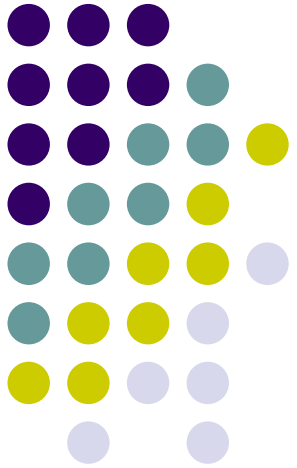
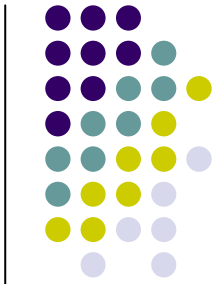
實驗七 UDP協定分析



實驗目的

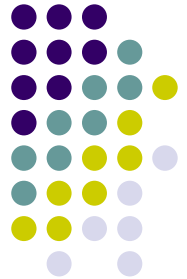
- 明瞭不可靠傳輸層的基礎觀念
- 解析UDP協定下區段資料傳送的格式

背景資料



- TCP協定與UDP協定各有其傳輸特性，主要差異在於訊息的處理時間與傳輸的可靠度問題，協定的選擇期望在處理時間與可靠度間找到一個平衡點。
- UDP協定（User Datagram Protocol）是一個相當簡單的協定，僅提供Host-To-Host（End-to-End）最基本的功能，也就是提供連接埠號給主機判斷是由何應用程式處理資訊。

背景資料



- UDP和IP都是以非連接導向性（Connectionless）的方式來傳送封包，所以傳送過程較為單純，相對地可靠性較差，無法保證資料到達目的地的順序，在傳送過程中若發生問題，並不具有確認、重送等機制，所以一般而言要使用UDP協定來傳送資料必須滿足底下條件：
  - 允許資料損失。
  - 不管資料到達目的地的順序，所以最好資訊均封裝在單一區段中。
  - 對電腦資源的需求高。

背景資料

- 所以DNS查詢、網路多媒體視訊和網路廣播（Multicast或Broadcast）等，在資料損失時並不會造成重大影響，但對時效需求較高，或者應用層有能力來處理這些問題，如一些P2P程式，此時才會使用UDP協定。
- UDP協定的主要作用是將區段的表頭壓縮成為一個較為簡易的格式，一個典型的UDP區段就是一個二進制的格式，每一個區段的前八個字元是用來包含區段表頭的訊息，其他的就用來當作包含具體的資料。

傳輸層連接埠

- 傳輸層協定使用2 Bytes來存放連接埠號，所以埠號的有效範圍是從0到65535，為不同的應用程式保留其各自的資料傳送的通道，連接埠號的規範在 http://www.iana.org/assignments/port-numbers。
- UDP和TCP協定正是採用這類機制，來實現對同一個時間點中多個應用程式同時發送和接收資料的支援，發送資料的一方（可以是客戶端或是伺服器端）將UDP資料通過來源埠號發送出去，而資料接收的一方則是通過目標埠口來接收資料，有的網路應用程式只能使用事先為其預留的固定埠號，而另外有一些網路應用程式則可以使用未被使用的動態埠號。
- 按IANA的規定，編號0-1023的連接埠號稱為Well-Known埠，Well-Known連接埠僅是約定俗成的意思，並不具有強制性質，主要供伺服器應用程式使用，一般來說，大於49151的連接埠號都是代表動態連接埠號。

常見的保留埠編號

協定	連接埠號	伺服器描述
TCP	20	File Transfer [Default Data]
TCP	21	File Transfer [Control]
TCP	22	SSH Remote Login Protocol
TCP	23	Telnet
TCP	25	Simple Mail Transfer Protocol
UDP	53	Domain Name Server
UDP	67	Bootstrap Protocol Server
UDP	68	Bootstrap Protocol Client
UDP	69	Trivial File Transfer
TCP	80	World Wide Web HTTP
TCP	110	Post Office Protocol - Version 3
TCP	123	Network Time Protocol
TCP	137	NETBIOS Name Service
TCP	138	NETBIOS Datagram Service
TCP	139	NETBIOS Session Service
TCP	143	Internet Message Access Protocol
TCP	161	Simple Network Management Protocol
TCP	443	http protocol over TLS/SSL
TCP	993	imap4 protocol over TLS/SSL
TCP	995	pop3 protocol over TLS/SSL (was spop3)
TCP	1863	MSN protocol
TCP	3306	MySQL

