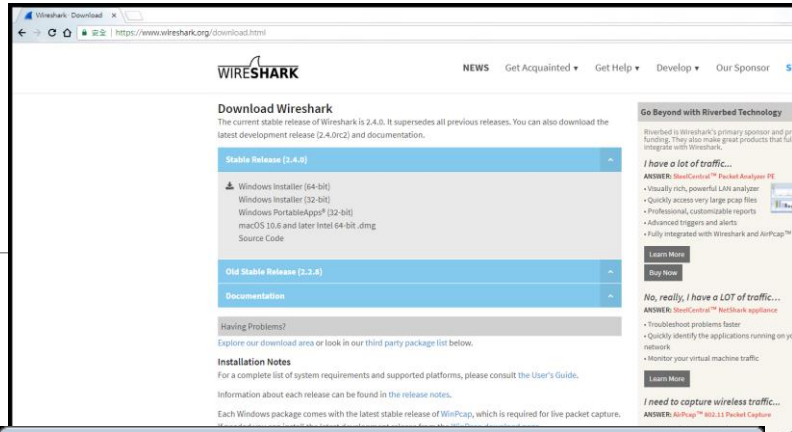
擷取封包實作

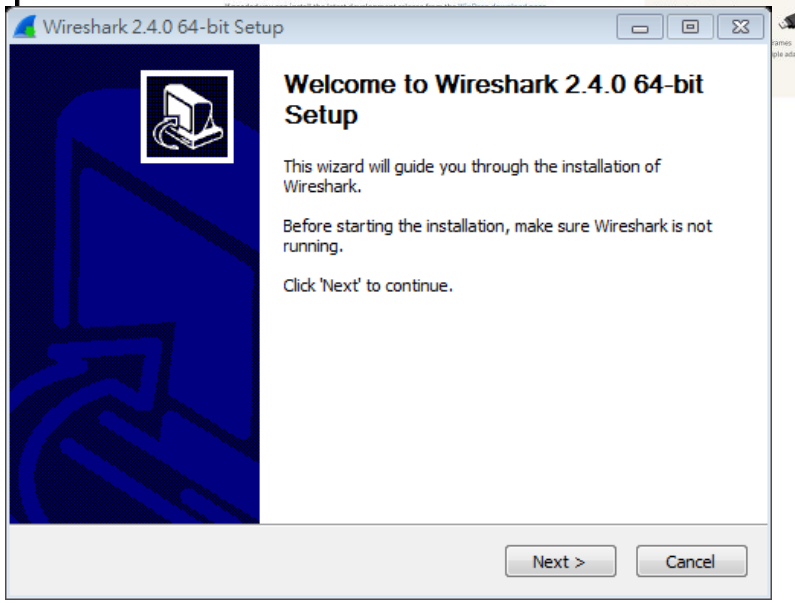
Wireshark

1.到官網(http://www.wireshark.org/)下載符合自己作業系統的軟體版本

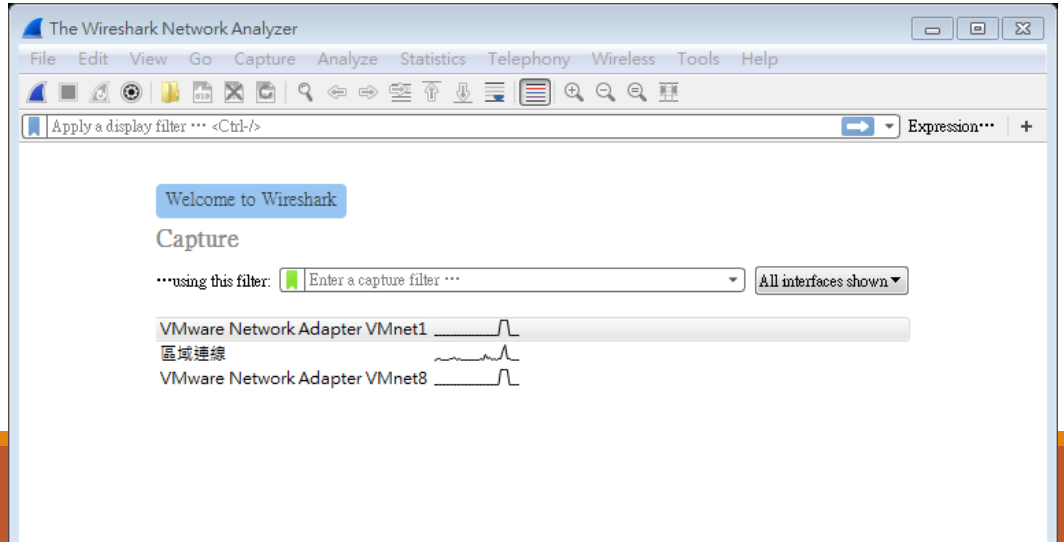


2.下載完成後，安裝完成

- WinPcap要安裝

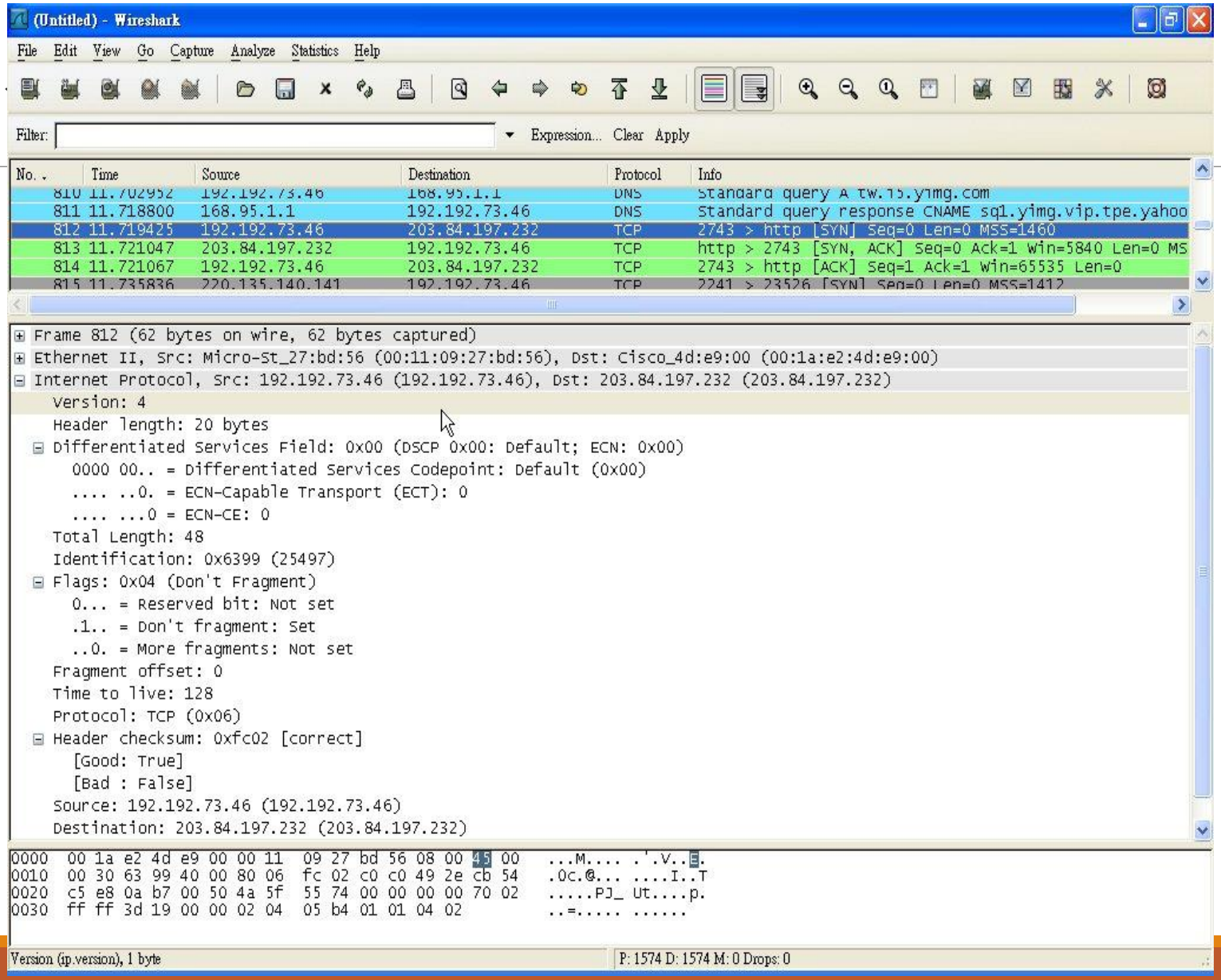


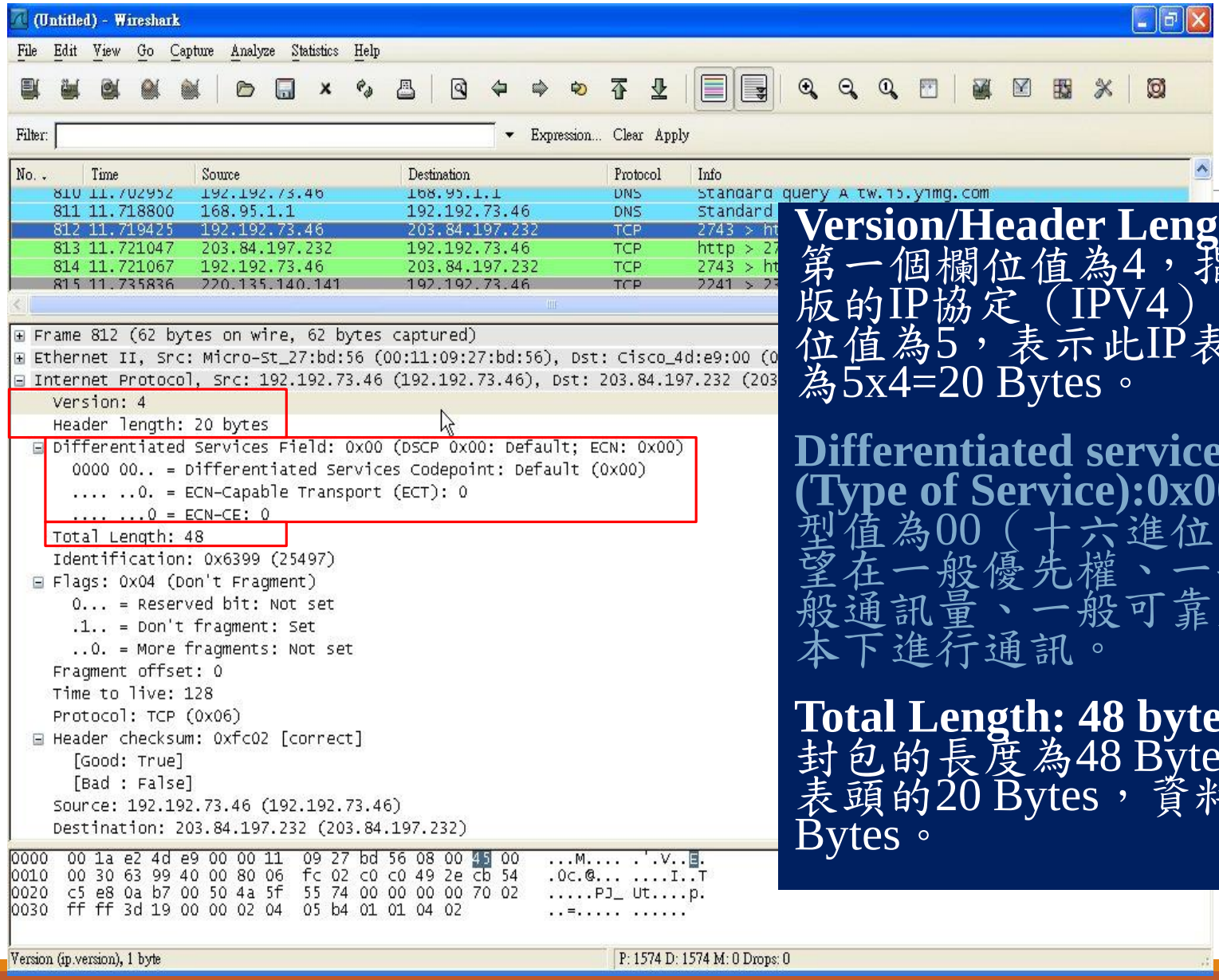
3.開始→執行上網動作，擷取封包→暫停



WinPcap 4.1.3


softcans.blogspot.tw/2013/11/winpcap-413.html
系統工具
多媒體
防毒軟體
檔案工具
網路工具
美工軟體
Free Writing Tool
