MỤC LỤC

LỜI NÓI ĐẦU

Mục đích của tập bài thí nghiệm phân tích giao thức mạng này là giúp cho sinh viên nắmvững quá trình trao đổi dữ liệu diễn ra giữa các giao thức thuộc các lớp mạng tương ứng củabộ giao thức IP sử dụng trong Internet.Các bài thí nghiệm phân tích giao thức mạng sẽgiúp cho sinh viên trực tiếp thực hiện thiết lập cấu hình, thu kết dữ liệu và phân tích kết quả,quan sát chuỗi các bản tin trao đổi giữa hai thực thể (entities) giao thức, đào sâu vào chi tiết của hoạt động giao thức, và điều khiển các giao thức thực hiện một số hoạt động nhất định rồiquan sát các hoạt động đó và hiệu quả của chúng. Các nội dung này có thể được thực hiệntheo hai phương pháp: mô phỏng hoặc phân tích môi trường mạng thực. Trong phạm vi bài thínghiệm này chúng ta sẽ sử dụng phương pháp thứ hai nhờ sử dụng gói phần mềm phân tíchgiao thức mạng Wireshark. Đây là phần mềm được sử dụng phổ biến ở nhiều trường đại học,cao đẳng và công ty trên thế giới.

I. TÌM HIỂU VỀ PHẦN MỀM WIRESHARK

1.Giới Thiệu:

Quản Trị Mạng - Wireshark., hay còn gọi là Ethereal, công cụ này có lẽ không quá xa lạ với phần lớn người sử dụng chúng ta, vốn được xem là 1 trong những ứng dụng phân tích dữ liệu hệ thống mạng, với khả năng theo dõi, giám sát các gói tin theo thời gian thực, hiển thị chính xác báo cáo cho người dùng qua giao diện khá đơn giản và thân thiện. Trong bài viết dưới đây, chúng tôi sẽ giới thiệu với các bạn một số đặc điểm cơ bản cũng như cách dùng, phân tích và kiểm tra hệ thống mạng bằng Wireshark.

Các bạn có thể tải **Wireshark** phiên bản mới nhất tại http://wiresharkdownloads.riverbed.com/wireshark/win32/Wireshark-win32-1.7.1.exe

Nếu dùng **Linux** hoặc các hệ thống **UNIX** khác thì có thể tìm thấy **Wireshark** trong phần **PackageRepositories**. Ví dụ, với **Ubuntu** thì **Wireshark** sẽ có ở trong **Ubuntu Software Center.** Tuy nhiên, các bạn cần lưu ý rằng không nên tự tiện sử dụng, vì có công ty, tổ chức hoặc doanh nghiệp không cho phép dùng Wireshark trong hệ thống mạng của họ.

Giới thiệu về Wireshark

WireShark có một bề dầy lịch sử. Gerald Combs là người đầu tiên phát triển phần mềm này. Phiên bản đầu tiên được gọi là Ethereal được phát hành năm 1998. Tám năm sau kể từ khi phiên bản đầu tiên ra đời, Combs từ bỏ công việc hiện tại để theo đuổi một cơ hội nghề nghiệp khác. Thật không may, tại thời điểm đó, ông không thể đạt được thoả thuận với công ty đã thuê ông về việc bản quyền của thương hiệu Ethereal. Thay vào đó, Combs và phần còn lại của đội phát triển đã xây dựng một thương hiệu mới cho sản phẩm "Ethereal" vào năm 2006, dự án tên là Wireshark

WireShark đã phát triển mạnh mẽ và đến nay, nhóm phát triển cho đến nay đã lên tới 500 cộng tác viên. Sản phẩm đã tồn tại dưới cái tên Ethereal không được phát triển thêm.

Lợi ích Wireshark đem lại đã giúp cho nó trở nên phổ biến như hiện nay. Nó có thể đáp ứng nhu cầu của cả các nhà phân tích chuyên nghiệp và nghiệp dư và nó đưa ra nhiều tính năng để thu hút mỗi đối tượng khác nhau.

2.Các giao thực được hỗ trợ bởi WireShark:

WireShark vượt trội về khả năng hỗ trợ các giao thức (khoảng 850 loại), từ những loại phổ biến như TCP, IP đến những loại đặc biệt như là AppleTalk và Bit Torrent. Và cũng bởi Wireshark được phát triển trên mô hình mã nguồn mở, những giao thức mới sẽ được thêm vào. Và có thể nói rằng không có giao thức nào mà Wireshark không thể hỗ trợ.

Thân thiện với người dùng: Giao diện của Wireshark là một trong những giao diện phần mềm phân tích gói dễ dùng nhất. Wireshark là ứng dụng đồ hoạ với hệ thống menu rất rõ ràng và được bố trí dễ hiểu. Không như một số sản phẩm sử dụng dòng lệnh phức tạp như TCPdump, giao diện đồ hoạ của Wireshark thật tuyệt vời cho những ai đã từng nghiên cứu thế giới của phân tích giao thức.

Giá rẻ: Wireshark là một sản phẩm miễn phí GPL. Bạn có thể tải về và sử dụng Wireshark cho bất kỳ mục đích nào, kể cả với mục đích thương mại.

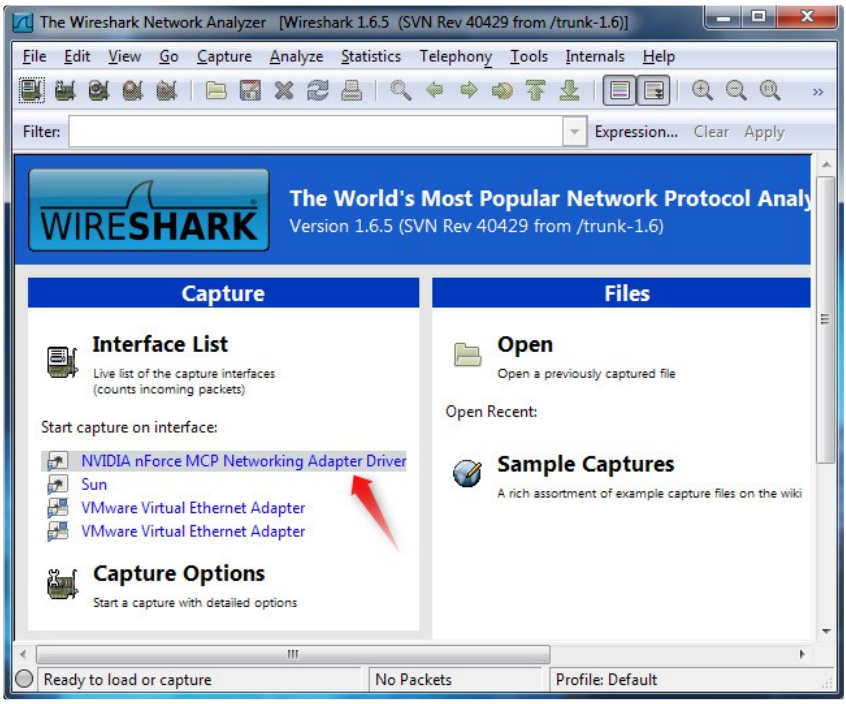
Hỗ trợ: Cộng đồng của Wireshark là một trong những cộng đồng tốt và năng động nhất của các dự án mã nguồn mở.

Hệ điều hành hỗ trợ Wireshark: Wireshark hỗ trợ hầu hết các loại hệ điều hành hiện nay.

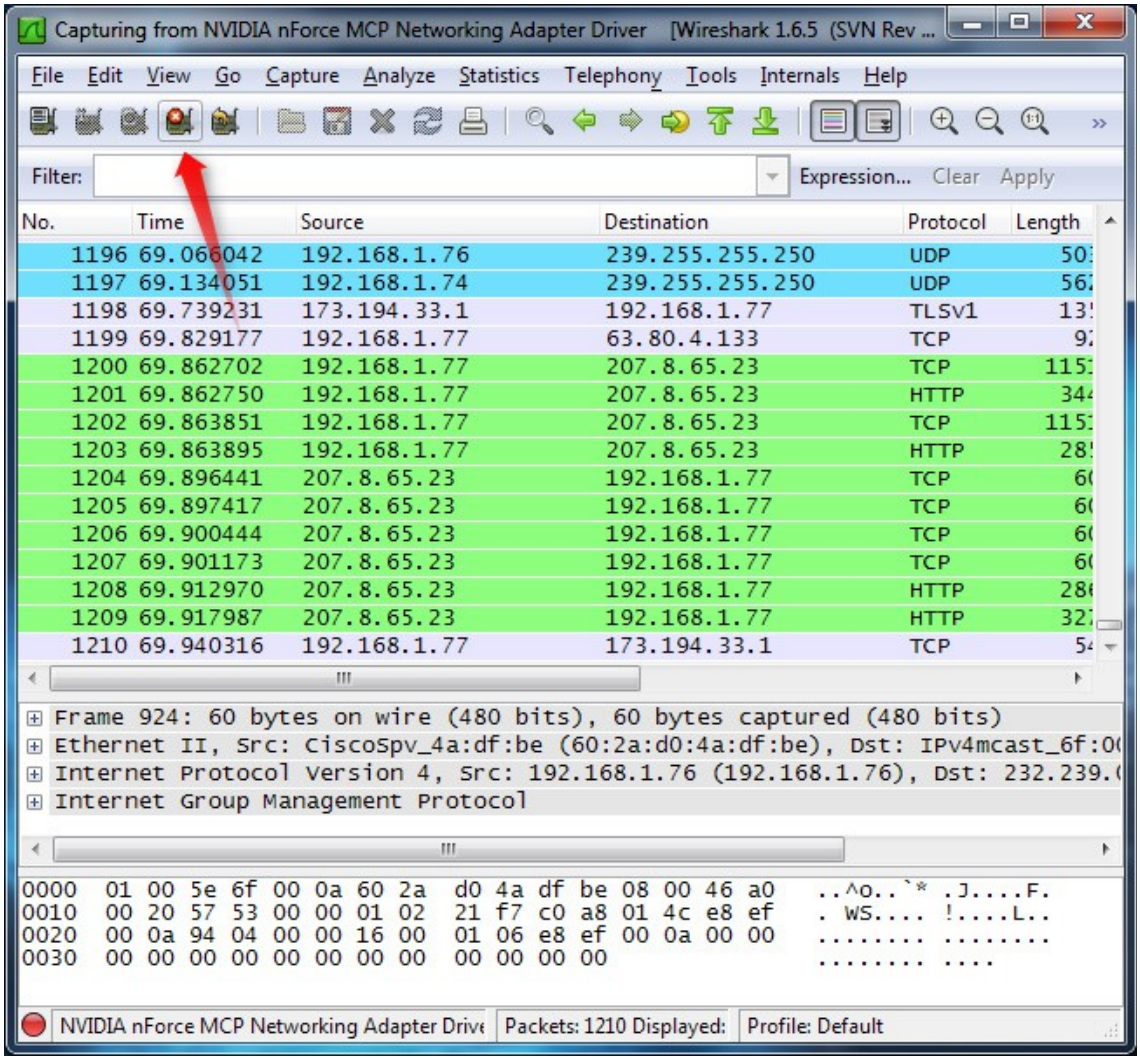
3.Capturing Packets: Phân tích Gói Tin

Sau khi cài đặt, các bạn hãy khởi động chương trình và chọn thành phần trong **Interface List** để bắt đầu hoạt động. Ví dụ, nếu muốn giám sát lưu lượng mạng qua mạng Wireless thì chọn card mạng Wifi tương ứng. Nhấn nút **Capture Options** để hiển thị thêm nhiều tùy chọn khác:

Ngay sau đó, chúng ta sẽ thấy các gói dữ liệu bắt đầu xuất hiện, Wireshark sẽ "bắt" từng gói – package ra và vào hệ thống mạng. Nếu đang giám sát thông tin trên Wireless trong chế độ **Promiscuous** thì sẽ nhìn thấy các gói dữ liệu khác trong toàn bộ hệ thống:



Nếu muốn tạm ngừng quá trình này thì các bạn nhấn nút **Stop** ở phía trên:



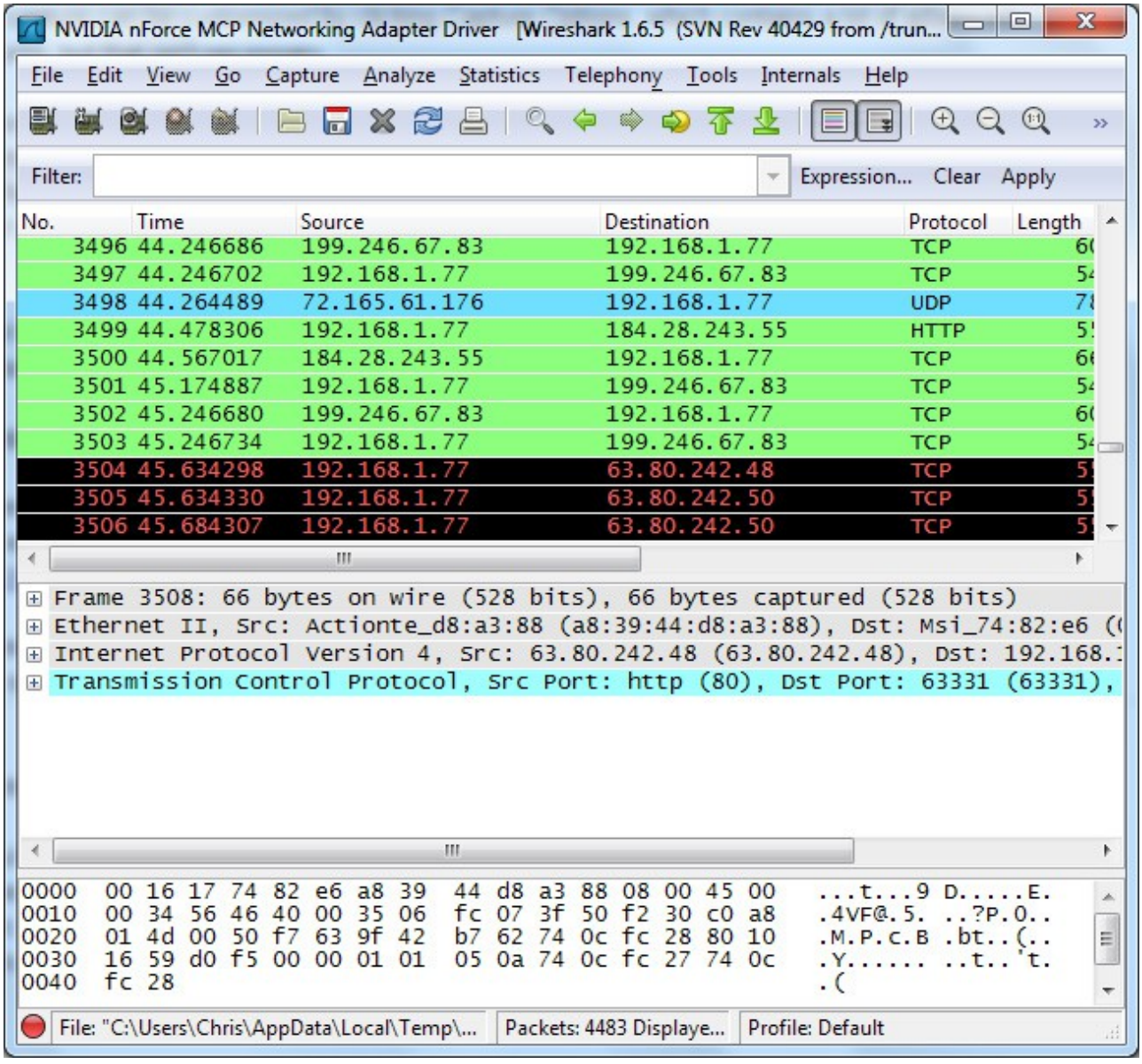
Tại đây, chúng ta sẽ thấy có nhiều màu sắc khác nhau, bao gồm:

a.Xanh lá cây

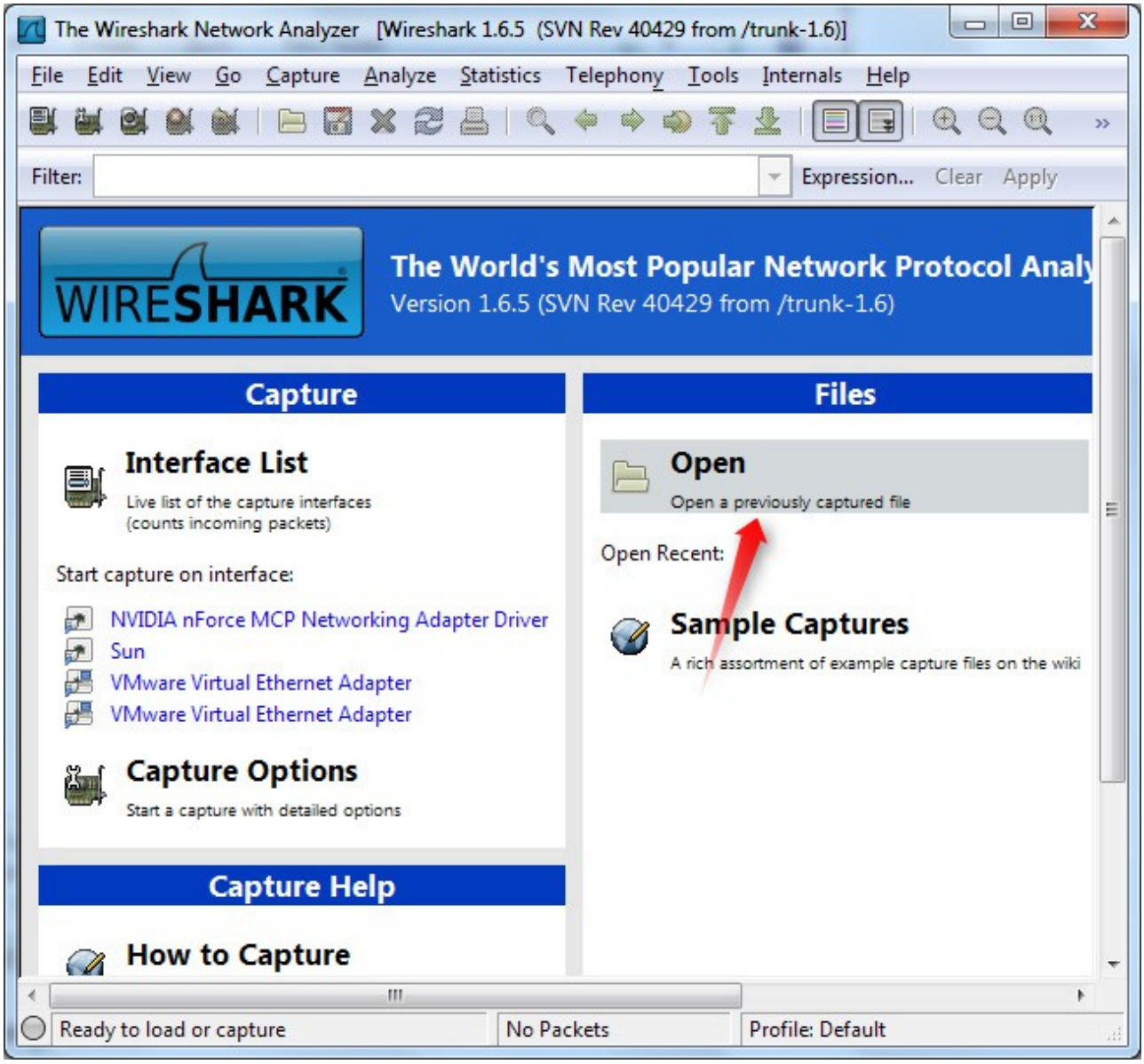
b.Xanh da trời

c.Đen

Wireshark dựa vào cơ chế này để giúp người dùng phân biệt được các loại traffic khác nhau. Ở chế độ mặc định, màu xanh lá cây là **traffic TCP**, xanh da trời đậm là **traffic DNS**, xanh da trời nhạt là **traffic UDP** và màu đen là gói **TCP** đang có vấn đề.



