**1. Một số tình huống cơ bản**

Trong phần này chúng ta sẽ đề cập đến vấn đề cụ thể hơn. Sử dụng Wireshark và phân tích gói tin để giải quyết một vấn đề cụ thể của mạng.

Chúng tôi xin đưa ra một số tình huống điển hình.

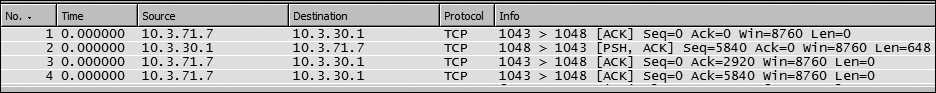
**A Lost TCP Connection (mất kết nối TCP)**

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:

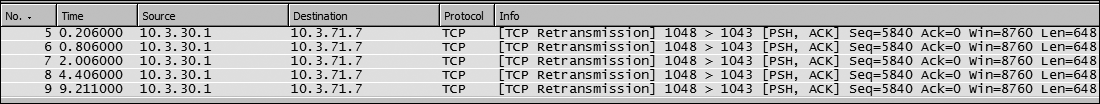
Một ví truyền file bị mất kết nối:

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



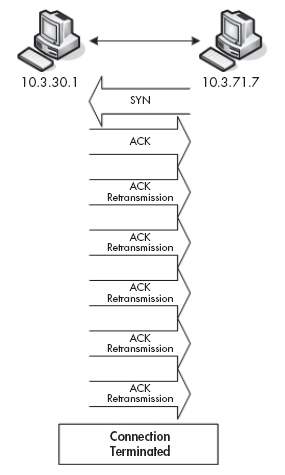
Hình 3.1-1: This capture begins simply enough with a few ACK packets.

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



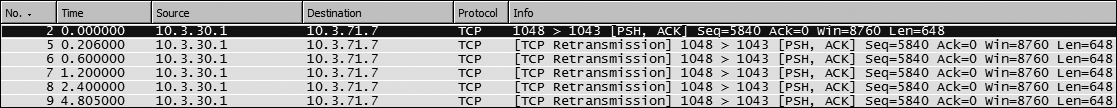
Hình 3.1-2: These TCP retransmissions are a sign of a weak or dropped connection.

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:

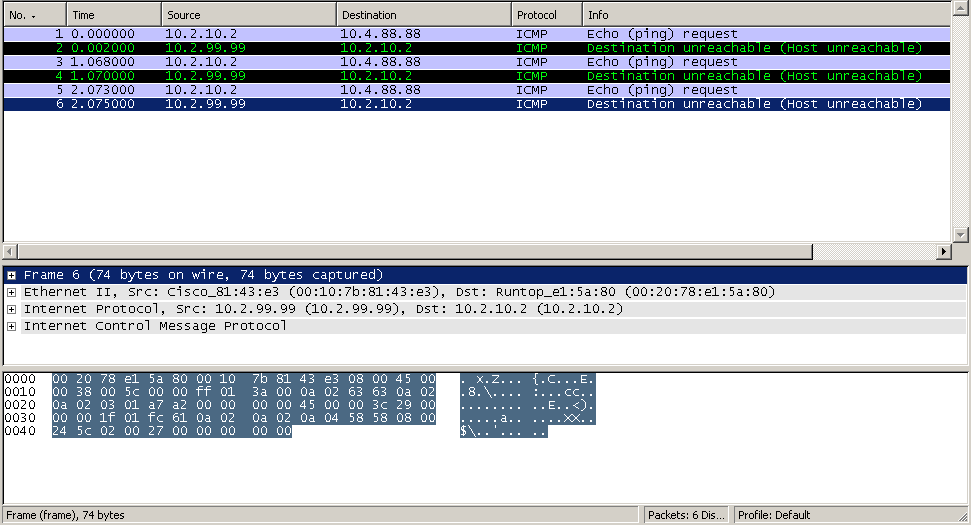


Hình 3.1-4: Windows will retransmit up to five times by default.

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.

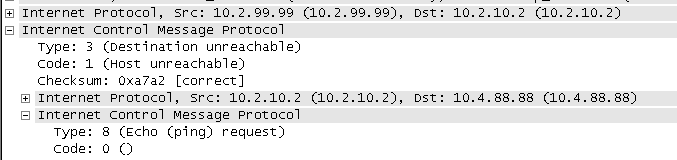


http://docs.google.com/File?id=dg34rcvn_84dgxj6bd3_b

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.

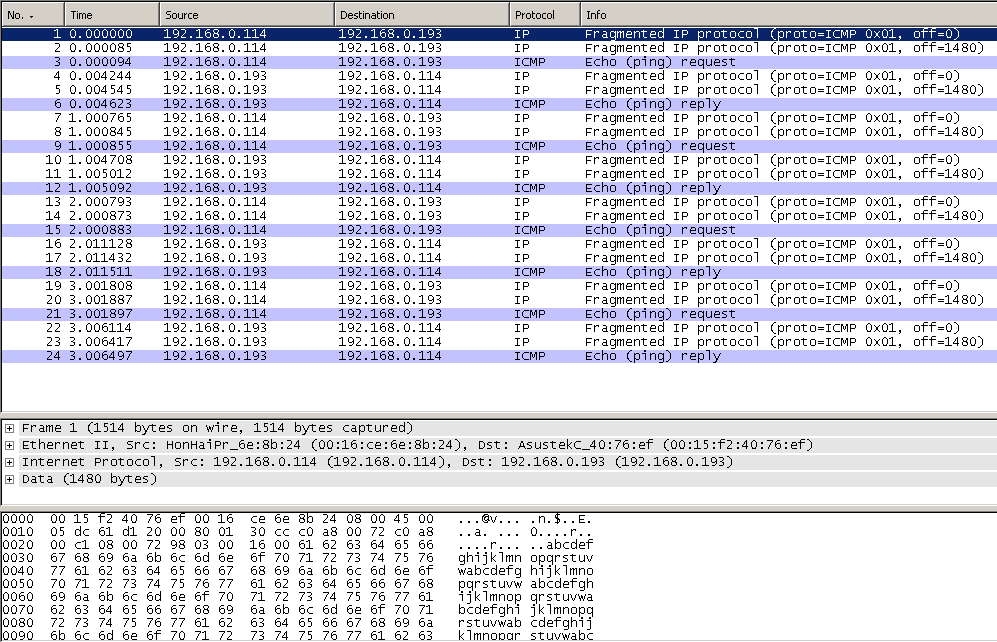
Kích thước gói tin ở đây là 3,072 bytes.

