封包分析實務分析

本課程所使用之圖片歸原著作權所有，不做商業用途。

課程宗旨

- 本課程以 wireshark教導學生，讓學生由實作中了解TCP/IP網路協定
- 課程提供Connection2Google.pcap封包檔作為實戰分析的範例:學生須完成
- [1] DNS查詢分析
- [2] TCP封包格式分析
- [3] TCP 三向交握分析
- [4] UDP封包格式分析
- [5] IP封包格式分析

[1] DNS查詢分析

- 查詢的IP=?
- DNS server =?
- Google IP=?

[2] TCP 封包格式分析

- port的查詢=?

[3] TCP 三向交握分析

- 找出tcp三向交握的封包

[4] UDP 封包格式分析

- udp Destination Port查看

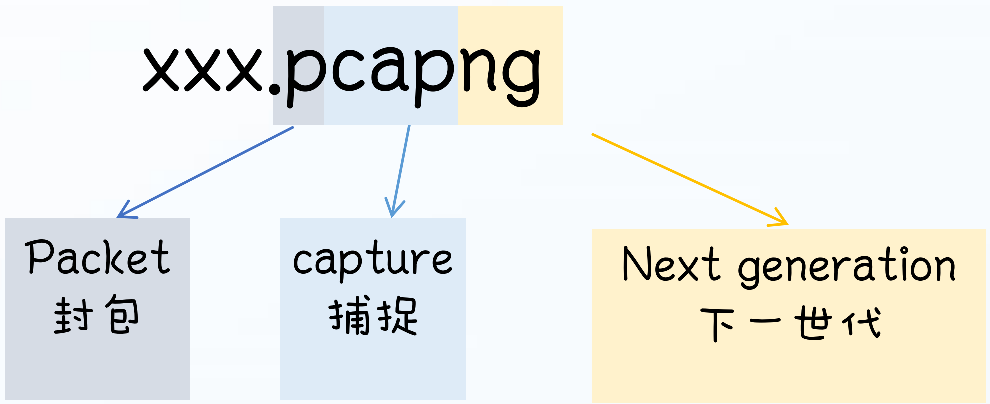
[5] IP 封包格式分析

- IP完整封包查看
- Time to live查看

檔案格式

Connection2Google.pcap

packet capture



xxx.pcapng

Packet
封包

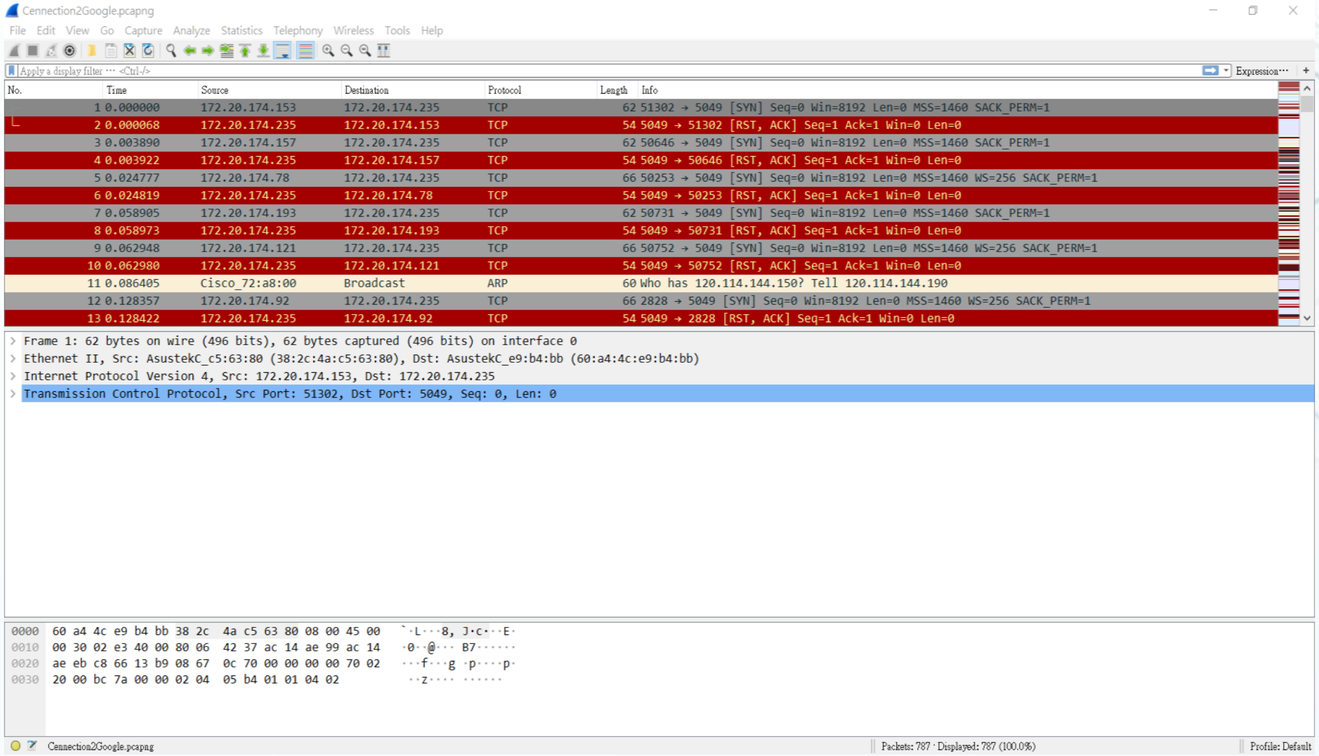
capture
捕捉

Next generation
下一世代

請打開Cennection2Google.pcapng
這次課程使用這個檔案進行教學

Cennection2Google.pcapng

打開
Cennection2Google.pcapng
之後的樣子


Cennection2Google.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.20.174.153	172.20.174.235	TCP	62	51302 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
2	0.000068	172.20.174.235	172.20.174.153	TCP	54	5049 → 51302 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.003890	172.20.174.157	172.20.174.235	TCP	62	50646 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
4	0.003922	172.20.174.235	172.20.174.157	TCP	54	5049 → 50646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.024777	172.20.174.78	172.20.174.235	TCP	66	50253 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
6	0.024819	172.20.174.235	172.20.174.78	TCP	54	5049 → 50253 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.058905	172.20.174.193	172.20.174.235	TCP	62	50731 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8	0.058973	172.20.174.235	172.20.174.193	TCP	54	5049 → 50731 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	0.062948	172.20.174.121	172.20.174.235	TCP	66	50752 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	0.062980	172.20.174.235	172.20.174.121	TCP	54	5049 → 50752 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.086405	Cisco_72:a8:00	Broadcast	ARP	60	Who has 120.114.144.150? Tell 120.114.144.190
12	0.128357	172.20.174.92	172.20.174.235	TCP	66	2828 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	0.128422	172.20.174.235	172.20.174.92	TCP	54	5049 → 2828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

```
> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
> Ethernet II, Src: AsustekC_c5:63:80 (38:2c:4a:c5:63:80), Dst: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb)
> Internet Protocol Version 4, Src: 172.20.174.153, Dst: 172.20.174.235
> Transmission Control Protocol, Src Port: 51302, Dst Port: 5049, Seq: 0, Len: 0
```

```
0000  60 a4 4c e9 b4 bb 38 2c  4a c5 63 80 08 00 45 00   `·L···8, J·c···E·
0010  00 30 02 e3 40 00 80 06  42 37 ac 14 ae 99 ac 14   ·0··@··· B7······
0020  ae eb c8 66 13 b9 08 67  0c 70 00 00 00 00 70 02   ···f···g ·p····p·
0030  20 00 bc 7a 00 00 02 04  05 b4 01 01 04 02          ··z····  ······
```

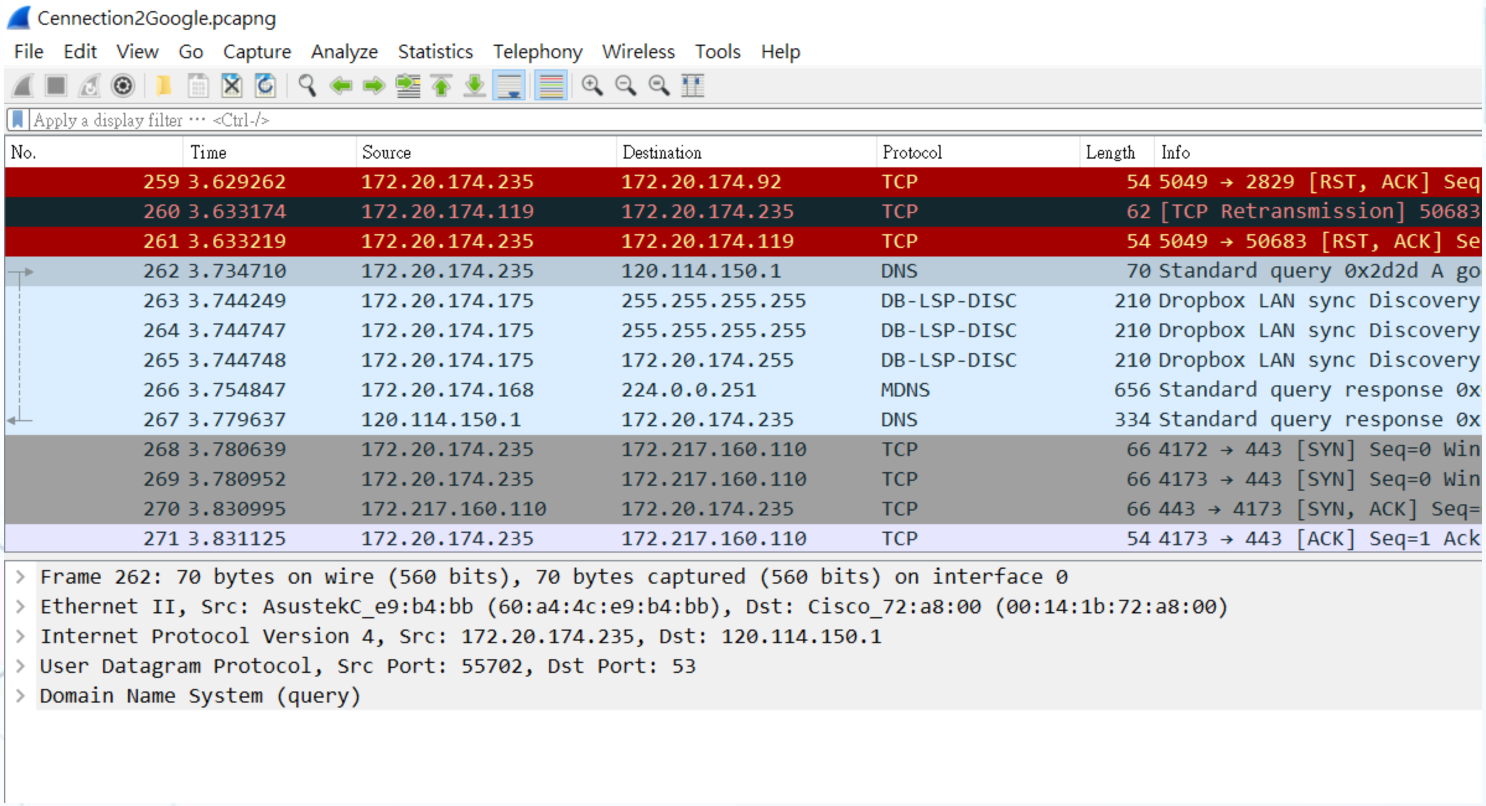
Cennection2Google.pcapng | Packets: 787 · Displayed: 787 (100.0%) | Profile: Default

DNS查詢分析

DNS Lab1:

第262個封包所查詢的域名是什麼?

Lab1:第262個封包所查詢的域名是什麼



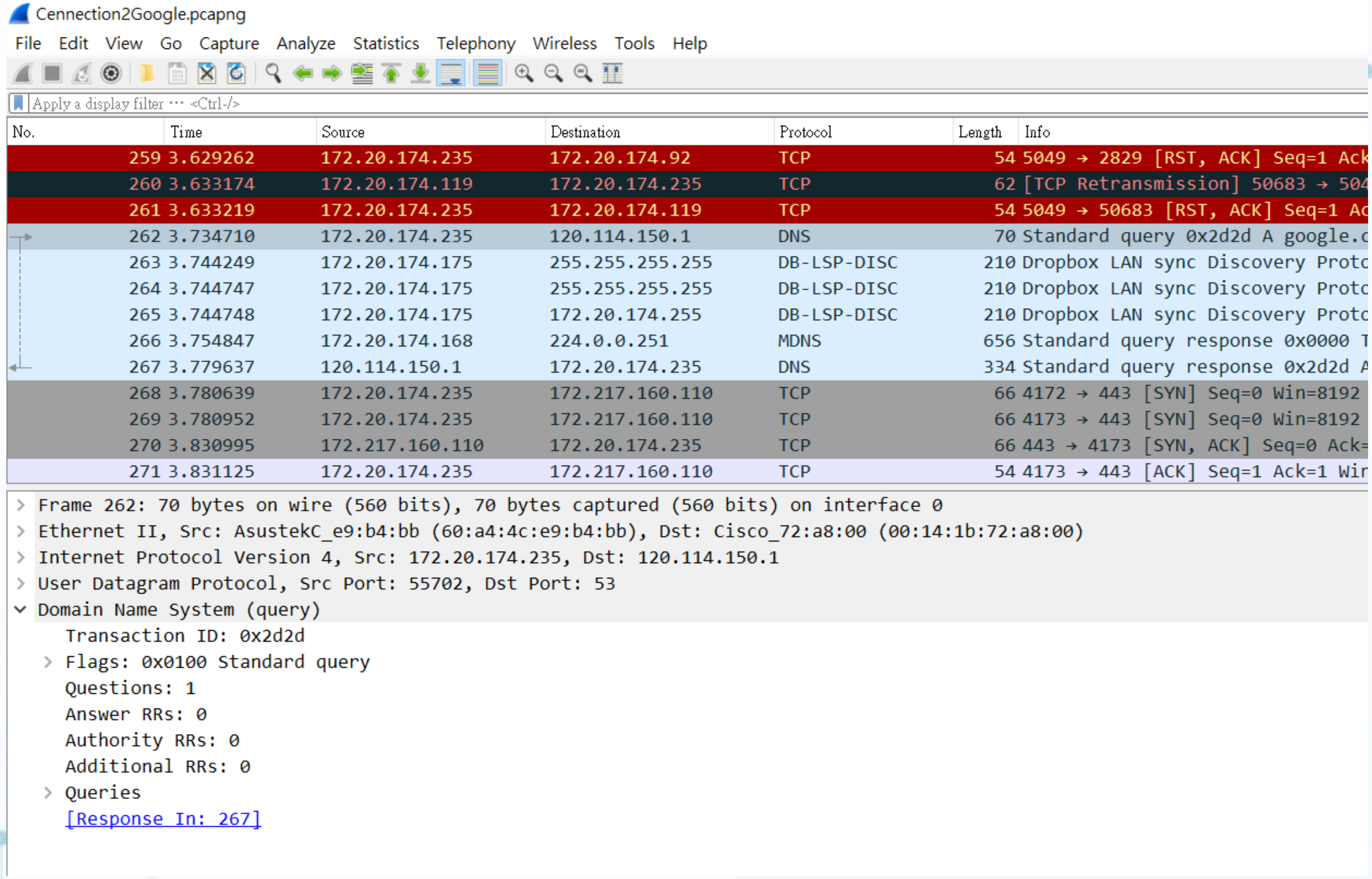
Cennection2Google.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
259	3.629262	172.20.174.235	172.20.174.92	TCP	54	5049 → 2829 [RST, ACK] Seq
260	3.633174	172.20.174.119	172.20.174.235	TCP	62	[TCP Retransmission] 50683
261	3.633219	172.20.174.235	172.20.174.119	TCP	54	5049 → 50683 [RST, ACK] Se
262	3.734710	172.20.174.235	120.114.150.1	DNS	70	Standard query 0x2d2d A go
263	3.744249	172.20.174.175	255.255.255.255	DB-LSP-DISC	210	Dropbox LAN sync Discovery
264	3.744747	172.20.174.175	255.255.255.255	DB-LSP-DISC	210	Dropbox LAN sync Discovery
265	3.744748	172.20.174.175	172.20.174.255	DB-LSP-DISC	210	Dropbox LAN sync Discovery
266	3.754847	172.20.174.168	224.0.0.251	MDNS	656	Standard query response 0x
267	3.779637	120.114.150.1	172.20.174.235	DNS	334	Standard query response 0x
268	3.780639	172.20.174.235	172.217.160.110	TCP	66	4172 → 443 [SYN] Seq=0 Win
269	3.780952	172.20.174.235	172.217.160.110	TCP	66	4173 → 443 [SYN] Seq=0 Win
270	3.830995	172.217.160.110	172.20.174.235	TCP	66	443 → 4173 [SYN, ACK] Seq=
271	3.831125	172.20.174.235	172.217.160.110	TCP	54	4173 → 443 [ACK] Seq=1 Ack

```
> Frame 262: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb), Dst: Cisco_72:a8:00 (00:14:1b:72:a8:00)
> Internet Protocol Version 4, Src: 172.20.174.235, Dst: 120.114.150.1
> User Datagram Protocol, Src Port: 55702, Dst Port: 53
> Domain Name System (query)
```