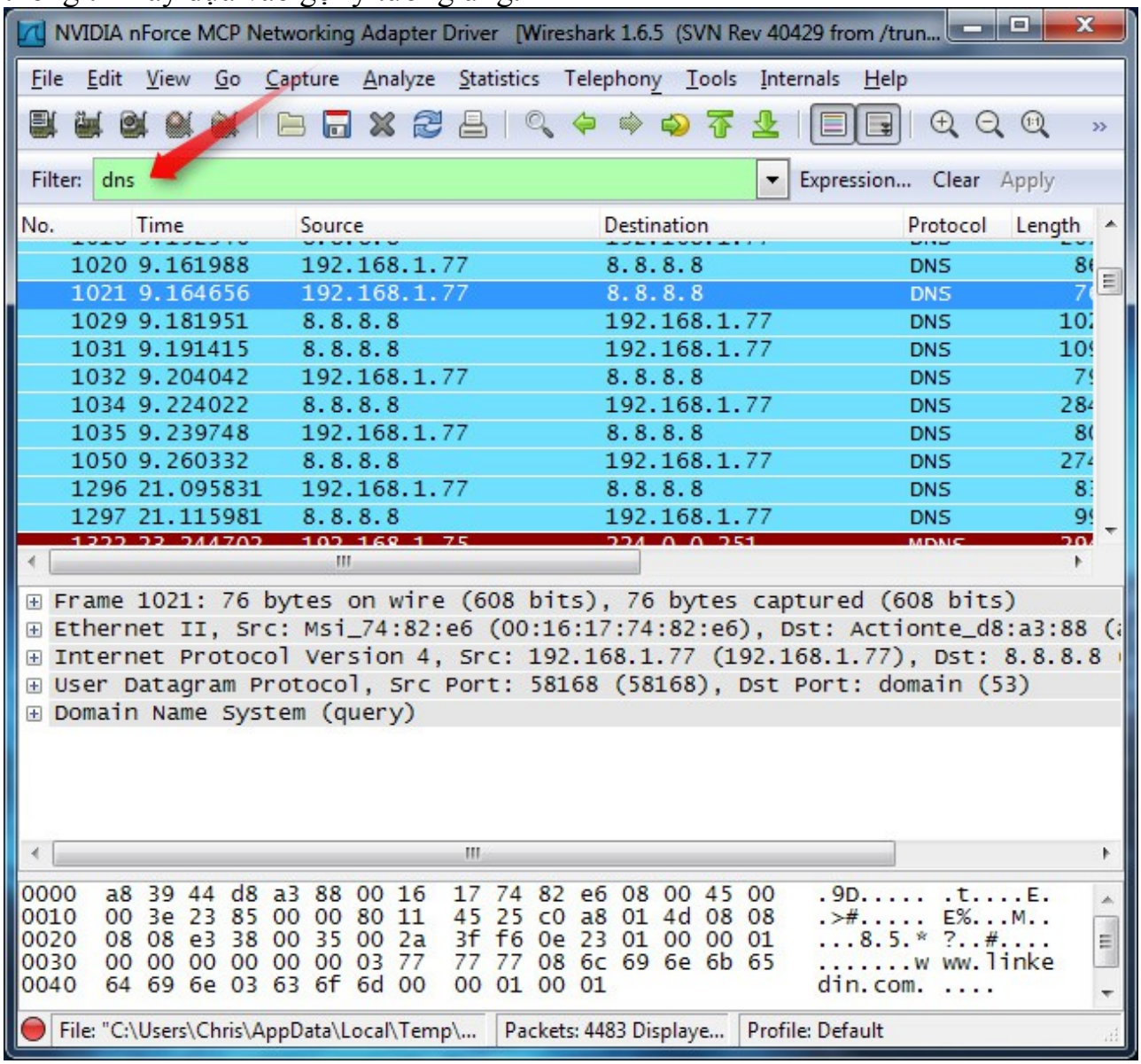
Mở 1 file capture khá dễ dàng, nhấn nút **Open** và trỏ tới file gốc, người dùng còn có thể tự lưu dữ liệu capture trong Wireshark và sử dụng sau đó:



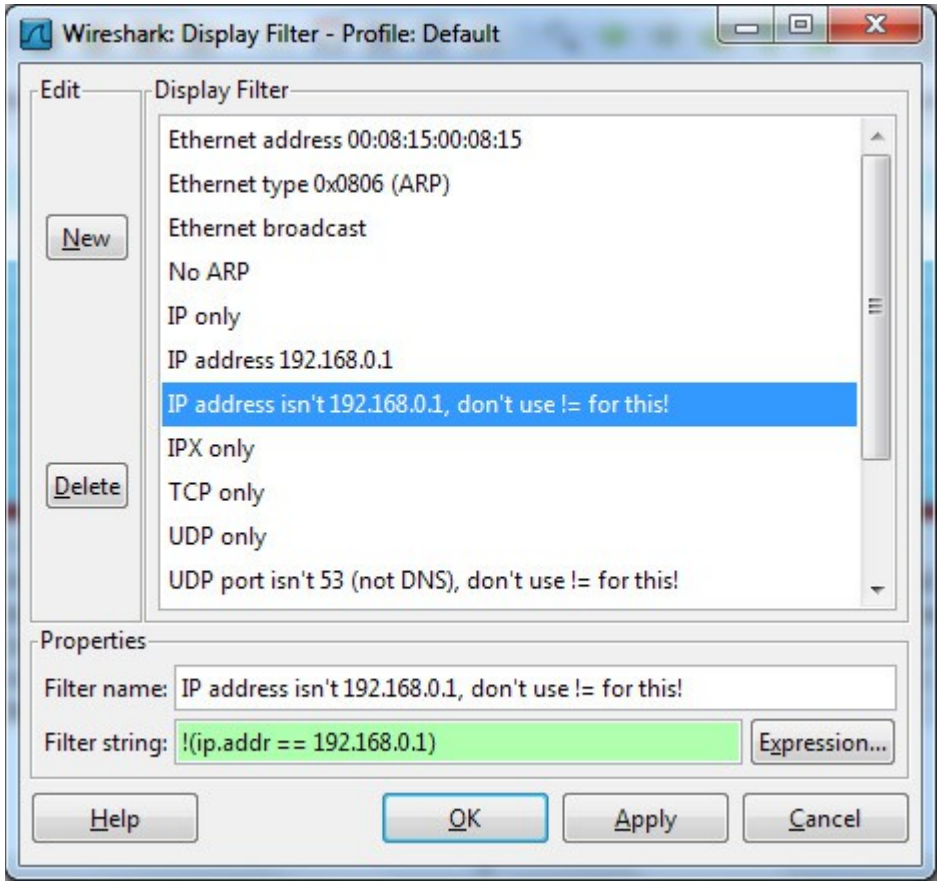
Filtering Packets:

Cách cơ bản nhất để áp dụng filter là nhập thông tin vào ô Filter, sau đó nhấn Apply hoặc nhấn Enter. Ví dụ, nếu gõ dns thì chúng ta sẽ chỉ nhìn thấy các gói dữ liệu DNS. Ngay khi nhập từ khóa, Wireshark sẽ tự động hoàn chỉnh chuỗi

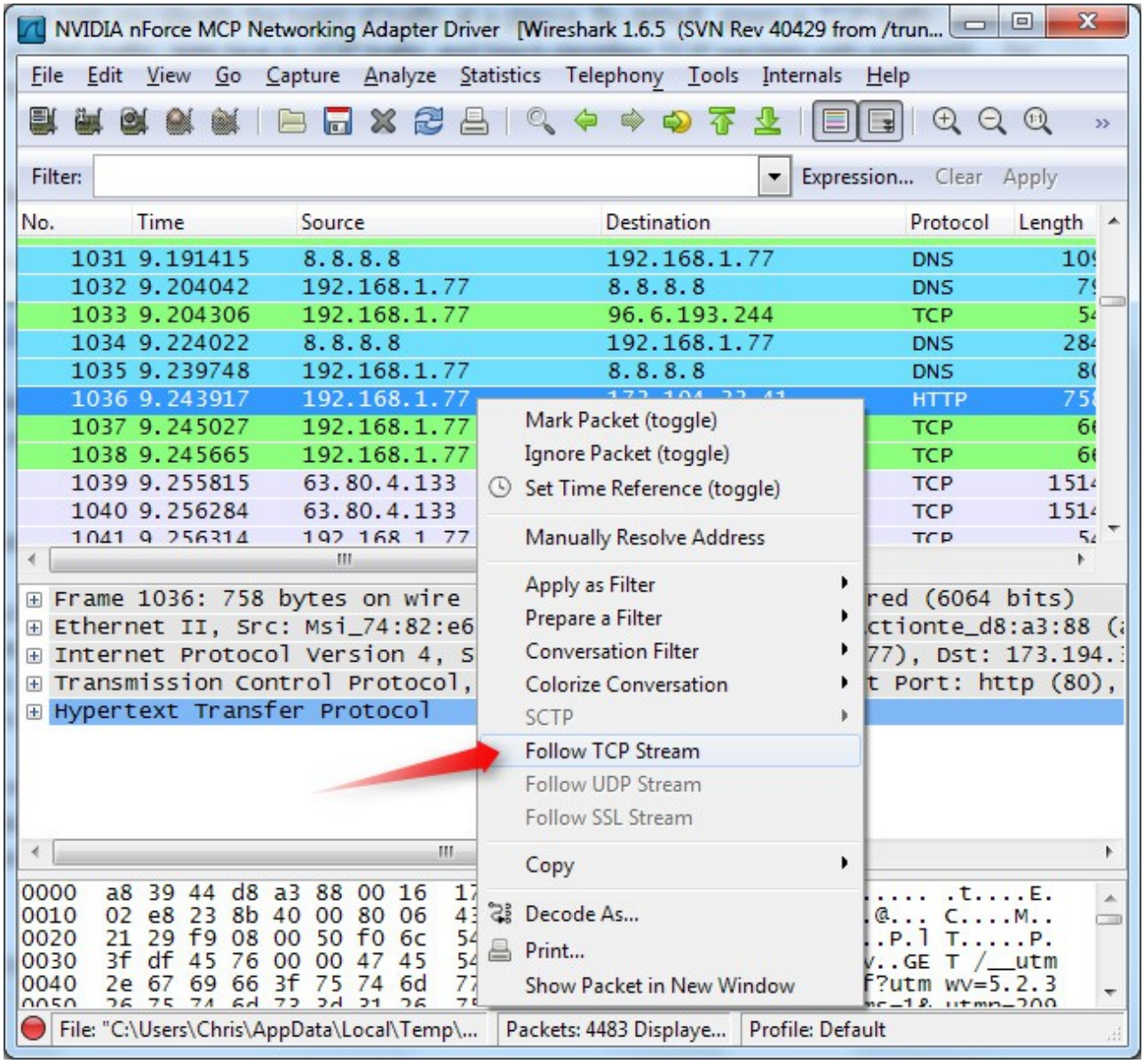
thông tin này dựa vào gợi ý tương ứng.



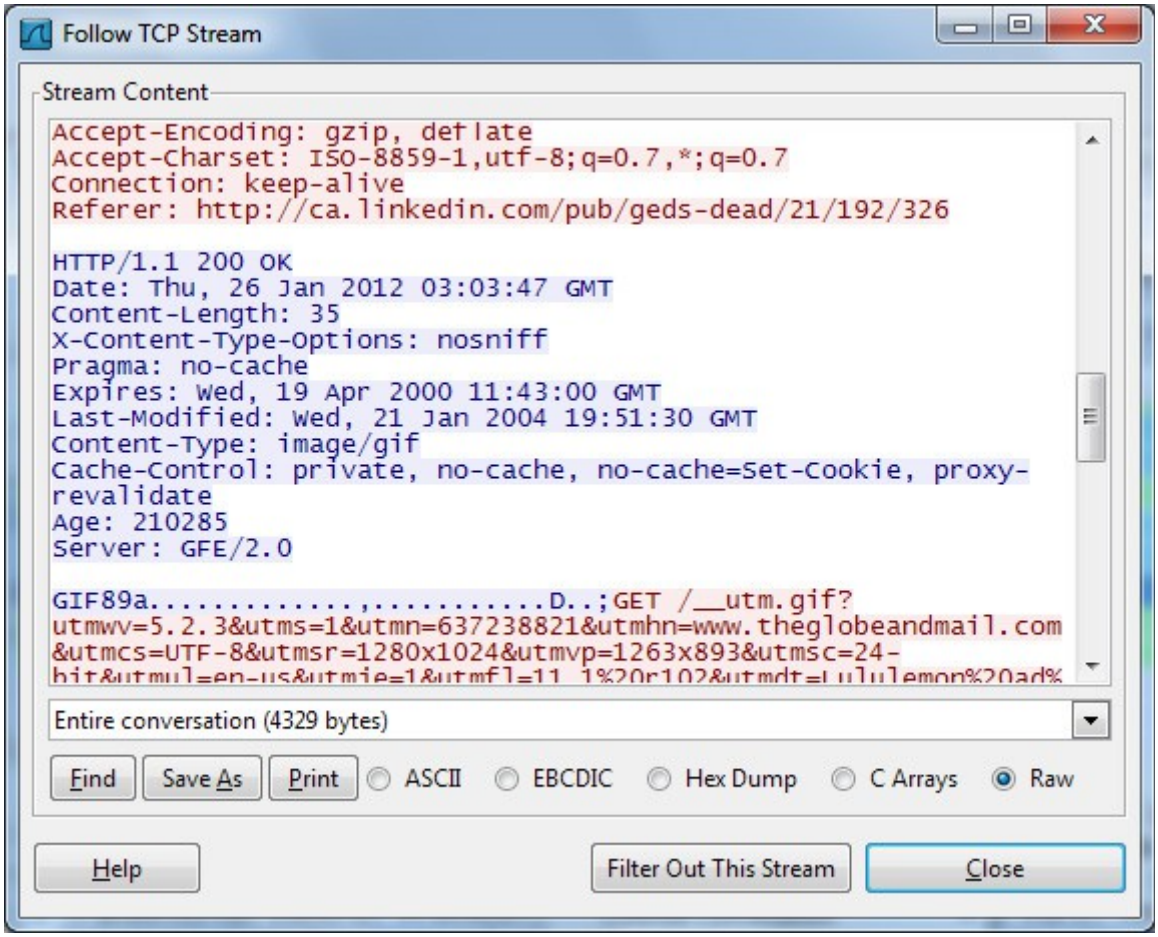
Hoặc nhấn menu Analyze > Display Filters để tạo filter mới:



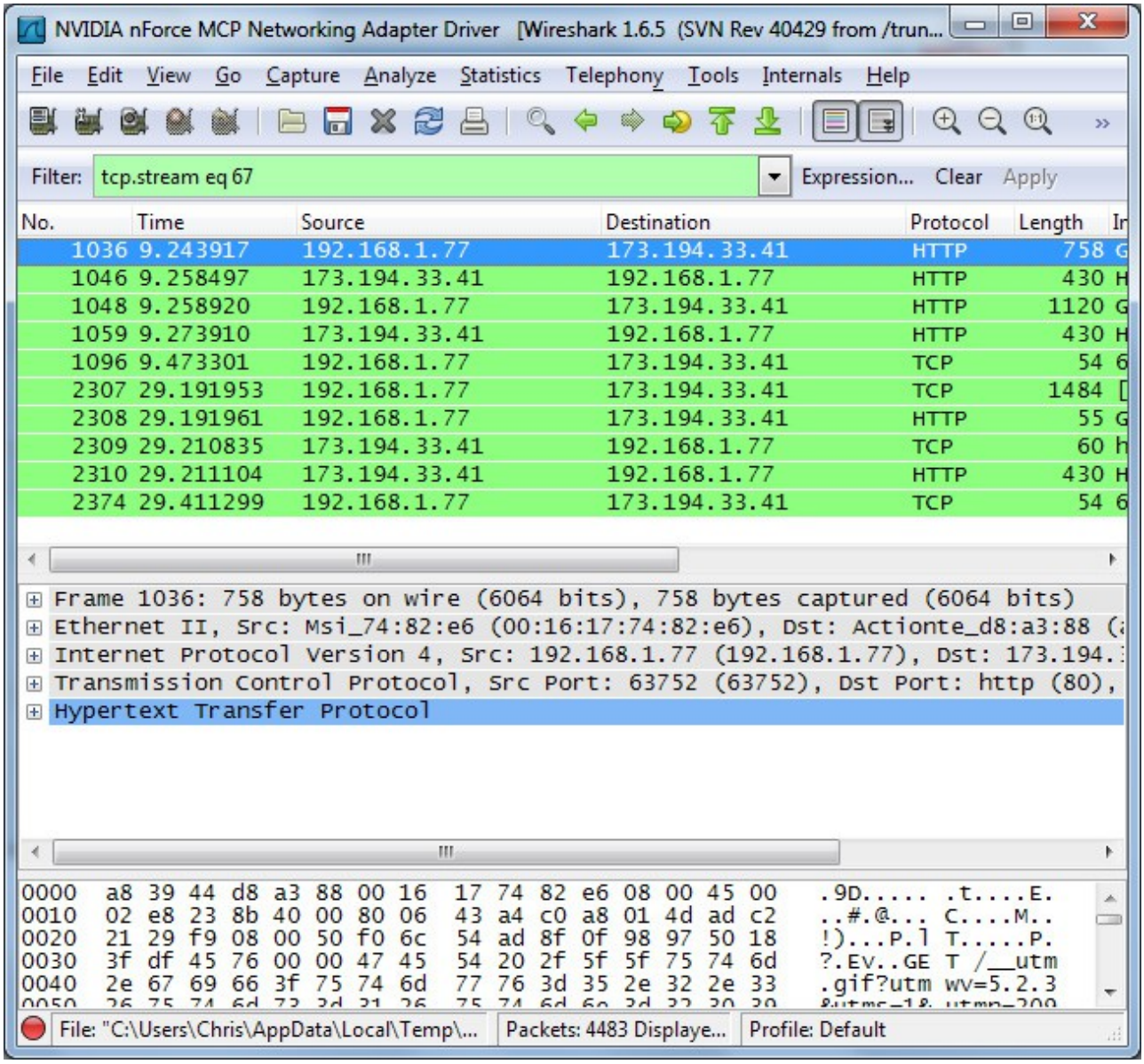
Nhấn chuột phải vào từng package và chọn Follow TCP Stream:



Chúng ta sẽ thấy toàn bộ quãng thời gian giao tiếp giữa server và client:

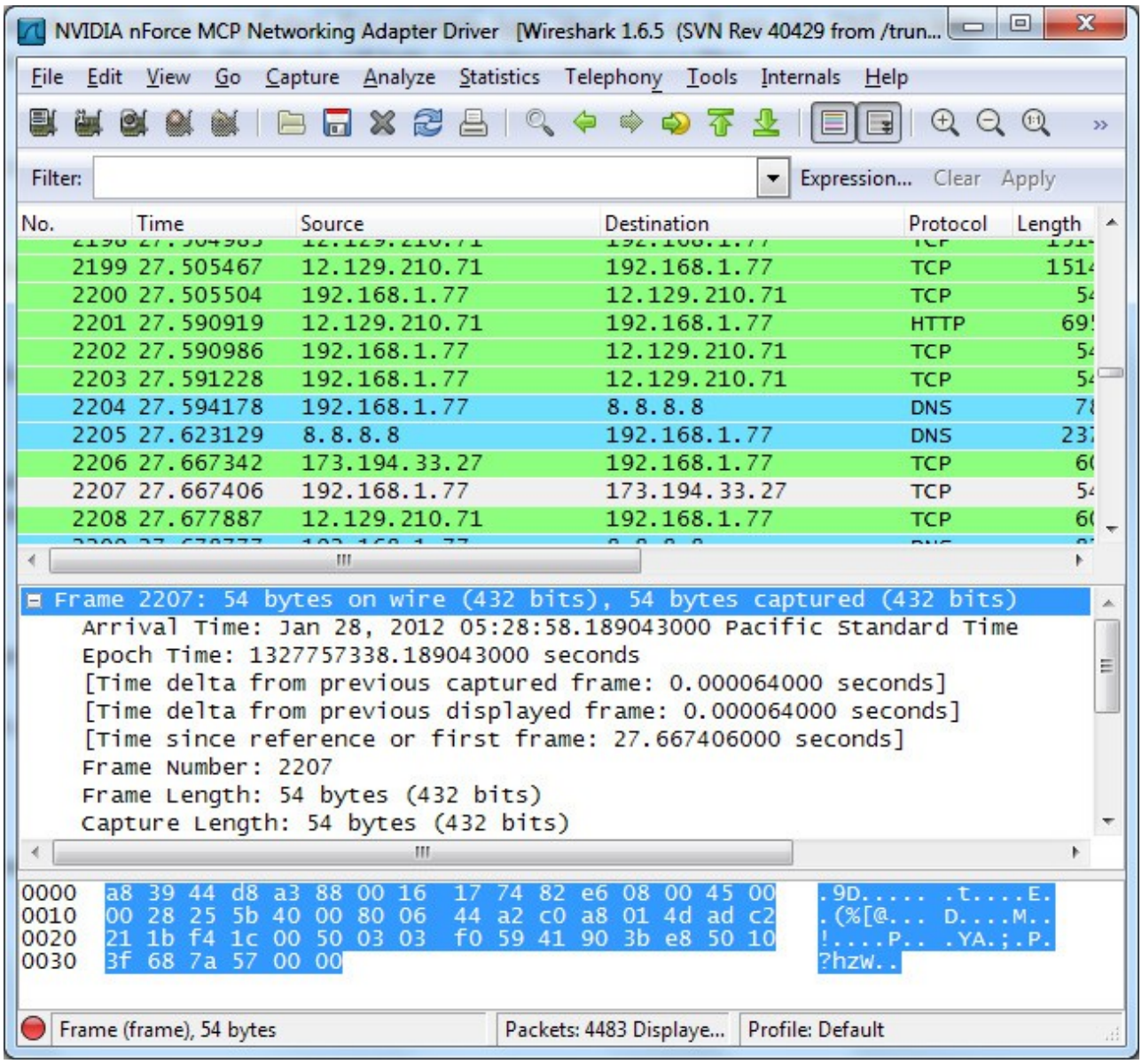


Đóng cửa sổ này lại và filter sẽ tự động được áp dụng, Wireshark tiếp tục hiển thị đầy đủ và chính xác các package có liên quan:

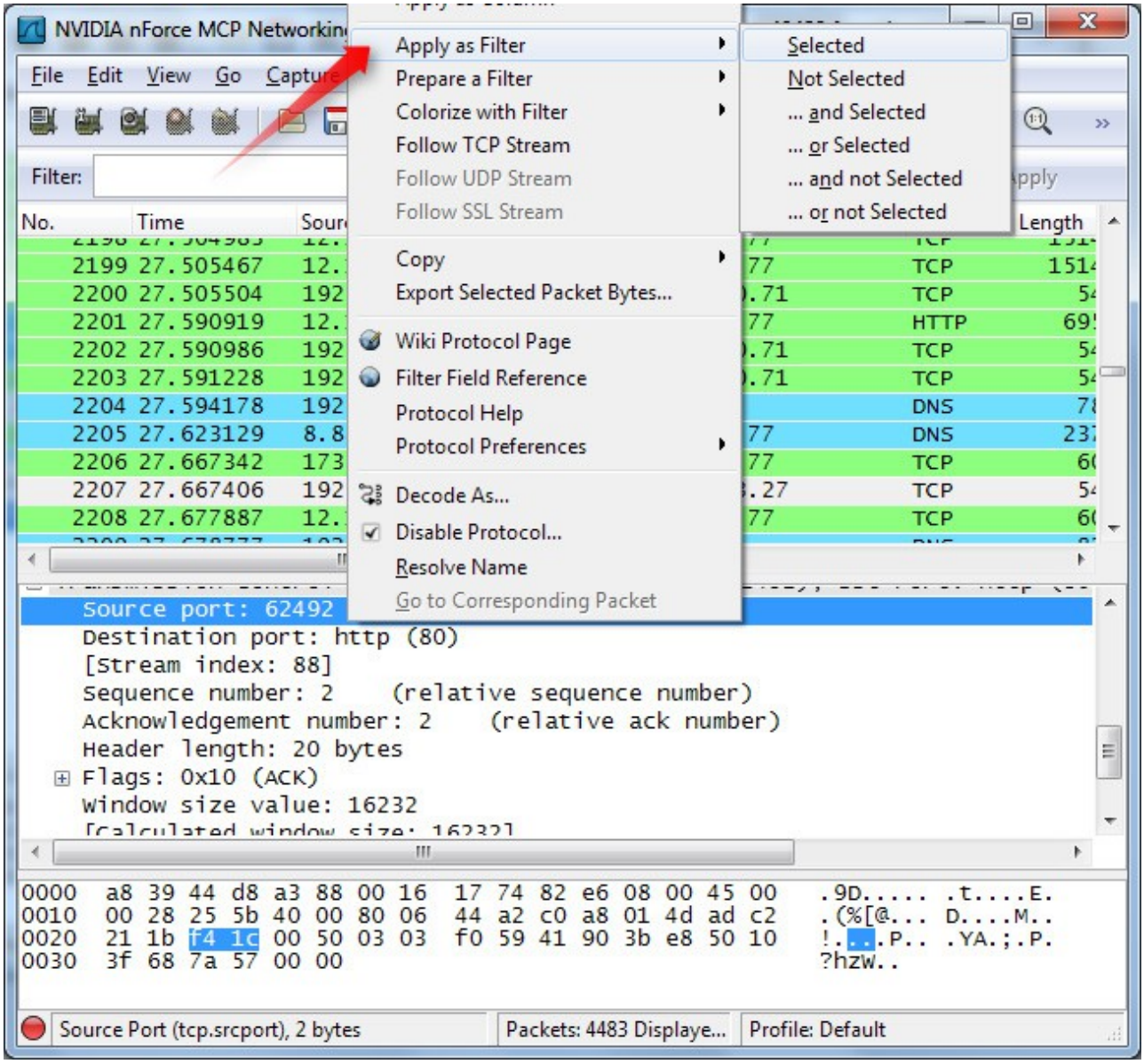

NVIDIA nForce MCP Networking Adapter Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trun...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 67
Expression... Clear Apply
No. Time Source Destination Protocol Length
1036 9.243917 192.168.1.77 173.194.33.41 HTTP 758
1046 9.258497 173.194.33.41 192.168.1.77 HTTP 430
1048 9.258920 192.168.1.77 173.194.33.41 HTTP 1120
1059 9.273910 173.194.33.41 192.168.1.77 HTTP 430
1096 9.473301 192.168.1.77 173.194.33.41 TCP 54
2307 29.191953 192.168.1.77 173.194.33.41 TCP 1484
2308 29.191961 192.168.1.77 173.194.33.41 HTTP 55
2309 29.210835 173.194.33.41 192.168.1.77 TCP 60
2310 29.211104 173.194.33.41 192.168.1.77 HTTP 430
2374 29.411299 192.168.1.77 173.194.33.41 TCP 54
Frame 1036: 758 bytes on wire (6064 bits), 758 bytes captured (6064 bits)
Ethernet II, Src: Msi_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte_d8:a3:88
Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 173.194.
Transmission Control Protocol, Src Port: 63752 (63752), Dst Port: http (80),
Hypertext Transfer Protocol
0000 a8 39 44 d8 a3 88 00 16 17 74 82 e6 08 00 45 00 .9D..... .t....E.
0010 02 e8 23 8b 40 00 80 06 43 a4 c0 a8 01 4d ad c2 ..#.@... C....M..
0020 21 29 f9 08 00 50 f0 6c 54 ad 8f 0f 98 97 50 18 !)...P.l T.....P.
0030 3f df 45 76 00 00 47 45 54 20 2f 5f 5f 75 74 6d ?.Ev..GE T /__utm
0040 2e 67 69 66 3f 75 74 6d 77 76 3d 35 2e 32 2e 33 .gif?utm wv=5.2.3
File: "C:\Users\Chris\AppData\Local\Temp\...
Packets: 4483 Displaye...
Profile: Default

Inspecting Packets:

Nhấn và chọn 1 package bất kỳ để kiểm tra các phần thông tin cụ thể hơn:



Hoặc cũng có thể trực tiếp tạo filter tại đây, nhấn chuột phải vào phần thông tin chi tiết và chọn Apply as Filter để áp dụng:


NVIDIA nForce MCP Networking
File Edit View Go Capture
Filter:
No. Time Source Length
2199 27.505467 TCP 1514
2200 27.505504 TCP 54
2201 27.590919 HTTP 69
2202 27.590986 TCP 54
2203 27.591228 TCP 54
2204 27.594178 DNS 78
2205 27.623129 DNS 237
2206 27.667342 TCP 60
2207 27.667406 TCP 54
2208 27.677887 TCP 60
Apply as Filter
Prepare a Filter
Colorize with Filter
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Export Selected Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Help
Protocol Preferences
Decode As...
Disable Protocol...
Resolve Name
Go to Corresponding Packet
Selected
Not Selected
... and Selected
... or Selected
... and not Selected
... or not Selected
Source port: 62492
Destination port: http (80)
[Stream index: 88]
Sequence number: 2 (relative sequence number)
Acknowledgement number: 2 (relative ack number)
Header length: 20 bytes
Flags: 0x10 (ACK)
Window size value: 16232
0000 a8 39 44 d8 a3 88 00 16 17 74 82 e6 08 00 45 00
0010 00 28 25 5b 40 00 80 06 44 a2 c0 a8 01 4d ad c2
0020 21 1b f4 1c 00 50 03 03 f0 59 41 90 3b e8 50 10
0030 3f 68 7a 57 00 00
Source Port (tcp.srcport), 2 bytes
Packets: 4483 Displaye...
Profile: Default

4.Ứng dụng thử nghiệm

Trường hợp 1

A Lost TCP Connection (mất kết nối TCP)

Một trong các vấn đề phổ biến nhất là mất kết nối mạng.Chúng ta sẽ bỏ qua nguyên nhân tại sao kêt nối bị mất, chúng ta sẽ nhìn hiện tượng đó ở mức gói tin.

Ví dụ:

Một ví truyền file bị mất kết nối:

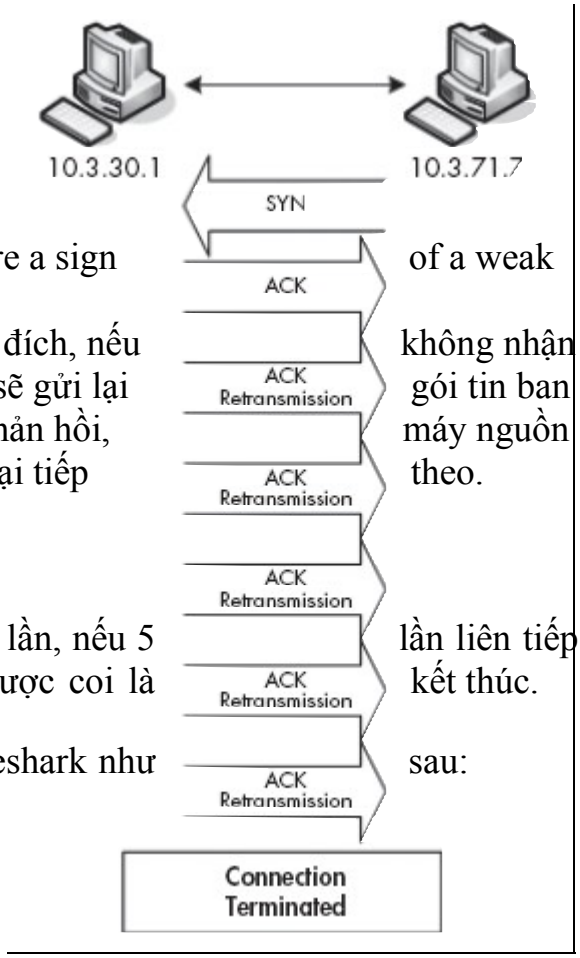
Bắt đầu bằng việc gửi 4 gói TCP ACK từ 10.3.71.7 đến 10.3.30.1.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.3.71.7	10.3.30.1	TCP	1043 > 1048 [ACK] Seq=0 Ack=0 Win=8760 Len
2	0.000000	10.3.30.1	10.3.71.7	TCP	1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Win=
3	0.000000	10.3.71.7	10.3.30.1	TCP	1043 > 1048 [ACK] Seq=0 Ack=2920 Win=8760
4	0.000000	10.3.71.7	10.3.30.1	TCP	1043 > 1048 [ACK] Seq=0 Ack=5840 Win=8760

Hình 3.1-1: This capture begins simply enough with a few ACK packets.

Lỗi bắt đầu từ gói thứ 5, chúng ta nhìn thấy xuất hiện việc gửi lại gói của TCP.

No.	Time	Source	Destination	Protocol	Info
5	0.206000	10.3.30.1	10.3.71.7	TCP	[TCP Retransmission] 1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Wi
6	0.806000	10.3.30.1	10.3.71.7	TCP	[TCP Retransmission] 1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Wi
7	2.006000	10.3.30.1	10.3.71.7	TCP	[TCP Retransmission] 1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Wi
8	4.406000	10.3.30.1	10.3.71.7	TCP	[TCP Retransmission] 1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Wi
9	9.211000	10.3.30.1	10.3.71.7	TCP	[TCP Retransmission] 1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Wi



Hình 3.1-2: These TCP retransmissions are a sign of a weak or dropped connection.

Theo thiết kế, TCP sẽ gửi một gói tin đến đích, nếu không nhận được trả lời sau một khoảng thời gian nó sẽ gửi lại gói tin ban đầu. Nếu vẫn tiếp tục không nhận được phản hồi, máy nguồn sẽ tăng gấp đôi thời gian đợi cho lần gửi lại tiếp theo.

Như ta thấy ở hình trên, TCP sẽ gửi lại 5 lần, nếu 5 lần liên tiếp không nhận được phản hồi thì kết nối được coi là kết thúc.

Hiện tượng này ta có thể thấy trong Wireshark như sau:

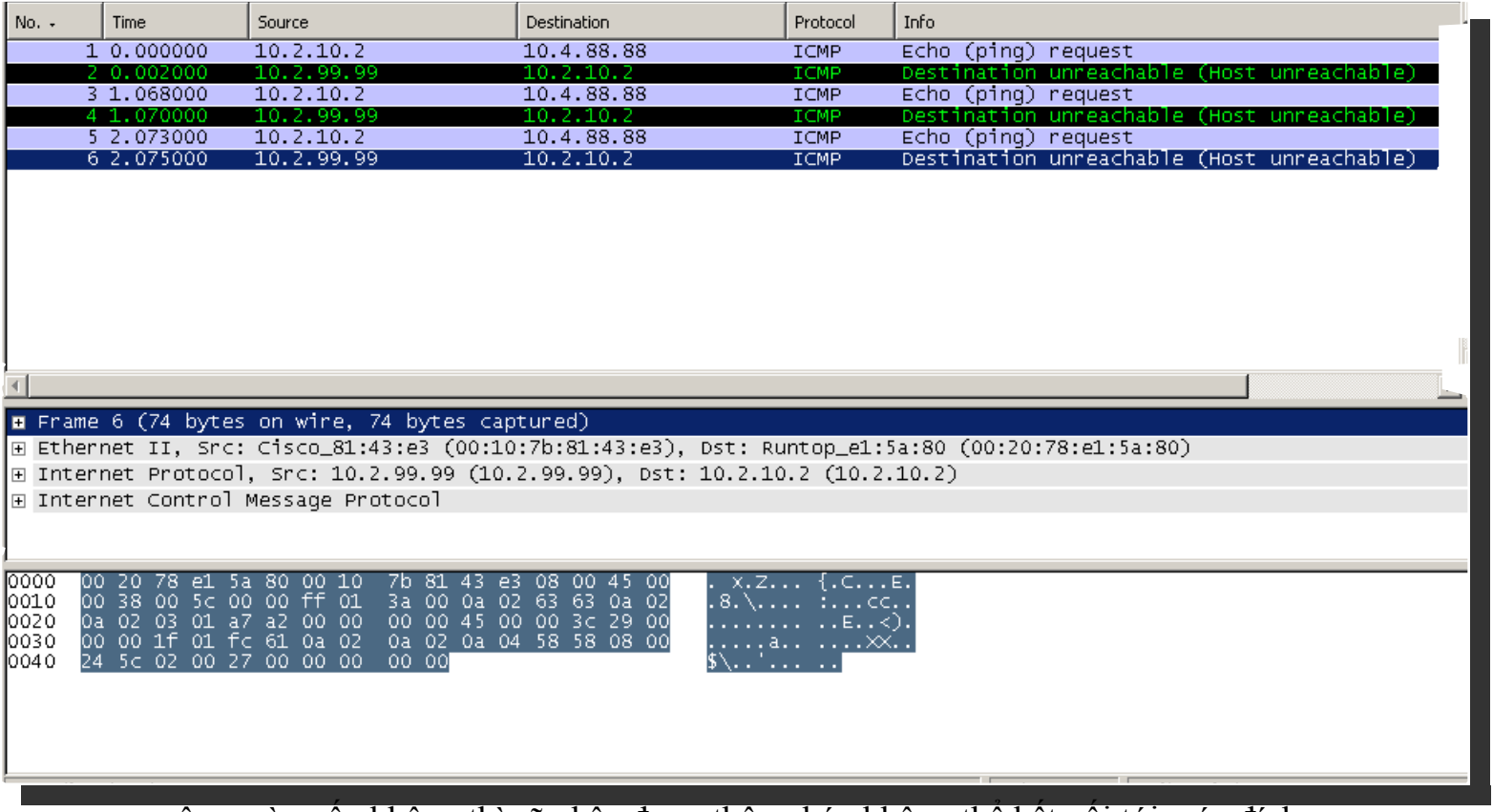
No.	Time	Source	Destination	Protocol	Info
2	0.000000	10.3.30.1	10.3.71.7	TCP	1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Win=8760 Len=648
5	0.206000	10.3.30.1	10.3.71.7	TCP	[TCP Retransmission] 1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Wi
6	0.600000	10.3.30.1	10.3.71.7	TCP	[TCP Retransmission] 1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Wi
7	1.200000	10.3.30.1	10.3.71.7	TCP	[TCP Retransmission] 1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Wi
8	2.400000	10.3.30.1	10.3.71.7	TCP	[TCP Retransmission] 1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Wi
9	4.805000	10.3.30.1	10.3.71.7	TCP	[TCP Retransmission] 1048 > 1043 [PSH, ACK] Seq=5840 Ack=0 Wi

Hình 3.1-4: Windows will retransmit up to five times by default.

Khả năng xác định gói tin bị lỗi đôi khi sẽ giúp chúng ta có thể phát hiện ra mấu trốt mạng bị mất là do đâu.

Unreachable Destinations and ICMP Codes (không thể chạm tới điểm cuối và các mã ICMP)

Một trong các công cụ khi kiểm tra kết nối mạng là công cụ ICMP ping. Nếu may mắn thì phía mục tiêu trả lời lại điều đó có nghĩa là bạn đã ping thành

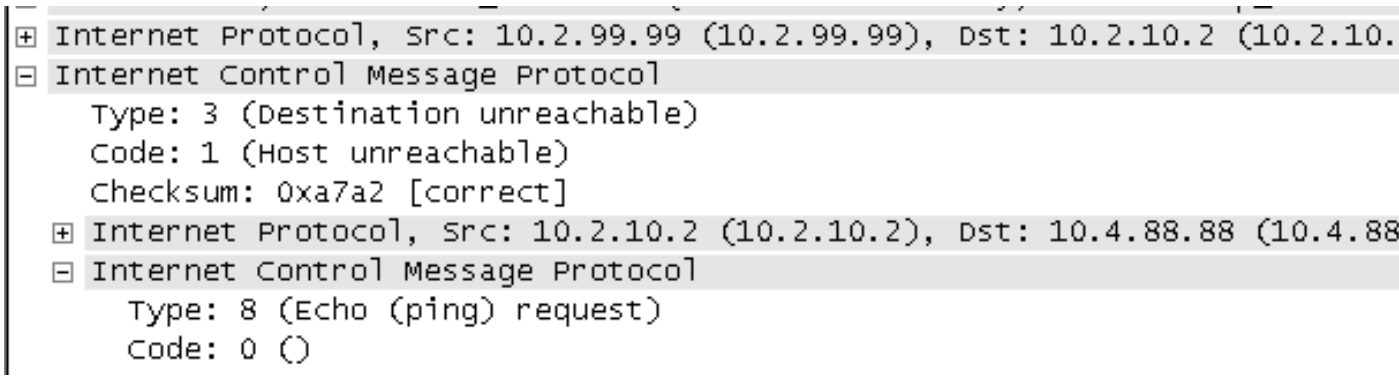


công, còn nếu không thì sẽ nhận được thông báo không thể kết nối tới máy đích. Sử dụng công cụ bắt gói tin trong việc này sẽ cho bạn nhiều thông tin hơn thay vì chỉ dung ICMP ping bình thường. Chúng ta sẽ nhìn rõ hơn các lỗi của ICMP.

Hình 3.1-5: A standard ping request from 10.2.10.2 to 10.4.88.88

Hình dưới đây cho thấy thông báo không thể ping tới 10.4.88.88 từ máy 10.2.99.99.

Như vậy so với ping thông thường thì ta có thể thấy kết nối bị đứt từ 10.2.99.99. Ngoài ra còn có các mã lỗi của ICMP, ví dụ : code 1 (Host unreachable)



Hình 3.1-6: This ICMP type 3 packet is not what we expected.

Unreachable Port (không thể kết nối tới cổng)

Một trong các nhiệm vụ thông thường khác là kiểm tra kết nối tới một cổng trên một máy đích. Việc kiểm tra này sẽ cho thấy cổng cần kiểm tra có mở hay không, có sẵn sang nhận các yêu cầu gửi đến hay không.