UDP區段

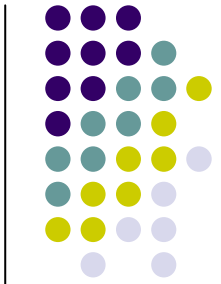
- UDP整個區段的長度，是指包括區段表頭和資料部分在內，區段表頭的長度是固定的，資料區段的最大長度根據使用環境的不同會有差異，理論上來說，包含表頭在內的區段大小的最大長度為65535 bytes。
- UDP協定使用表頭中的確認值來確保資料的正確性，確認值首先在資料發送方利用特殊的演算法來得到，在傳送到接收端之後，還要重新的再計算一次，如果有某一個資料區段在傳送的過程中被第三者更改而損壞的話，那麼發送端和接收端的確認值會不相同，由此可見UDP協定可以檢測是否出錯。這個和TCP協定是不同的。

UDP區段

- **UDP區段格式**

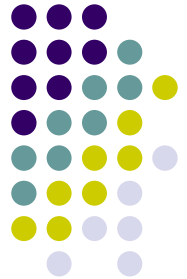
- **UDP表頭欄位**

UDP區段



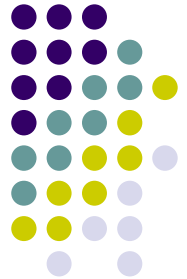
- Source Port：長度為2 Bytes，用來記錄來源端應用程式所用的連接埠號。
- Destination Port：長度為2 Bytes，用來記錄目的端應用程式所用的連接埠號。
- Length：長度為2 Bytes，用來記錄UDP區段的總長度，以Byte單位。欄位最小值為8，也就是只有UDP表頭，沒有任何UDP資料，最大值則受限於IP Payload的長度。
- Checksum：長度為2 Bytes，用來檢查來源主機與目的主機所送出的資料區段是否正確。

UDP虛擬表頭



- UDP與TCP執行其Checksum值運算時，除了表頭與資料外，還有一個所謂的虛擬表頭（Pseudo Header）作輔助。它包含以下的欄位：
  - Source IP Address：IP表頭中來源端的IP位址
  - Destination IP Address：IP表頭中目的端的IP位址
  - Unused：長度為8 Bits，填入0
  - Protocol：IP表頭中紀錄上層協定的欄位
  - Length：UDP表頭中的Length欄位
- UDP的錯誤檢查碼可視為雙重保險的機制，當區段在傳遞中發生錯誤，而位於UDP下的各層協定都沒有找出錯誤時，Pseudo Header提供了一道額外的防線。