Lab1:第262個封包所查詢的域名是什麼

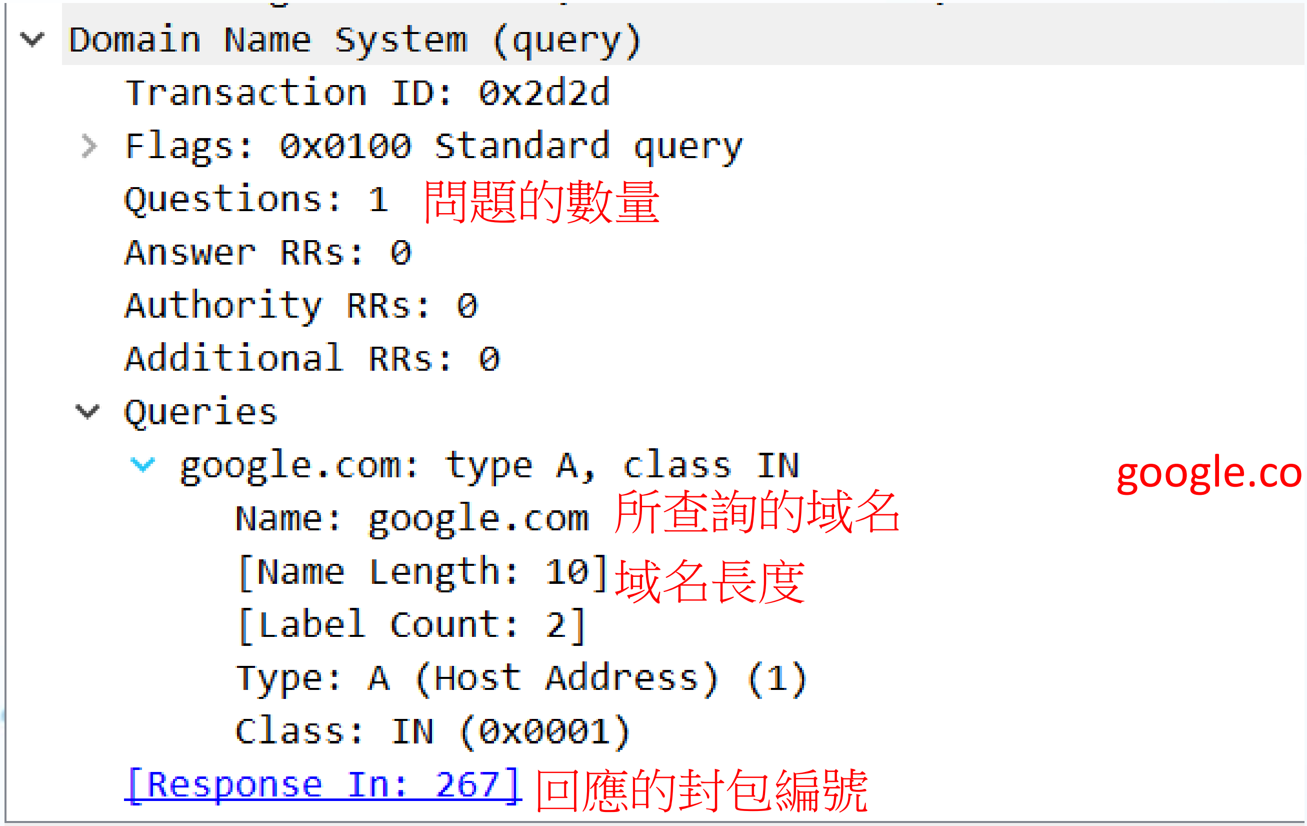

Cennection2Google.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
259	3.629262	172.20.174.235	172.20.174.92	TCP	54	5049 → 2829 [RST, ACK] Seq=1 Ack
260	3.633174	172.20.174.119	172.20.174.235	TCP	62	[TCP Retransmission] 50683 → 504
261	3.633219	172.20.174.235	172.20.174.119	TCP	54	5049 → 50683 [RST, ACK] Seq=1 Ac
262	3.734710	172.20.174.235	120.114.150.1	DNS	70	Standard query 0x2d2d A google.c
263	3.744249	172.20.174.175	255.255.255.255	DB-LSP-DISC	210	Dropbox LAN sync Discovery Protc
264	3.744747	172.20.174.175	255.255.255.255	DB-LSP-DISC	210	Dropbox LAN sync Discovery Protc
265	3.744748	172.20.174.175	172.20.174.255	DB-LSP-DISC	210	Dropbox LAN sync Discovery Protc
266	3.754847	172.20.174.168	224.0.0.251	MDNS	656	Standard query response 0x0000 T
267	3.779637	120.114.150.1	172.20.174.235	DNS	334	Standard query response 0x2d2d A
268	3.780639	172.20.174.235	172.217.160.110	TCP	66	4172 → 443 [SYN] Seq=0 Win=8192
269	3.780952	172.20.174.235	172.217.160.110	TCP	66	4173 → 443 [SYN] Seq=0 Win=8192
270	3.830995	172.217.160.110	172.20.174.235	TCP	66	443 → 4173 [SYN, ACK] Seq=0 Ack=
271	3.831125	172.20.174.235	172.217.160.110	TCP	54	4173 → 443 [ACK] Seq=1 Ack=1 Wir

```
> Frame 262: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb), Dst: Cisco_72:a8:00 (00:14:1b:72:a8:00)
> Internet Protocol Version 4, Src: 172.20.174.235, Dst: 120.114.150.1
> User Datagram Protocol, Src Port: 55702, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x2d2d
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 267]
```

Lab1:第262個封包所查詢的域名是什麼

完成



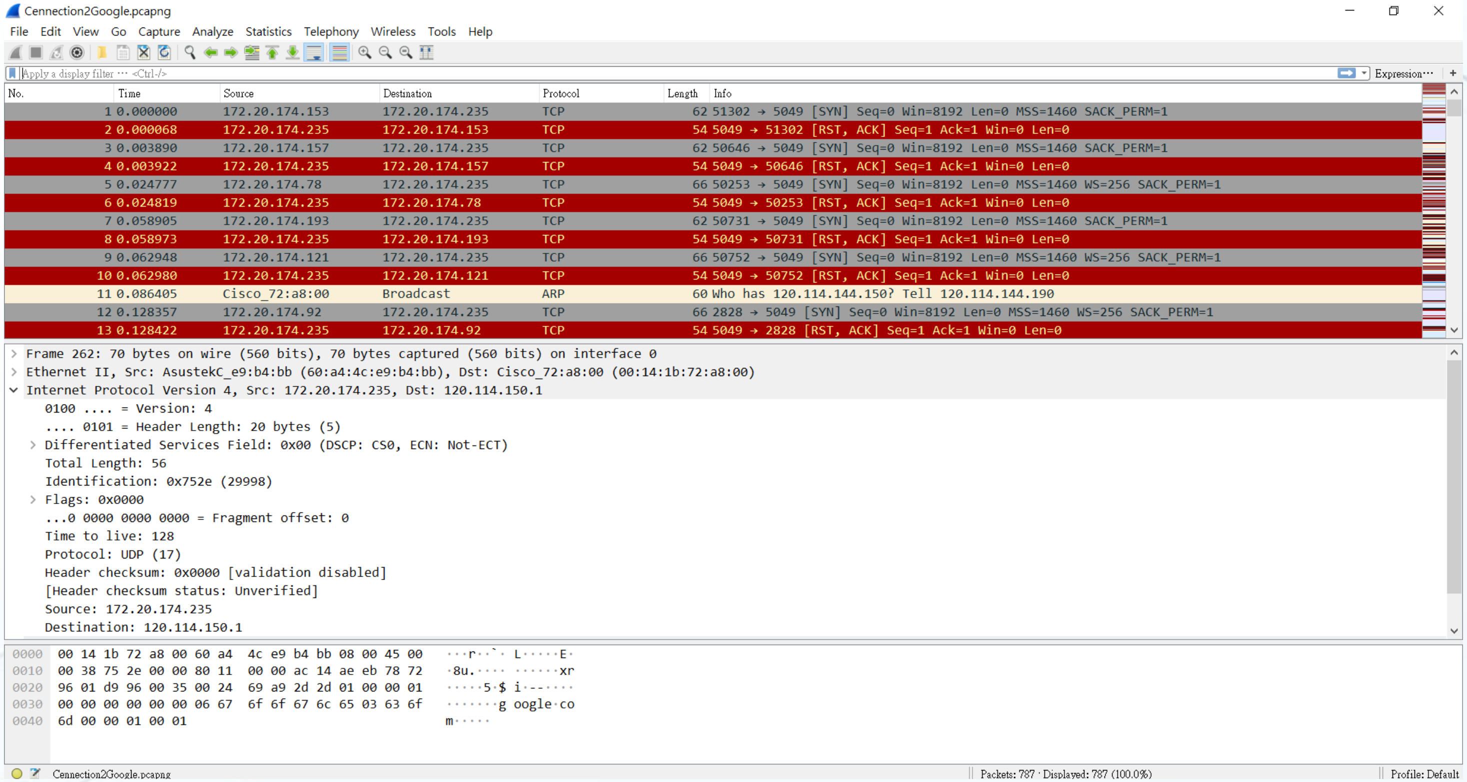
```
∨ Domain Name System (query)
    Transaction ID: 0x2d2d
  > Flags: 0x0100 Standard query
    Questions: 1  問題的數量
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ∨ Queries
    ∨ google.com: type A, class IN
        Name: google.com 所查詢的域名
        [Name Length: 10]域名長度
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 267] 回應的封包編號
```

google.com

DNS Lab2:

DNS的server是多少？

Lab2:DNS的server是多少


Cennection2Google.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
Cennection2Google.pcapng
Packets: 787 · Displayed: 787 (100.0%)
Profile: Default

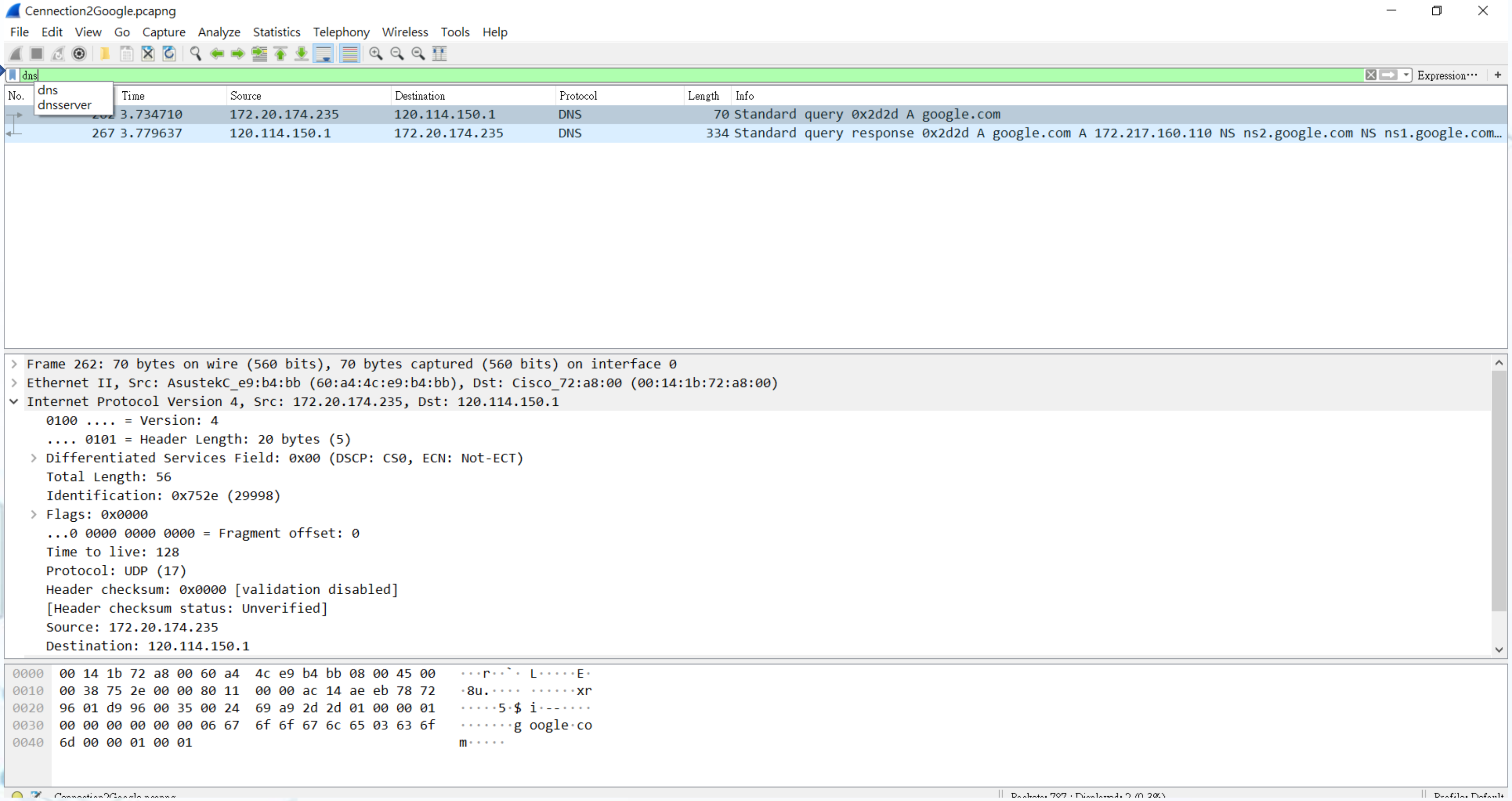
```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  172.20.174.153  172.20.174.235  TCP      62 51302 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
    2 0.000068  172.20.174.235  172.20.174.153  TCP      54 5049 → 51302 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    3 0.003890  172.20.174.157  172.20.174.235  TCP      62 50646 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
    4 0.003922  172.20.174.235  172.20.174.157  TCP      54 5049 → 50646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    5 0.024777  172.20.174.78   172.20.174.235  TCP      66 50253 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    6 0.024819  172.20.174.235  172.20.174.78   TCP      54 5049 → 50253 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    7 0.058905  172.20.174.193  172.20.174.235  TCP      62 50731 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
    8 0.058973  172.20.174.235  172.20.174.193  TCP      54 5049 → 50731 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    9 0.062948  172.20.174.121  172.20.174.235  TCP      66 50752 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   10 0.062980  172.20.174.235  172.20.174.121  TCP      54 5049 → 50752 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   11 0.086405  Cisco_72:a8:00  Broadcast       ARP      60 Who has 120.114.144.150? Tell 120.114.144.190
   12 0.128357  172.20.174.92   172.20.174.235  TCP      66 2828 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   13 0.128422  172.20.174.235  172.20.174.92   TCP      54 5049 → 2828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
> Frame 262: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb), Dst: Cisco_72:a8:00 (00:14:1b:72:a8:00)
v Internet Protocol Version 4, Src: 172.20.174.235, Dst: 120.114.150.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x752e (29998)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.20.174.235
    Destination: 120.114.150.1
```

```
0000  00 14 1b 72 a8 00 60 a4  4c e9 b4 bb 08 00 45 00   ···r··`· L·····E·
0010  00 38 75 2e 00 00 80 11  00 00 ac 14 ae eb 78 72   ·8u.···· ······xr
0020  96 01 d9 96 00 35 00 24  69 a9 2d 2d 01 00 00 01   ·····5·$ i·--····
0030  00 00 00 00 00 00 06 67  6f 6f 67 6c 65 03 63 6f   ·······g oogle·co
0040  6d 00 00 01 00 01                                  m·····
```