Ví dụ, để kiểm tra dịch vụ FTP có chạy trên một server hay không, mặc định FTP sẽ làm việc qua cổng 21 ở chế độ thông thường. Ta sẽ gửi gói tin ICMP đến cổng 21 của máy đích, nếu máy đích trả lời lại gói ICMP loại o và mã lỗi 2 thì có nghĩa là không thể kết nối tới cổng đó.s

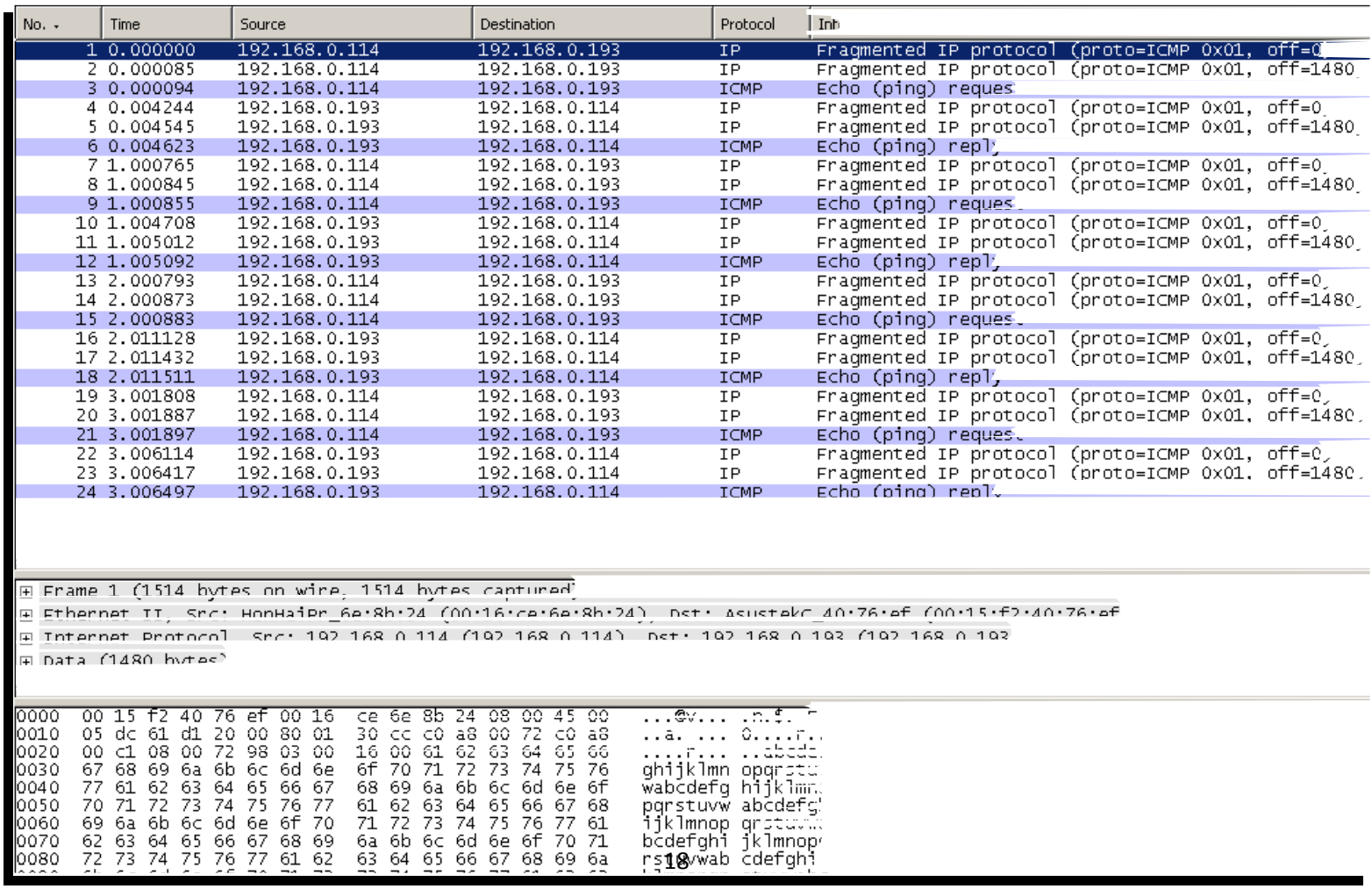
Fragmented **Packets**

Hình 3.1-7: This ping request requires three packets rather than one because the data being transmitted is

above average size.

Ở đây có thể thấy kích thước gói tin ghi nhận được lớn hơn kích thước gói tin mặc định gửi đi khi ping là 32 bytes tới một máy tính chạy Windows.

Kích thước gói tin ở đây là 3,072 bytes.



Trường hợp 2

Determining Whether a Packet Is Fragmented (xác định vị trí gói tin bị phân đoạn)

No Connectivity (không kết nối)

Vấn đề : chúng ta có 2 nhân viên mới Hải và Thanh và được sắp ngồi cạnh nhau và đương nhiên là được trang bị 2 máy tính. Sauk hi được trang bị và làm các thao tác để đưa 2 máy tính vào mạng, có một vấn đề xảy ra là máy tính của Hải chạy tốt, kết nối mạng bình thường, máy tính của Thanh không thể truy nhập Internet.

Mục tiêu : tìm hiểu tại sao máy tính của Thanh không kết nối được Internet và sửa lỗi đó.

Các thông tin chúng ta có

- cả 2 máy tính đều mới
- cả 2 máy đều được đặt IP và có thể ping đến các máy khác trong mạng

Nói tóm lại là 2 máy này được cấu hình không có gì khác nhau.

Tiến hành

Cài đặt Wireshark trực tiếp lên cả 2 máy.

Phân tích

Trước hết trên máy của Hải ta nhìn thấy một phiên làm việc bình thường với HTTP. Đầu tiên sẽ có một ARP broadcast để tìm địa chỉ của gateway ở tầng 2, ở đây là 192.168.0.10. Khi máy tính của Hải nhận được thông tin nó sẽ bắt tay với máy gateway và từ đó có phiên làm việc với HTTP ra bên ngoài.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Microsof_2a:45:d2	Broadcast	ARP	Who has 192.168.0.10? Tell 192.168.0.183
2	0.002196	D-Link_21:99:4c	Microsof_2a:45:d2	ARP	192.168.0.10 is at 00:05:5d:21:99:4c
3	0.002259	192.168.0.183	64.233.161.104	TCP	hpvmmagent > http [SYN] Seq=0 Win=65535 Len=0 MSS=1
4	0.054708	64.233.161.104	192.168.0.183	TCP	http > hpvmmagent [SYN, ACK] Seq=0 Ack=1 Win=8190 L
5	0.054871	192.168.0.183	64.233.161.104	TCP	hpvmmagent > http [ACK] Seq=1 Ack=1 Win=65535 Len=(
6	0.055737	192.168.0.183	64.233.161.104	HTTP	GET / HTTP/1.1
7	0.103969	64.233.161.104	192.168.0.183	TCP	http > hpvmmagent [ACK] Seq=1 Ack=284 Win=6432 Len=
8	0.158478	64.233.161.104	192.168.0.183	TCP	[TCP segment of a reassembled PDU]
9	0.161865	64.233.161.104	192.168.0.183	HTTP	HTTP/1.1 200 OK (text/html)
10	0.162010	192.168.0.183	64.233.161.104	TCP	hpvmmagent > http [ACK] Seq=284 Ack=2759 Win=65535
11	0.172422	192.168.0.183	64.233.161.104	HTTP	GET /intl/en_ALL/images/logo.gif HTTP/1.1
12	0.175990	192.168.0.183	64.233.161.104	TCP	hpvmmdata > http [SYN] Seq=0 Win=65535 Len=0 MSS=14

Hình 3.1-8: Hải's computer completes a handshake, and then HTTP data transfer begins.

Trường hợp máy tính của Thanh

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Microsof_2a:45:d2	Broadcast	ARP	Who has 192.168.0.11? Tell 192.168.0.122
2	1.271630	192.168.0.122	192.168.0.255	BROWSER	Request Announcement TESLA-MARKETING
3	2.424840	192.168.0.122	192.168.0.255	BROWSER	Host Announcement TESLA-MARKETING, Worksta
4	2.425448	192.168.0.122	192.168.0.255	BROWSER	Host Announcement TESLA-MARKETING, Worksta
5	2.774125	192.168.0.122	192.168.0.255	BROWSER	Request Announcement TESLA-MARKETING

Hình 3.1-9: Thanh's computer appears to be sending an ARP request to a different IP address.

Hình trên cho thấy yêu cầu ARP không giống như trường hợp ở trên. Địa chỉ gateway được trả về là 192.168.0.11.

Như vậy có thể thấy NetBIOS có vấn đề.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Microsof_2a:45:d2	Broadcast	ARP	Who has 192.168.0.11? Tell 1
2	1.271630	192.168.0.122	192.168.0.255	BROWSER	Request Announcement TESLA-MA
3	2.424840	192.168.0.122	192.168.0.255	BROWSER	Host Announcement TESLA-MARKE
4	2.425448	192.168.0.122	192.168.0.255	BROWSER	Host Announcement TESLA-MARKE
5	2.774125	192.168.0.122	192.168.0.255	BROWSER	Request Announcement TESLA-MA

```
⊞ Frame 2 (228 bytes on wire, 228 bytes captured)
⊞ Ethernet II, Src: Microsof_2a:45:d2 (00:03:ff:2a:45:d2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 192.168.0.122 (192.168.0.122), Dst: 192.168.0.255 (192.168.0.255)
⊞ User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)
⊟ NetBIOS Datagram Service
    Message Type: Direct_group datagram (17)
    More fragments follow: No
    This is first fragment: Yes
    Node Type: B node (0)
    Datagram ID: 0x8050
    Source IP: 192.168.0.122 (192.168.0.122)
    Source Port: 138
    Datagram length: 172 bytes
    Packet offset: 0 bytes
    Source name: TESLA-MARKETING<00> (Workstation/Redirector)
    Destination name: TESLA<1d> (Local Master Browser)
⊞ SMB (Server Message Block Protocol)
⊞ SMB MailSlot Protocol
⊞ Microsoft Windows Browser Protocol
```

NetBIOS là giao thức cũ nó sẽ được thay thế TCP/IP khi TCP/IP không hoạt động. Như vậy là máy của Thanh không thể kết nối Internet với TCP/IP.

Chi tiết yêu cầu ARP trên 2 máy :

Máy Hải

```
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: Microsof_2a:45:d2 (00:03:ff:2a:45:d2)
    Sender IP address: 192.168.0.183 (192.168.0.183)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.10 (192.168.0.10)
```

Máy Thanh

```
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: Microsof_2a:45:d2 (00:03:ff:2a:45:d2)
    Sender IP address: 192.168.0.122 (192.168.0.122)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.11 (192.168.0.11)
```

Kết luận : máy Thanh đặt sai địa chỉ gateway nên không thể kết nối Internet, cần đặt lại là 192.168.0.10.

Trường hợp 3

The Ghost in Internet Explorer (con ma trong trình duyệt IE)

Hiện tượng : máy tính của A có hiện tượng như sau, khi sử dụng trình duyệt IE, trình duyệt tự động trỏ đến rất nhiều trang quảng cáo. Khi A thay đổi bằng tay thì vẫn bị hiện tượng đó thậm chí khở động lại máy cũng vẫn bị như thế.

Thông tin chúng ta có

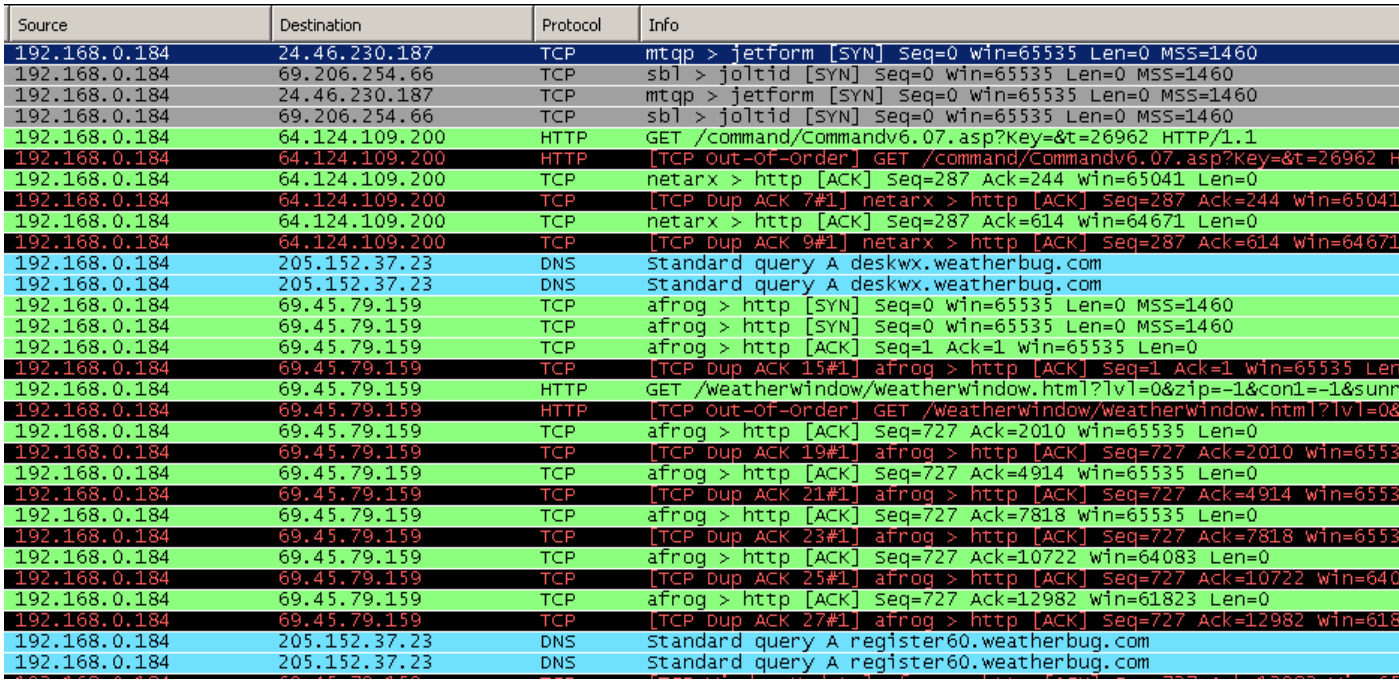
- A không thạo về máy tính lắm
- Máy tính của A dùng Widows XP, IE 6

Tiến hành

Vì hiện tượng này chỉ xảy ra trên máy của A và trang home page của A bị thay đổi khi bật IE nên chúng ta sẽ tiếp hành bắt gói tin từ máy của A. Chúng ta không nhất thiết phải cài Wireshark trực tiếp từ máy của A. Chúng ta có thể dùng kỹ thuật

“Hubbing Out” .

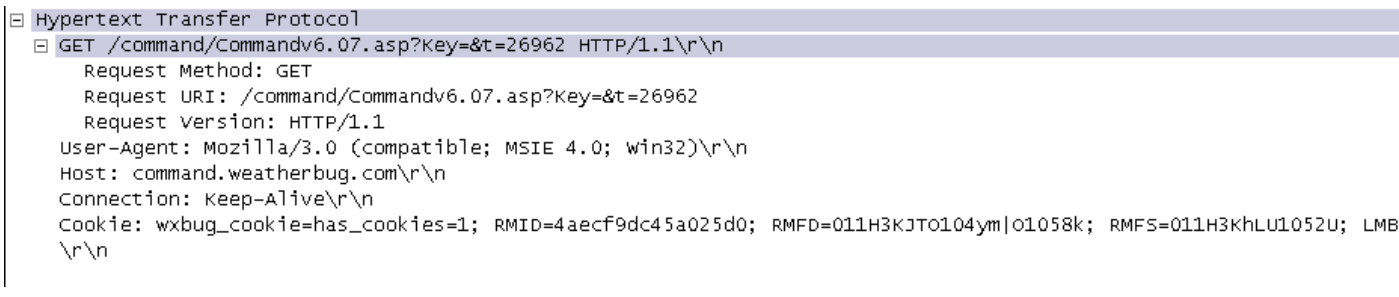
Phân tích



Source	Destination	Protocol	Info
192.168.0.184	24.46.230.187	TCP	mtqp > jetform [SYN] Seq=0 Win=65535 Len=0 MSS=1460
192.168.0.184	69.206.254.66	TCP	sbl > joltid [SYN] Seq=0 Win=65535 Len=0 MSS=1460
192.168.0.184	24.46.230.187	TCP	mtqp > jetform [SYN] Seq=0 Win=65535 Len=0 MSS=1460
192.168.0.184	69.206.254.66	TCP	sbl > joltid [SYN] Seq=0 Win=65535 Len=0 MSS=1460
192.168.0.184	64.124.109.200	HTTP	GET /command/Commandv6.07.asp?Key=&t=26962 HTTP/1.1
192.168.0.184	64.124.109.200	HTTP	[TCP Out-Of-Order] GET /command/Commandv6.07.asp?Key=&t=26962 H
192.168.0.184	64.124.109.200	TCP	netarx > http [ACK] Seq=287 Ack=244 Win=65041 Len=0
192.168.0.184	64.124.109.200	TCP	[TCP Dup ACK 7#1] netarx > http [ACK] Seq=287 Ack=244 Win=65041
192.168.0.184	64.124.109.200	TCP	netarx > http [ACK] Seq=287 Ack=614 Win=64671 Len=0
192.168.0.184	64.124.109.200	TCP	[TCP Dup ACK 9#1] netarx > http [ACK] Seq=287 Ack=614 Win=64671
192.168.0.184	205.152.37.23	DNS	Standard query A deskwx.weatherbug.com
192.168.0.184	205.152.37.23	DNS	Standard query A deskwx.weatherbug.com
192.168.0.184	69.45.79.159	TCP	afrog > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
192.168.0.184	69.45.79.159	TCP	afrog > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
192.168.0.184	69.45.79.159	TCP	afrog > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
192.168.0.184	69.45.79.159	TCP	[TCP Dup ACK 15#1] afrog > http [ACK] Seq=1 Ack=1 Win=65535 Len
192.168.0.184	69.45.79.159	HTTP	GET /WeatherWindow/WeatherWindow.html?lvl=0&zip=-1&con1=-1&sunr
192.168.0.184	69.45.79.159	HTTP	[TCP Out-Of-Order] GET /WeatherWindow/WeatherWindow.html?lvl=0&
192.168.0.184	69.45.79.159	TCP	afrog > http [ACK] Seq=727 Ack=2010 Win=65535 Len=0
192.168.0.184	69.45.79.159	TCP	[TCP Dup ACK 19#1] afrog > http [ACK] Seq=727 Ack=2010 Win=6553
192.168.0.184	69.45.79.159	TCP	afrog > http [ACK] Seq=727 Ack=4914 Win=65535 Len=0
192.168.0.184	69.45.79.159	TCP	[TCP Dup ACK 21#1] afrog > http [ACK] Seq=727 Ack=4914 Win=6553
192.168.0.184	69.45.79.159	TCP	afrog > http [ACK] Seq=727 Ack=7818 Win=65535 Len=0
192.168.0.184	69.45.79.159	TCP	[TCP Dup ACK 23#1] afrog > http [ACK] Seq=727 Ack=7818 Win=6553
192.168.0.184	69.45.79.159	TCP	afrog > http [ACK] Seq=727 Ack=10722 Win=64083 Len=0
192.168.0.184	69.45.79.159	TCP	[TCP Dup ACK 25#1] afrog > http [ACK] Seq=727 Ack=10722 Win=640
192.168.0.184	69.45.79.159	TCP	afrog > http [ACK] Seq=727 Ack=12982 Win=61823 Len=0
192.168.0.184	69.45.79.159	TCP	[TCP Dup ACK 27#1] afrog > http [ACK] Seq=727 Ack=12982 Win=618
192.168.0.184	205.152.37.23	DNS	Standard query A register60.weatherbug.com
192.168.0.184	205.152.37.23	DNS	Standard query A register60.weatherbug.com

Hình 3.1-13: Since there is no user interaction happening on A’s computer at the time of this capture, all of these packets going across the wire should set off some alarms.