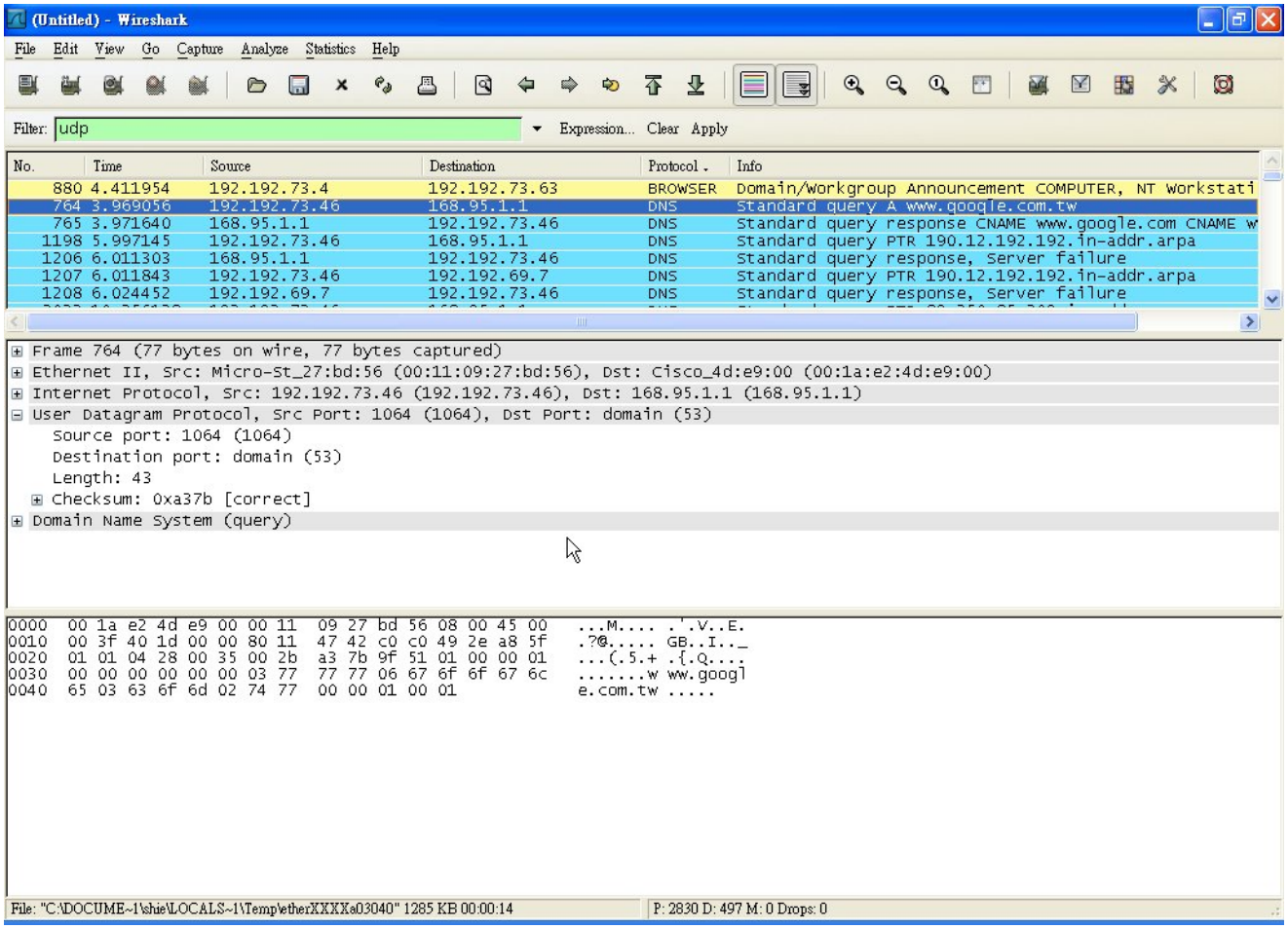
UDP協定的應用



- UDP雖然負責傳送訊息，但本層並不提供軟體來查核區段遞送狀況。
- UDP提供的優勢是速度快。由於UDP不提供確認，所以透過網路傳送的流量較少，使傳輸作業速度加快，若用在語音、影像來說會有不錯效果。
- UDP提供了較為簡易的資料傳輸協定，它的訊息可能會在網路傳送過程中遺失、重複或不依順序，但它可以提供一個較快的傳送機制，在某些場合中可能需要，如DNS。