Improve grammar, word choice, and sentence structure in your writing. It's free!
Home » 網路工具 » [下載] WinPcap 4.1.3 擷取網路封包必備工具
[下載] WinPcap 4.1.3 擷取網路封包必備工具
WinPcap是一套資料連結層網路(link-layer network)存取的工具，它允許應用程式繞過通訊協定堆疊(protocol stack)來擷取和發送網路封包，並具有額外的實用功能，包括核心層封包過濾、網路統計資料引擎，並支援遠端封包擷取。
【軟體名稱】：WinPcap
【軟體版本】：4.1.3
【軟體分類】：網路工具
【軟體介面】：英文
【軟體性質】：免費軟體
【檔案大小】：893KB
【作業系統】：Windows
【軟體螢幕截圖】：
WinPcap 4.1.3 Setup
License Agreement
Please review the license terms before installing WinPcap 4.1.3.
Press Page Down to see the rest of the agreement.
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
Copyright (c) 2010 - 2013 Riverbed Technology, San Francisco (California).
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
搜尋
熱門文章
[下載]PotPlayer v1.6.48186 免安裝 繁體中文版 萬能的播放器
[下載] GIMP 2.8.8 免安裝 繁體中文版 影像處理軟體 PhotoShop 替代軟體
[下載] FreeMind 1.0.0 免費心智圖軟體 免安裝 繁體中文版
[下載] LibreCAD 2.0.2 免安裝 繁體中文版 免費CAD繪圖應用程式