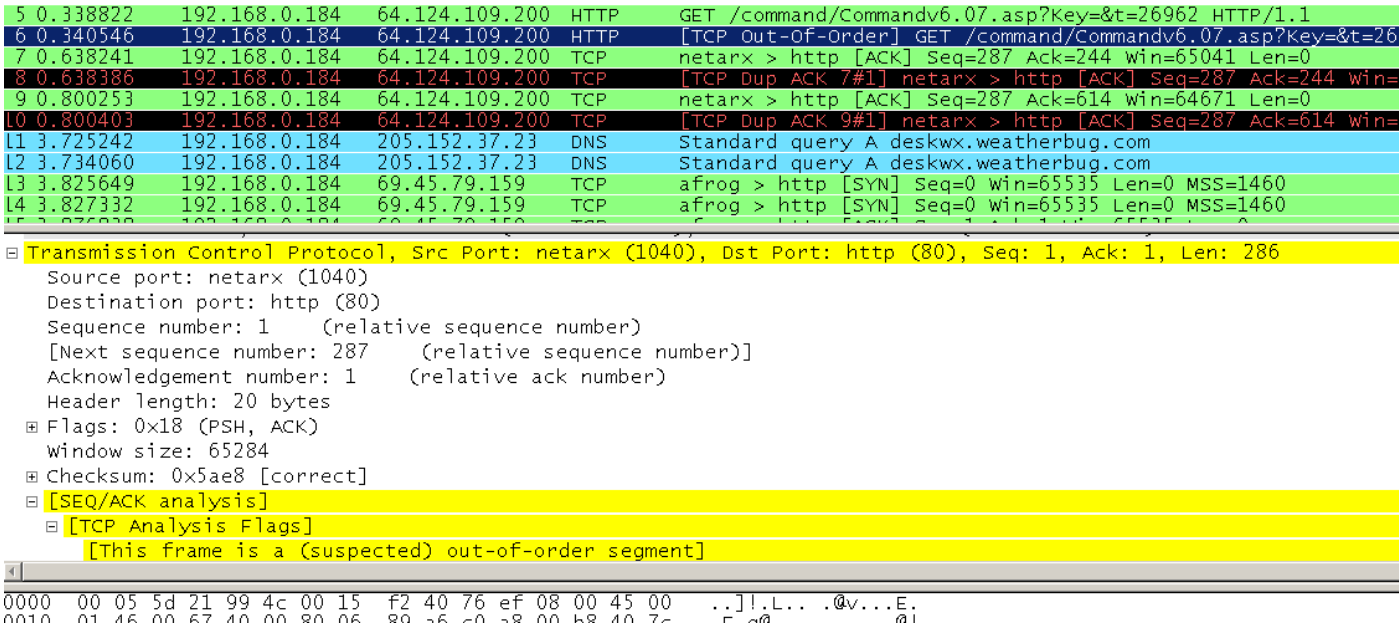
Chi tiết gói tin thứ 5:



```
⊟ Hypertext Transfer Protocol
  ⊟ GET /command/Commandv6.07.asp?Key=&t=26962 HTTP/1.1\r\n
      Request Method: GET
      Request URI: /command/Commandv6.07.asp?Key=&t=26962
      Request Version: HTTP/1.1
    User-Agent: Mozilla/3.0 (compatible; MSIE 4.0; Win32)\r\n
    Host: command.weatherbug.com\r\n
    Connection: Keep-Alive\r\n
    Cookie: wxbug_cookie=has_cookies=1; RMID=4aecf9dc45a025d0; RMFD=011H3KJTO104ym|01058k; RMFS=011H3KhLU1052U; LMB
    \r\n
```

Hình 3.1-14: Looking more closely at packet 5, we see it is trying to download data from the Internet.

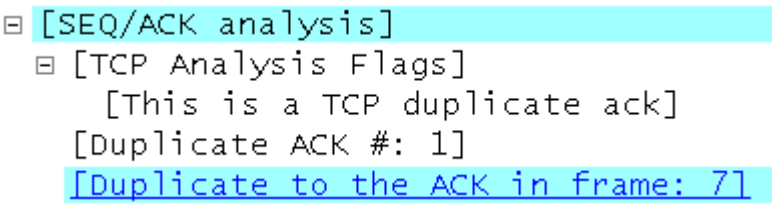
Từ máy tính gửi yêu cầu GET của HTTP đến địa chỉ như trên hình.



Hình 3.1-15: A DNS query to the weatherbug.com domain gives a clue to the culprit.

Gói tin trả lại bắt đầu có vấn đề : thứ tự các phần bị thay đổi.

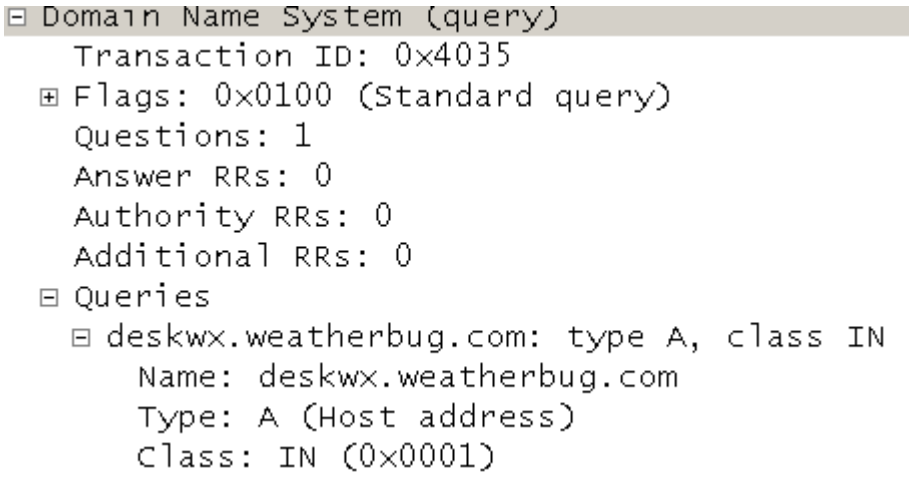
Một số gói tiếp theo có sự lặp ACK.



Hình 3.1-16: A DNS query to the weatherbug.com domain gives a clue to the culprit.

Sau một loạt các thay đổi trên thì có truy vấn DNS đến deskwx.weatherbug.com

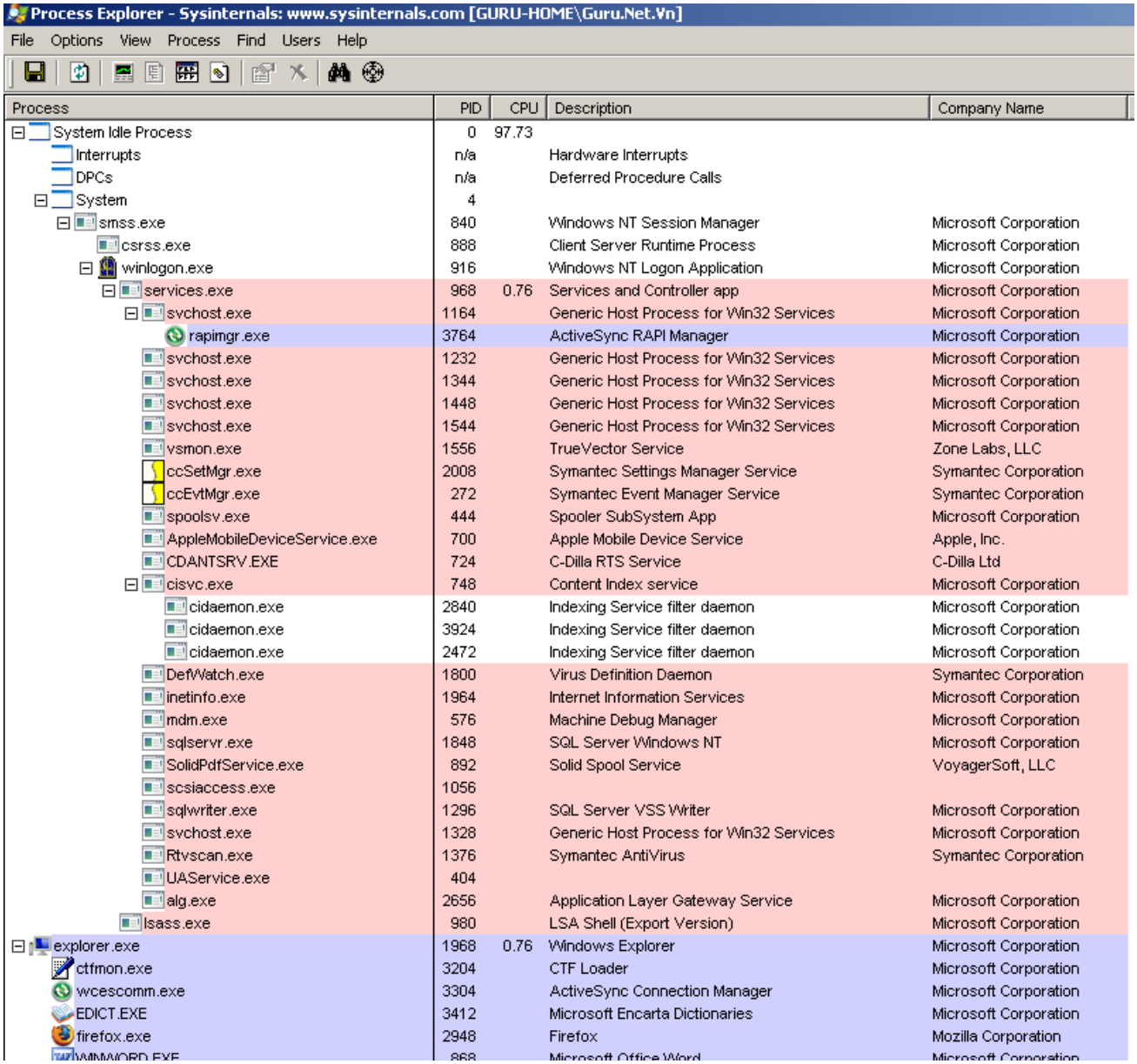
Đây là địa chỉ A không hề biết và không có ý định truy cập.



Như vậy có thể là có một process nào đó đã làm thay đổi địa chỉ trang chủ mỗi khi IE được bật lên. Dùng một công cụ kiểm tra process ẩn ví dụ như Process Explore và thấy rằng có tiến trình weatherbug.exe đang chạy. Sau khi tắt tiến trình này đi không còn hiện tượng trên nữa.

Thông thường các tiến trình như weatherbug có thể là virus, spyware.

Giao diện Process Explore



Process	PID	CPU	Description	Company Name
System Idle Process	0	97.73		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4			
smss.exe	840		Windows NT Session Manager	Microsoft Corporation
csrss.exe	888		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	916		Windows NT Logon Application	Microsoft Corporation
services.exe	968	0.76	Services and Controller app	Microsoft Corporation
svchost.exe	1164		Generic Host Process for Win32 Services	Microsoft Corporation
rapimgr.exe	3764		ActiveSync RAPI Manager	Microsoft Corporation
svchost.exe	1232		Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	1344		Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	1448		Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	1544		Generic Host Process for Win32 Services	Microsoft Corporation
vsmon.exe	1556		TrueVector Service	Zone Labs, LLC
ccSetMgr.exe	2008		Symantec Settings Manager Service	Symantec Corporation
ccEvtMgr.exe	272		Symantec Event Manager Service	Symantec Corporation
spoolsv.exe	444		Spooler SubSystem App	Microsoft Corporation
AppleMobileDeviceService.exe	700		Apple Mobile Device Service	Apple, Inc.
CDANTSRV.EXE	724		C-Dilla RTS Service	C-Dilla Ltd
cisvc.exe	748		Content Index service	Microsoft Corporation
cidaemon.exe	2840		Indexing Service filter daemon	Microsoft Corporation
cidaemon.exe	3924		Indexing Service filter daemon	Microsoft Corporation
cidaemon.exe	2472		Indexing Service filter daemon	Microsoft Corporation
DefWatch.exe	1800		Virus Definition Daemon	Symantec Corporation
inetinfo.exe	1964		Internet Information Services	Microsoft Corporation
mdm.exe	576		Machine Debug Manager	Microsoft Corporation
sqlservr.exe	1848		SQL Server Windows NT	Microsoft Corporation
SolidPdfService.exe	892		Solid Spool Service	VoyagerSoft, LLC
scsiaccess.exe	1056			
sqlwriter.exe	1296		SQL Server VSS Writer	Microsoft Corporation
svchost.exe	1328		Generic Host Process for Win32 Services	Microsoft Corporation
Rtvscan.exe	1376		Symantec AntiVirus	Symantec Corporation
UAService.exe	404			
alg.exe	2656		Application Layer Gateway Service	Microsoft Corporation
lsass.exe	980		LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	1968	0.76	Windows Explorer	Microsoft Corporation
ctfmon.exe	3204		CTF Loader	Microsoft Corporation
wcescomm.exe	3304		ActiveSync Connection Manager	Microsoft Corporation
EDICT.EXE	3412		Microsoft Encarta Dictionaries	Microsoft Corporation
firefox.exe	2948		Firefox	Mozilla Corporation
WINWORD.EXE	868		Microsoft Office Word	Microsoft Corporation

Trường hợp 4

Lỗi kết nối FTP

Tình huống : có tài khoản FTP trên Windows Server 2003 đã update service packs vừa cài đặt xong, phần mềm FTP Server hoàn toàn bình thường, khoản đúng nhưng không truy nhập được.

Thông tin chúng ta có

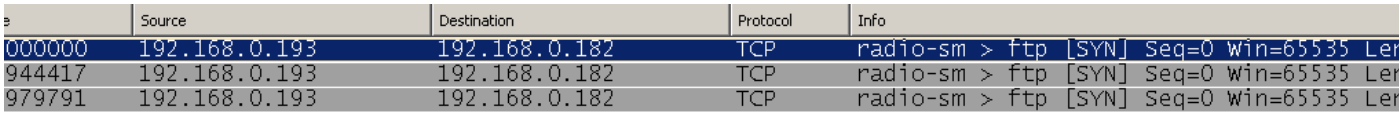
- FTP làm việc trên cổng 21

Tiến hành

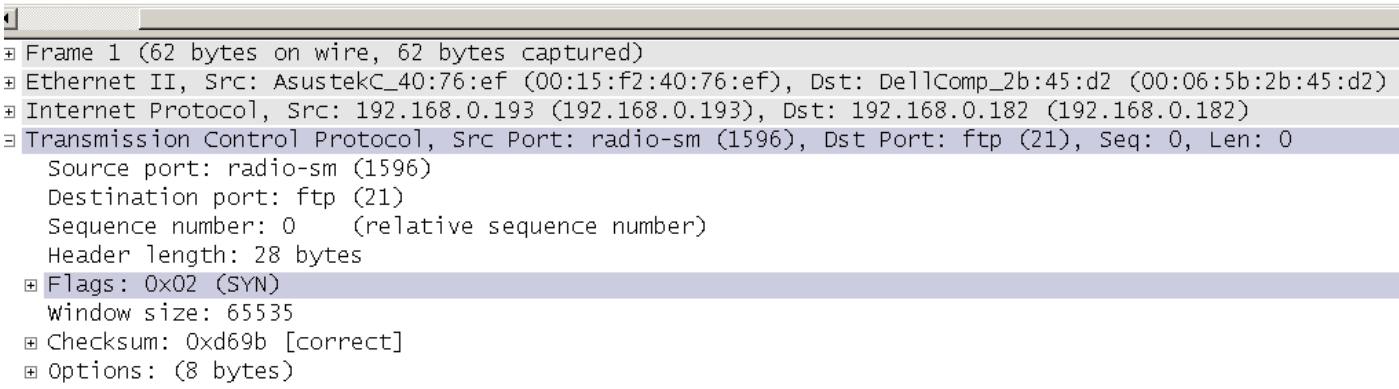
Cài đặt Wireshark trên cả 2 máy.

Phân tích

Client:



	Source	Destination	Protocol	Info
000000	192.168.0.193	192.168.0.182	TCP	radio-sm > ftp [SYN] Seq=0 Win=65535 Len
944417	192.168.0.193	192.168.0.182	TCP	radio-sm > ftp [SYN] Seq=0 Win=65535 Len
979791	192.168.0.193	192.168.0.182	TCP	radio-sm > ftp [SYN] Seq=0 Win=65535 Len



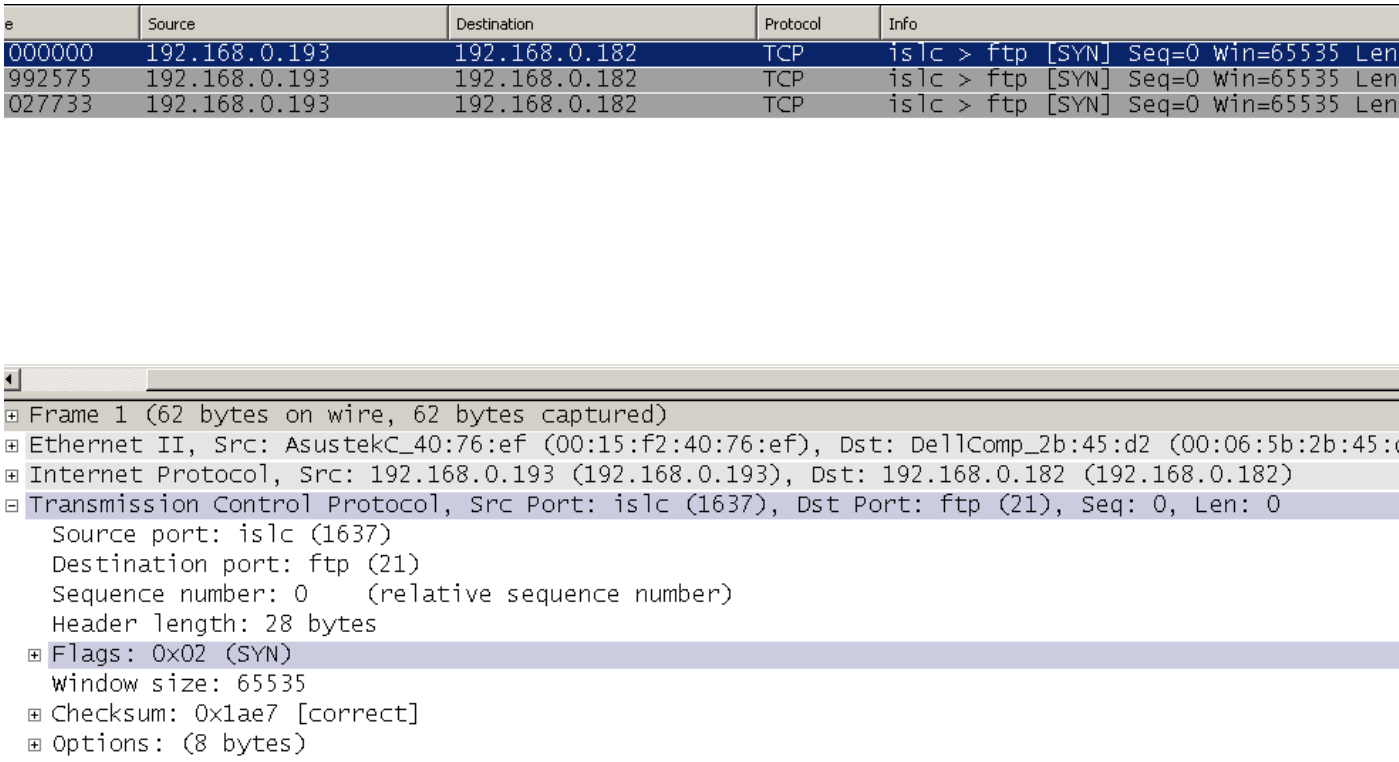
```
⊞ Frame 1 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: AsustekC_40:76:ef (00:15:f2:40:76:ef), Dst: DellComp_2b:45:d2 (00:06:5b:2b:45:d2)
⊞ Internet Protocol, Src: 192.168.0.193 (192.168.0.193), Dst: 192.168.0.182 (192.168.0.182)
⊟ Transmission Control Protocol, Src Port: radio-sm (1596), Dst Port: ftp (21), Seq: 0, Len: 0
    Source port: radio-sm (1596)
    Destination port: ftp (21)
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size: 65535
  ⊞ Checksum: 0xd69b [correct]
  ⊞ Options: (8 bytes)
```

Hình 3.1-19: The client tries to establish connection with SYN packets but gets no response; then it sends a

few more.

Client gửi các gói tin SYN để bắt tay với server nhưng không có phản hồi từ server.