實驗方法

- DNS query

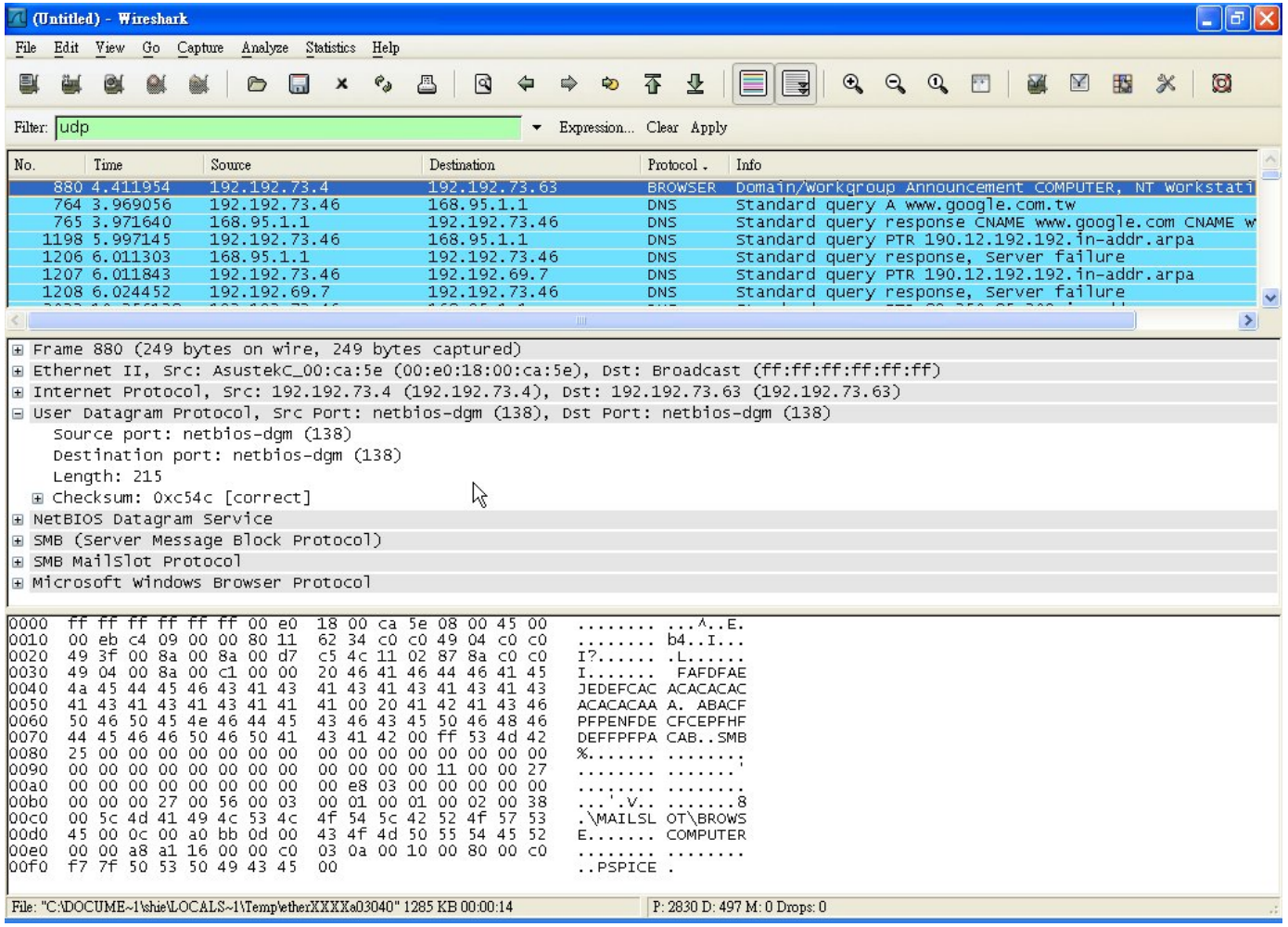


DNS query

說明：UDP表頭包含：

- 1.Source port = 1064；
- 2.Destination port = (domain) 53；
- 3.Length = 43；
- 4.Checksum = 0xa37b(十六進位)