**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

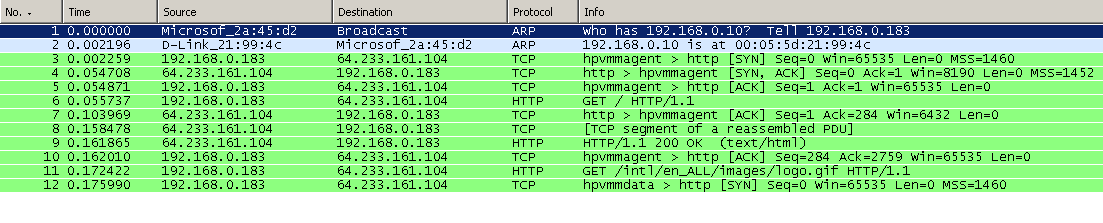
Nói tóm lại là 2 máy này được cấu hình không có gì khác nhau.

**Tiến hành**

Cài đặt Wireshark trực tiếp lên cả 2 máy.

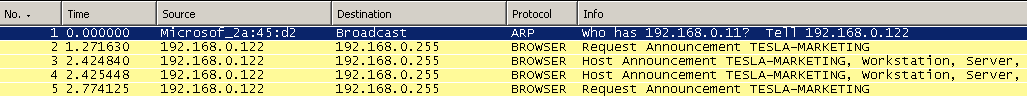
**Phân tích**

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.



Hình 3.1-12: Hải’s computer completes a handshake, and then HTTP data transfer begins.

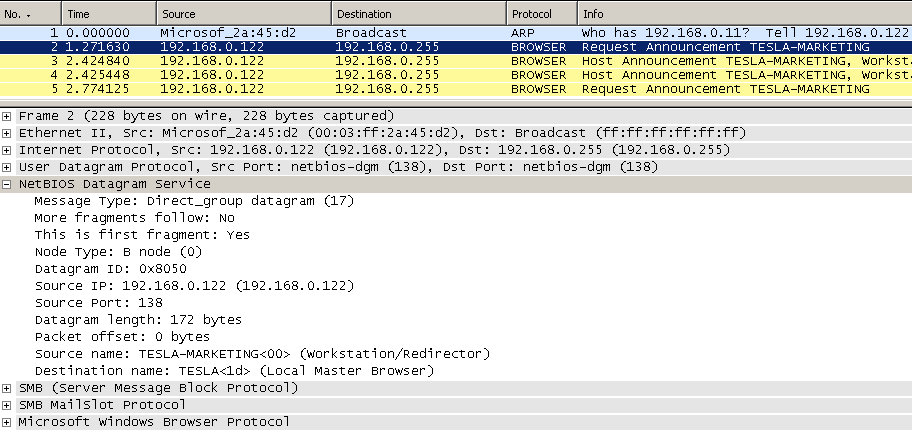
Trường hợp máy tính của Thanh



Hình 3.1-13: 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.

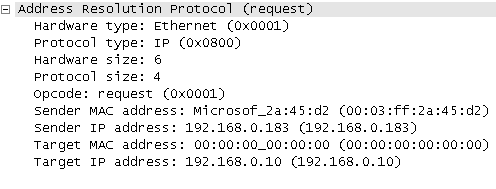
Như vậy có thể thấy NetBIOS có vấn đề.



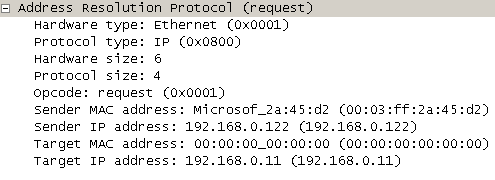
NetBIOS là giao thức cũ nó sẽ được thay thế TCP/IP khi TCP/IP không hoạt động. Như vậy là máy của Thanh không thể kết nối Internet với TCP/IP.

Chi tiết yêu cầu ARP trên 2 máy :

Máy Hải



Máy Thanh



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

**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**

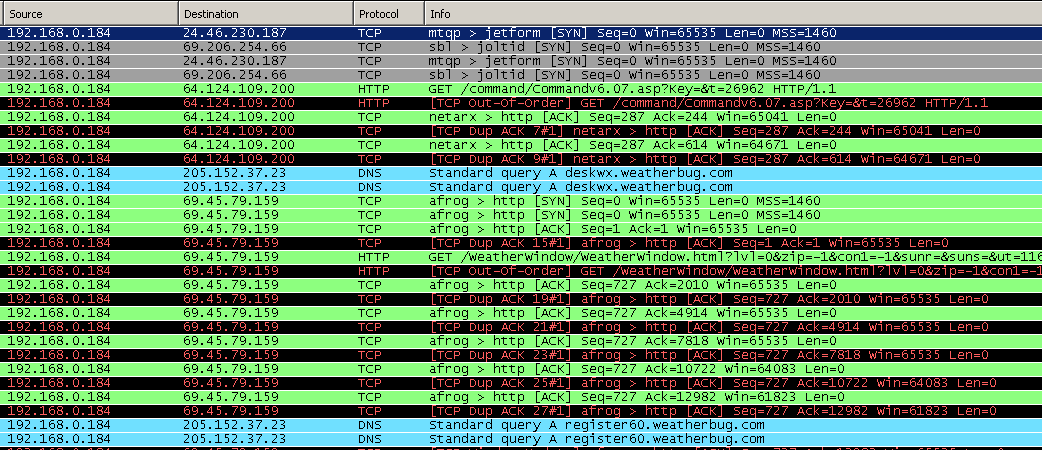
* A không thạo về máy tính lắm
* Máy tính của A dùng Widows XP, IE 6

**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

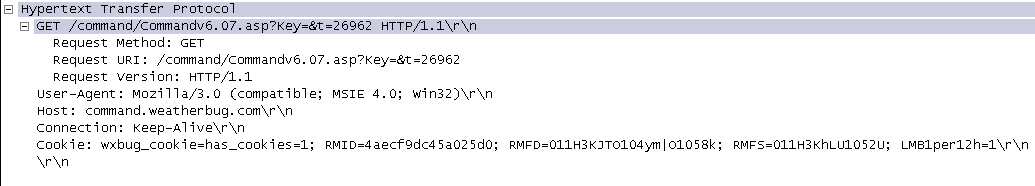
“Hubbing Out” .

