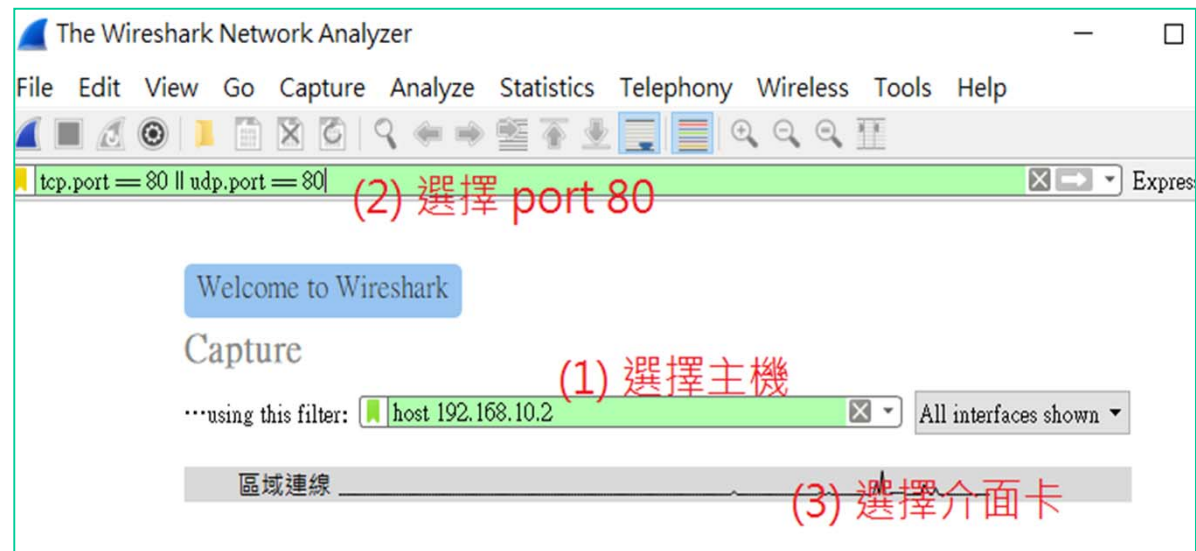
4-3-6 IP 封包擷取 – Wireshark (一)



✦ 系統分析



✦ 開啟Wireshark



4-3-6 IP 封包擷取 – Wireshark (二)



✦ IP 協定分析

The screenshot shows the Wireshark interface with a packet capture table and a detailed view of a selected packet. The table lists several TCP packets from source 192.168.1.102 to destination 120.118.165.191. The detailed view shows the structure of the IP header, including version, header length, differentiated services field, total length, identification, flags, time to live, protocol, and checksum.

No.	Time	Source	Destination	Protocol	Length
10	3.335771	192.168.1.102	120.118.165.191	TCP	54
11	3.335812	192.168.1.102	120.118.165.191	TCP	54
12	3.335827	192.168.1.102	120.118.165.191	TCP	54
13	3.335839	192.168.1.102	120.118.165.191	TCP	54
14	3.335851	192.168.1.102	120.118.165.191	TCP	54
15	3.335862	192.168.1.102	120.118.165.191	TCP	54

```
> Frame 10: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface
> Ethernet II, Src: AsustekC_83:d1:c3 (34:97:f6:83:d1:c3), Dst: D-LinkIn_e6:a
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 120.118.165.191
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x0712 (1810)
  > Flags: 0x4000, Don't fragment
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.102
  Destination: 120.118.165.191
```