Lab2:DNS的server是多少

輸入DNS



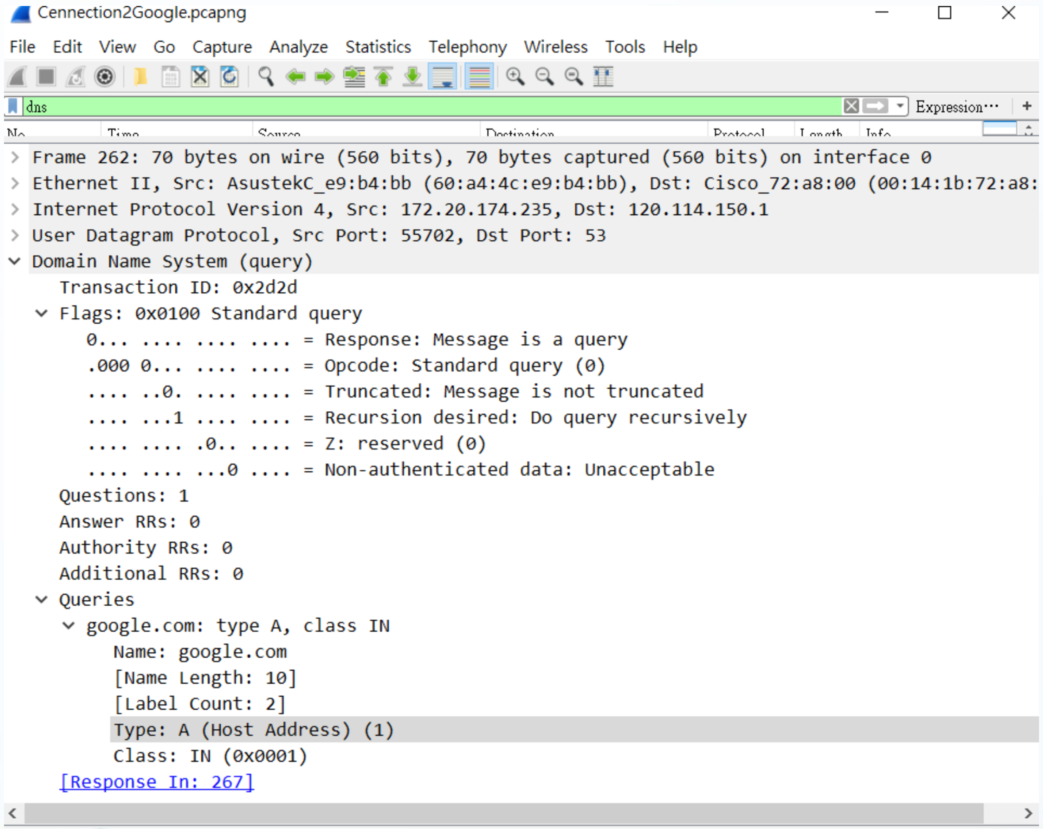
```
No.  Time      Source          Destination     Protocol  Length Info
262  3.734710  172.20.174.235  120.114.150.1   DNS           70 Standard query 0x2d2d A google.com
267  3.779637  120.114.150.1   172.20.174.235  DNS          334 Standard query response 0x2d2d A google.com A 172.217.160.110 NS ns2.google.com NS ns1.google.com…
```

```
> Frame 262: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb), Dst: Cisco_72:a8:00 (00:14:1b:72:a8:00)
v Internet Protocol Version 4, Src: 172.20.174.235, Dst: 120.114.150.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x752e (29998)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.20.174.235
    Destination: 120.114.150.1
```

```
0000  00 14 1b 72 a8 00 60 a4  4c e9 b4 bb 08 00 45 00   ···r··`· L·····E·
0010  00 38 75 2e 00 00 80 11  00 00 ac 14 ae eb 78 72   ·8u.···· ······xr
0020  96 01 d9 96 00 35 00 24  69 a9 2d 2d 01 00 00 01   ·····5·$ i·--····
0030  00 00 00 00 00 00 06 67  6f 6f 67 6c 65 03 63 6f   ·······g oogle·co
0040  6d 00 00 01 00 01                                  m·····
```

Lab2:DNS的server是多少

完成

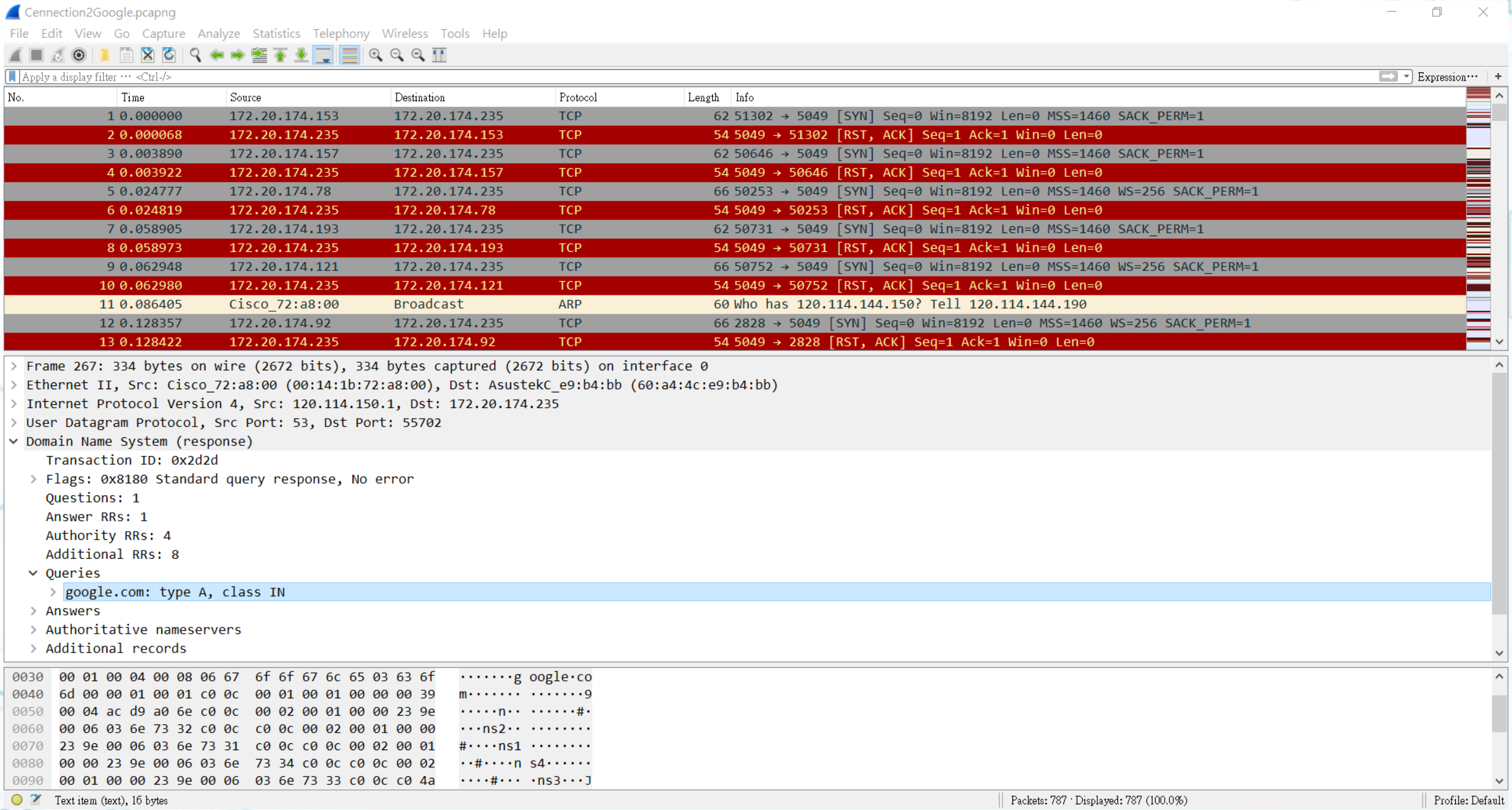


```
> Frame 262: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb), Dst: Cisco_72:a8:00 (00:14:1b:72:a8:
> Internet Protocol Version 4, Src: 172.20.174.235, Dst: 120.114.150.1
> User Datagram Protocol, Src Port: 55702, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x2d2d
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..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
  v Queries
    v google.com: type A, class IN
        Name: google.com
        [Name Length: 10]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 267]
```

DNS Lab3:

GOOGLE的ip是多少？

Lab3:GOOGLE的ip是多少


Cennection2Google.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
Expression···
+

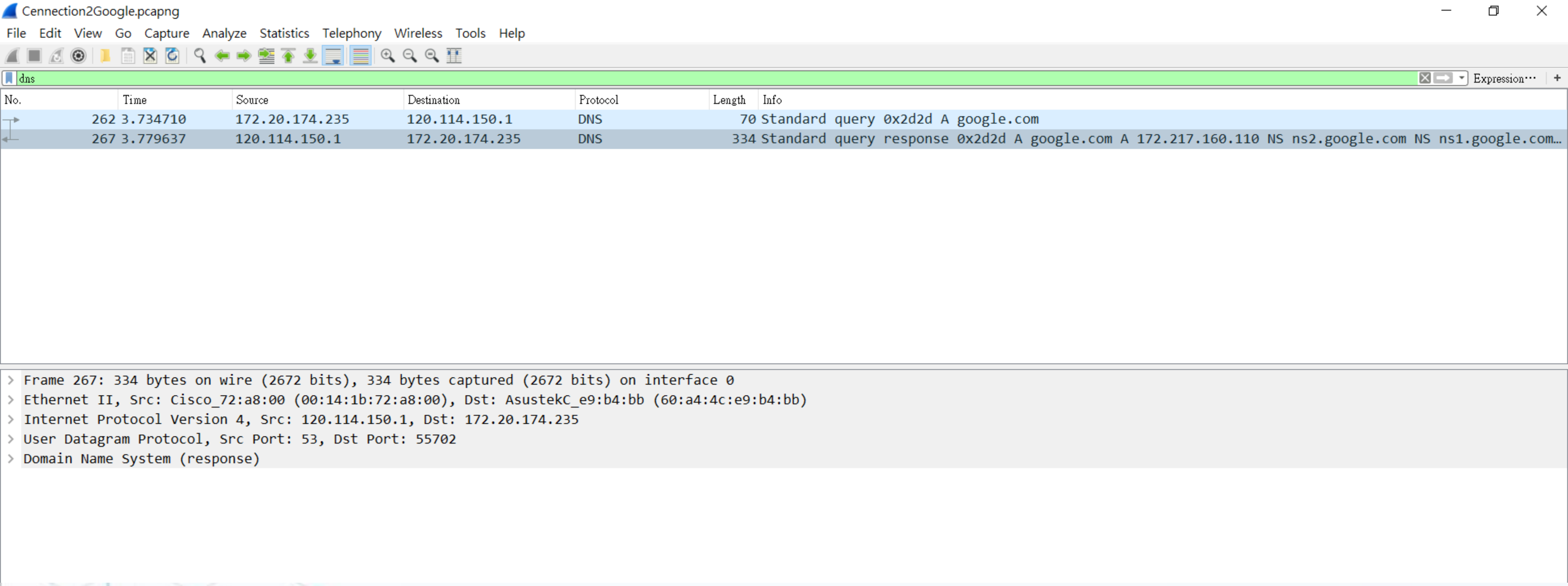
```
No.   Time      Source          Destination     Protocol  Length Info
    1 0.000000  172.20.174.153  172.20.174.235  TCP       62 51302 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
    2 0.000068  172.20.174.235  172.20.174.153  TCP       54 5049 → 51302 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    3 0.003890  172.20.174.157  172.20.174.235  TCP       62 50646 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
    4 0.003922  172.20.174.235  172.20.174.157  TCP       54 5049 → 50646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    5 0.024777  172.20.174.78   172.20.174.235  TCP       66 50253 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    6 0.024819  172.20.174.235  172.20.174.78   TCP       54 5049 → 50253 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    7 0.058905  172.20.174.193  172.20.174.235  TCP       62 50731 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
    8 0.058973  172.20.174.235  172.20.174.193  TCP       54 5049 → 50731 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    9 0.062948  172.20.174.121  172.20.174.235  TCP       66 50752 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   10 0.062980  172.20.174.235  172.20.174.121  TCP       54 5049 → 50752 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   11 0.086405  Cisco_72:a8:00  Broadcast       ARP       60 Who has 120.114.144.150? Tell 120.114.144.190
   12 0.128357  172.20.174.92   172.20.174.235  TCP       66 2828 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   13 0.128422  172.20.174.235  172.20.174.92   TCP       54 5049 → 2828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
> Frame 267: 334 bytes on wire (2672 bits), 334 bytes captured (2672 bits) on interface 0
> Ethernet II, Src: Cisco_72:a8:00 (00:14:1b:72:a8:00), Dst: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb)
> Internet Protocol Version 4, Src: 120.114.150.1, Dst: 172.20.174.235
> User Datagram Protocol, Src Port: 53, Dst Port: 55702
v Domain Name System (response)
    Transaction ID: 0x2d2d
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 8
  v Queries
    > google.com: type A, class IN
  > Answers
  > Authoritative nameservers
  > Additional records
```

```
0030  00 01 00 04 00 08 06 67  6f 6f 67 6c 65 03 63 6f   ·······g oogle·co
0040  6d 00 00 01 00 01 c0 0c  00 01 00 01 00 00 00 39   m······· ·······9
0050  00 04 ac d9 a0 6e c0 0c  00 02 00 01 00 00 23 9e   ·····n·· ······#·
0060  00 06 03 6e 73 32 c0 0c  c0 0c 00 02 00 01 00 00   ···ns2·· ········
0070  23 9e 00 06 03 6e 73 31  c0 0c c0 0c 00 02 00 01   #····ns1 ········
0080  00 00 23 9e 00 06 03 6e  73 34 c0 0c c0 0c 00 02   ··#····n s4······
0090  00 01 00 00 23 9e 00 06  03 6e 73 33 c0 0c c0 4a   ····#··· ·ns3···J
```

Text item (text), 16 bytes | Packets: 787 · Displayed: 787 (100.0%) | Profile: Default