**Phân tích**



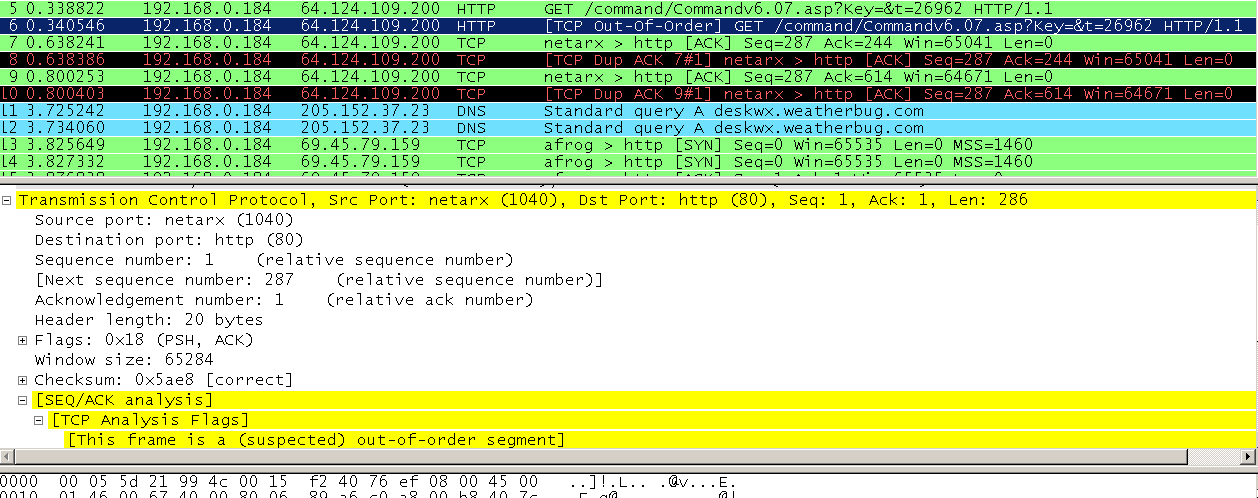
Hình 3.1-16: Since there is no user interaction happening on A’s computer at the time of this capture, all of these packets going across the wire should set off some alarms.

Chi tiết gói tin thứ 5:



Hình 3.1-17: Looking more closely at packet 5, we see it is trying to download data from the Internet.

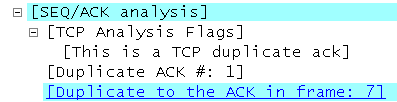
Từ máy tính gửi yêu cầu GET của HTTP đến địa chỉ như trên hình.



Hình 3.1-18: A DNS query to the weatherbug.com domain gives a clue to the culprit.

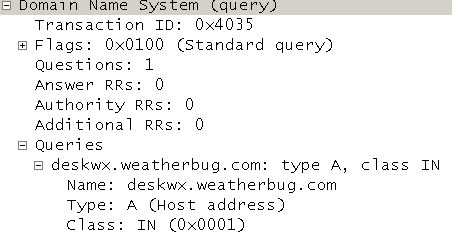
Gói tin trả lại bắt đầu có vấn đề : thứ tự các phần bị thay đổi.

Một số gói tiếp theo có sự lặp ACK.