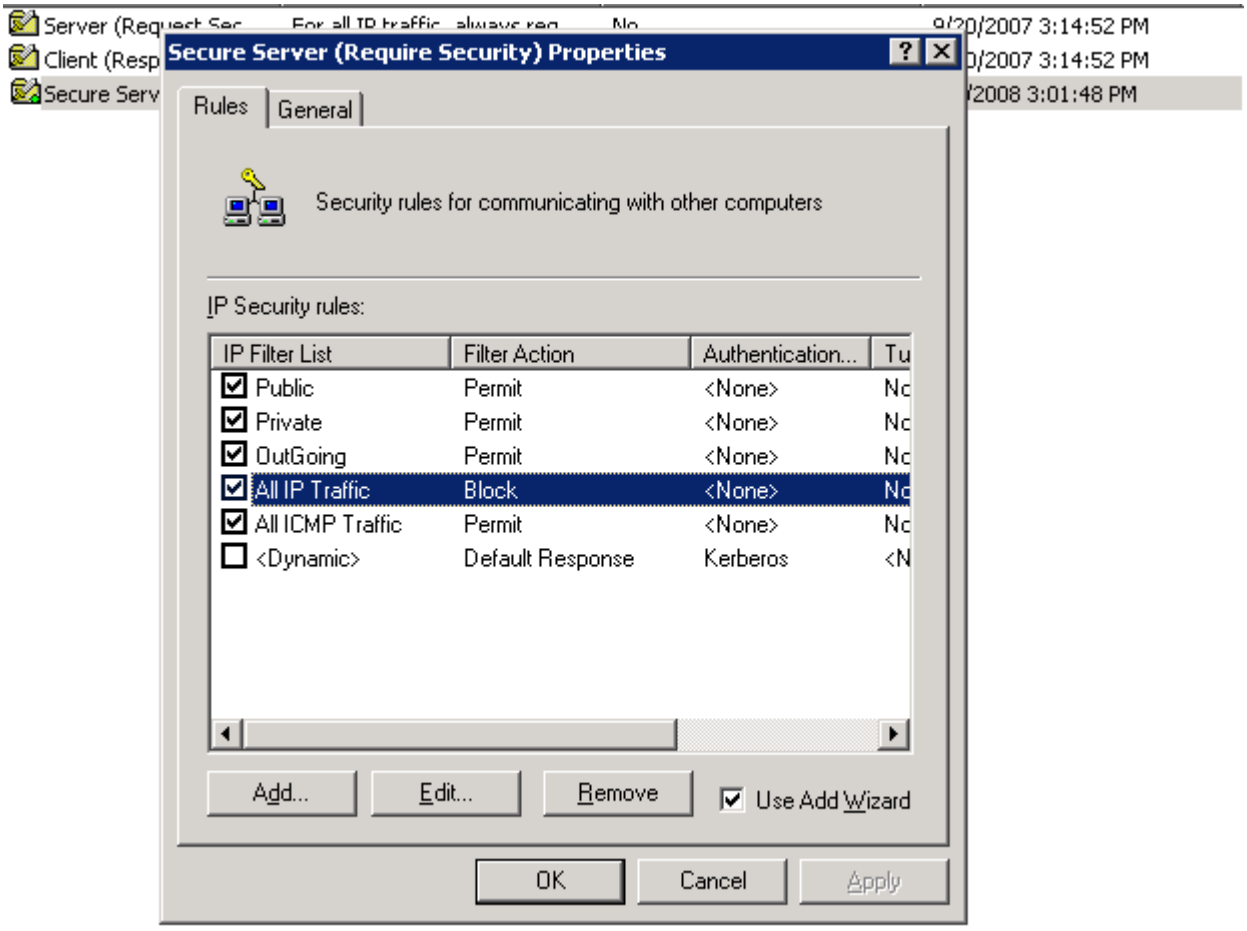
Server :



Hình 3.1-20: The client and server trace files are almost identical.

Có 3 lý do có thể dẫn đến hiện tượng trên

- FTP server chưa chạy, điều này không đúng vì FTP server của chúng ta đã chạy như kiểm tra lúc đầu
- Server quá tải hoặc có lưu lượng quá lớn khiến không thể đáp ứng yêu cầu. Điều này cũng không chính xác vì server vừa mới được cài đặt.
- Cổng 21 bị cấm ở phía clien hoặc phía server hoặc ở cả 2 phía. Sau khi kiểm tra và thấy rằng ở phía Server cấm cổng 21 cả chiều Incoming và Outgoing trong Local Security Policy



Kết luận

Đôi khi bắt gói tin không cho ta biết trực tiếp vấn đề nhưng nó đã hạn chế được rất nhiều trường hợp và giúp ta đưa ra suy đoán chính xác vấn đề là gì.

II.LÝ THUYẾT VỀ ĐỊA CHỈ IP

1.Khái niệm:

IP là chữ viết tắt của Internet Protocol (giao thức Internet). Mỗi gói tin IP sẽ bao gồm một địa chỉ IP nguồn và một địa chỉ IP đích. Tất nhiên, hệ thống "số nhà" trên Internet phức tạp và thú vị hơn nhiều so với nhà cửa trong thực tế.
Địa chỉ IP là một số nguyên 32 bit, thường được biểu diễn dưới dạng một dãy 4 số nguyên cách nhau bởi dấu chấm (dotted format). Một số nguyên trong địa chỉ IP là một byte, thường được gọi là một octet (8 bits).
Ví dụ về một địa chỉ IP điển hình là 123.255.0.15. Các thành phần 123, 255, 0 và 15 là các octet.
Một địa chỉ IP gồm có 3 phần. Phần đầu tiên là địa chỉ mạng (network address), phần thứ cuối cùng là địa chỉ máy (host address) và phần còn lại (nếu có) là địa chỉ mạng con (subnet address).
Địa chỉ mạng của một địa chỉ IP được tìm ra khi thực hiện phép toán logic AND giữa địa chỉ IP đấy và một giá trị gọi là mặt nạ mạng (network mask, tôi sẽ không dùng từ "mặt nạ mạng" trong tất cả các bài về sau mà chỉ dùng "network mask" cũng như sẽ không dịch từ "mask" thành "mặt nạ" nữa). Network mask cho biết bao nhiêu bit trong địa chỉ IP là địa chỉ mạng.

2. Các giao thức trong mạng IP

Để mạng với giao thức IP hoạt động được tốt người ta cần một số giao thức bổ sung, các giao thức này đều không phải là bộ phận của giao thức IP và giao thức IP sẽ dùng đến chúng khi cần.

+Giao thức ARP (Address Resolution Protocol): Ở đây cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải tìm được ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý của một trạm. Giao thức ARP đã được xây dựng để tìm địa chỉ vật lý từ địa chỉ IP khi cần thiết.
+Giao thức RARP (Reverse Address Resolution Protocol): Là giao thức ngược với giao thức ARP. Giao thức RARP được dùng để tìm địa chỉ IP từ địa chỉ vật lý.
+Giao thức ICMP (Internet Control Message Protocol): Giao thức này thực hiện truyền các thông báo điều khiển (báo cáo về các tình trạng các lỗi trên mạng.) giữa các gateway hoặc một nút của liên mạng. Tình trạng lỗi có thể là: một gói tin IP không thể tới đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một gói tin IP, Một thông báo ICMP được tạo và chuyển cho IP. IP sẽ "bọc" (encapsulate) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

3. Các bước hoạt động của giao thức IP

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.

Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

Tạo một IP datagram dựa trên tham số nhận được.
Tính checksum và ghép vào header của gói tin.
Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.
Chuyển gói tin xuống tầng dưới để truyền qua mạng.
Đối với router, khi nhận được một gói tin đi qua, nó thực hiện các động tác sau:

1) Tính chesksum, nếu sai thì loại bỏ gói tin.
2) Giảm giá trị tham số Time - to Live. nếu thời gian đã hết thì loại bỏ gói tin.
3) Ra quyết định chọn đường.
4) Phân đoạn gói tin, nếu cần.
5) Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to -Live, Fragmentation và Checksum.
6) Chuyển datagram xuống tầng dưới để chuyển qua mạng.
Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện bởi các công việc sau:
1) Tính checksum. Nếu sai thì loại bỏ gói tin.
2) Tập hợp các đoạn của gói tin (nếu có phân đoạn)
3) Chuyển dữ liệu và các tham số điều khiển lên tầng trên**.**

4. Phân lớp địa chỉ IP

Địa chỉ IP (Internet Protocol) là một địa chỉ duy nhất mà các thiết bị điện tử sử dụng để nhận biết và giao tiếp lẫn nhau trên mạng máy tính. Địa chỉ này được xác định bằng cách sử dụng chuẩn IP (Internet Protocol). Định nghĩa một cách đơn giản hơn thì địa chỉ IP là địa chỉ máy tính sử dụng trên Internet. Do vậy mà địa chỉ IP là duy nhất đối với mỗi thiết bị.
Ngoài máy tính, những thiết bị khác có thể có địa chỉ IP duy nhất bao gồm router, switch, các máy chủ cơ sở hạ tầng, máy in, máy fax Internet và thậm chí là một số máy điện thoại.
Địa chỉ IP đươc gán và quản lý bởi IANA (Internet Assigned Numbers Authority). IANA chỉ định các khối địa chỉ IP tới bất kỳ 4 khu vực đăng ký Internet (ARIN, RIPE NCC, APNIC và LACNIC), những nơi này sau đó sẽ gán các khối địa chỉ IP nhỏ hơn tới các nhà cung cấp dịch vụ Internet và doanh nghiệp.
Một địa chỉ IP thông thường gồm có 32 bit hoặc 4 byte địa chỉ thường được hiển thị bởi 4 chữ số (mỗi số giới hạn từ 0 đến 255) và cách nhau bởi dấu chấm. Ta có một ví dụ về địa chỉ IP như sau: '192.135.67.201'. Phạm vi của các số trong khoảng từ 0 tới 255 thường được hiển thị bởi 8 bit, hay còn gọi là một ‘Octet’.
Tuy nhiên, hạn chế của phiên bản địa chỉ IP này là số lượng địa chỉ IP bị giới hạn đối với 4, 294, 967, 296. Vì thế một phương pháp gán địa chỉ IP mới có tên là CIDR đã thay thế cho phương pháp trên. Phương pháp CIRD cũng được áp dụng vào phiên bản tiếp theo (IPv6) của địa chỉ IP.
Phiên bản mới của địa chỉ IP là 128 bit hoặc 16 byte chiều rộng, phiên bản này sẽ cho phép một khối lượng lớn địa chỉ IP trở nên sẵn có cho các máy tính trên Internet.

5.Phân loại địa chỉ IP

Có hai loại địa chỉ IP: IP tĩnh và IP động. Khi địa chỉ IP của máy tính là như nhau mỗi lần máy tính kết nối vào mạng thì đó được gọi là địa chỉ IP tĩnh. Tuy nhiên, khi địa chỉ IP của máy tính thay đổi khác nhau mỗi lần máy tính kết nối mạng thì đó là địa chỉ IP động (mạng MegaVN thường dùng IP động).
Địa chỉ IP máy bạn là gì?

Cho đến bây giờ chắc hẳn bạn vẫn đang thắc mắc "Địa chỉ IP của tôi là gì?" và "Làm thế nào để tôi có thể xác định được địa chỉ IP của tôi".
Không khó để bạn có thể xác định địa chỉ IP. Tuy nhiên các phương pháp sẽ khác nhau qua các tình huống khác nhau. Dưới đây sẽ là một số phương pháp đơn giản để xác định địa chỉ IP của máy tính khi đang kết nối Internet, khi bạn sử dụng máy tính Macintosh hay khi sử dụng máy tính Windows, và thậm chí cả cách nhận diện địa chỉ IP của người gửi thư điện tử.
Khi kết nối Internet

Trên Internet có rất nhiều trang web có thể dò tìm địa chỉ IP khi máy tính được kết nối qua Internet. Tuy nhiên, nếu như bạn đang trên một mạng LAN hay một mạng tại nhà, thì các trang web đó có thể sẽ dò tìm địa chỉ IP của router mạng.

Khi sử dụng máy tính Macintosh

Trên máy Mac, địa chỉ IP được tìm thấy tại bảng điều khiển TCP/IP, khi máy tính là Mac OS X thì địa chỉ IP được tìm thấy tại System Preferences trong mục 'Internet and Network' .

Khi sử dụng máy tính HĐH Windows

Nếu bạn muốn dò tìm địa chỉ IP của máy tính (trường hợp đang sử dụng Windows) thì quá trình hoàn dò tìm rất đơn giản: Kích vào 'Start' trên thanh tác vụ Windows. Chọn 'Run'. Nhập 'CMD' tại hộp nhập text. Lệnh này sẽ chuyển tới trình đơn dấu nhắc lệnh. Tại trình đơn này, nhập 'ipconfig/all'. Bạn sẽ tìm thấy địa chỉ IP của máy tính tại trường địa chỉ IP.

Địa chỉ IP được phân ra làm 5 lớp mạng (lớp A, B, C, D, và E). Trong đó bốn lớp đầu được sử dụng, lớp E được dành riêng cho nghiên cứu. Lớp D được dùng cho việc phát các thông tin broadcast/multicastt (broadcast/multicast IPs). Lớp A, B và C được dùng trong cuộc sống hàng ngày.

6. Cách phân biệt IP lớp A, B, C, và D

Một địa chỉ IP với bit đầu tiên là 0 thuộc về lớp A, bit đầu tiên là 1 và bit thứ 2 là 0 thuộc lớp B, bit đầu là 1, bit 2 là 1, bit 3 là 0 thuộc lớp C, bit đầu là 1, bit 2 là 1, bit 3 là 1, bit 4 là 0 thuộc lớp D. Lớp E là các địa chỉ còn lại. Bảng sau tóm tắt ý tưởng này:

Lớp IP	Dạng địa chỉ IP	Network mask mặc định
A	0xxxx…….xxx	255.0.0.0
B	10xxx…….xxx	255.255.0.0
C	110xx…….xxx	255.255.255.0
D	1110x…….xxx	(không dùng)

Ví dụ:địa chỉ 10.243.100.56 là một địa chỉ IP lớp A vì octet đầu được biểu diễn dưới dạng nhị phân thành 00001010. Bit đầu tiên là 0 nên địa chỉ đó thuộc về lớp A.

Mỗi lớp có 2 địa chỉ dành riêng là địa chỉ thấp nhất (phần địa chỉ máy toàn bit 0), và địa chỉ cao nhất của lớp đó (phần địa chỉ máy toàn bit 1). Như vậy, địa chỉ mạng có thể có trong một lớp sẽ phụ thuộc vào số bit trong network mask (bit mang giá trị 1). Nếu gọi số bit 1 trong network mask là x thì số địa chỉ mạng tối đa có thể có trong một lớp là 2^x

Tuy nhiên, vì mỗi lớp bị phụ thuộc vào vài bit đầu tiên quy định nên số địa chỉ mạng tối đa thật sự trong mỗi lớp sẽ là 2^x – 2^(số bit cố định của lớp tương ứng).
Như vậy lớp A có 126 địa chỉ, lớp B có tối đa 16382 địa chỉ, lớp C có 2097150 địa chỉ.
Phần còn lại ngoài địa chỉ mạng sẽ là địa chỉ máy. Tương tự cũng có 2 địa chỉ máy dành riêng (địa chỉ thấp nhất và địa chỉ cao nhất) trong mỗi địa chỉ mạng. Như vậy, số địa chỉ máy có thể có trong mỗi mạng sẽ là 2^(32 – x) – 2. Công thức tính đơn giản giống công thức tính số địa chỉ mạng. Chỉ khác một điều là ta dùng số bit 0 (32-x) thay vì dùng số bit 1 (x).
Như vậy, một địa chỉ mạng lớp C sẽ có 254 địa chỉ máy, tương tự cho địa chỉ mạng lớp B, và A.
Tổng số địa chỉ của một lớp mạng là tích của số địa chỉ mạng và số địa chỉ máy trong một mạng thuộc lớp đó.

7. Subnet

Các nhà quản trị mạng thường phân chia mạng của họ ra thành nhiều mạng nhỏ hơn gọi là mạng con subnet. Tương tự với địa chỉ mạng, địa chỉ mạng con cũng được quy định bởi một mask, gọi là subnet mask. Subnet mask của một địa chỉ mạng có số bit 1 nhiều hơn hoặc bằng (trường hợp bằng có nghĩa là không có chia mạng ra thành subnet) số bit 1 trong network mask của địa chỉ đó. Ví dụ subnet mask của một mạng thuộc lớp B sẽ có dạng 255.255.xxx.xxx với xxx là số bất kỳ từ 0 đến 255.

Cách tính số địa chỉ mạng con của một địa chỉ mạng sẽ phụ thuộc vào bao nhiêu bit của network mask đã được dùng để làm subnet mask (tạm gọi là y). Hai công thức bên trên đều được sử dụng với việc thay biến x thành y. Đặc biệt cách tính số địa chỉ IP trong mỗi subnet sẽ dùng cả x và y theo công thức sau: 2^(32 – x – y) – 2
Ví dụ subnet mask của một mạng lớp A (network mask mặc định 255.0.0.0) là 255.192.0.0 thì y sẽ là 2 (vì 192 biểu diễn ở dạng nhị phân là 11000000, có nghĩa là đã có 2 bit đã được sử dụng để làm subnet mask). Subnet mask phải là một dãy liên tục các bit 1 ngay sau network mask. Điều này nói lên rằng subnet mask dành một số bit 0 trong network mask (phần dành cho địa chỉ máy). Cũng có 2 địa chỉ máy dành riêng trong mỗi subnet. Hai địa chỉ đó là subnet address (địa chỉ thấp nhất trong subnet) và broadcast address (địa chỉ cao nhất trong subnet). Địa chỉ thấp nhất trong subnet không nhất thiết có tất cả các bit là 0 như đối với địa chỉ thấp nhất trong một mạng, cũng như địa chỉ cao nhất không nhất thiết phải là toàn bit 1. Lưu ý là trong một vài tài liệu cũ nói rằng cũng có 2 subnet dành riêng trong mỗi mạng nhưng bây giờ điều đó không còn dùng nữa. Hai subnet đó vẫn được dùng, gọi là zero subnet (subnet thấp nhất) và broadcast subnet (subnet cao nhất).
Ngoài ra, mỗi lớp mạng còn có 1 địa chỉ mạng dành riêng (private network address). Lớp A có địa chỉ 10.0.0.0. Lớp B có địa chỉ 172.16.0.0. Lớp C có địa

chỉ 192.168.0.0. Địa chỉ broadcast của lớp A còn được gọi là địa chỉ universal broadcast (toàn bit 1 hay 255.255.255.255).

8. Broadcast và multicast

Các phần trên đề cập đến broadcast và multicast nhưng chưa giải thích. Địa chỉ broadcast là một địa chỉ mà khi thông tin gửi tới địa chỉ đó sẽ được gửi đến toàn bộ các máy trong mạng. Multicast cũng như broadcast nhưng chỉ có tác dụng trong một subnet.

Trên đây là các kiến thức cơ bản về việc đánh địa chỉ IP. Vài ví dụ dưới sẽ giúp làm sáng tỏ các kiến thức trên.

Ví dụ 1: Địa chỉ 192.168.0.1 thuộc lớp nào?

Có 2 cách trả lời câu hỏi này: Một là dựa vào việc phân tích octet đầu ra dạng nhị phân, căn cứ vào các bit đầu mà có thể trả lời. Cách thứ hai là vì địa chỉ này thuộc mạng riêng của lớp C nên có thể trả lời ngay.

Ví dụ 2: Chỉ rõ địa chỉ mạng của địa chỉ 192.168.0.5 với network mask mặc định.

Câu hỏi này buộc ta phải biết địa chỉ 192.168.0.5 thuộc lớp nào và biết network mask của lớp đó.

192.168.0.5 thuộc lớp C.

Lớp C có network mask là 255.255.255.0.

Thực hiện phép AND sẽ ra 192.168.0.0.

Câu trả lời là 192.168.0.0. Câu hỏi này cũng có thể trả lời nếu ta biết là địa chỉ 192.168.0.5 là một trong 3 địa chỉ riêng.

Ví dụ 3: Chỉ rõ phần địa chỉ mạng (bỏ phần địa chỉ máy) của địa chỉ 192.168.0.10 với network mask mặc định.

Như câu trên ta đã biết network mask của địa chỉ 192.168.0.10 là 255.255.255.0. Câu hỏi yêu cầu chỉ rõ PHẦN địa chỉ mạng, nên ta chỉ lấy các bit còn nằm trong network mask:

Địa chỉ đầu 11000000.10101000.00000000.00001010

Network mask 11111111.11111111.11111111.00000000

Lấy phần trong network mask 11000000.10101000.00000000

Câu trả lời sẽ là 192.168.0.

Ví dụ 4: Địa chỉ IP 129.56.7.8 có subnet mask là 255.255.128.0. Hỏi có bao nhiêu subnet, bao nhiêu địa chỉ IP trong mỗi subnet, bao nhiêu địa chỉ IP trong mạng đó?

Việc trả lời đòi hỏi chút tính toán. Sau khi nhận biết địa chỉ IP này là thuộc lớp B, network mask mặc định là 255.255.0.0 (x là 16), ta biết quản trị mạng đã lấy 1 bit để chia subnet. Như vậy, y là 1. Số subnet là 2^1 là 2. Số địa chỉ IP trong mỗi subnet là 2^(32-y-x) – 2 là 32766. Suy ra số địa chỉ IP trong mạng đó là 2 * 32766 là 65532.