Lab3:GOOGLE的ip是多少

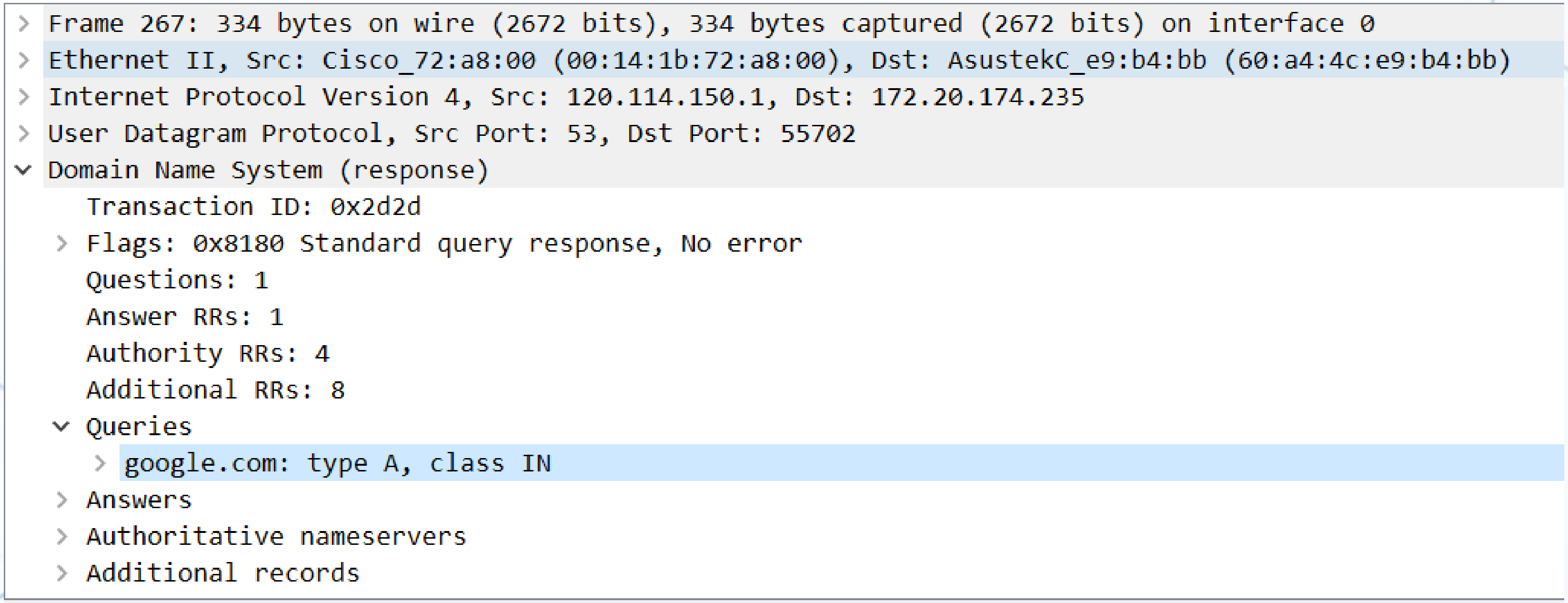

Cennection2Google.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

dns

```
No.      Time       Source           Destination      Protocol   Length  Info
    262 3.734710    172.20.174.235   120.114.150.1    DNS            70  Standard query 0x2d2d A google.com
    267 3.779637    120.114.150.1    172.20.174.235   DNS           334  Standard query response 0x2d2d A google.com A 172.217.160.110 NS ns2.google.com NS ns1.google.com…
```

```
> Frame 267: 334 bytes on wire (2672 bits), 334 bytes captured (2672 bits) on interface 0
> Ethernet II, Src: Cisco_72:a8:00 (00:14:1b:72:a8:00), Dst: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb)
> Internet Protocol Version 4, Src: 120.114.150.1, Dst: 172.20.174.235
> User Datagram Protocol, Src Port: 53, Dst Port: 55702
> Domain Name System (response)
```

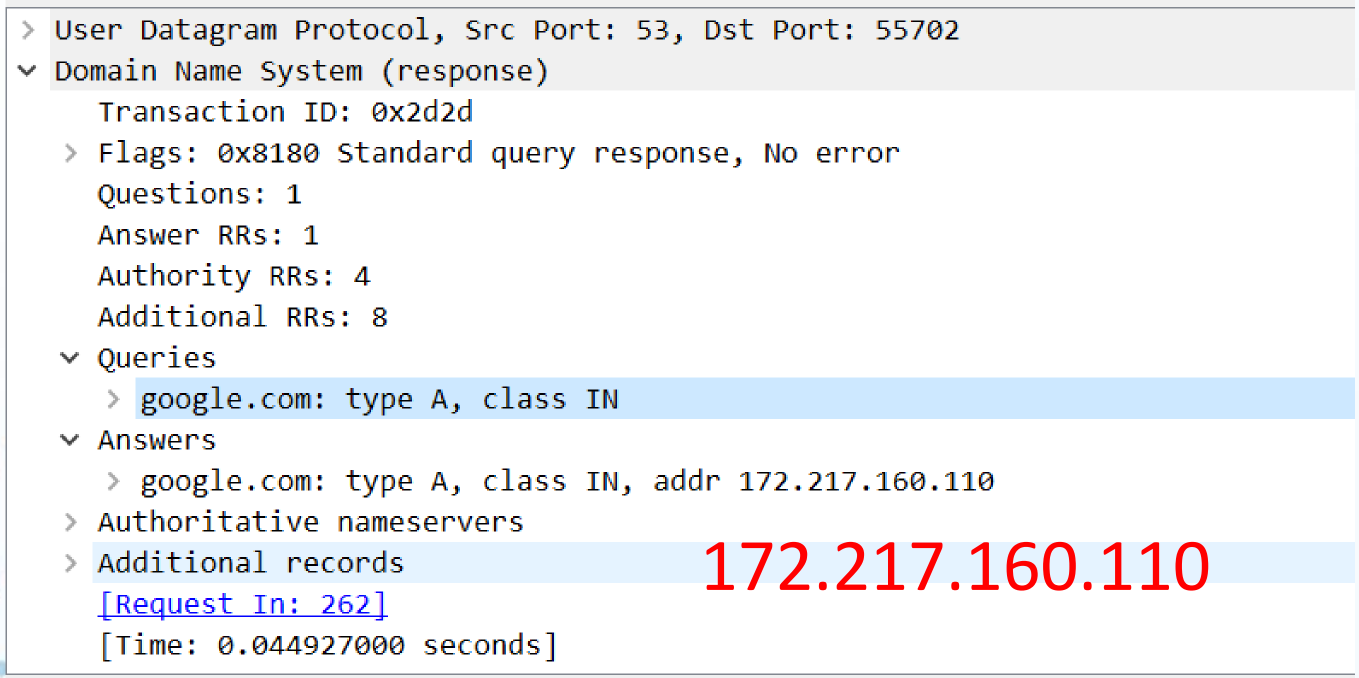
Lab3:GOOGLE的ip是多少



```
> Frame 267: 334 bytes on wire (2672 bits), 334 bytes captured (2672 bits) on interface 0
> Ethernet II, Src: Cisco_72:a8:00 (00:14:1b:72:a8:00), Dst: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb)
> Internet Protocol Version 4, Src: 120.114.150.1, Dst: 172.20.174.235
> User Datagram Protocol, Src Port: 53, Dst Port: 55702
v Domain Name System (response)
    Transaction ID: 0x2d2d
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 8
  v Queries
    > google.com: type A, class IN
  > Answers
  > Authoritative nameservers
  > Additional records
```

Lab3:GOOGLE的ip是多少

完成



```
> User Datagram Protocol, Src Port: 53, Dst Port: 55702
v Domain Name System (response)
    Transaction ID: 0x2d2d
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 8
  v Queries
    > google.com: type A, class IN
  v Answers
    > google.com: type A, class IN, addr 172.217.160.110
  > Authoritative nameservers
  > Additional records
    [Request In: 262]
    [Time: 0.044927000 seconds]
```

172.217.160.110

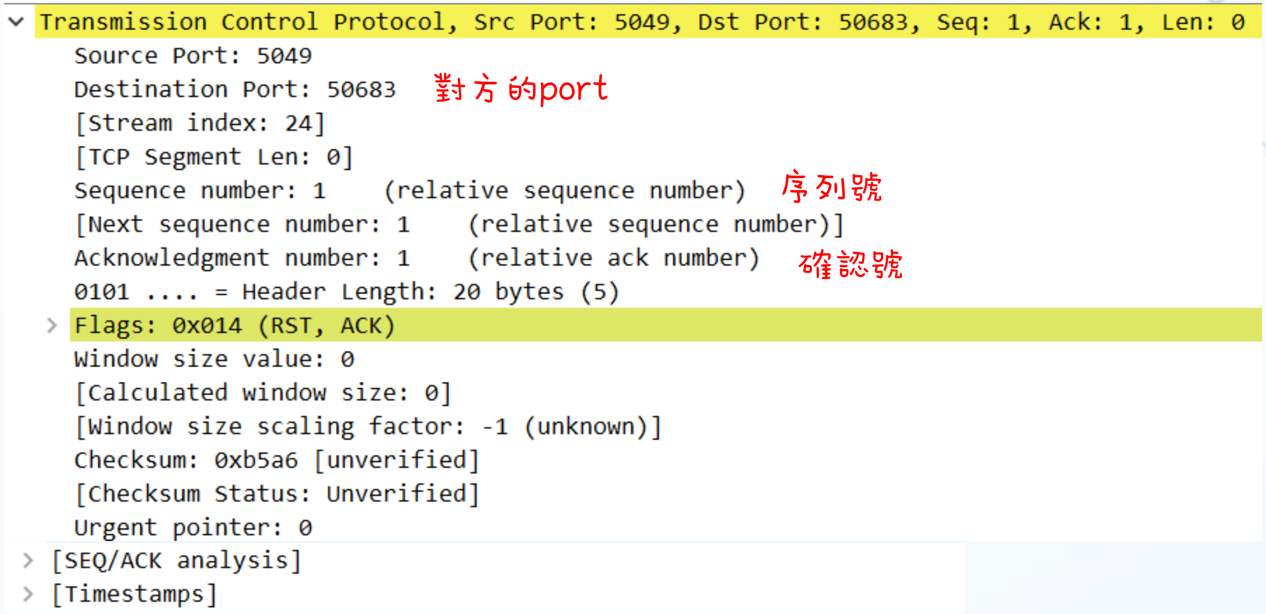
TCP的封包格式

TCP封包格式

<table>
<tr><th>4bit</th><th>6bit</th><th colspan="6">6bit</th><th>16 bit</th></tr>
<tr><td colspan="8">來源端口 Source Port</td><td>目的端口 Destination Port</td></tr>
<tr><td colspan="9">Sequence Number (序列號)</td></tr>
<tr><td colspan="9">Acknowledgment Number(確認號)</td></tr>
<tr><td>Data Offset
(資料偏移量)</td><td>Reserved
(保留)</td><td>U
R
G</td><td>A
C
K</td><td>P
S
H</td><td>R
S
T</td><td>S
Y
N</td><td>F
I
N</td><td>Window(視窗)</td></tr>
<tr><td colspan="8">Checksum(驗檢和)</td><td>Urgent Pointer (緊急指標)</td></tr>
<tr><td colspan="9">Options(選項)+Padding(填充)</td></tr>
<tr><td colspan="9">Data(資料)</td></tr>
</table>

TCP封包

我們來看一下完整的封包吧!



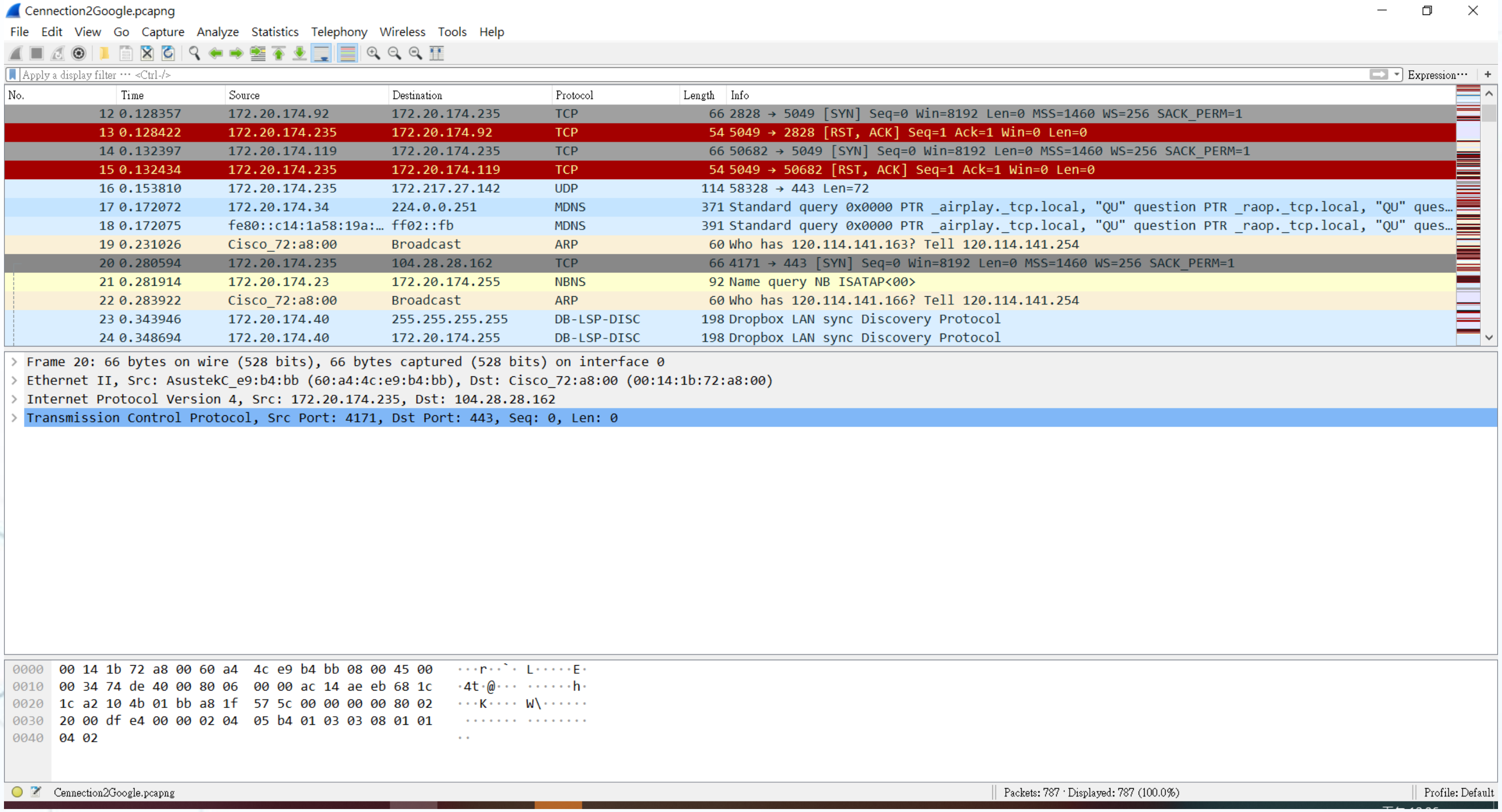
```
v Transmission Control Protocol, Src Port: 5049, Dst Port: 50683, Seq: 1, Ack: 1, Len: 0
    Source Port: 5049
    Destination Port: 50683  對方的port
    [Stream index: 24]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)  序列號
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)  確認號
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x014 (RST, ACK)
    Window size value: 0
    [Calculated window size: 0]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xb5a6 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
```

TCP的封包格式分析

TCP Lab1:

第20個封包的port是什麼

Lab1:找出 20號封包的PORT



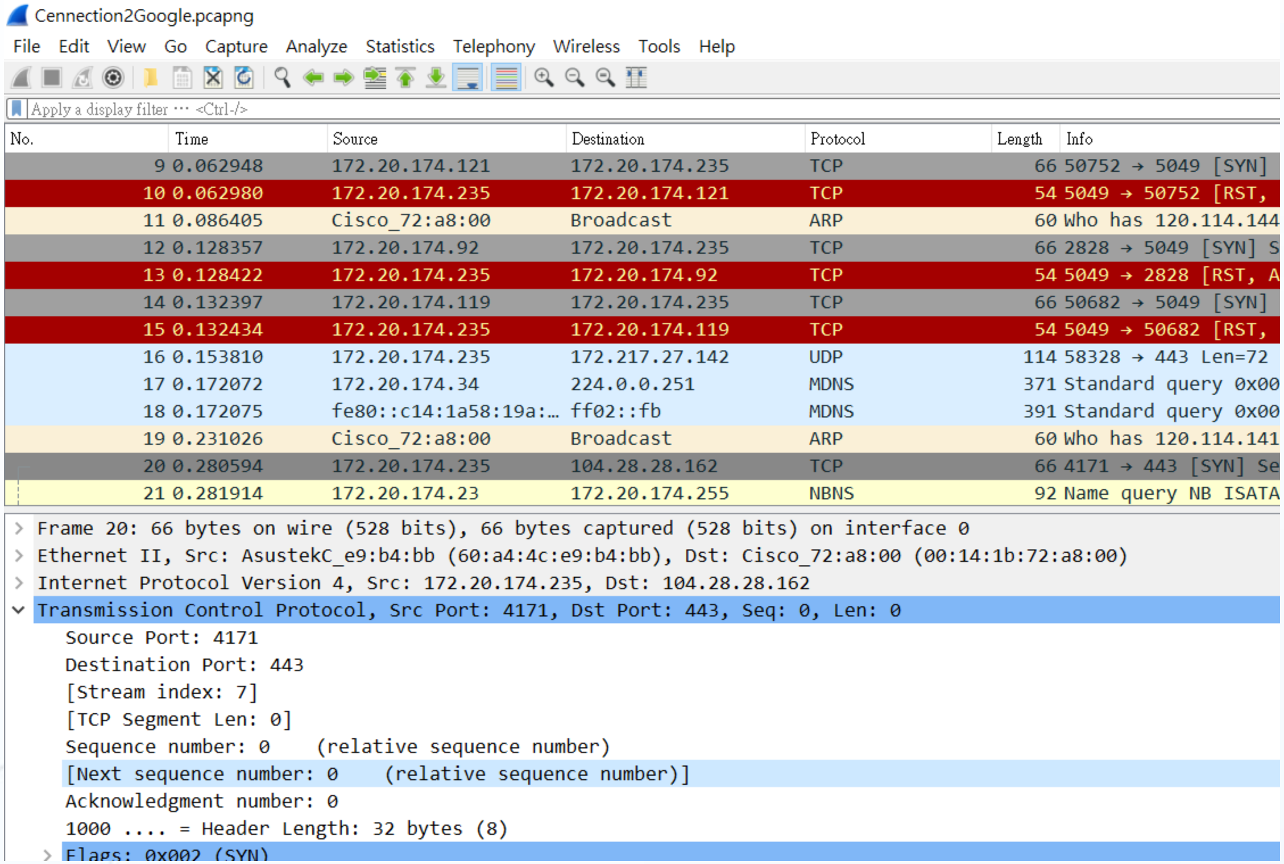
Cennection2Google.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

No.	Time	Source	Destination	Protocol	Length	Info
12	0.128357	172.20.174.92	172.20.174.235	TCP	66	2828 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	0.128422	172.20.174.235	172.20.174.92	TCP	54	5049 → 2828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	0.132397	172.20.174.119	172.20.174.235	TCP	66	50682 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	0.132434	172.20.174.235	172.20.174.119	TCP	54	5049 → 50682 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	0.153810	172.20.174.235	172.217.27.142	UDP	114	58328 → 443 Len=72
17	0.172072	172.20.174.34	224.0.0.251	MDNS	371	Standard query 0x0000 PTR _airplay._tcp.local, "QU" question PTR _raop._tcp.local, "QU" ques…
18	0.172075	fe80::c14:1a58:19a:…	ff02::fb	MDNS	391	Standard query 0x0000 PTR _airplay._tcp.local, "QU" question PTR _raop._tcp.local, "QU" ques…
19	0.231026	Cisco_72:a8:00	Broadcast	ARP	60	Who has 120.114.141.163? Tell 120.114.141.254
20	0.280594	172.20.174.235	104.28.28.162	TCP	66	4171 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
21	0.281914	172.20.174.23	172.20.174.255	NBNS	92	Name query NB ISATAP<00>
22	0.283922	Cisco_72:a8:00	Broadcast	ARP	60	Who has 120.114.141.166? Tell 120.114.141.254
23	0.343946	172.20.174.40	255.255.255.255	DB-LSP-DISC	198	Dropbox LAN sync Discovery Protocol
24	0.348694	172.20.174.40	172.20.174.255	DB-LSP-DISC	198	Dropbox LAN sync Discovery Protocol

```
> Frame 20: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb), Dst: Cisco_72:a8:00 (00:14:1b:72:a8:00)
> Internet Protocol Version 4, Src: 172.20.174.235, Dst: 104.28.28.162
> Transmission Control Protocol, Src Port: 4171, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  00 14 1b 72 a8 00 60 a4  4c e9 b4 bb 08 00 45 00   ···r··`· L·····E·
0010  00 34 74 de 40 00 80 06  00 00 ac 14 ae eb 68 1c   ·4t·@··· ······h·
0020  1c a2 10 4b 01 bb a8 1f  57 5c 00 00 00 00 80 02   ···K···· W\······
0030  20 00 df e4 00 00 02 04  05 b4 01 03 03 08 01 01    ······· ········
0040  04 02                                              ··
```

Lab1:找出 20號封包的PORT



No.	Time	Source	Destination	Protocol	Length	Info
9	0.062948	172.20.174.121	172.20.174.235	TCP	66	50752 → 5049 [SYN]
10	0.062980	172.20.174.235	172.20.174.121	TCP	54	5049 → 50752 [RST,
11	0.086405	Cisco_72:a8:00	Broadcast	ARP	60	Who has 120.114.144
12	0.128357	172.20.174.92	172.20.174.235	TCP	66	2828 → 5049 [SYN] S
13	0.128422	172.20.174.235	172.20.174.92	TCP	54	5049 → 2828 [RST, A
14	0.132397	172.20.174.119	172.20.174.235	TCP	66	50682 → 5049 [SYN]
15	0.132434	172.20.174.235	172.20.174.119	TCP	54	5049 → 50682 [RST,
16	0.153810	172.20.174.235	172.217.27.142	UDP	114	58328 → 443 Len=72
17	0.172072	172.20.174.34	224.0.0.251	MDNS	371	Standard query 0x00
18	0.172075	fe80::c14:1a58:19a:…	ff02::fb	MDNS	391	Standard query 0x00
19	0.231026	Cisco_72:a8:00	Broadcast	ARP	60	Who has 120.114.141
20	0.280594	172.20.174.235	104.28.28.162	TCP	66	4171 → 443 [SYN] Se
21	0.281914	172.20.174.23	172.20.174.255	NBNS	92	Name query NB ISATA

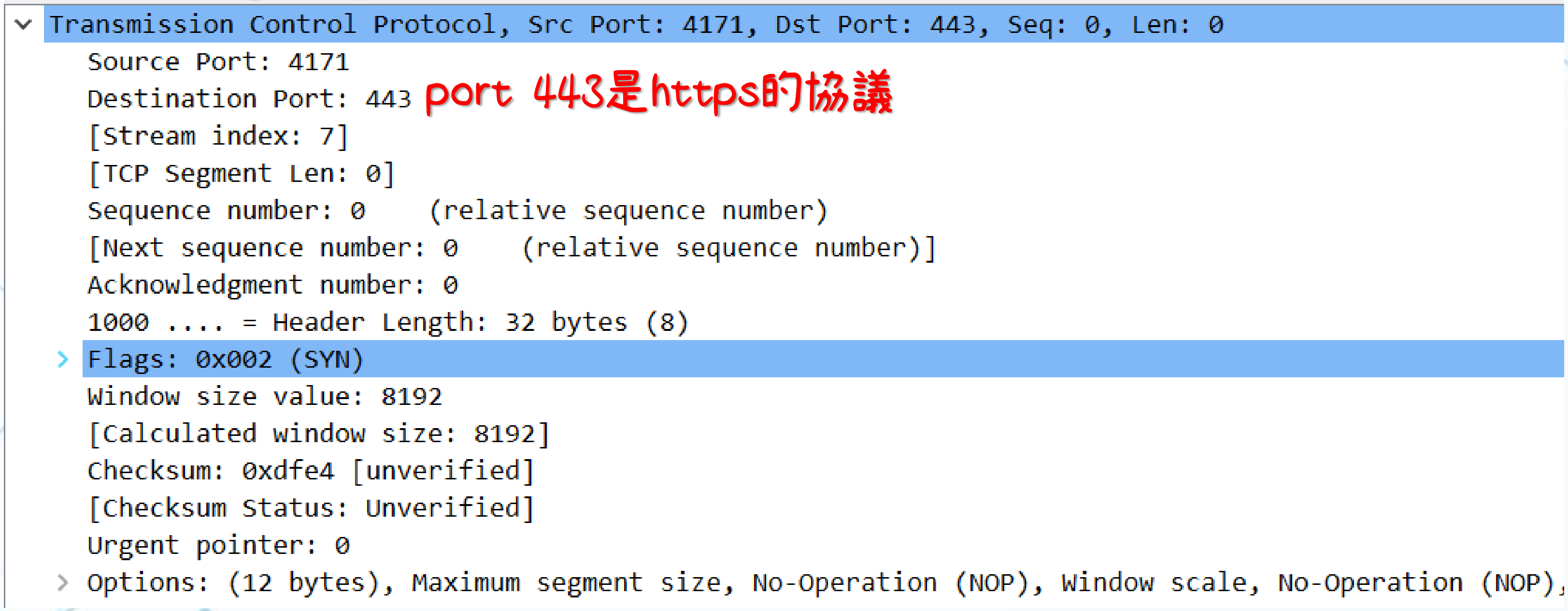
```
> Frame 20: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb), Dst: Cisco_72:a8:00 (00:14:1b:72:a8:00)
> Internet Protocol Version 4, Src: 172.20.174.235, Dst: 104.28.28.162
v Transmission Control Protocol, Src Port: 4171, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 4171
    Destination Port: 443
    [Stream index: 7]
    [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)
```

教育部

新型態資安實務課程計畫

Lab1:找出 20號封包的PORT

完成



```
⌄ Transmission Control Protocol, Src Port: 4171, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 4171
    Destination Port: 443
    [Stream index: 7]
    [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: 8192
    [Calculated window size: 8192]
    Checksum: 0xdfe4 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  › Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP),
```

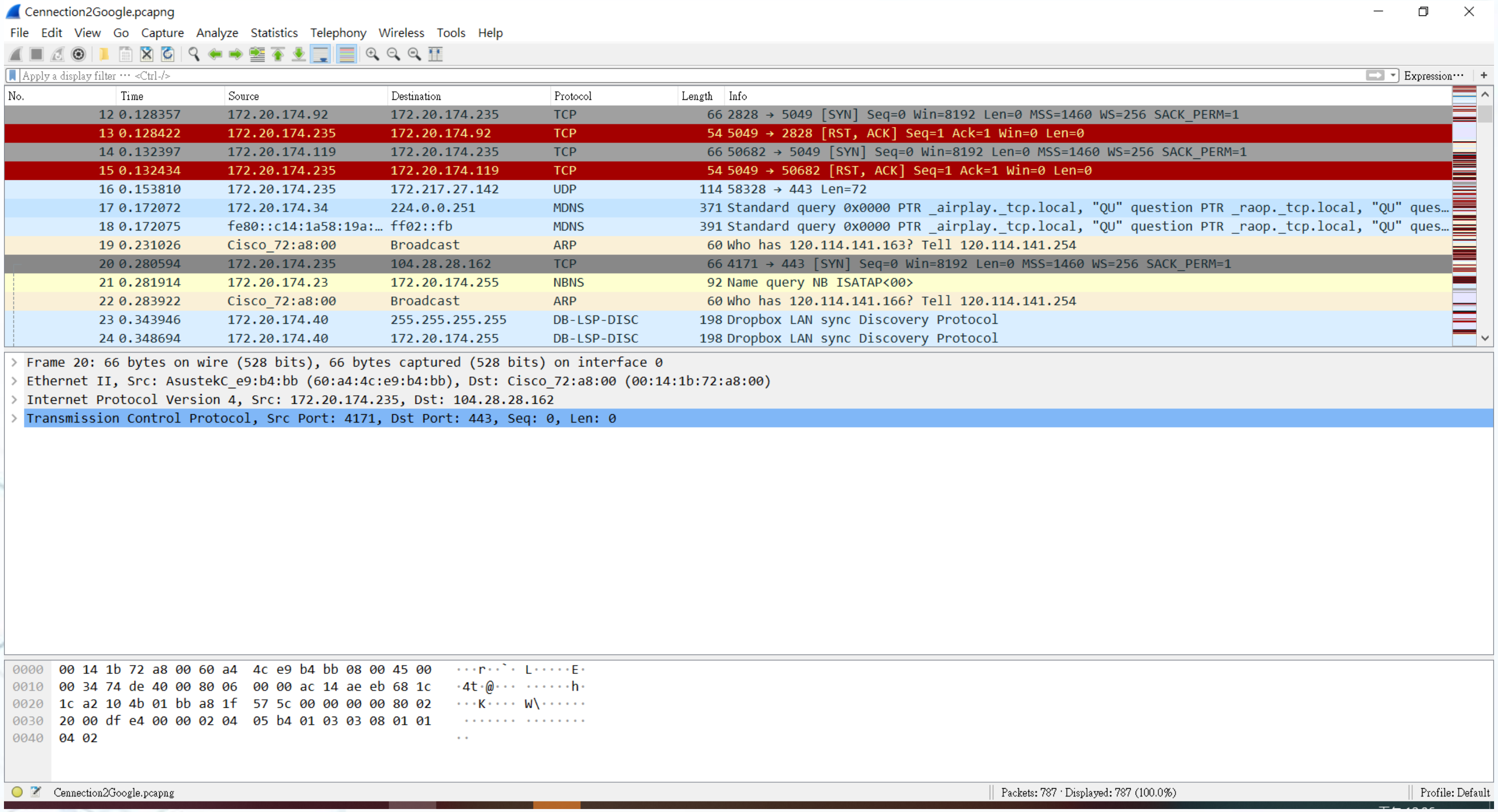
port 443是https的協議

TCP的 三向交握

TCP Lab2:

找出跟20號封包有關的另外兩個封包

Lab2:找出 20號封包三向交握有關的另外兩個封包


Cennection2Google.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

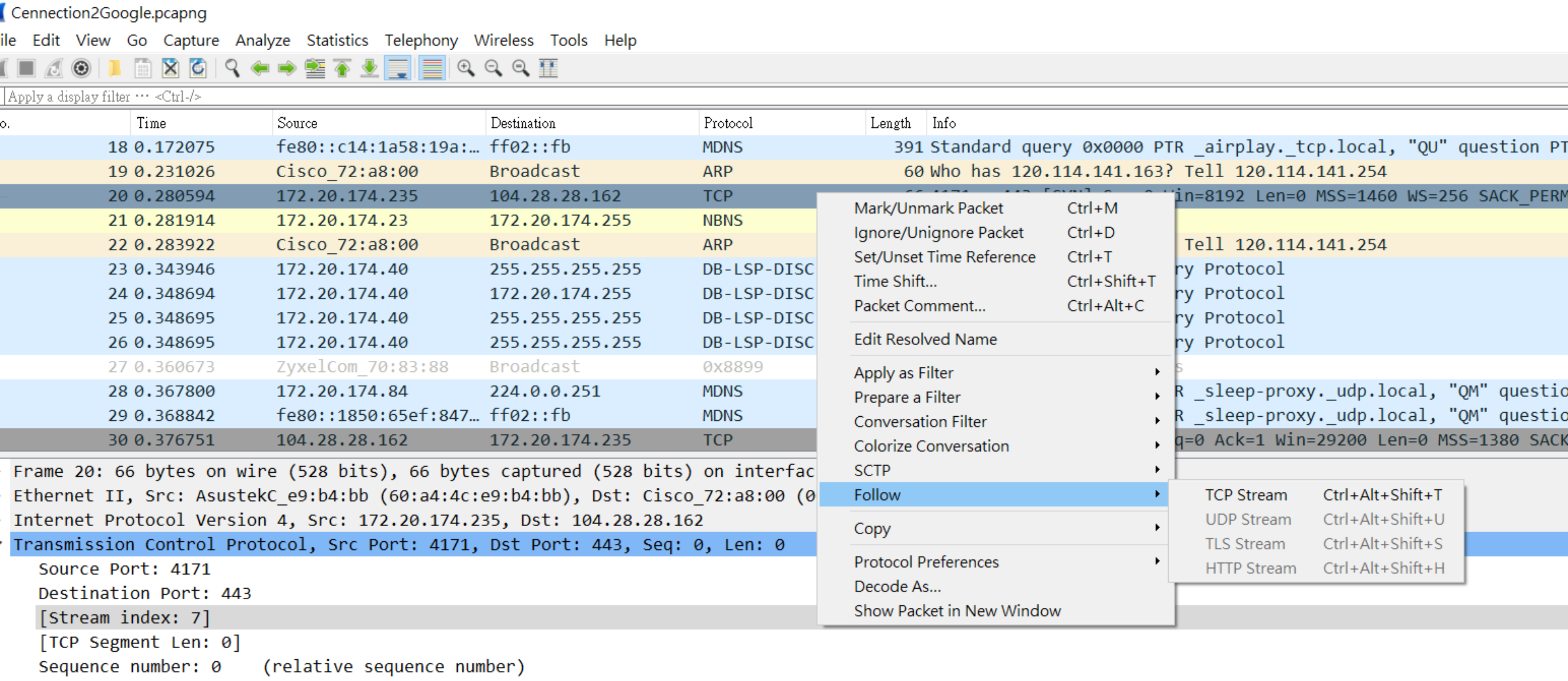
```
No.    Time       Source                 Destination       Protocol     Length Info
    12 0.128357   172.20.174.92          172.20.174.235    TCP              66 2828 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    13 0.128422   172.20.174.235         172.20.174.92     TCP              54 5049 → 2828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    14 0.132397   172.20.174.119         172.20.174.235    TCP              66 50682 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    15 0.132434   172.20.174.235         172.20.174.119    TCP              54 5049 → 50682 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    16 0.153810   172.20.174.235         172.217.27.142    UDP             114 58328 → 443 Len=72
    17 0.172072   172.20.174.34          224.0.0.251       MDNS            371 Standard query 0x0000 PTR _airplay._tcp.local, "QU" question PTR _raop._tcp.local, "QU" ques…
    18 0.172075   fe80::c14:1a58:19a:…   ff02::fb          MDNS            391 Standard query 0x0000 PTR _airplay._tcp.local, "QU" question PTR _raop._tcp.local, "QU" ques…
    19 0.231026   Cisco_72:a8:00         Broadcast         ARP              60 Who has 120.114.141.163? Tell 120.114.141.254
    20 0.280594   172.20.174.235         104.28.28.162     TCP              66 4171 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    21 0.281914   172.20.174.23          172.20.174.255    NBNS             92 Name query NB ISATAP<00>
    22 0.283922   Cisco_72:a8:00         Broadcast         ARP              60 Who has 120.114.141.166? Tell 120.114.141.254
    23 0.343946   172.20.174.40          255.255.255.255   DB-LSP-DISC     198 Dropbox LAN sync Discovery Protocol
    24 0.348694   172.20.174.40          172.20.174.255    DB-LSP-DISC     198 Dropbox LAN sync Discovery Protocol
```

```
> Frame 20: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb), Dst: Cisco_72:a8:00 (00:14:1b:72:a8:00)
> Internet Protocol Version 4, Src: 172.20.174.235, Dst: 104.28.28.162
> Transmission Control Protocol, Src Port: 4171, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  00 14 1b 72 a8 00 60 a4  4c e9 b4 bb 08 00 45 00   ···r··`· L·····E·
0010  00 34 74 de 40 00 80 06  00 00 ac 14 ae eb 68 1c   ·4t·@··· ······h·
0020  1c a2 10 4b 01 bb a8 1f  57 5c 00 00 00 00 80 02   ···K···· W\······
0030  20 00 df e4 00 00 02 04  05 b4 01 03 03 08 01 01    ······· ········
0040  04 02                                              ··
```

Cennection2Google.pcapng | Packets: 787 · Displayed: 787 (100.0%) | Profile: Default

Lab2:找出 20號封包三向交握有關的另外兩個封包

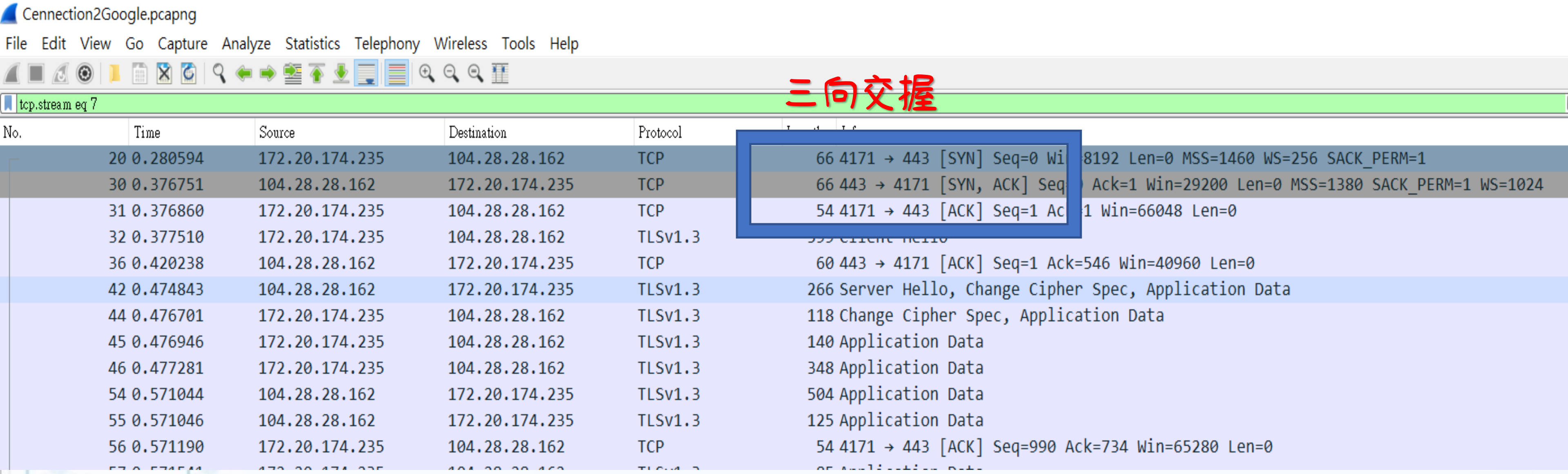

Cennection2Google.pcapng
ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H

```
o.        Time      Source                 Destination      Protocol       Length Info
       18 0.172075  fe80::c14:1a58:19a:…   ff02::fb         MDNS              391 Standard query 0x0000 PTR _airplay._tcp.local, "QU" question PT
       19 0.231026  Cisco_72:a8:00         Broadcast        ARP                60 Who has 120.114.141.163? Tell 120.114.141.254
       20 0.280594  172.20.174.235         104.28.28.162    TCP                                  in=8192 Len=0 MSS=1460 WS=256 SACK_PERM
       21 0.281914  172.20.174.23          172.20.174.255   NBNS
       22 0.283922  Cisco_72:a8:00         Broadcast        ARP                                   Tell 120.114.141.254
       23 0.343946  172.20.174.40          255.255.255.255  DB-LSP-DISC                          ry Protocol
       24 0.348694  172.20.174.40          172.20.174.255   DB-LSP-DISC                          ry Protocol
       25 0.348695  172.20.174.40          255.255.255.255  DB-LSP-DISC                          ry Protocol
       26 0.348695  172.20.174.40          255.255.255.255  DB-LSP-DISC                          ry Protocol
       27 0.360673  ZyxelCom_70:83:88      Broadcast        0x8899                               s
       28 0.367800  172.20.174.84          224.0.0.251      MDNS                                 R _sleep-proxy._udp.local, "QM" questio
       29 0.368842  fe80::1850:65ef:847…   ff02::fb         MDNS                                 R _sleep-proxy._udp.local, "QM" questio
       30 0.376751  104.28.28.162          172.20.174.235   TCP                                  q=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK

 Frame 20: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interfac
 Ethernet II, Src: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb), Dst: Cisco_72:a8:00 (0
 Internet Protocol Version 4, Src: 172.20.174.235, Dst: 104.28.28.162
 Transmission Control Protocol, Src Port: 4171, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 4171
    Destination Port: 443
    [Stream index: 7]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
```

Lab2:找出 20號封包三向交握有關的另外兩個封包

完成



Cennection2Google.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

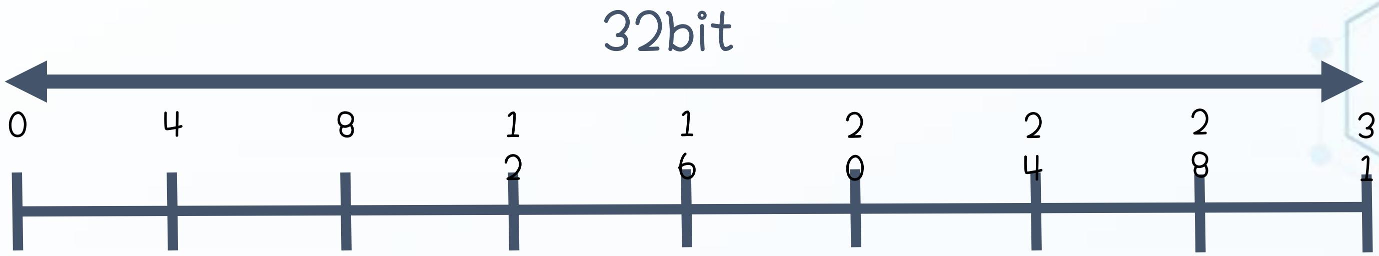
三向交握

```
tcp.stream eq 7

No.        Time       Source            Destination      Protocol   Length Info
        20 0.280594   172.20.174.235    104.28.28.162    TCP          66 4171 → 443 [SYN] Seq=0 Wi 8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
        30 0.376751   104.28.28.162     172.20.174.235   TCP          66 443 → 4171 [SYN, ACK] Seq  Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=1024
        31 0.376860   172.20.174.235    104.28.28.162    TCP          54 4171 → 443 [ACK] Seq=1 Ac 1 Win=66048 Len=0
        32 0.377510   172.20.174.235    104.28.28.162    TLSv1.3     595 Client Hello
        36 0.420238   104.28.28.162     172.20.174.235   TCP          60 443 → 4171 [ACK] Seq=1 Ack=546 Win=40960 Len=0
        42 0.474843   104.28.28.162     172.20.174.235   TLSv1.3     266 Server Hello, Change Cipher Spec, Application Data
        44 0.476701   172.20.174.235    104.28.28.162    TLSv1.3     118 Change Cipher Spec, Application Data
        45 0.476946   172.20.174.235    104.28.28.162    TLSv1.3     140 Application Data
        46 0.477281   172.20.174.235    104.28.28.162    TLSv1.3     348 Application Data
        54 0.571044   104.28.28.162     172.20.174.235   TLSv1.3     504 Application Data
        55 0.571046   104.28.28.162     172.20.174.235   TLSv1.3     125 Application Data
        56 0.571190   172.20.174.235    104.28.28.162    TCP          54 4171 → 443 [ACK] Seq=990 Ack=734 Win=65280 Len=0
        57 0.571541   172.20.174.235    104.28.28.162    TLSv1.3      85 Application Data
```