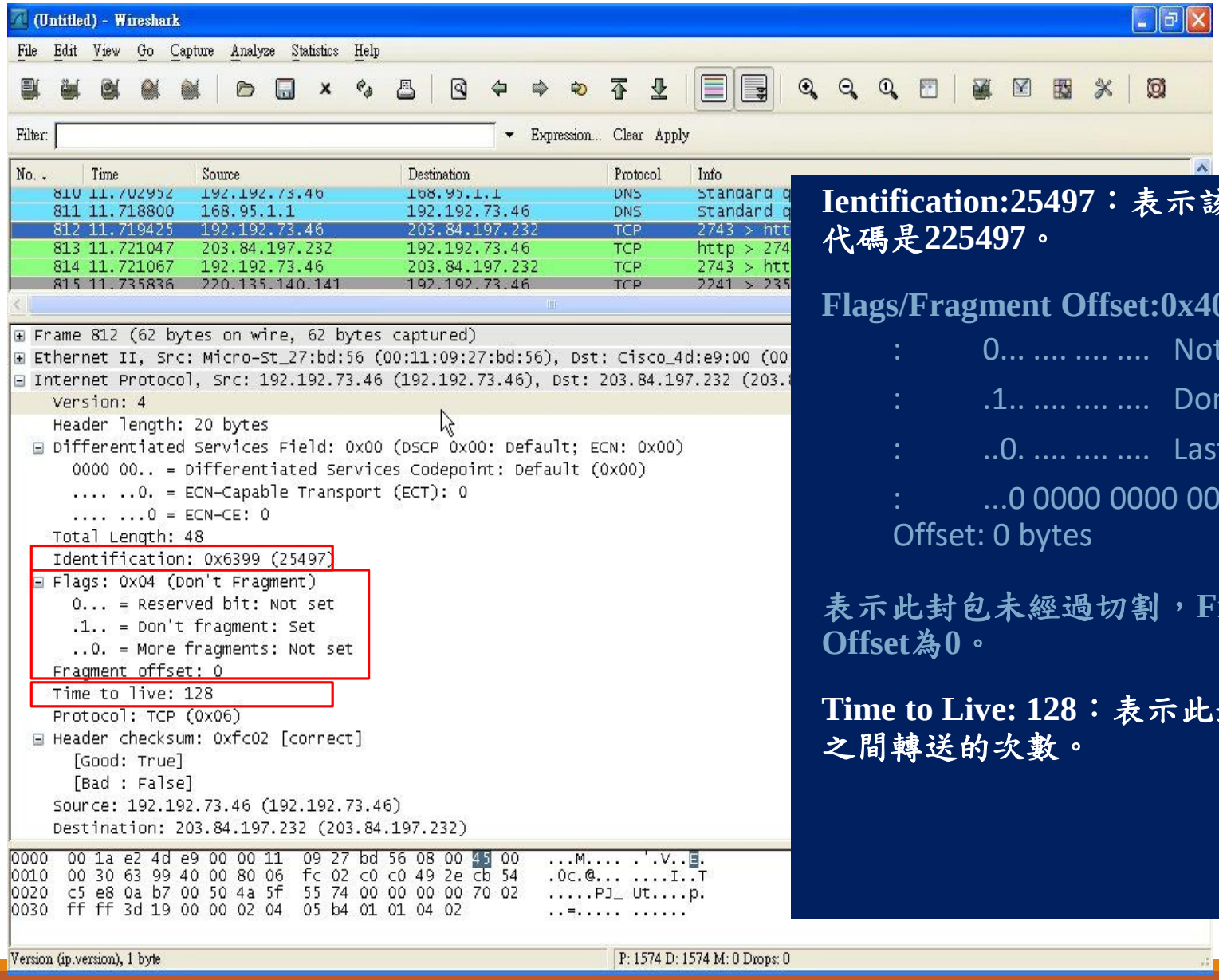

(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
811 11.718800 168.95.1.1 192.192.73.46 DNS Standard query response CNAME sq1.yimg.vip.tpe.yahoo
812 11.719425 192.192.73.46 203.84.197.232 TCP 2743 > http [SYN] Seq=0 Len=0 MSS=1460
813 11.721047 203.84.197.232 192.192.73.46 TCP http > 2743 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MS
814 11.721067 192.192.73.46 203.84.197.232 TCP 2743 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
Frame 812 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: Micro-St_27:bd:56 (00:11:09:27:bd:56), Dst: Cisco_4d:e9:00 (00:1a:e2:4d:e9:00)
Internet Protocol, Src: 192.192.73.46 (192.192.73.46), Dst: 203.84.197.232 (203.84.197.232)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 48
Identification: 0x6399 (25497)
Flags: 0x04 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0xfc02 [correct]
[Good: True]
[Bad : False]
Source: 192.192.73.46 (192.192.73.46)
Destination: 203.84.197.232 (203.84.197.232)
0000 00 1a e2 4d e9 00 00 11 09 27 bd 56 08 00 45 00 ...M.... .'.V..E.
0010 00 30 63 99 40 00 80 06 fc 02 c0 c0 49 2e cb 54 .0c.@... ....I..T
0020 c5 e8 0a b7 00 50 4a 5f 55 74 00 00 00 00 70 02 .....PJ_ Ut....p.
0030 ff ff 3d 19 00 00 02 04 05 b4 01 01 04 02 ..=..... ......
Version (ip.version), 1 byte
P: 1574 D: 1574 M: 0 Drops: 0



Version/Header Length:0x45：第一個欄位值為4，指採用第四版的IP協定（IPV4）；第二個欄位值為5，表示此IP表頭的長度為5x4=20 Bytes。

Differentiated services Field (Type of Service):0x00：服務類型值為00（十六進位），表示期望在一般優先權、一般延遲、一般通訊量、一般可靠度及一般成本下進行通訊。