9.Cách phân chia địa chỉ mạng con:

Về bản chất, ta sẽ tận dùng các bộ số không dùng đến của địa chỉ máy chủ để mở rộng quy mô cho mạng. Subnet Mask (giá trị trần của từng mạng con) cho phép bạn chuyển đổi một mạng lớp A, B hay C thành nhiều mạng nhỏ, tùy theo

nhu cầu sử dụng. Với mỗi giá trị trần này, bạn có thể tạo ra một tiền tố mạng mở rộng để thêm bit từ số máy chủ vào tiền tố mạng. Việc phân chia này sẽ dễ hiểu hơn khi bạn dùng hệ đếm nhị phân.
- Các bit được đánh số 1 nếu bit tương ứng trong địa chỉ IP là một phần của tiền tố mạng mở rộng.
- Các bit được đánh số 0 nếu bit là một phần của số máy chủ.
Ví dụ tiền tố mạng lớp B luôn bao gồm 2 bộ số đầu của địa chỉ IP, nhưng tiền tố mạng mở rộng của lớp B lại dùng cả bộ số thứ 3.
Ví dụ 1: Nếu có địa chỉ IP lớp B là 129.10.0.0 và bạn muốn dùng cả bộ số thứ 3 làm một phần của tiền tố mạng mở rộng thay cho số máy chủ, bạn phải xác định một giá trị trần của mạng con là: 11111111.11111111.11111111.00000000 (255.255.255.0). Như vậy, giá trị trần này chuyển địa chỉ của lớp B sang địa chỉ lớp C, nơi số máy chủ chỉ gồm bộ số thứ 4. Ký hiệu /24 thể hiện bạn đã dùng 24 bit đầu để làm tiền tố mạng mở rộng.
Ví dụ 2: Nếu bạn chỉ muốn dùng một phần của bộ số thứ 3 cho tiền tố mạng mở rộng, hãy xác định giá trị trần của địa chỉ mạng con là 11111111.11111111.11111000.00000000 (255.255.248.0), trong đó chỉ có 5 bit của bộ số thứ 3 được đưa vào tiền tố mạng mở rộng. Lúc này ta có ký hiệu /21.
Để xác định Subnet Mask dựa trên số máy chủ mình muốn, bạn có thể tham khảo bảng sau:

Chú ý: Địa chỉ đầu tiên và cuối cùng của mạng con được giữ lại, trừ /32 vì đây là địa chỉ máy chủ duy nhất.
Xác định địa chỉ để sử dụng với giá trị trần của mạng con
Địa chỉ cho lớp C
Đối với một mạng có từ 2 đến 254 máy chủ, bộ số thứ 4 sẽ được dùng đến, bắt đầu từ 0. Ví dụ, mạng con 8 máy chủ (/29) sẽ có vùng địa chỉ như sau:

Chú ý: địa chỉ đầu tiên và cuối cùng của mạng con được giữ lại. Bạn không dùng được 192.168.0.0 hay 192.168.0.7.
Nói tóm lại, các vùng địa chỉ sau được chỉ định cho mạng riêng:
* 10.0.0.0 – 10.255.255.255 (lớp A)
* 172.16.0.0 – 172.31.255.255 (lớp)
* 192.168.0.0 – 192.168.255.255 (lớp C)
Thiết lập và xem địa chỉ IP trên máy tính
Khi xây dựng một mạng nội bộ gồm máy chủ và máy khách, bạn sẽ phải vào hệ thống để lập địa chỉ IP. Nhấn chuột phải vào biểu tượng My network places, chọn Properties. Tiếp tục nhấp chuột phải vào biểu tượng Local Area Connection > Properties > chọn Internet Protocol (TCP/IP) > Properties. Một bảng sau hiện ra:

Muốn xem địa chỉ này, bạn vào menu Start > All Programs > Accessories > Command Prompt. Khi màn hình Dos hiện ra, gõ ngay vào vị trí con trỏ chữ "ipconfig". Cách khác: Start > Run > gõ ipconfig > OK.
Khi một thiết bị nào đó trên network riêng cần liên hệ với các mạng khác, người dùng phải đảm bảo mạng ngoài có dùng địa chỉ IP thực để các router chấp nhận kết nối. Thường thì "cánh cổng" router này chính là thiết bị dịch địa chỉ mạng (NAT – network address translation) hoặc công đoạn đó được thực hiện nhờ một máy chủ proxy.

Địa chỉ IP (Internet Protocol) là một địa chỉ duy nhất mà các thiết bị điện tử sử dụng để nhận biết và giao tiếp lẫn nhau trên mạng máy tính. Địa chỉ này được xác định bằng cách sử dụng chuẩn IP (Internet Protocol). Định nghĩa một cách đơn giản hơn thì địa chỉ IP là địa chỉ máy tính sử dụng trên Internet. Do vậy mà địa chỉ IP là duy nhất đối với mỗi thiết bị.
Ngoài máy tính, những thiết bị khác có thể có địa chỉ IP duy nhất bao gồm router, switch, các máy chủ cơ sở hạ tầng, máy in, máy fax Internet và thậm chí là một số máy điện thoại.

Địa chỉ IP đươc gán và quản lý bởi IANA (Internet Assigned Numbers Authority). IANA chỉ định các khối địa chỉ IP tới bất kỳ 4 khu vực đăng ký Internet (ARIN, RIPE NCC, APNIC và LACNIC), những nơi này sau đó sẽ gán các khối địa chỉ IP nhỏ hơn tới các nhà cung cấp dịch vụ Internet và doanh nghiệp.
Một địa chỉ IP thông thường gồm có 32 bit hoặc 4 byte địa chỉ thường được hiển thị bởi 4 chữ số (mỗi số giới hạn từ 0 đến 255) và cách nhau bởi dấu chấm. Ta có một ví dụ về địa chỉ IP như sau: '192.135.67.201'. Phạm vi của các số trong khoảng từ 0 tới 255 thường được hiển thị bởi 8 bit, hay còn gọi là một 'Octet'.
Tuy nhiên, hạn chế của phiên bản địa chỉ IP này là số lượng địa chỉ IP bị giới hạn đối với 4, 294, 967, 296. Vì thế một phương pháp gán địa chỉ IP mới có tên là CIDR đã thay thế cho phương pháp trên. Phương pháp CIRD cũng được áp dụng vào phiên bản tiếp theo (IPv6) của địa chỉ IP.
Phiên bản mới của địa chỉ IP là 128 bit hoặc 16 byte chiều rộng, phiên bản này sẽ cho phép một khối lượng lớn địa chỉ IP trở nên sẵn có cho các máy tính trên Internet

III. PHÂN TÍCH CÁC GÓI TIN DÙNG WIRESHARK

3.1 Mục đích

Trong bài thí nghiệm này học viên sẽ nghiên cứu giao thức lớp mạng IP (Internet Protocol) sửdụng trong Internet. Học viên sẽ tiến hành quá trình bắt các IP datagram trao đổi giữa máytính client của học viên và một máy tính khác trên Internet. Sau khi bắt được một trace (vết)các IP datagrams, học viên sẽ tiến hành phân tích các trường dữ liệu trong IP datagram, vànghiên cứu chi tiết thao tác phân đoạn trong giao thức IP. Kết thúc bài thí nghiệm học viên sẽnắm chắc hoạt động của giao thức IP, củng cố thêm kiến thức đã học trên lớp.

3.2 Phương pháp

Để phân tích hoạt động của giao thức IP, chúng ta sẽ sử dụng chương trình traceroute đểphát đi các packet [đối với Unix và Linux là các UDP datagram với các port đích trongkhoảng 33434 to 33534, còn với Windows là các ICMP (Internet ControlMessage Protocol)echo request] đến một địa chỉ đích định trước trên mạng IP và nhận lại các packet phản hồi từcác router, và nhờ đó biết được route đi từ host đích đến host nguồn. Để theo dõi quá trìnhtrao đổi thông tin giữa trạm nguồn, các router và địa chỉ đích, chúng ta sử dụng chương trìnhnetwork protocol analyzer Wireshark để bắt và lưu lại một trace của các IP datagram vàpacket đã phát và thu.

3.3 Bắt các gói nhờ chương trình traceroute

Để tạo một trace của các IP datagrams cho thí nghiệm, chúng ta sẽ sử dụng chương trìnhtraceroute để gửi đi các packet có kích thước khác nhau tới một địa chỉ *X* nào đó trênInternet. Nguyên tắc làm việc của chương trình traceroute, dựa trên chương trình ping,thực hiện trước tiên gửi đi một hoặc nhiều packet được đóng gói vào trong IP datagram vớitrường TTL (Time to Live) ở trong header được đặt bằng 1; sau đó gửi tiếp một loạt cácpacket về phía cùng địa chỉ với giá trị TTL bằng 2; rồi bằng 3 và tương tự. Chú ý rằng mỗikhi nhận được một IP datagram, mỗi router sẽ giảm giá trị trường TTL ở IP datagram thu được đi 1. Khi giá trị của TTL bằng 0, router sẽ nhận biết đây là một IP datagram lỗi do thờigian tồn tại đã hết và sẽ tự động gửi trả lại host nguồn thông báo lỗi bằng một bản tin ICMP(type 11 – Time-to-live exceeded). Kết quả là một IP

datagram với TTL bằng 1 do chươngtrình traceroute gửi sẽ làm cho router cách host nguồn một hop tự động gửi một bản tin"ICMP Time-to-live exceeded" ngược trở về phía host nguồn; IP datagram được gửi với TTLbằng 2 sẽ làm cho router cách 2 hop gửi một bản tin ICMP ngược về phía nguồn; và tương tự. Dựa vào địa chỉ nguồn chứa trong các bản tin ICMP vượt quá TTL, chúng ta có thể xác địnhđược địa chỉ của router gửi bản tin ICMP. Và như vậy, bằng cách này, host chạy chương trìnhtraceroute có thể xác định được các routers đặt giữa nó và đích *X*.
Để sử dụng traceroute trong Windows, chúng ta có thể sử dụng chương trình tracert có sẵn từ command window. Tuy nhiên, do chương trình tracert trong Windowskhông cho phép thay đổi kích thước của bản in yêu cầu tiếng vọng ICMP (ping) do chươngtrình tracert gửi, nên không thể sử dụng nó để nghiên cứu quá trình phân đoạn trong giao thứcIP. Vì vậy, trong bài thí nghiệm này chúng ta sẽ sử dụng một chương trình shareware hỗ trợtraceroute là PingPlotter.

3.4 Chuẩn bị bài thí nghiệm

Để phục vụ cho bài thí nghiệm, sinh viên cần chuẩn bị các bước sau đây'
• Chương trình tracert được sử dụng phổ biến cho windows là PingPlotter. Để cóPingPlotter, có thể download từ địa chỉ http://www.pingplotter.com/download.html. Ở địachỉ của trang PingPlotter, có 3 chương trình là *Freeware*, *Standard* và *Pro*. Phiên bản*Freeware* hiện tại (version 3.20.1) không cho phép thay đổi kích thước của gói, trong khiphiên bản *Pro* lại không cho chạy thử, nên chỉ có bản *Standard* có thể sử dụng được ởdạng shareware với 30 ngày dùng thử, đủ cho thời gian làm thí nghiệm của học viên. Saukhi đã download được chương trình PingPlotter phiên bản *Standard,* học viên cần cài đặtvào trong máy tính để phục vụ cho thí nghiệm sau này.
• Máy tính có nối tới mạng Internet (qua mạng LAN hay ADSL).
• Chương trình network protocol anlyzer Wireshark hay phiên bản cũ của nó là Ethereal,đã được cài đặt vào trong máy tính.

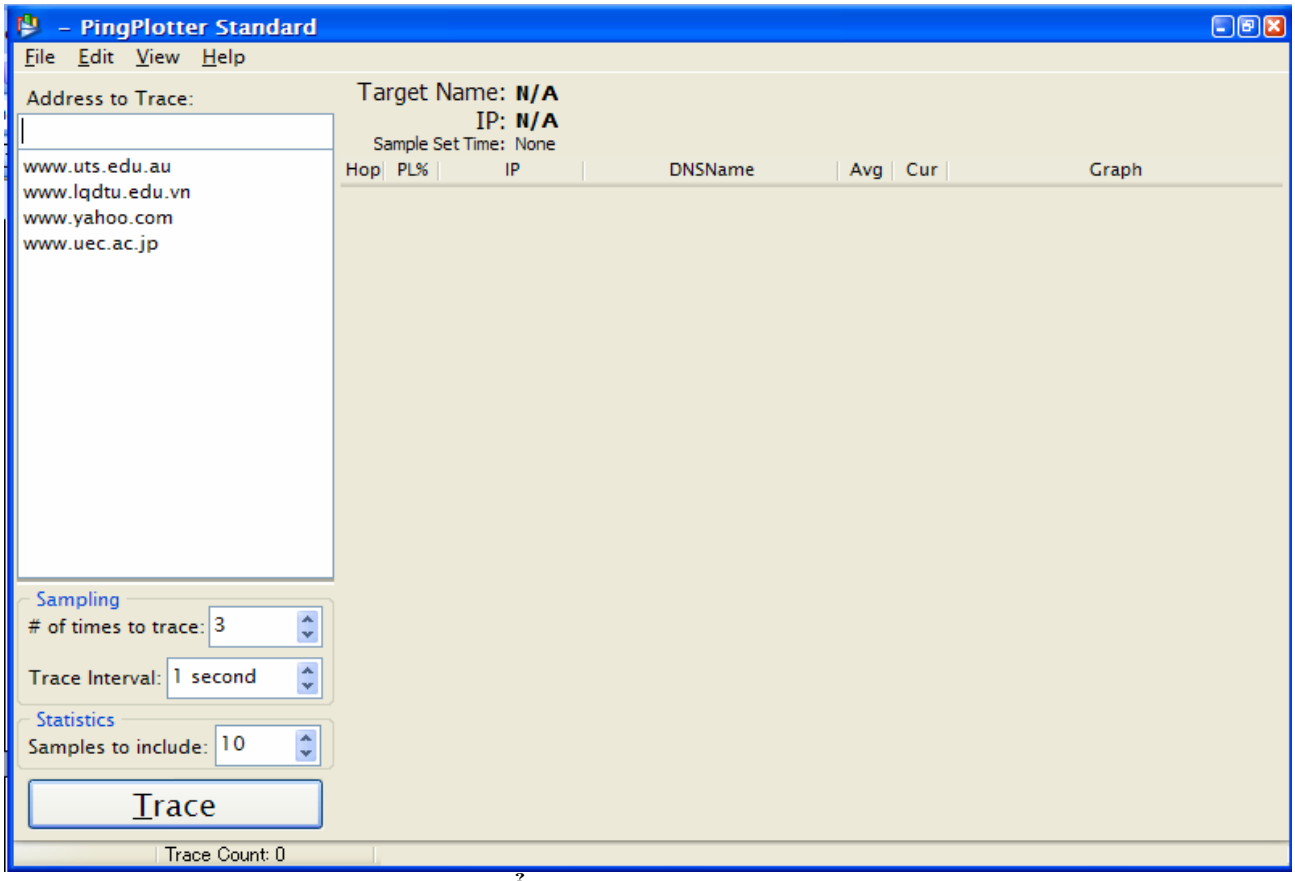
3.5 Nội dung bài thí nghiệm

Nội dung bài thí nghiệm gồm các bước chính sau đây:

3.5.1 Thiết lập tham số trace

1. **Bước 1**: Khởi động Wireshark và bắt đầu bắt gói *(Capture□Start),* sau đó bấm *OK* trênmàn hình Packet Capture Options của cửa sổ. Xem hướng dẫn chi tiết ở Bài 2.
2. **Bước 2:** Chọn một địa chỉ Internet để chương trình tracert (PingPlotter) tạo ra một
trace đến host có địa chỉ đó. Ví dụ: địa chỉ www.uts.edu.au của trường đại học Universityof Technology Sydney (UTS).

3. **Bước 3:** Khởi động PingPlotter. Sau khi khởi động xong trên màn hình sẽ xuất hiện cửasổ chương trình như trên Hình 3.1.

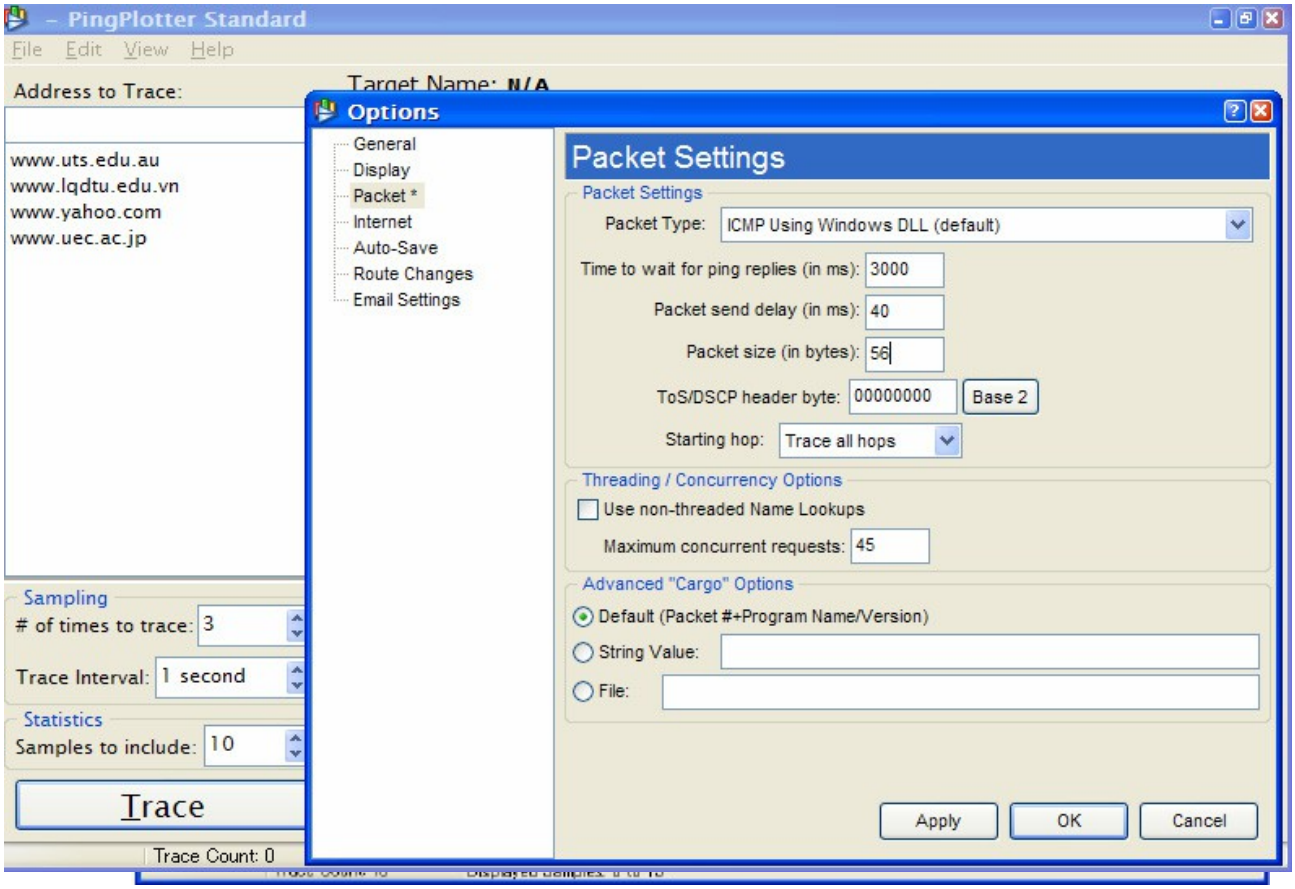


Hình 3.1 Cửa sổ chương trình PingPlotter

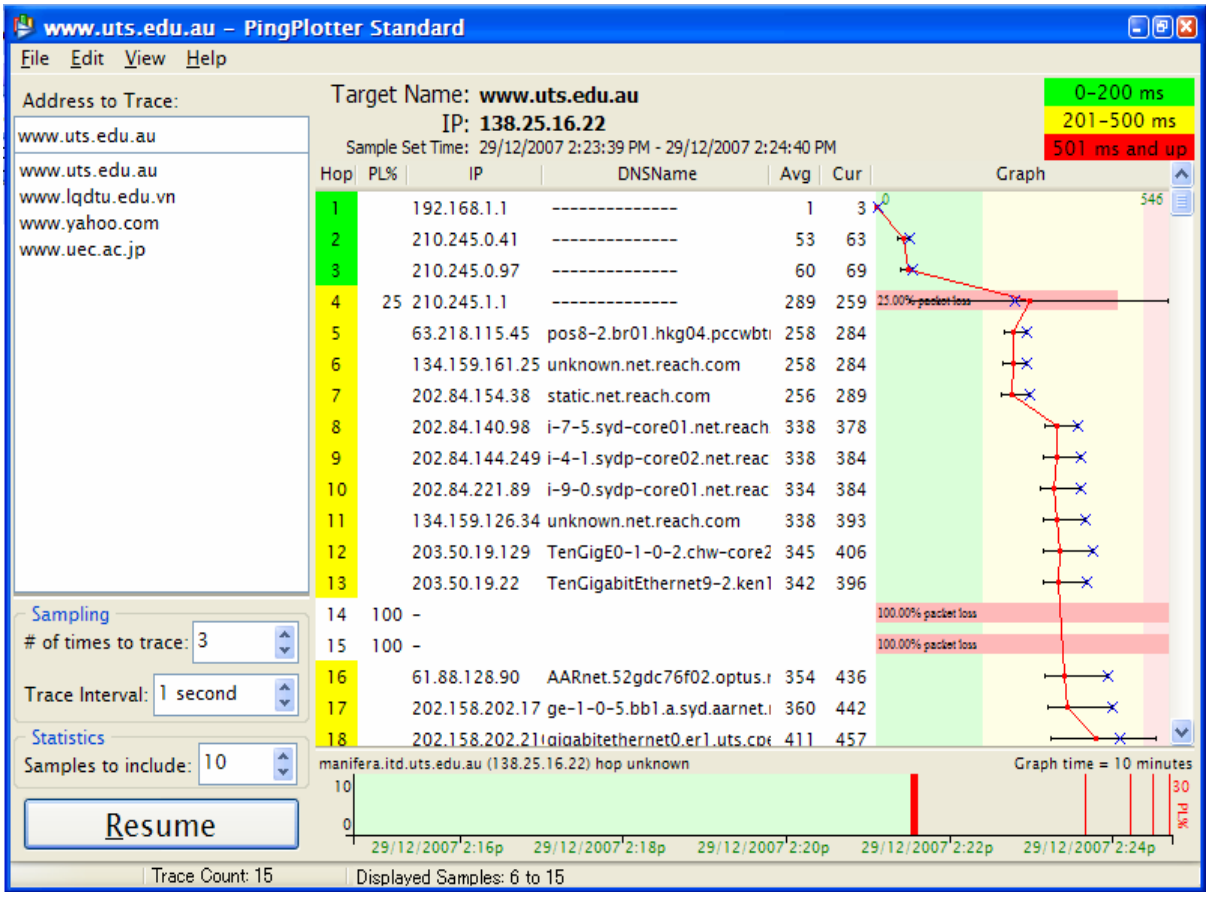
Một số điểm đáng chú ý trên cửa sổ là thanh nhập địa chỉ host cần trace *Address to Trace*,phần cài đặt *Sampling* với các trường thiết lập số lần *trace # of times to trace,* và khoảng thờigian giữa các lần trace *Trace Interval*. Trong phạm vi bài thí nghiệm này chúng ta đặt 3 cho *#of times to trace.*

3.5.2 Bắt đầu trace

4. **Bước 4:** trên thanh menu của PingPlotter, chọn menu *Edit□Advanced OptionsPacket Options* và nhập vào giá trị 56 ở trường *Packet Size* và bấm OK như mô tả trên Hình 3.2. Sau đó bấm phím *Trace.* Thao tác này cho phép chúng ta gửi đi cácICMP echo request packet có kích thước bằng 56bytes về host đích là www.uts.edu.au vànhận về các bản tin ICMP Time-to-live exceeded. Bạn sẽ thấy có cửa sổ PingPlottertương tự ở Hình 3.1 dưới đây.