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

**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.

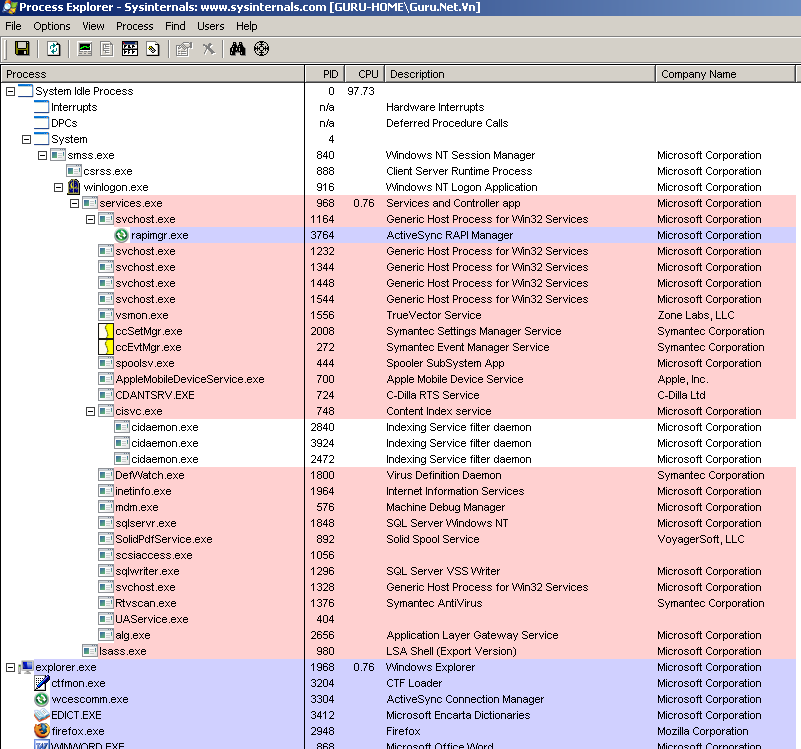
Thông tin chúng ta có

* FTP làm việc trên cổng 21

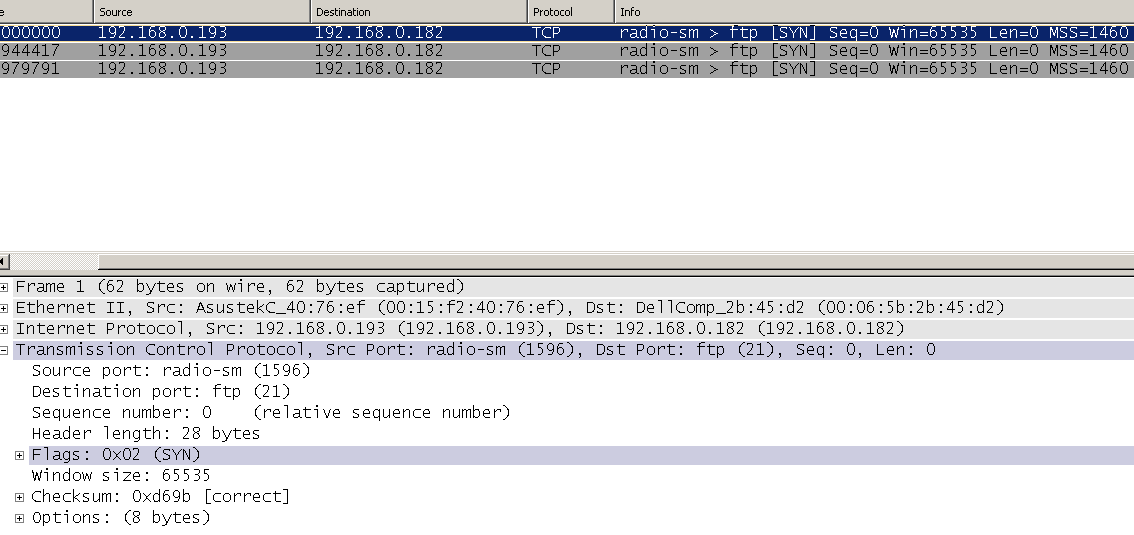
**Tiến hành**

Cài đặt Wireshark trên cả 2 máy.

**Phân tích**



Client:

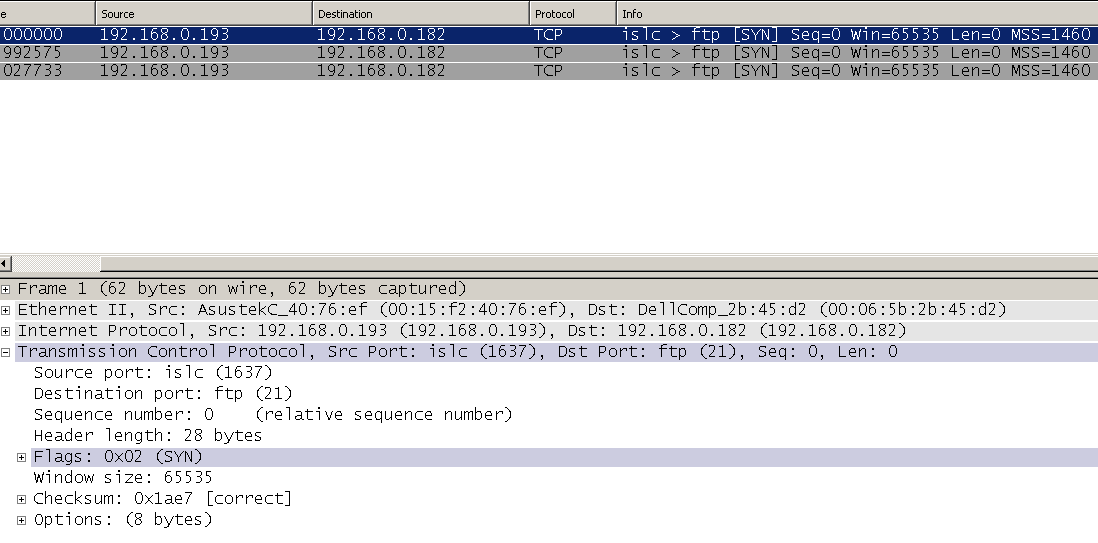


Hình 3.1-19: The client tries to establish connection with SYN packets but gets no response; then it sends a

few more.

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

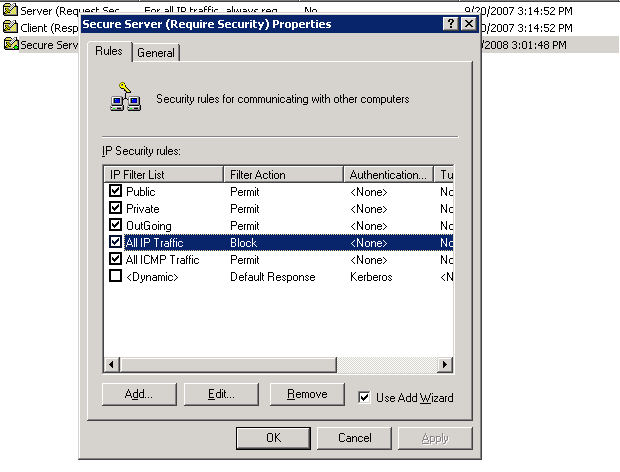
Server :



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.