Total Length: 48 bytes：表示該封包的長度為48 Bytes，扣掉IP表頭的20 Bytes，資料長度有28 Bytes。



Ientification:25497：表示該封包的識別代碼是225497。

Flags/Fragment Offset:0x4000：

: 0... .... Not Used

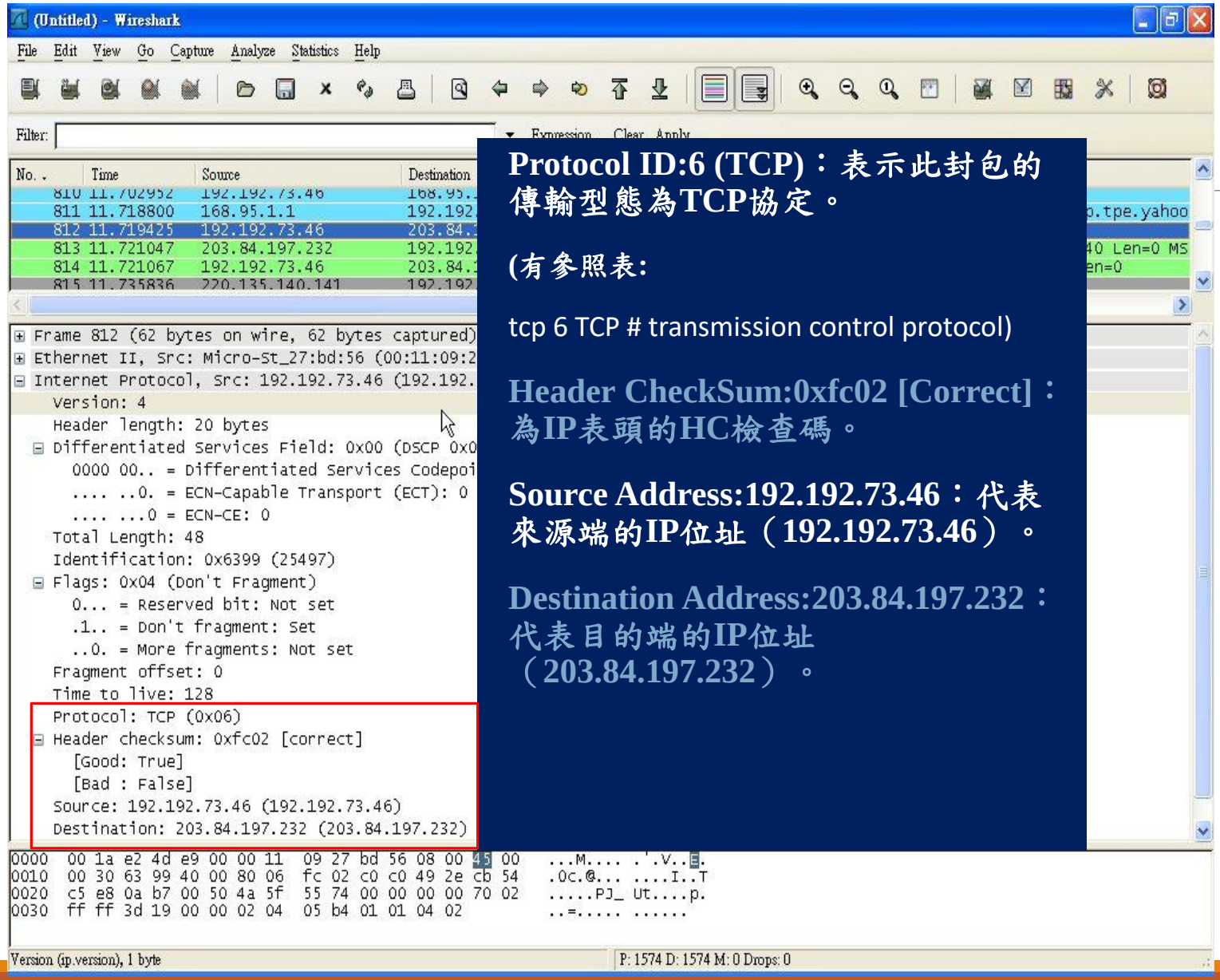
: .1.. .... Don't Fragment

: ..0. .... Last Fragment