微軟網路芳鄰協定

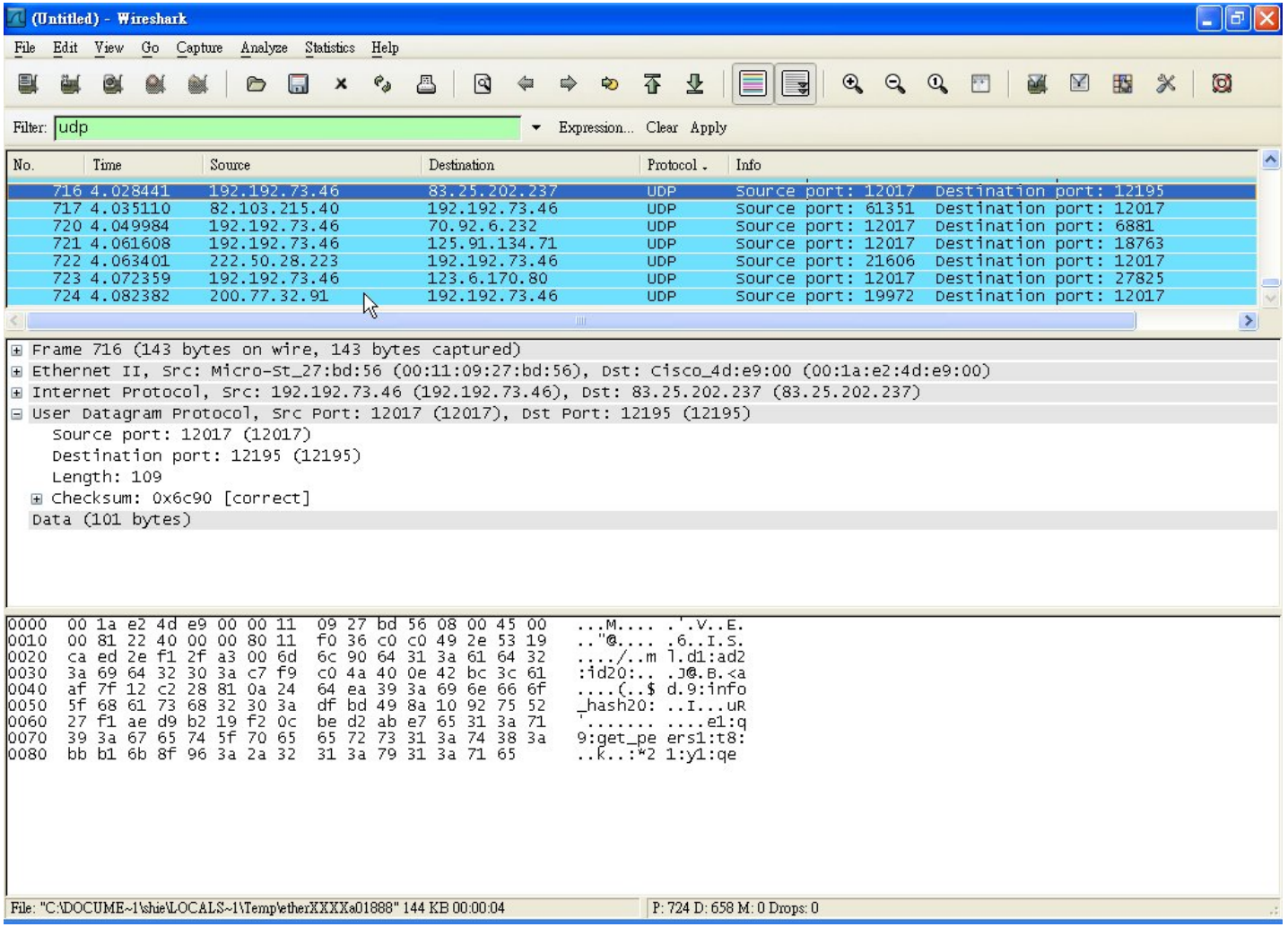

(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: udp
Expression... Clear Apply
No. Time Source Destination Protocol Info
880 4.411954 192.192.73.4 192.192.73.63 BROWSER Domain/Workgroup Announcement COMPUTER, NT Workstati
764 3.969056 192.192.73.46 168.95.1.1 DNS Standard query A www.google.com.tw
765 3.971640 168.95.1.1 192.192.73.46 DNS Standard query response CNAME www.google.com CNAME w
1198 5.997145 192.192.73.46 168.95.1.1 DNS Standard query PTR 190.12.192.192.in-addr.arpa
1206 6.011303 168.95.1.1 192.192.73.46 DNS Standard query response, Server failure
1207 6.011843 192.192.73.46 192.192.69.7 DNS Standard query PTR 190.12.192.192.in-addr.arpa
1208 6.024452 192.192.69.7 192.192.73.46 DNS Standard query response, Server failure
Frame 880 (249 bytes on wire, 249 bytes captured)
Ethernet II, Src: AsustekC_00:ca:5e (00:e0:18:00:ca:5e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.192.73.4 (192.192.73.4), Dst: 192.192.73.63 (192.192.73.63)
User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)
Source port: netbios-dgm (138)
Destination port: netbios-dgm (138)
Length: 215
Checksum: 0xc54c [correct]
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
0000 ff ff ff ff ff ff 00 e0 18 00 ca 5e 08 00 45 00 ....^..E.
0010 00 eb c4 09 00 00 80 11 62 34 c0 c0 49 04 c0 c0 ..... b4..I...
0020 49 3f 00 8a 00 8a 00 d7 c5 4c 11 02 87 8a c0 c0 I?..... .L.....
0030 49 04 00 8a 00 c1 00 00 20 46 41 46 44 46 41 45 I..... FAFDFAE
0040 4a 45 44 45 46 43 41 43 41 43 41 43 41 43 41 43 JEDEFCAC ACACACAC
0050 41 43 41 43 41 43 41 41 41 00 20 41 42 41 43 46 ACACACAA A. ABACF
0060 50 46 50 45 4e 46 44 45 43 46 43 45 50 46 48 46 PFPENFDE CFCEPFHF
0070 44 45 46 46 50 46 50 41 43 41 42 00 ff 53 4d 42 DEFFPFPA CAB..SMB
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 %..... .....
0090 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 27 ....'
00a0 00 00 00 00 00 00 00 00 00 e8 03 00 00 00 00 00 ....
00b0 00 00 00 27 00 56 00 03 00 01 00 01 00 02 00 38 ...'.V.. 8
00c0 00 5c 4d 41 49 4c 53 4c 4f 54 5c 42 52 4f 57 53 .\MAILSL OT\BROWS
00d0 45 00 0c 00 a0 bb 0d 00 43 4f 4d 50 55 54 45 52 E..... COMPUTER
00e0 00 00 a8 a1 16 00 00 c0 03 0a 00 10 00 80 00 c0 ....
00f0 f7 7f 50 53 50 49 43 45 00 ..PSPICE .
File: "C:\DOCUME~1\shie\LOCALS~1\Temp\etherXXXXa03040" 1285 KB 00:00:14
P: 2830 D: 497 M: 0 Drops: 0

微軟網路芳鄰協定

說明：UDP表頭包含：

- 1.Source port = (netbios-dgm) 138；
- 2.Destination port = (netbios-dgm) 138；
- 3.Length = 215；
- 4.Checksum = 0xc54c(十六進位)