-----------------------

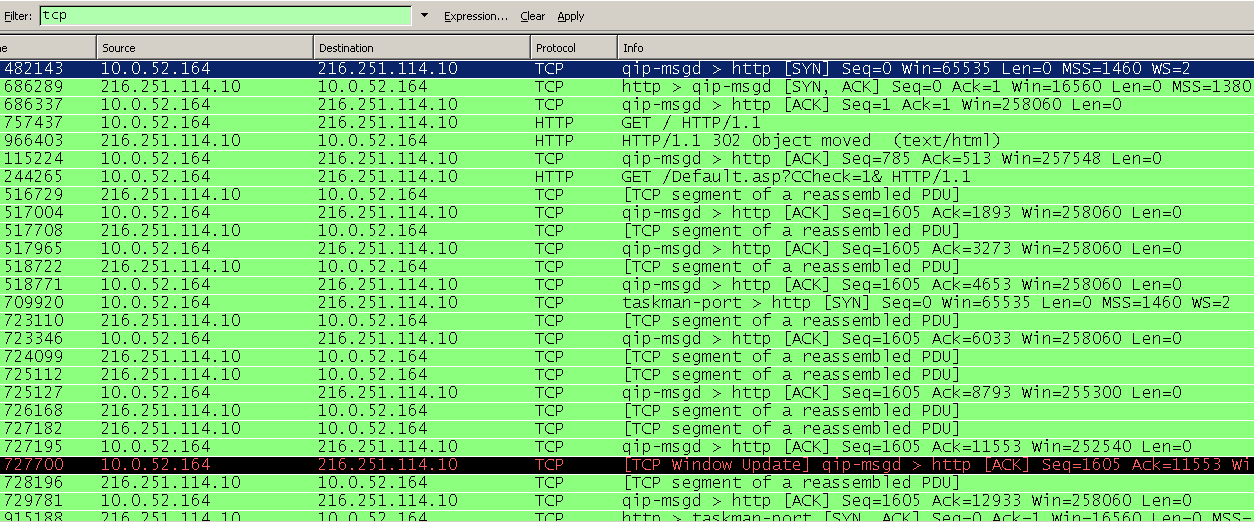
**2. Xử lý các tình huống về băng thông mạng**

**Anatomy of a Slow Download (cốt lõi của việc download chậm)**

**Tình huống:** cả mạng download rất chậm

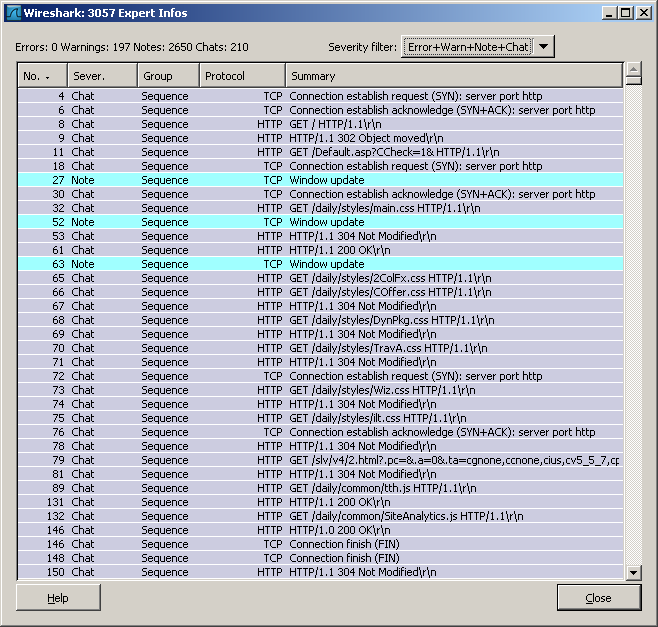
**Tiến hành :** đặt wireshark lắng nghe toàn bộ đầu ra của mạng

**Phân thích :** hình ảnh dưới đây cho thấy có rất nhiều kết nối TCP,HTTP điều này có nghĩa là có rất nhiều kết nối HTTP download dữ liệu về nên chiếm băng thông của mạng.

[](http://www.guru.net.vn/ct.ashx?id=253e84d1-26fb-407b-952e-9385396e16cb&url=http://docs.google.com/File?id=dg34rcvn_61fc67mfg9_b)

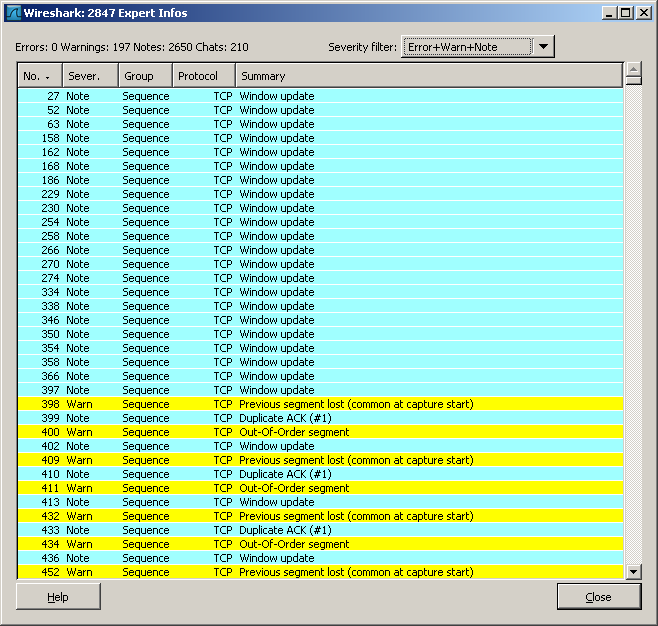
Hình 3.2-1: We need to filter out all of this HTTP and TCP traffic.

Mở cửa sổ **Alalyze->Expert Infos** để thấy thêm thông tin.



Hình 3.2-2: The Expert Infos window shows us chats, warnings, errors, and notes.

Mặc định **Expert Infos** hiển thị tất cả các thông tin. Nếu chỉ hiện thị **Error+Warn+Note** thì ta sẽ có các thông tin sau.



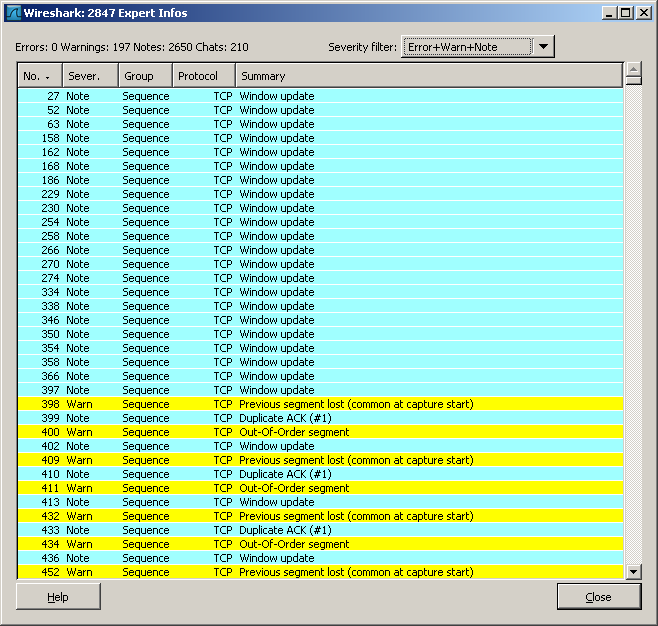
Hình 3.2-3: The Expert Infos window (sans chats) summarizes all of the problems with this download.