: ...0 0000 0000 0000 Fragment Offset: 0 bytes

表示此封包未經過切割，Fragment Offset為0。

Time to Live: 128：表示此封包在路由器之間轉送的次數。



Protocol ID:6 (TCP)：表示此封包的傳輸型態為TCP協定。

(有參照表:

tcp 6 TCP # transmission control protocol)

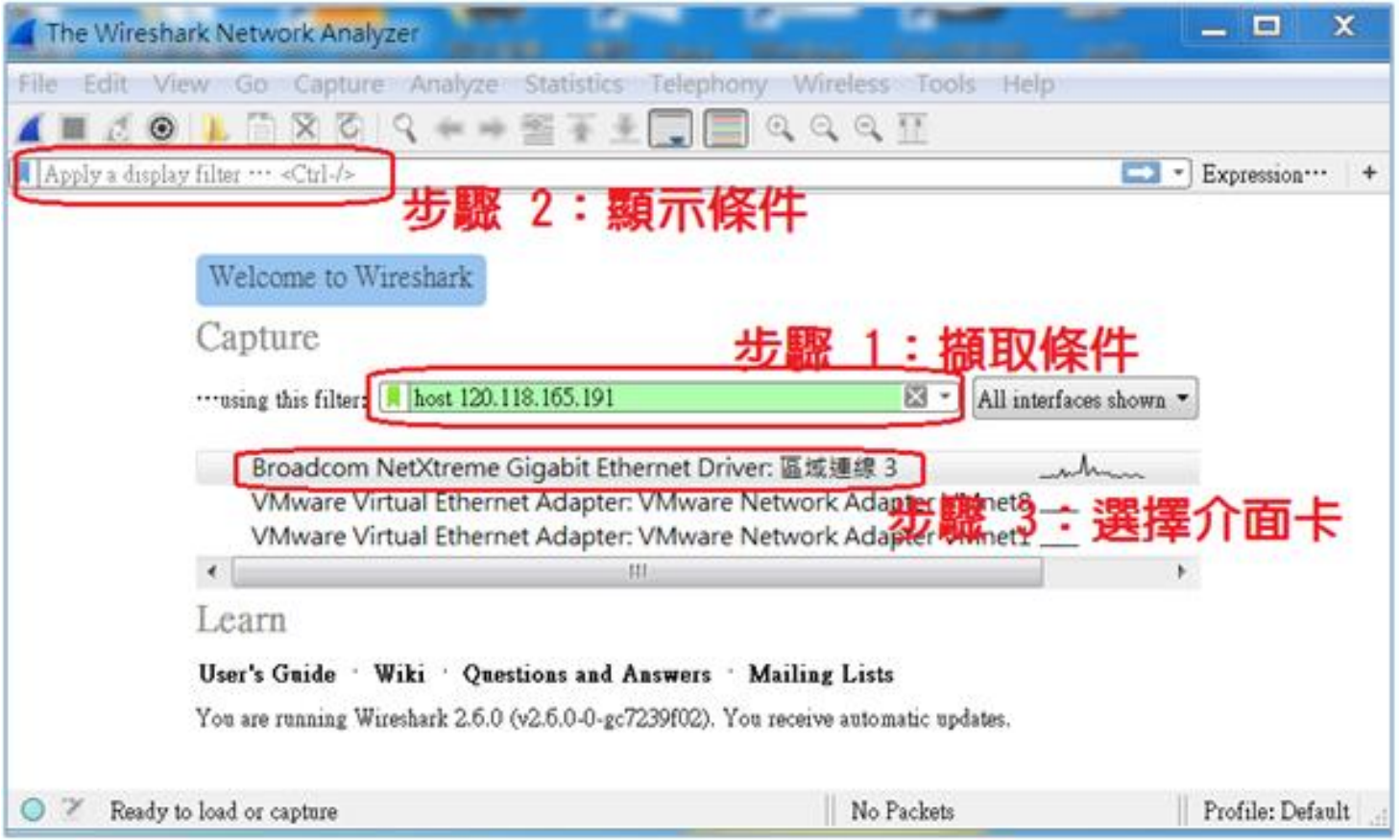
Header CheckSum:0xfc02 [Correct]：為IP表頭的HC檢查碼。