Bitcomet


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: udp
Expression... Clear Apply
No. Time Source Destination Protocol Info
716 4.028441 192.192.73.46 83.25.202.237 UDP Source port: 12017 Destination port: 12195
717 4.035110 82.103.215.40 192.192.73.46 UDP Source port: 61351 Destination port: 12017
720 4.049984 192.192.73.46 70.92.6.232 UDP Source port: 12017 Destination port: 6881
721 4.061608 192.192.73.46 125.91.134.71 UDP Source port: 12017 Destination port: 18763
722 4.063401 222.50.28.223 192.192.73.46 UDP Source port: 21606 Destination port: 12017
723 4.072359 192.192.73.46 123.6.170.80 UDP Source port: 12017 Destination port: 27825
724 4.082382 200.77.32.91 192.192.73.46 UDP Source port: 19972 Destination port: 12017
Frame 716 (143 bytes on wire, 143 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: 83.25.202.237 (83.25.202.237)
User Datagram Protocol, Src Port: 12017 (12017), Dst Port: 12195 (12195)
Source port: 12017 (12017)
Destination port: 12195 (12195)
Length: 109
Checksum: 0x6c90 [correct]
Data (101 bytes)
0000 00 1a e2 4d e9 00 00 11 09 27 bd 56 08 00 45 00 ...M.... .'.V..E.
0010 00 81 22 40 00 00 80 11 f0 36 c0 c0 49 2e 53 19 .."@.... .6..I.S.
0020 ca ed 2e f1 2f a3 00 6d 6c 90 64 31 3a 61 64 32 ..../..m l.d1:ad2
0030 3a 69 64 32 30 3a c7 f9 c0 4a 40 0e 42 bc 3c 61 :id20:.. .J@.B.<a
0040 af 7f 12 c2 28 81 0a 24 64 ea 39 3a 69 6e 66 6f ....(..$ d.9:info
0050 5f 68 61 73 68 32 30 3a df bd 49 8a 10 92 75 52 _hash20: ..I...uR
0060 27 f1 ae d9 b2 19 f2 0c be d2 ab e7 65 31 3a 71 '....... ....e1:q
0070 39 3a 67 65 74 5f 70 65 65 72 73 31 3a 74 38 3a 9:get_pe ers1:t8:
0080 bb b1 6b 8f 96 3a 2a 32 31 3a 79 31 3a 71 65 ..k..:*2 1:y1:qe
File: "C:\DOCUME~1\shie\LOCALS~1\Temp\etherXXXXa01888" 144 KB 00:00:04
P: 724 D: 658 M: 0 Drops: 0