Hình trên cho thấy:

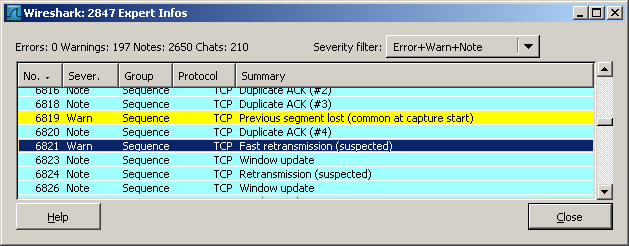
* có rất nhiều kết nối TCP do chương trình Window update mở
* có hiện tượng *TCP Previous segment lost packets* và các gói tin TCP gửi đi bị lặp ACK và bị drop, khiến TCP phải gửi lại gói tin.

⎝ có thể 2 nguyên nhân trên chiếm băng thông của mạng và làm giảm tốc độ download.

Khảo sát tiếp các thông tin theo hướng này ta nhận được các thông tin ở các hình phía dưới.

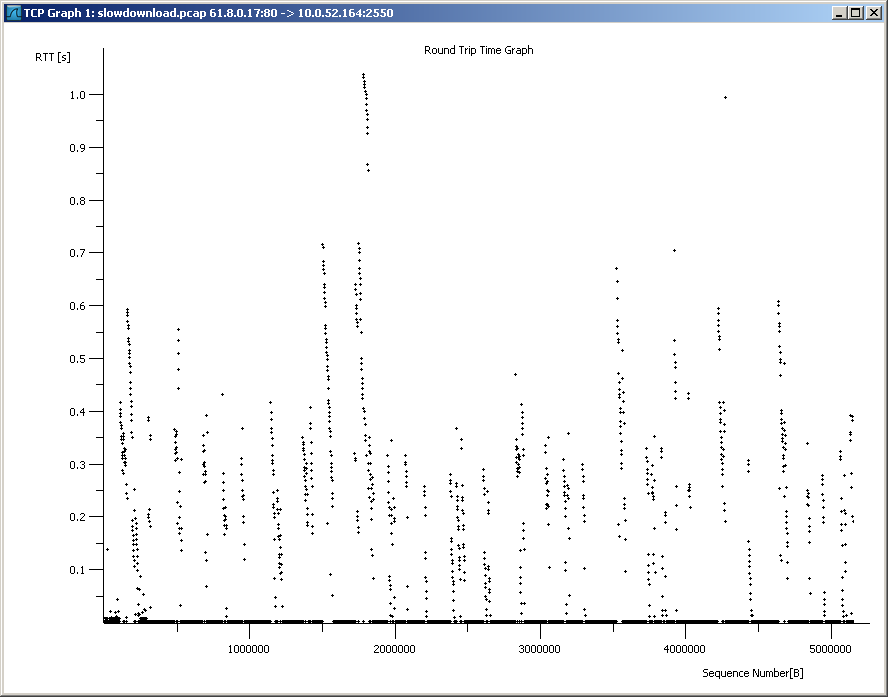


Hình 3.2-4: Previous segment lost packets indicate a problem.



Hình 3.2-5: A fast retransmission is seen after a packet is dropped.

**Statistics >TCP Stream Graph > Round Trip Time Graph**



Hình 3.2-6: The round trip time graph for this capture

Các hình cho thấy dự đoán ở bước trên là chính xác. Các file sẽ không thể được download về nếu thời gian lớn hơn 0.1 s, thời gian lý tưởng là 0,04s.

**Kết luận** : nguyên nhân do download chậm là có nhiều chương trình Windows update (có thể các máy để auto update) và hiện tượng mất gói tin. Như vậy cần tắt bớt các chương trình Windows update.

**Did That Server Flash Me?**

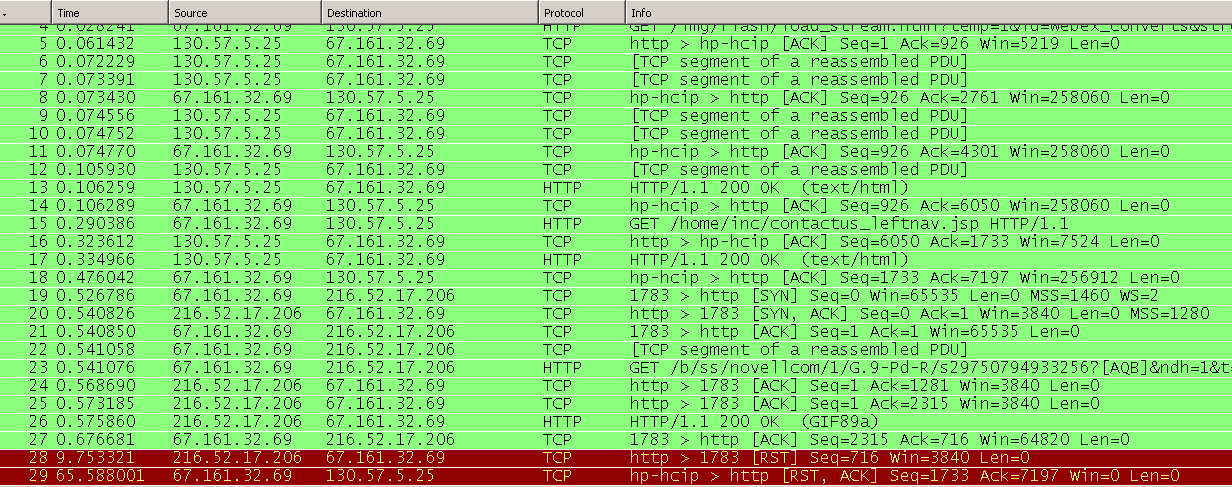
**Tình huống :** anh Thanh phàn nàn rằng không thể truy cập vào một phần website Novell để download một số phần mềm cần thiết. Mỗi lần truy cập vào site đó trình duyệt đều tải vài tải nhưng có gì hơn thế nữa. Mạng có vấn đề gì không ?