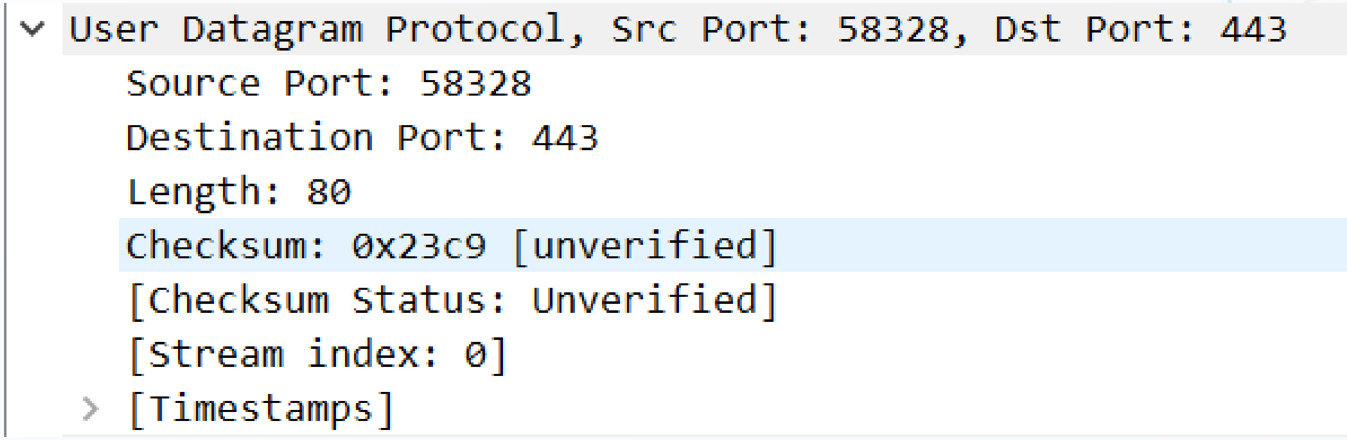
UCP的封包格式

UDP封包格式



來源端口 Source Port	目的端口 Destination Port
長度 Lehgth	校驗和 Checksurn
資料 Data	

UDP封包



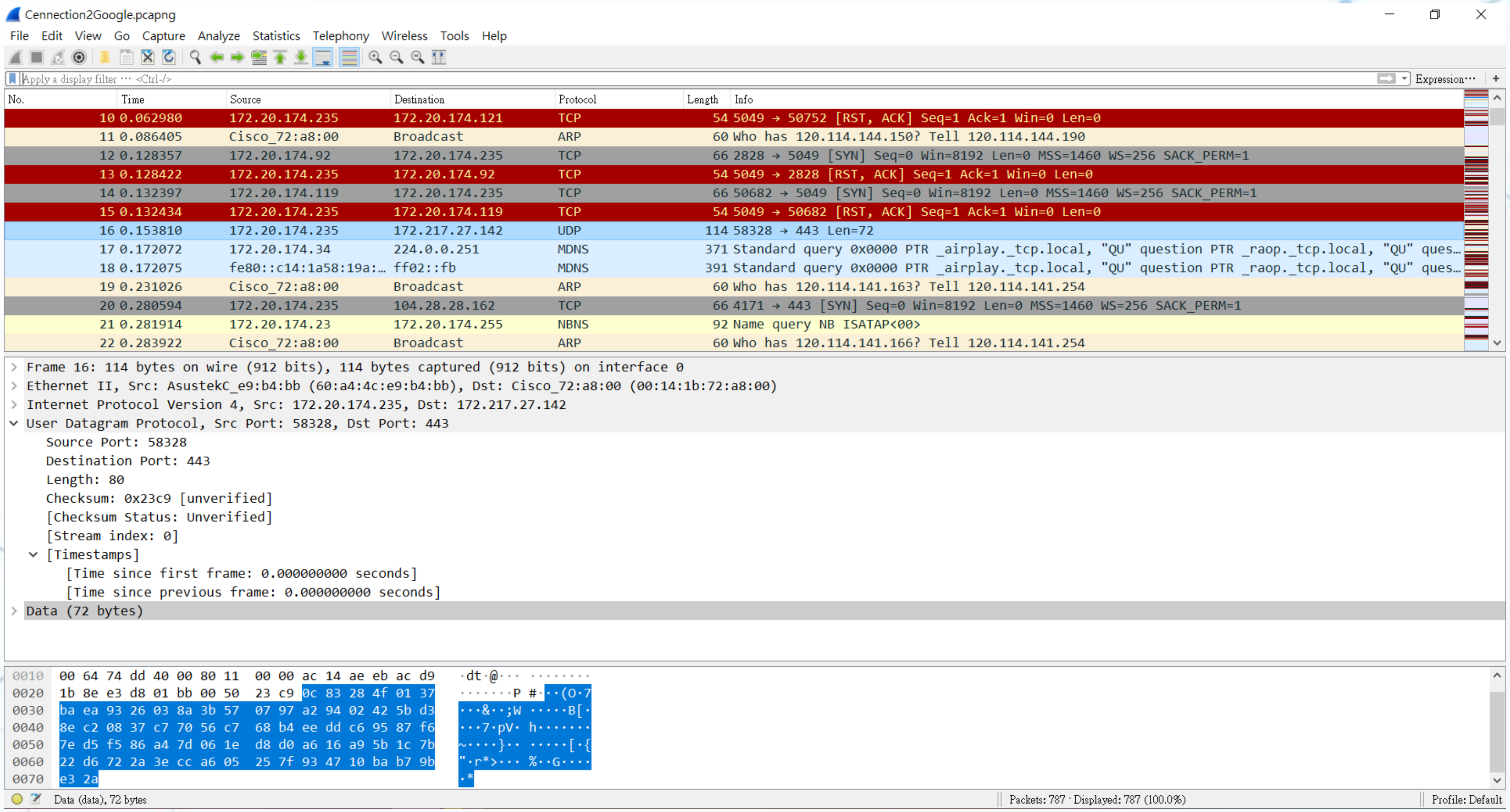
```
∨ User Datagram Protocol, Src Port: 58328, Dst Port: 443
      Source Port: 58328
      Destination Port: 443
      Length: 80
      Checksum: 0x23c9 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 0]
    > [Timestamps]
```

UCP的封包格式分析

UDP Lab1:

第16個封包的Destination Port是多少？

UDP Lab1:第16個封包的udp Destination Port是多少


Cennection2Google.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
Expression···
+

```
No.   Time      Source                Destination     Protocol Length Info
   10 0.062980  172.20.174.235        172.20.174.121  TCP        54 5049 → 50752 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   11 0.086405  Cisco_72:a8:00        Broadcast       ARP        60 Who has 120.114.144.150? Tell 120.114.144.190
   12 0.128357  172.20.174.92         172.20.174.235  TCP        66 2828 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   13 0.128422  172.20.174.235        172.20.174.92   TCP        54 5049 → 2828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   14 0.132397  172.20.174.119        172.20.174.235  TCP        66 50682 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   15 0.132434  172.20.174.235        172.20.174.119  TCP        54 5049 → 50682 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   16 0.153810  172.20.174.235        172.217.27.142  UDP       114 58328 → 443 Len=72
   17 0.172072  172.20.174.34         224.0.0.251     MDNS      371 Standard query 0x0000 PTR _airplay._tcp.local, "QU" question PTR _raop._tcp.local, "QU" ques…
   18 0.172075  fe80::c14:1a58:19a:…  ff02::fb        MDNS      391 Standard query 0x0000 PTR _airplay._tcp.local, "QU" question PTR _raop._tcp.local, "QU" ques…
   19 0.231026  Cisco_72:a8:00        Broadcast       ARP        60 Who has 120.114.141.163? Tell 120.114.141.254
   20 0.280594  172.20.174.235        104.28.28.162   TCP        66 4171 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   21 0.281914  172.20.174.23         172.20.174.255  NBNS       92 Name query NB ISATAP<00>
   22 0.283922  Cisco_72:a8:00        Broadcast       ARP        60 Who has 120.114.141.166? Tell 120.114.141.254
```

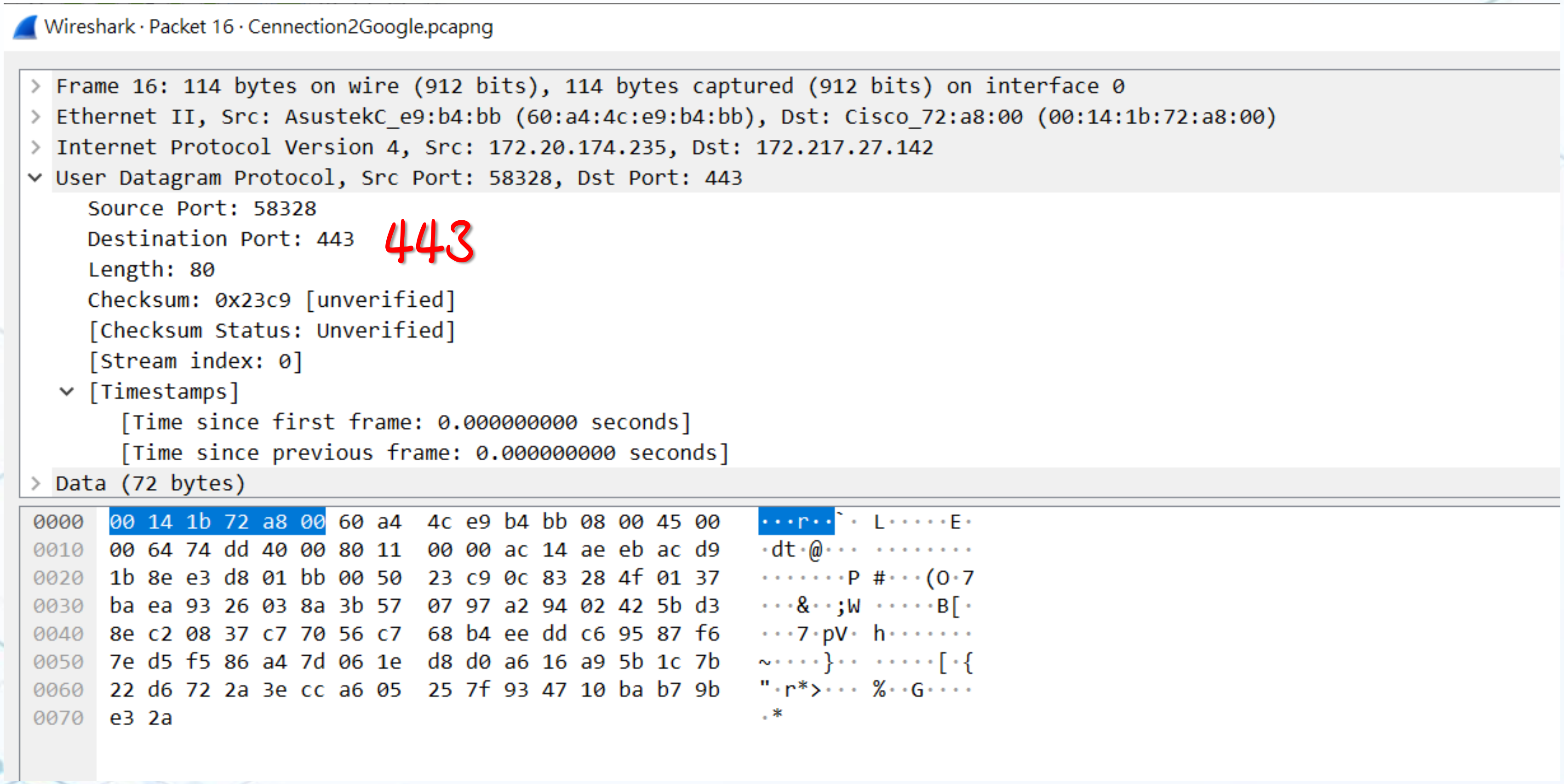
```
> Frame 16: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
> Ethernet II, Src: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb), Dst: Cisco_72:a8:00 (00:14:1b:72:a8:00)
> Internet Protocol Version 4, Src: 172.20.174.235, Dst: 172.217.27.142
v User Datagram Protocol, Src Port: 58328, Dst Port: 443
    Source Port: 58328
    Destination Port: 443
    Length: 80
    Checksum: 0x23c9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  v [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
> Data (72 bytes)
```

```
0010  00 64 74 dd 40 00 80 11  00 00 ac 14 ae eb ac d9   ·dt·@···  ········
0020  1b 8e e3 d8 01 bb 00 50  23 c9 0c 83 28 4f 01 37   ·······P  #···(O·7
0030  ba ea 93 26 03 8a 3b 57  07 97 a2 94 02 42 5b d3   ···&··;W  ·····B[·
0040  8e c2 08 37 c7 70 56 c7  68 b4 ee dd c6 95 87 f6   ···7·pV·  h·······
0050  7e d5 f5 86 a4 7d 06 1e  d8 d0 a6 16 a9 5b 1c 7b   ~····}··  ·····[·{
0060  22 d6 72 2a 3e cc a6 05  25 7f 93 47 10 ba b7 9b   "·r*>···  %··G····
0070  e3 2a                                              ·*
```

Data (data), 72 bytes | Packets: 787 · Displayed: 787 (100.0%) | Profile: Default

UDP Lab1:第16個封包的udp Destination Port是多少

完成



Wireshark · Packet 16 · Cennection2Google.pcapng

```
> Frame 16: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
> Ethernet II, Src: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb), Dst: Cisco_72:a8:00 (00:14:1b:72:a8:00)
> Internet Protocol Version 4, Src: 172.20.174.235, Dst: 172.217.27.142
v User Datagram Protocol, Src Port: 58328, Dst Port: 443
    Source Port: 58328
    Destination Port: 443
    Length: 80
    Checksum: 0x23c9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  v [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
> Data (72 bytes)
```

443

```
0000  00 14 1b 72 a8 00 60 a4  4c e9 b4 bb 08 00 45 00   ···r··`· L·····E·
0010  00 64 74 dd 40 00 80 11  00 00 ac 14 ae eb ac d9   ·dt·@··· ········
0020  1b 8e e3 d8 01 bb 00 50  23 c9 0c 83 28 4f 01 37   ·······P #···(O·7
0030  ba ea 93 26 03 8a 3b 57  07 97 a2 94 02 42 5b d3   ···&··;W ·····B[·
0040  8e c2 08 37 c7 70 56 c7  68 b4 ee dd c6 95 87 f6   ···7·pV· h·······
0050  7e d5 f5 86 a4 7d 06 1e  d8 d0 a6 16 a9 5b 1c 7b   ~····}·· ·····[·{
0060  22 d6 72 2a 3e cc a6 05  25 7f 93 47 10 ba b7 9b   "·r*>··· %··G····
0070  e3 2a                                              ·*
```

IP的封包格式

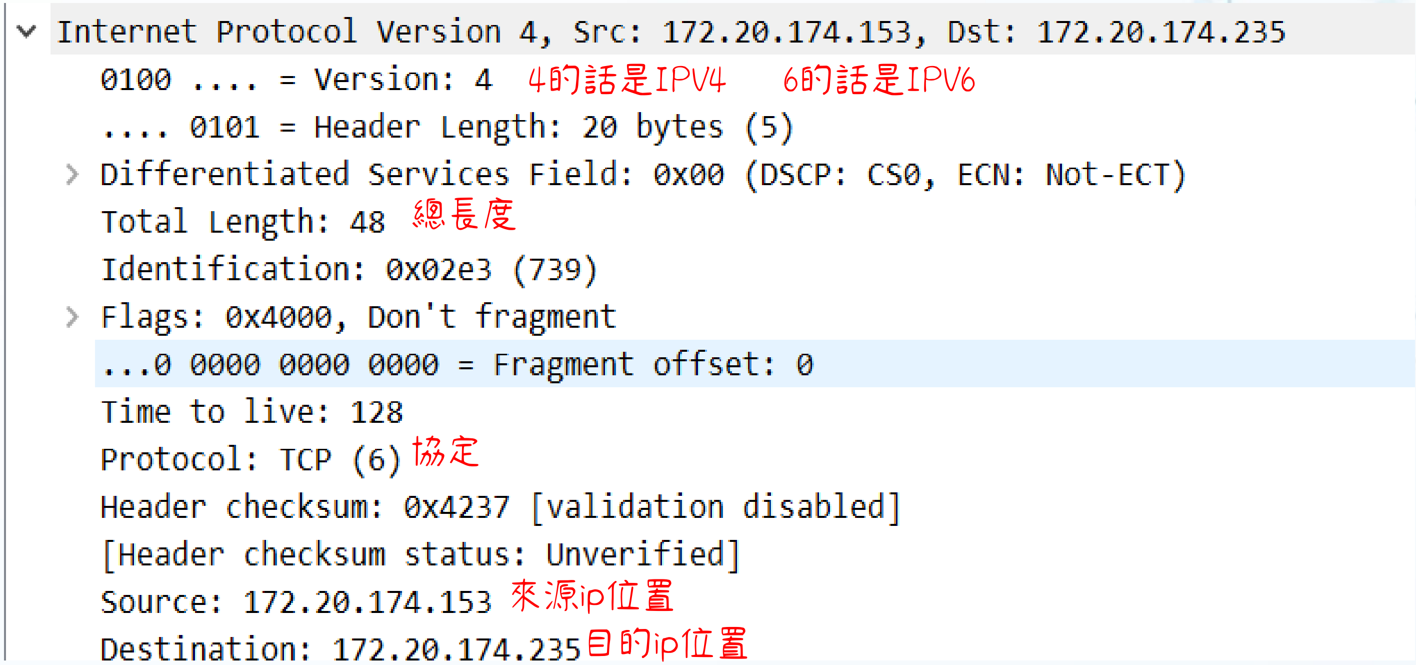
IP封包格式

32bit

8bit 8bit 8bit 8bit

<table>
<tr><td>版本(4)</td><td>表頭長(4)</td><td>服務類型(8)</td><td colspan="2">總長度(16)</td></tr>
<tr><td colspan="3">識別字(16)</td><td>旗標(3)</td><td>分段位移植(13)</td></tr>
<tr><td colspan="2">存活時間(8)</td><td>協定(8)</td><td colspan="2">表頭檢查碼(16)</td></tr>
<tr><td colspan="5">來源ip位置</td></tr>
<tr><td colspan="5">目的ip位置</td></tr>
<tr><td colspan="4">選項(變動長度)</td><td>補足長度(0~24)</td></tr>
<tr><td colspan="5">資料</td></tr>
</table>