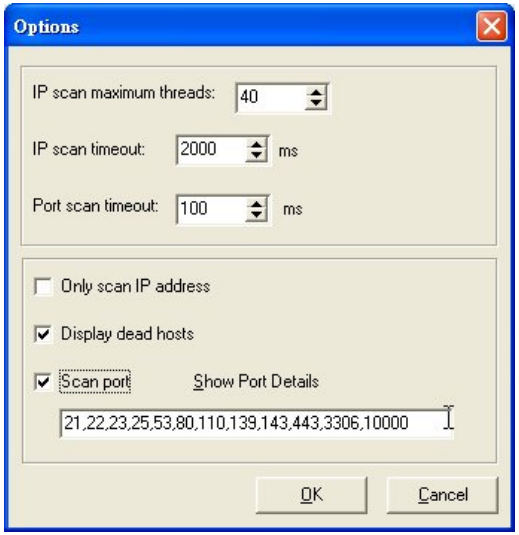
Bitcomet

說明：UDP表頭包含：

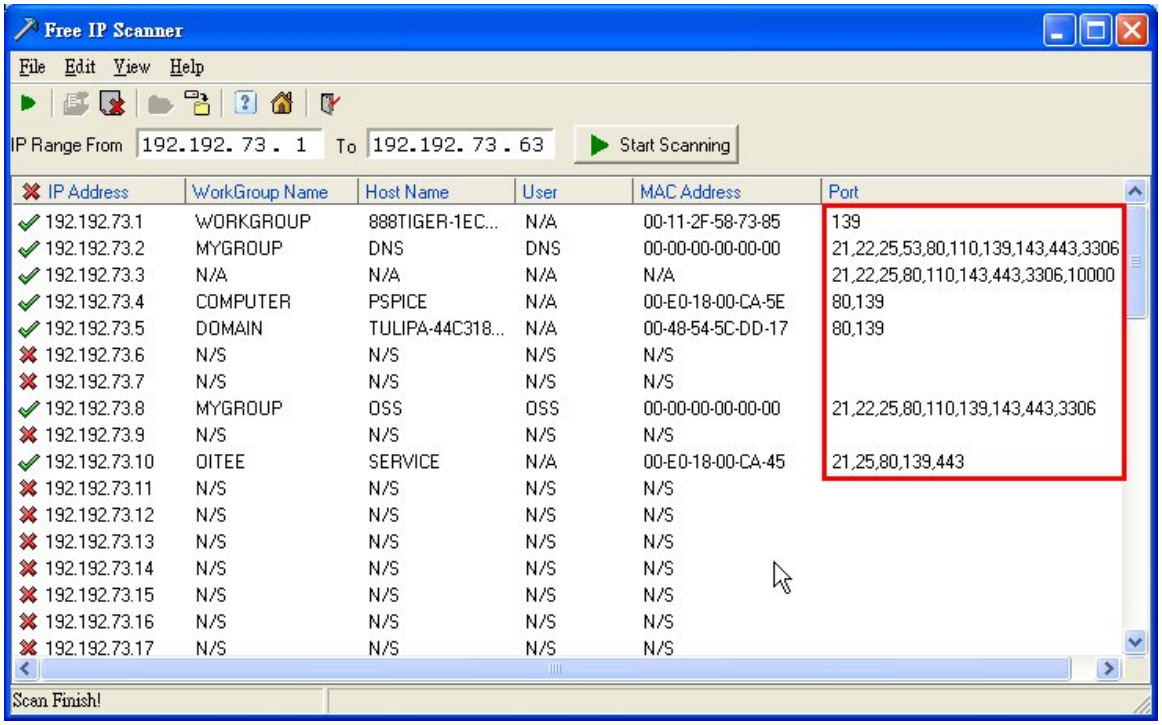
- 1.Source port = 12017；
- 2.Destination port = 12195；
- 3.Length = 109；
- 4.Checksum = 0x6c90(十六進位)

Port Scan

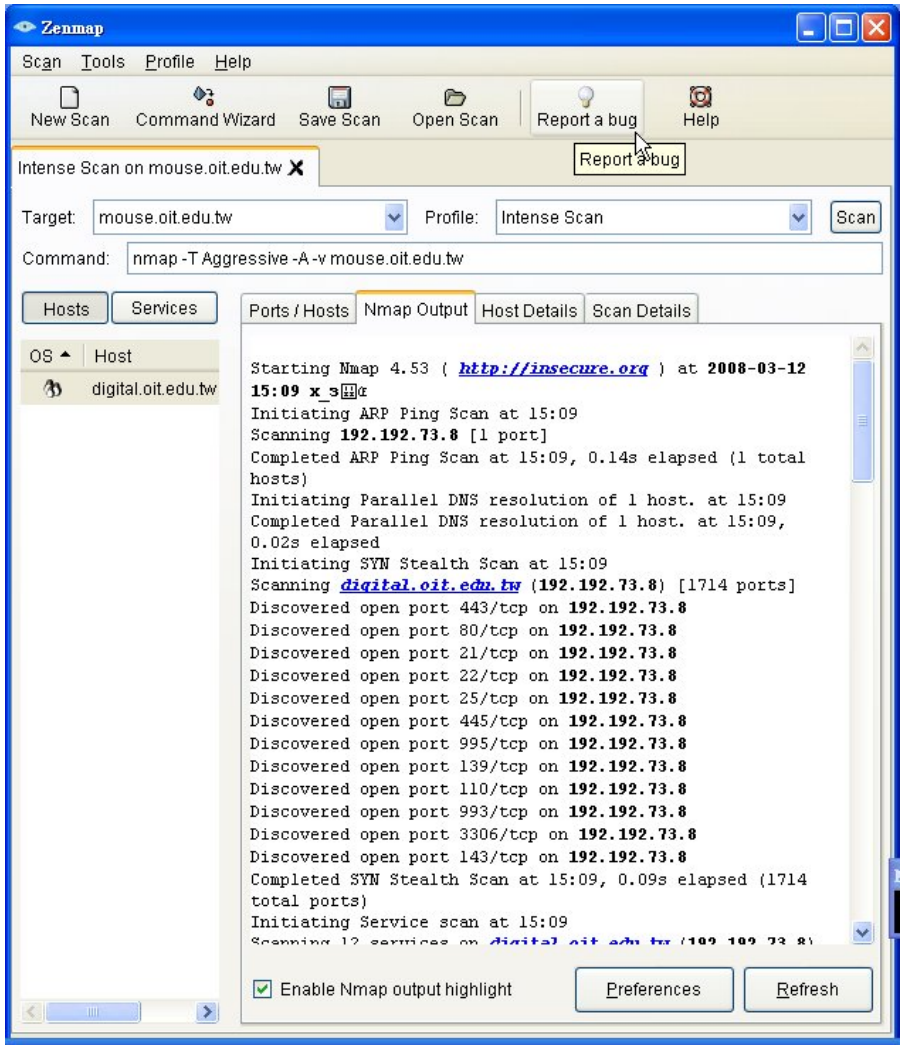
- 使用Free IP scanner也可以掃瞄IP機器Port的使用情況，首先需在[Edit]->[Options]將Scan port這選項勾選，並輸入欲掃瞄的Port號，Port號間需用逗號隔開。相同的重申一下請勿隨意掃瞄他人IP機器Port的使用情況，這會讓人以為你具有攻擊的意圖。