**Thông tin chúng ta có:** sau khi kiểm tra sơ bộ thì tất cả các máy tính đều bình thường trừ máy tính của anh Thanh. Như vậy vấn đề nằm ở máy tính của anh Thanh.

**Tiến hành:** cài Wireshark và bắt gói tin khi truy cập website Novell trên máy của Thanh

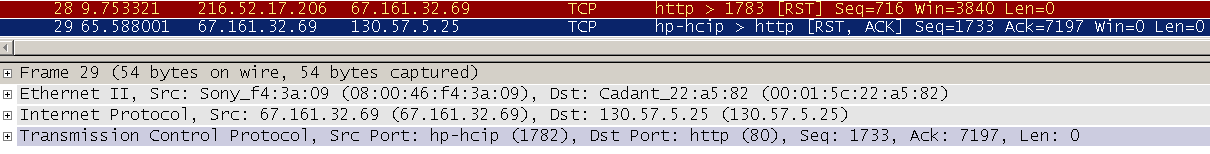
**Phân thích:**

Thông tin nhận được khi bắt đầu có kết nối HTTP đến website Novell:

[](http://www.guru.net.vn/ct.ashx?id=253e84d1-26fb-407b-952e-9385396e16cb&url=http://docs.google.com/File?id=dg34rcvn_669gpngnc7_b)

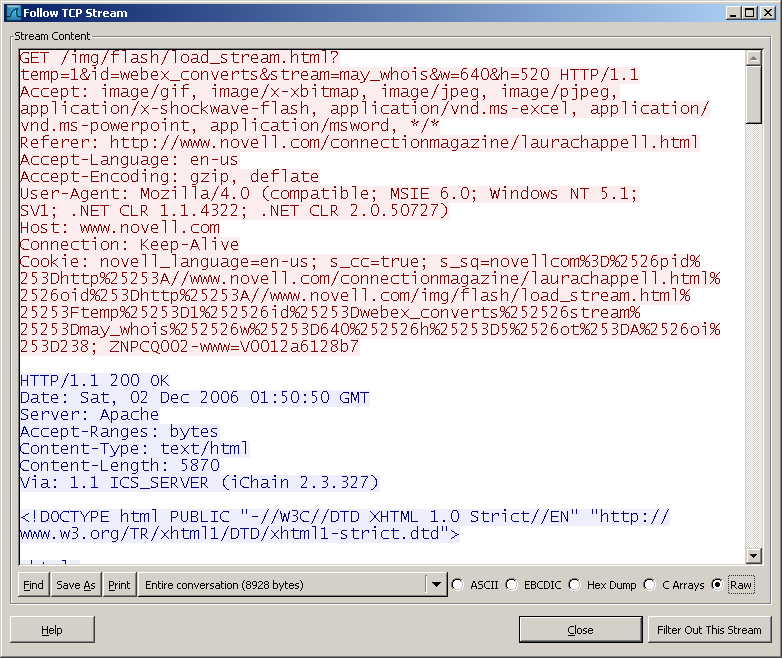
Hình 3.2-18: The capture begins with standard HTTP communication.

Từ phía client gửi gói tin RST để kết thúc kết nối HTTP:

[](http://www.guru.net.vn/ct.ashx?id=253e84d1-26fb-407b-952e-9385396e16cb&url=http://docs.google.com/File?id=dg34rcvn_67dbvcf3dq_b)

Hình 3.2-19: Packets 28 and 29 present a problem.

Lý do gì khiến client gửi gói tin RST ? Sử dụng một trong các tính năng cao cấp của Wireshark là Follow TCP Stream để thấy chi tiết nội dung mà phía server Novell trả về khi dùng hàm GET của HTTP.



Hình 3.2-20: This Flash request is the source of our problem.

Như vậy có thể nhìn thấy, phần Flash được mở dưới dạng PopUp nhưng Thanh không thấy gì. Kiểm tra thì thấy trình duyệt khóa tính năng PopUP.

**Kết luận :** trình duyệt block popup

**POP Goes the Email Server**

**Tình huống :** gửi thư chậm trong cùng domain và khác domain. Thời gian nhận được thư từ khi gửi từ 5-10 phút.

**Thông tin chúng ta có:**

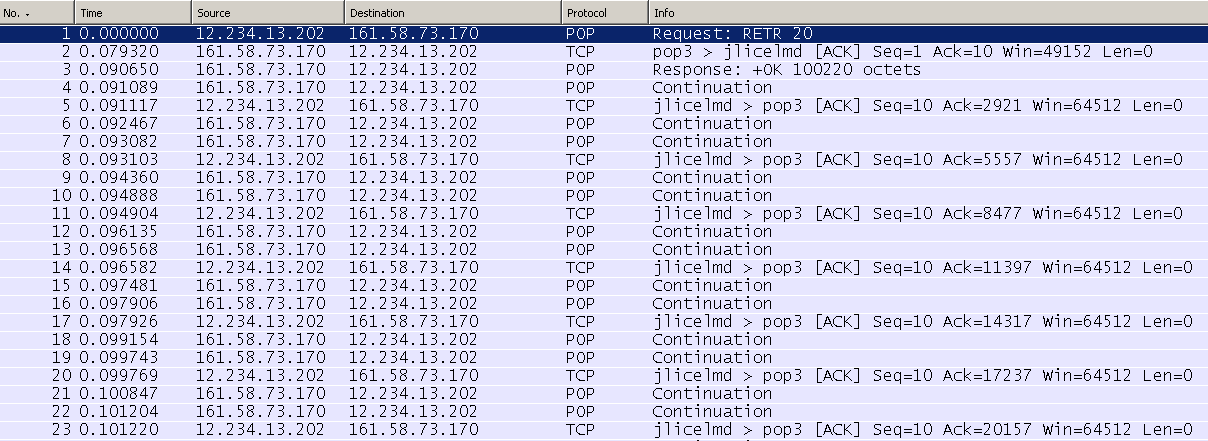
* Mail của công ty sử dụng một mail server riêng.
* Mail server dùng Post Office Protocol (POP) để nhận