Source Address:192.192.73.46：代表來源端的IP位址（192.192.73.46）。

Destination Address:203.84.197.232：代表目的端的IP位址（203.84.197.232）。

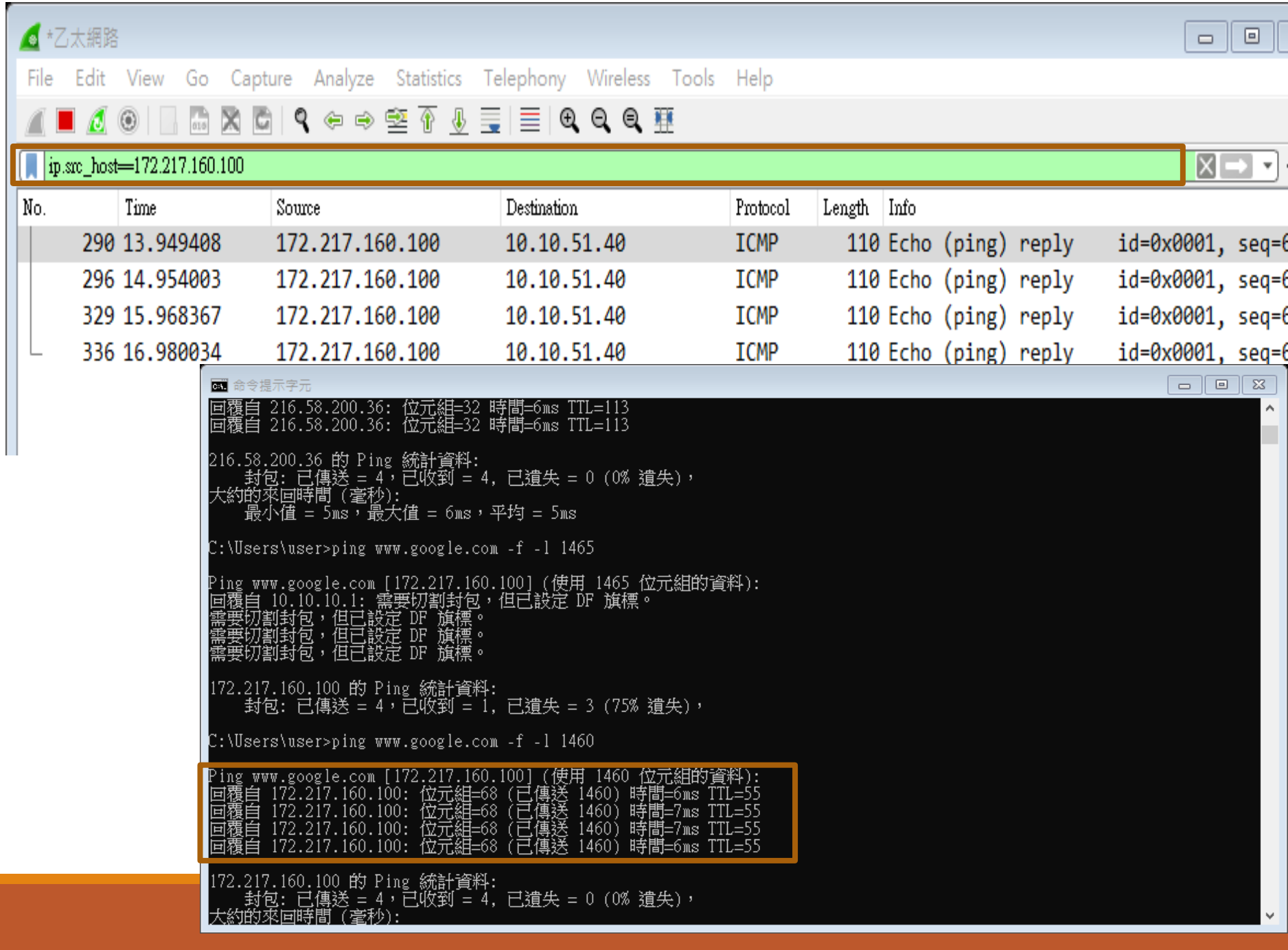
http://www.tsnien.idv.tw/Manager_WebBook/chap1/1-2%20Wireshark%20%E7%B6%B2%E8%B7%AF%E5%B0%81%E5%8C%85%E5%88%86%E6%9E%90%E5%99%A8.html