Hình 3.2 Đặt kích thước packet



Hình 3.3 Cửa sổ trace của PingPlotter

Tiếp theo, gửi một tập hợp các packet có độ dài lớn hơn bằng cách chọn *Edit-Advanced Option- Packet Options* và nhập vào giá trị 2000 (bytes) ở trường *PacketSize* và bấm OK. Sau đó bấm phím Resume. Cuối cùng, gửi một tập các packet với độ dài lớnhơn bằng cách chọn *Edit- Advanced Options - Packet Options* và nhập vào giá trị 3500(bytes) ở trường *Packet Size* và sau đó bấm OK. Sau đó bấm phím Resume.

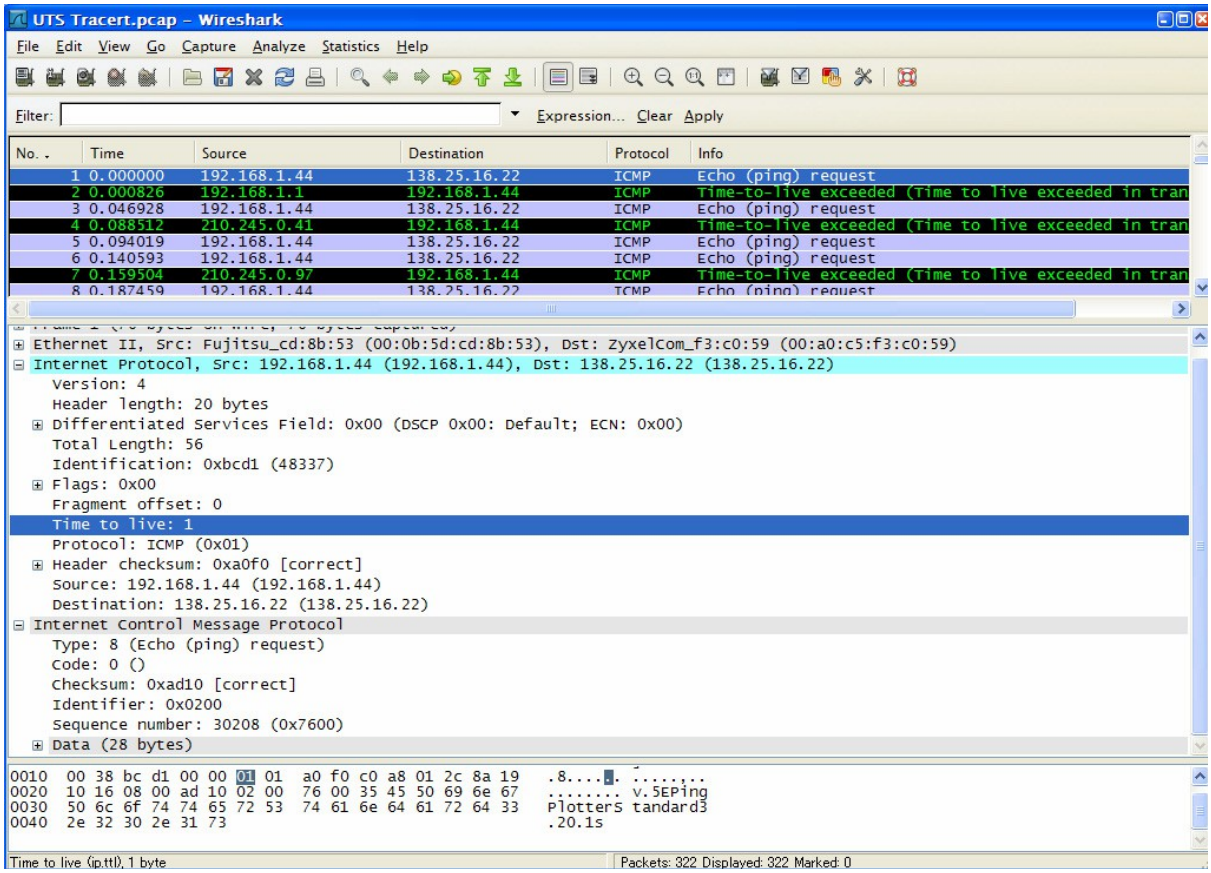
3.5.3 Kết thúc trace

5. **Bước 5:** Để kết thúc trace, dừng chương trình Wireshark bằng cách bấm Stop ở cửa sổCapture của Wireshark.

3.5.4 Phân tích trace bắt được

Ở trong trace do Wireshark thu được, bạn sẽ thấy một loạt các packet "ICMP Echo Request"gửi bởi host nguồn là máy tính của bạn và các packet chứa bản tin "ICMP Time-to-Liveexceeded" do các router trên tuyến gửi ngược trở lại về máy tính của bạn.

6. **Bước 6:** Bản tin "ICMP Echo Request". Trên cửa sổ phân tích của Wireshark chọn bảntin bắt được đầu tiên như ở Hình 3.4



Hình 3.4 Cửa sổ Wireshark hiển thị thông tin của packet đầu tiên

Trong phần hiển thị thông tin về header của các packet, chọn [+] Internet Protocol để xemcác thông tin về header của IP datagram chứa ICMP echo (ping) request packet. Dựa trênthông tin hiển thị trên cửa sổ (xem Hình 3.4) chúng ta có thể xác định được địa chỉ IP củahost nguồn là 192.168.1.44, địa chỉ host đích là 138.25.16.22, và giá trị trường TLL của IP
datagram bằng 1. Điều này cho chúng ta biết host www.uts.edu.au có địa chỉ IP là138.25.16.22.

7. **Bước 7:** Bản tin "ICMP Time-to-Live exceeded". Trên cửa sổ phân tích của Wireshark,chọn bản tin bắt được thứ hai. Như thấy trên cửa sổ đây là packet chứa bản tin ICMPTime-to-Live exceeded.

Hình 3.5 Cửa sổ Wireshark hiển thị thông tin của packet ICMP Time-to-Live exceededỞ phần hiển thị thông tin về packet chúng ta có thể thấy địa chỉ nguồn (địa chỉ của router
gửi ICMP packet) là 192.168.1.1 và địa chỉ đích [địa chỉ của host gửi ICMP echo (ping)request] là 192.168.1.44. Điều này có nghĩa là host (router) 192.168.1.1 là router đầu tiêntrên tuyến đến host www.uts.edu.au mà chúng ta đang trace. Khi thu được IP datagram
chứa ICMP echo (ping) request packet, router 192.168.1.1 giảm giá trị TTL đi1.DoTTL=0, nên router 192.168.1.1 loại bỏ IP datagram đó và tự động gửi về host nguồn chứabản tin "ICMP Time-to-Live exceeded".

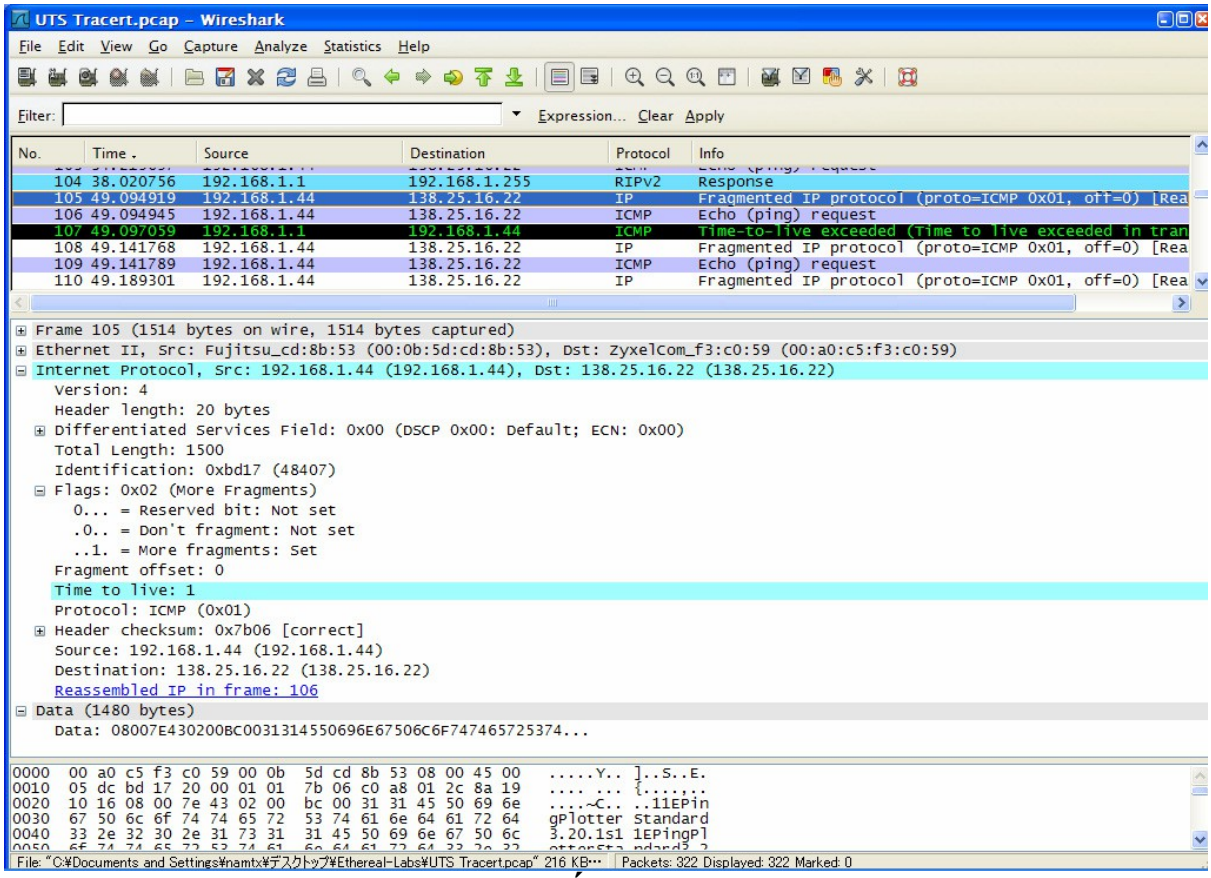
Trên cửa sổ thông tin chi tiết của Wireshark chọn [+] Internet Control Message Protocol,rồi chọn tiếp [+] Internet Protocol để hiển thị các thông tin về ICMP packet và header củaIP datagram như ở Hình 3.5. Trên Hình 3.5, ở phần hiển thị thông tin header của packet,
[-] Internet Control Message Protocol - [-] Internet Protocol, chúng ta có thể thấy địa chỉnguồn là 192.168.1.44 và địa chỉ đích là 138.25.16.22. Hai địa chỉ nguồn và đich này làhai địa chỉ nguồn và đích chứa trong IP datagram của packet" ICMP echo (ping) request"trước đó.

8. **Bước 8:** Kích thước IP header. Trên cửa sổ chi tiết về header của packet, ở phần [-]Internet Protocol (xem Hình 3.5) chúng ta thấy có thông tin Header length: 20 bytes, cho biếtđộ dài header của IP datagram. Từ kích thước của IP datagram và IP header chúng ta cóthể biết được độ dài của phần payload trong IP datagram.

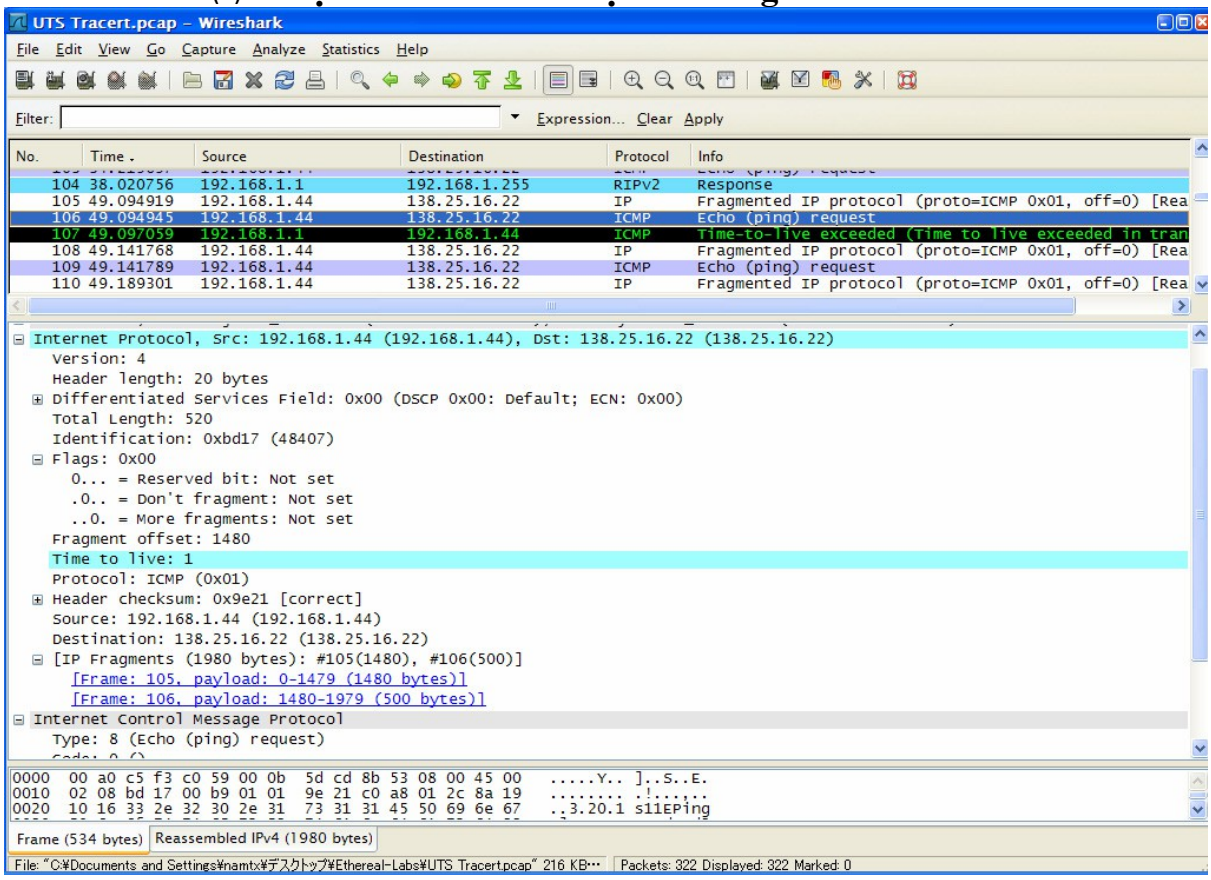
9. **Bước 9:** Phân đoạn IP (IP fragment). Theo lý thuyết chúng ta biết mạng Ethernet là lớpcung cấp dịch vụ cho lớp mạng IP chỉ cho phép truyền đi các frame với độ dài tối đa 1500bytes. Vì vậy, các IP datagram có độ dài lớn hơn 1500 bytes sẽ bị phân đoạn và truyềntrên các Ethernet frame khác nhau. Trong trường hợp bài thí nghiệm đang tiến hành, khigửi đi các packet có kích thước 2000 bytes và 3500 bytes, Ethernet sẽ phân đoạn cácpacket đó thành các fragment và gửi đi trên các Ethernet frame liên tiếp nhau. Xét ví dụ
trường hợp packet có kích thước 2000bytes. Do kích thước packet (chính là kích thước IPdatagram) đặt là 2000 bytes nên trừ đi 20 bytes header, phần payload còn chứa 1980 bytes.Phần dữ liệu này được chia thành 2 hai đoạn: một có kích thước 1480 bytes để đóngkhung vừa đủ vào 1500 bytes của Ethernet frame, và một đoạn thứ hai chứa phần payloadcòn lại, tức là, 500bytes.

Trên cửa sổ Captured packet list của Wireshark, chọn dòng sự kiện có chứa Fragmented IPprotocol…như ở Hình 3.6(a). Trên cửa sổ chứa thông tin header chi tiết của packet, ở phầnphía dưới của [-] Internet Prototocol có thông tin Reassembled IP in frame:106 cho biết
packet hiện tại là một phân đoạn (fragement) của một IP datagram và phân đoạn còn lạicủa IP datagram được chứa trong frame số 106 tương ứng với dòng sự kiện thứ 106.

Chọn tiếp dòng tiếp theo (106 trong ví dụ này) sẽ thấy cửa sổ tương tự Hình 3.6(b). Dòngnày chứa mô tả nội dung Echo (ping) request cho biết toàn bộ nội dung của IP datagramgửi trong phân đoạn trước và phân đoạn này chứa bản tin Echo (ping) request. Ở phầnthông tin chi tiết của packet header chúng ta thấy các thông tin:



(a) **Đoạn thứ nhất của một IP datagram**



Hình 3.6 Phân đoạn IP. (b) Đoạn thứ hai của một IP datagram

Thông tin này, giống như đã phân tích ở trên, có nghĩa là tổng số payload trong IPdatagram là 1980bytes, được phân thành 2 đoạn. Đoạn thứ nhất chứa 1480bytes, bao gồmcác byte từ số 0 đến 1479 trong IP datagram gốc, được truyền đi bởi frame số 105. Đoạn
thứ hai chứa 500 bytes còn lại, từ byte số 1480 đến byte 1979, và được truyền đi bởiframe số 106.

10. **Bước 10:** Bản tin "ICMP Echo Request". Trên cửa sổ phân tích của Wireshark chọnbản tin bắt được đầu tiên như ở Hình 3.4

LỜI CẢM ƠN!

Chúng em xin chân thành cảm ơn sự tận tình giúp đỡ của thầy Đoàn Văn Trung đã động viên giúp đỡ và tạo mọi điều kiện thuận lợi nhất để em có thể hoàn thành đề tài của mình. Vì khả năng và thời gian còn hạn chế nên quá trình tìm hiểu và phân tích chương trình còn chưa tối ưu nên không thể tránh khỏi những thiếu sót. Chúng em rất mong nhận được sự góp ý, bổ sung của các thầy cô giáo và các bạn để chương trình có thể hoàn thiện hơn.

TÀI LIỆU THAM KHẢO

- Giáo trình mang máy tính –Th.s:Nguyễn Văn Toàn
- Kỹ thuật truyền dữ liệu –Dương quang Thiện
- Bùi Đức Huy-Mạng và Truyền Thông