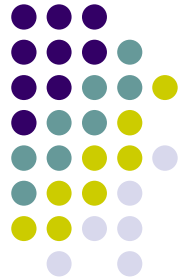
Port Scan


Free IP Scanner
File Edit View Help
IP Range From 192.192.73.1 To 192.192.73.63
Start Scanning
IP Address | WorkGroup Name | Host Name | User | MAC Address | Port
192.192.73.1 | WORKGROUP | 888TIGER-1EC... | N/A | 00-11-2F-58-73-85 | 139
192.192.73.2 | MYGROUP | DNS | DNS | 00-00-00-00-00-00 | 21,22,25,53,80,110,139,143,443,3306
192.192.73.3 | N/A | N/A | N/A | N/A | 21,22,25,80,110,143,443,3306,10000
192.192.73.4 | COMPUTER | PSPICE | N/A | 00-E0-18-00-CA-5E | 80,139
192.192.73.5 | DOMAIN | TULIPA-44C318... | N/A | 00-48-54-5C-DD-17 | 80,139
192.192.73.6 | N/S | N/S | N/S | N/S |
192.192.73.7 | N/S | N/S | N/S | N/S |
192.192.73.8 | MYGROUP | OSS | OSS | 00-00-00-00-00-00 | 21,22,25,80,110,139,143,443,3306
192.192.73.9 | N/S | N/S | N/S | N/S |
192.192.73.10 | OITEE | SERVICE | N/A | 00-E0-18-00-CA-45 | 21,25,80,139,443
192.192.73.11 | N/S | N/S | N/S | N/S |
192.192.73.12 | N/S | N/S | N/S | N/S |
192.192.73.13 | N/S | N/S | N/S | N/S |
192.192.73.14 | N/S | N/S | N/S | N/S |
192.192.73.15 | N/S | N/S | N/S | N/S |
192.192.73.16 | N/S | N/S | N/S | N/S |
192.192.73.17 | N/S | N/S | N/S | N/S |
Scan Finish!

nmap


Zenmap
Scan Tools Profile Help
New Scan
Command Wizard
Save Scan
Open Scan
Report a bug
Help
Report a bug
Intense Scan on mouse.oit.edu.tw
Target: mouse.oit.edu.tw
Profile: Intense Scan
Scan
Command: nmap -T Aggressive -A -v mouse.oit.edu.tw
Hosts
Services
OS
Host
digital.oit.edu.tw
Ports / Hosts
Nmap Output
Host Details
Scan Details
Starting Nmap 4.53 (http://insecure.org) at 2008-03-12 15:09
Initiating ARP Ping Scan at 15:09
Scanning 192.192.73.8 [1 port]
Completed ARP Ping Scan at 15:09, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:09
Completed Parallel DNS resolution of 1 host. at 15:09, 0.02s elapsed
Initiating SYN Stealth Scan at 15:09
Scanning digital.oit.edu.tw (192.192.73.8) [1714 ports]
Discovered open port 443/tcp on 192.192.73.8
Discovered open port 80/tcp on 192.192.73.8
Discovered open port 21/tcp on 192.192.73.8
Discovered open port 22/tcp on 192.192.73.8
Discovered open port 25/tcp on 192.192.73.8
Discovered open port 445/tcp on 192.192.73.8
Discovered open port 995/tcp on 192.192.73.8
Discovered open port 139/tcp on 192.192.73.8
Discovered open port 110/tcp on 192.192.73.8
Discovered open port 993/tcp on 192.192.73.8
Discovered open port 3306/tcp on 192.192.73.8
Discovered open port 143/tcp on 192.192.73.8
Completed SYN Stealth Scan at 15:09, 0.09s elapsed (1714 total ports)
Initiating Service scan at 15:09
Enable Nmap output highlight
Preferences
Refresh

學習評量



1. 應用層如何決定選擇傳輸層中是使用TCP或UDP協定？
2. 說明連接埠編號的原則？
3. 使用UDP傳送封包是否有大小限制，如果有限制的話，大小超過限制會出現什麼情況？
4. 說明UPD的checksum值的運算機制。
5. 說明UDP協定中潛在的風險？