IP封包



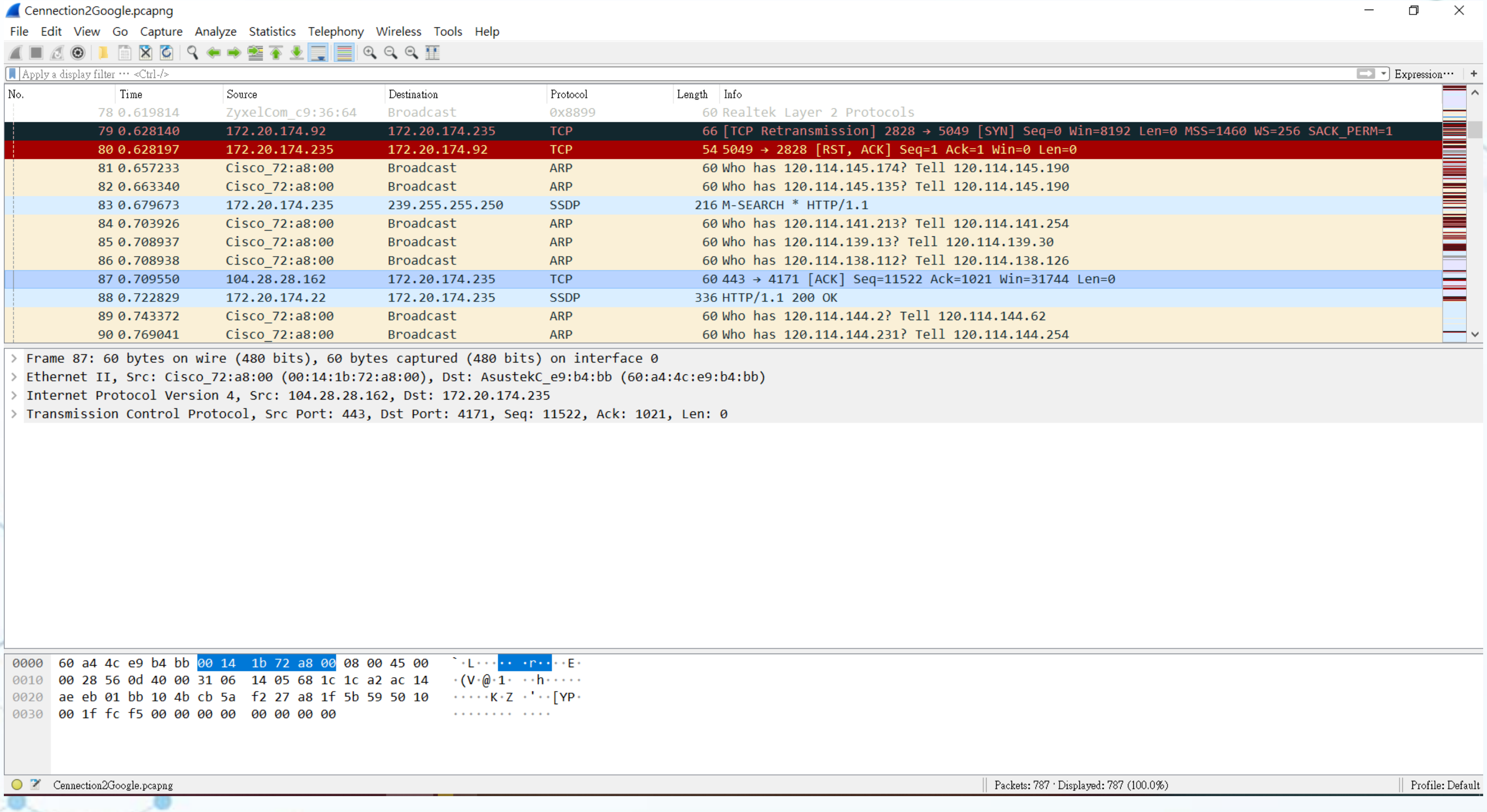
```
⌄ Internet Protocol Version 4, Src: 172.20.174.153, Dst: 172.20.174.235
    0100 .... = Version: 4  4的話是IPV4    6的話是IPV6
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48 總長度
    Identification: 0x02e3 (739)
  > Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6) 協定
    Header checksum: 0x4237 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.20.174.153 來源ip位置
    Destination: 172.20.174.235 目的ip位置
```

iP的封包格式分析

IP Lab1:

第87個封包的IP裡面有一個 Time to live 後面的數字是多少?

Lab1:第87個封包的IP裡面有一個 Time to live 後面的數字是多少?



Cennection2Google.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

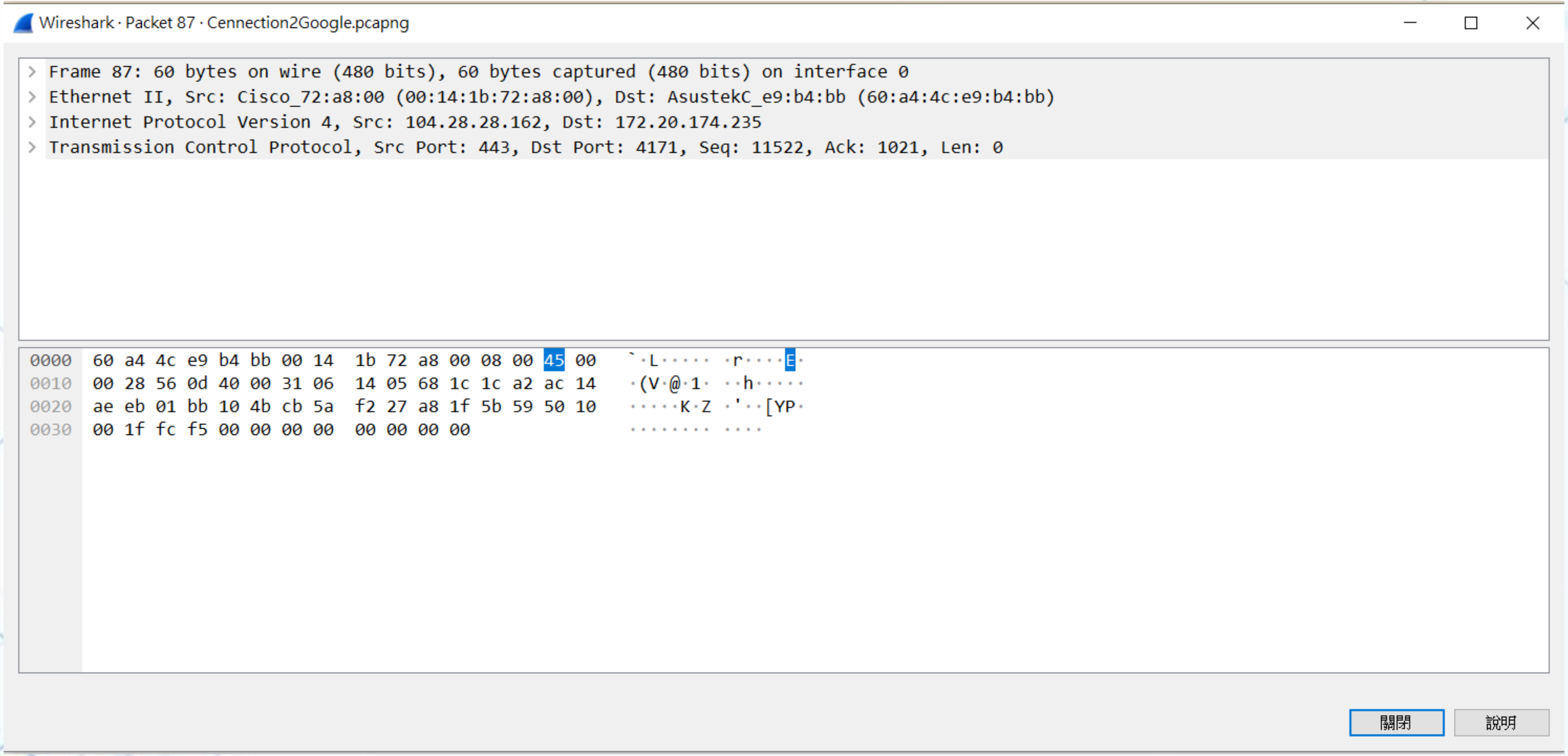
```
No.   Time      Source             Destination       Protocol  Length Info
   78 0.619814  ZyxelCom_c9:36:64  Broadcast         0x8899        60 Realtek Layer 2 Protocols
   79 0.628140  172.20.174.92      172.20.174.235    TCP           66 [TCP Retransmission] 2828 → 5049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   80 0.628197  172.20.174.235     172.20.174.92     TCP           54 5049 → 2828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   81 0.657233  Cisco_72:a8:00     Broadcast         ARP           60 Who has 120.114.145.174? Tell 120.114.145.190
   82 0.663340  Cisco_72:a8:00     Broadcast         ARP           60 Who has 120.114.145.135? Tell 120.114.145.190
   83 0.679673  172.20.174.235     239.255.255.250   SSDP         216 M-SEARCH * HTTP/1.1
   84 0.703926  Cisco_72:a8:00     Broadcast         ARP           60 Who has 120.114.141.213? Tell 120.114.141.254
   85 0.708937  Cisco_72:a8:00     Broadcast         ARP           60 Who has 120.114.139.13? Tell 120.114.139.30
   86 0.708938  Cisco_72:a8:00     Broadcast         ARP           60 Who has 120.114.138.112? Tell 120.114.138.126
   87 0.709550  104.28.28.162      172.20.174.235    TCP           60 443 → 4171 [ACK] Seq=11522 Ack=1021 Win=31744 Len=0
   88 0.722829  172.20.174.22      172.20.174.235    SSDP         336 HTTP/1.1 200 OK
   89 0.743372  Cisco_72:a8:00     Broadcast         ARP           60 Who has 120.114.144.2? Tell 120.114.144.62
   90 0.769041  Cisco_72:a8:00     Broadcast         ARP           60 Who has 120.114.144.231? Tell 120.114.144.254
```

```
> Frame 87: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Cisco_72:a8:00 (00:14:1b:72:a8:00), Dst: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb)
> Internet Protocol Version 4, Src: 104.28.28.162, Dst: 172.20.174.235
> Transmission Control Protocol, Src Port: 443, Dst Port: 4171, Seq: 11522, Ack: 1021, Len: 0
```

```
0000  60 a4 4c e9 b4 bb 00 14  1b 72 a8 00 08 00 45 00   `·L·····  ·r····E·
0010  00 28 56 0d 40 00 31 06  14 05 68 1c 1c a2 ac 14   ·(V·@·1·  ··h·····
0020  ae eb 01 bb 10 4b cb 5a  f2 27 a8 1f 5b 59 50 10   ·····K·Z  ·'··[YP·
0030  00 1f fc f5 00 00 00 00  00 00 00 00               ········  ····
```

Cennection2Google.pcapng   Packets: 787 · Displayed: 787 (100.0%)   Profile: Default

Lab1：第87個封包的IP裡面有一個 Time to live 後面的數字是多少?

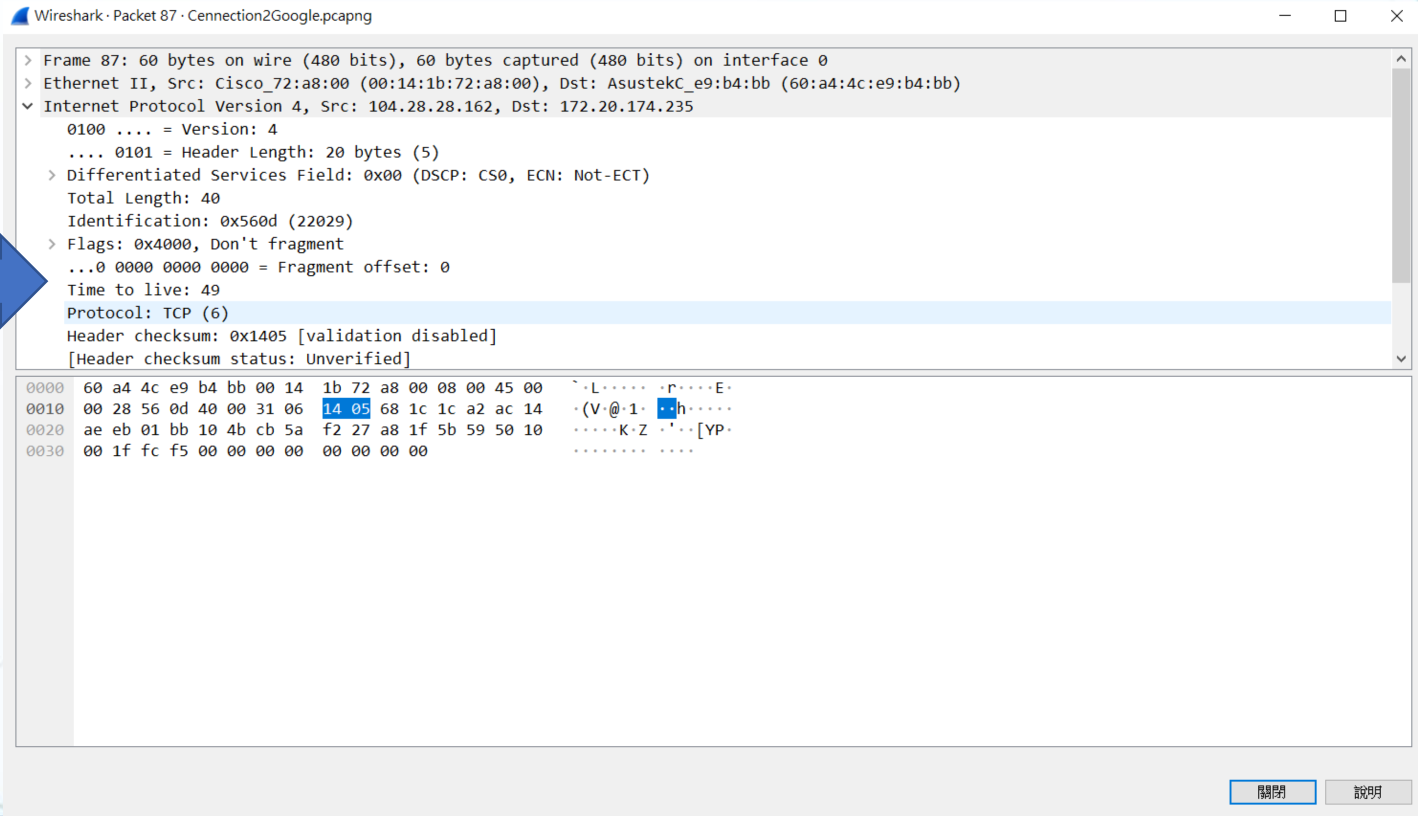


```
> Frame 87: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Cisco_72:a8:00 (00:14:1b:72:a8:00), Dst: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb)
> Internet Protocol Version 4, Src: 104.28.28.162, Dst: 172.20.174.235
> Transmission Control Protocol, Src Port: 443, Dst Port: 4171, Seq: 11522, Ack: 1021, Len: 0

0000  60 a4 4c e9 b4 bb 00 14  1b 72 a8 00 08 00 45 00   `·L····· ·r····E·
0010  00 28 56 0d 40 00 31 06  14 05 68 1c 1c a2 ac 14   ·(V·@·1· ··h·····
0020  ae eb 01 bb 10 4b cb 5a  f2 27 a8 1f 5b 59 50 10   ·····K·Z ·'··[YP·
0030  00 1f fc f5 00 00 00 00  00 00 00 00               ········ ····
```

Lab1：第87個封包的IP裡面有一個 Time to live 後面的數字是多少?

完成



Wireshark · Packet 87 · Connection2Google.pcapng

```
> Frame 87: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Cisco_72:a8:00 (00:14:1b:72:a8:00), Dst: AsustekC_e9:b4:bb (60:a4:4c:e9:b4:bb)
v Internet Protocol Version 4, Src: 104.28.28.162, Dst: 172.20.174.235
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x560d (22029)
  > Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 49
    Protocol: TCP (6)
    Header checksum: 0x1405 [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  60 a4 4c e9 b4 bb 00 14  1b 72 a8 00 08 00 45 00   `·L·····  ·r····E·
0010  00 28 56 0d 40 00 31 06  14 05 68 1c 1c a2 ac 14   ·(V·@·1·  ··h·····
0020  ae eb 01 bb 10 4b cb 5a  f2 27 a8 1f 5b 59 50 10   ·····K·Z  ·'··[YP·
0030  00 1f fc f5 00 00 00 00  00 00 00 00               ········  ····
```

Time to live(存活時間)

當封包每經過一個路由器，
存活次數就減一，當存活次數為0，
就不會繼續轉發這個封包

更多詳閱
http://www.tsnien.idv.tw/Network_WebBook/chap13/13-3%20IP%20%E9%80%9A%E8%A8%8A%E5%8D%94%E5%AE%9A.html