限制擷取條件


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
Expression···
步驟 2：顯示條件
Welcome to Wireshark
Capture
步驟 1：擷取條件
···using this filter:
host 120.118.165.191
All interfaces shown
Broadcom NetXtreme Gigabit Ethernet Driver: 區域連線 3
VMware Virtual Ethernet Adapter: VMware Network Adapter VMnet8
VMware Virtual Ethernet Adapter: VMware Network Adapter VMnet1
步驟 3：選擇介面卡
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.6.0 (v2.6.0-0-gc7239f02). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

常用過濾範例

類型		說明	範例
eth	dst	目的 MAC	Eth.dst == ff:ff:ff:ff:ff:ff
	src	來源 MAC	Eth.src == 01:34:45:56:a2:c2
	addr	MAC 位址	Eth.addr == 01:34:45:56:a2:c2
	type	下一層協定	Eth.type == 0x0800 (IP) Eth.type == 0x0806 (ARP)
ip	dst	目的 IP	Ip.dst == 192.168.10.3
	src	來源 IP	Ip.src == 192.168.10.4
	addr	IP 位址	Ip.addr == 192.168.10.5
	proto	下一層協定	Ip.proto == 0x06 (TCP) Ip.proto == 0x01 (ICMP) Ip.proto == 0x11 (UDP)
tcp	dstport	目的 Port	Tcp.dstport == 80 (HTTP)
	srcport	來源 Port	Tcp.srcport == 21 (FTP)
	port	埠口編號	Tcp.port == 23 (telnet)
udp	dstport	目的 Port	Udp.dstport == 53 (DNS)
	srcport	來源 Port	Udp.srcport == 53
	port	埠口編號	Udp.port == 53


*乙太網路
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src_host==172.217.160.100
No. Time Source Destination Protocol Length Info
290 13.949408 172.217.160.100 10.10.51.40 ICMP 110 Echo (ping) reply id=0x0001, seq=6
296 14.954003 172.217.160.100 10.10.51.40 ICMP 110 Echo (ping) reply id=0x0001, seq=6
329 15.968367 172.217.160.100 10.10.51.40 ICMP 110 Echo (ping) reply id=0x0001, seq=6
336 16.980034 172.217.160.100 10.10.51.40 ICMP 110 Echo (ping) reply id=0x0001, seq=6
命令提示字元
回覆自 216.58.200.36: 位元組=32 時間=6ms TTL=113
回覆自 216.58.200.36: 位元組=32 時間=6ms TTL=113
216.58.200.36 的 Ping 統計資料:
封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
最小值 = 5ms，最大值 = 6ms，平均 = 5ms
C:\Users\user>ping www.google.com -f -l 1465
Ping www.google.com [172.217.160.100] (使用 1465 位元組的資料):
回覆自 10.10.10.1: 需要切割封包，但已設定 DF 旗標。
需要切割封包，但已設定 DF 旗標。
需要切割封包，但已設定 DF 旗標。
需要切割封包，但已設定 DF 旗標。
172.217.160.100 的 Ping 統計資料:
封包: 已傳送 = 4，已收到 = 1，已遺失 = 3 (75% 遺失)，
C:\Users\user>ping www.google.com -f -l 1460
Ping www.google.com [172.217.160.100] (使用 1460 位元組的資料):
回覆自 172.217.160.100: 位元組=68 (已傳送 1460) 時間=6ms TTL=55
回覆自 172.217.160.100: 位元組=68 (已傳送 1460) 時間=7ms TTL=55
回覆自 172.217.160.100: 位元組=68 (已傳送 1460) 時間=7ms TTL=55
回覆自 172.217.160.100: 位元組=68 (已傳送 1460) 時間=6ms TTL=55
172.217.160.100 的 Ping 統計資料:
封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):

參考資料

鯊魚咬電纜：30天玩Wireshark 系列

- [Day 2] 工欲善其事，必先利其器：安裝Wireshark
- [Day 3] Wireshark長怎樣？
- [Day 8] 到底怎樣下指令才能找到自己要觀察的封包？
- [Day 9] 繼續玩過濾指令
- [Day 13] Wireshark除了看封包還可以統計資料！
- [Day 29] Wireshark漏洞補破網
- [Bonus Day 6] 電子商務資安服務中心 EC-CERT