**Tiến hành:**

Bắt gói tin tại máy mail server

**Phân thích:**

Thông tin về giao thức POP qua Wireshark

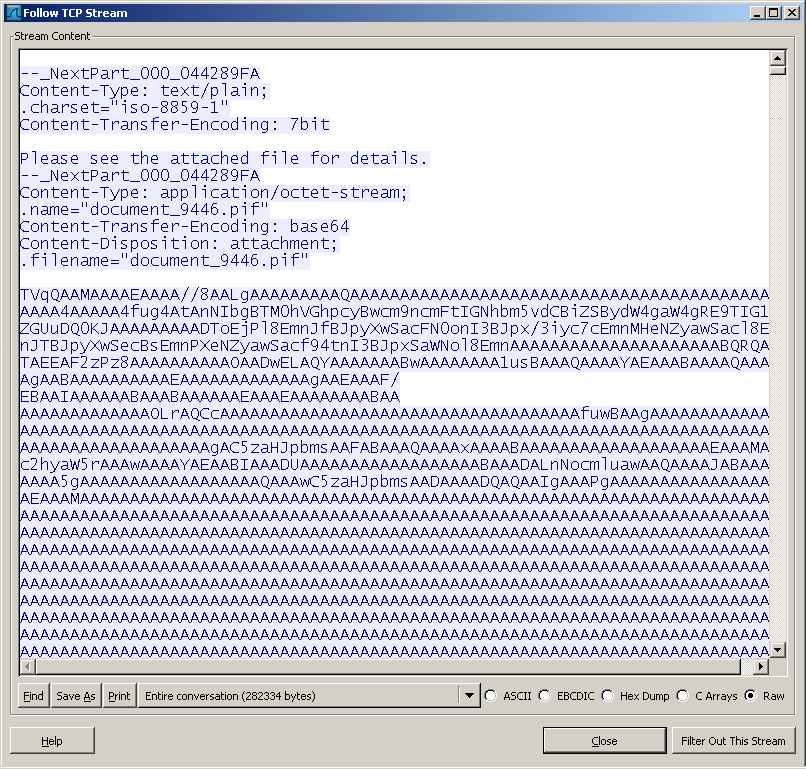
[](http://www.guru.net.vn/ct.ashx?id=253e84d1-26fb-407b-952e-9385396e16cb&url=http://docs.google.com/File?id=dg34rcvn_69fvphdjc7_b)

Hình 3.2-25: This capture includes a lot of POP packets.

http://docs.google.com/File?id=dg34rcvn_70c2299ccp_b

Hình 3.2-26: Changing the time display format gives us an idea of how much data we are receiving in what amount of time.

Sử dụng Follow TCP Stream để xem nội dung thư có file đính kèm thì nhận thấy như sau:



Hình 3.2-27: The details of packet 1 show information about the email being sent.

File đính kèm được chèn rất nhiều kí tự giống nhau vào để tăng kích thước file đính kèm, kiểm tra tiếp số lượng mail như thế này thì thấy số lượng lớn.

Có thể đi đến kết luận mail server bị spam làm cho năng lực xử lý các yêu cầu gửi đến bị giảm xuống, tương tự như tấn công từ chối dịch vụ.

**Hướng giải quyết :** tìm và phát hiện nguồn của thư rác, có thể dùng blacklist để cấm các địa chỉ gửi thư rác.

**Kết luận :** spam mail với file attach lớn

**3. Một số tình huống an ninh mạng cơ bản**

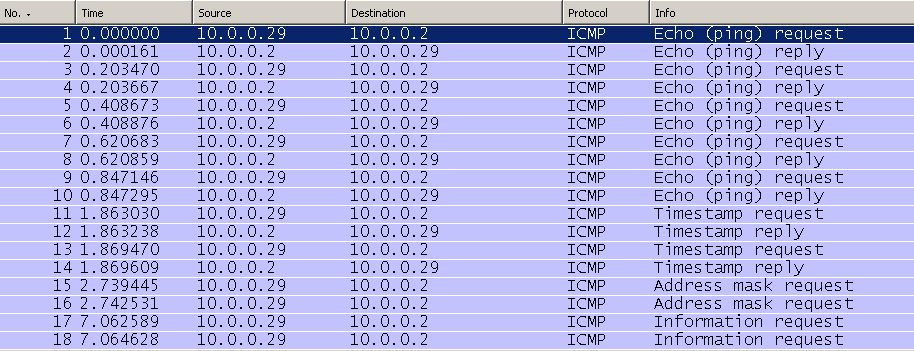
**OS Fingerprinting (Nhận dạng OS)**

**OS Fingerprinting** là một kỹ thuật phổ biến được các haker sử dụng để thu thập các thông tin về server từ xa, từ đó có những thông tin hữu ích để thực hiện các bước tấn công tiếp theo.

Như xác định các lỗi có thể có với server mục tiêu, chuẩn bị các công cụ phù hợp cho cuộc tấn công.

Một trong các kỹ thuật xử dụng là gửi các gói tin ICMP ít thông dụng.

* Sử dụng ICMP traffic,dùng ping sẽ không bị “cảnh báo”
* Sử dụng traffic like Timestamp request/reply, Address mask request, Information request không phổ biến lắm.



Hình 3.3-1: This is the kind of ICMP traffic you don’t want to see.

Dùng các ICMP request không phổ biến như trên đôi khi sẽ nhận được những thông tin từ mục tiêu phản hồi lại.

Nếu các request đó được chấp nhận thì có thể dùng *ICMP-based OS fingerprinting scans* để quét thử.

**Xử lý :** vì các traffic thông thường sẽ không bao giờ thấy các gói ICMP loại 13,15,17 do đó chúng ta có thể tạo ra bộ lọc để lọc các gói này.

Ví dụ : icmp .type==13 || icmp .type==15 || icmp .type==17.

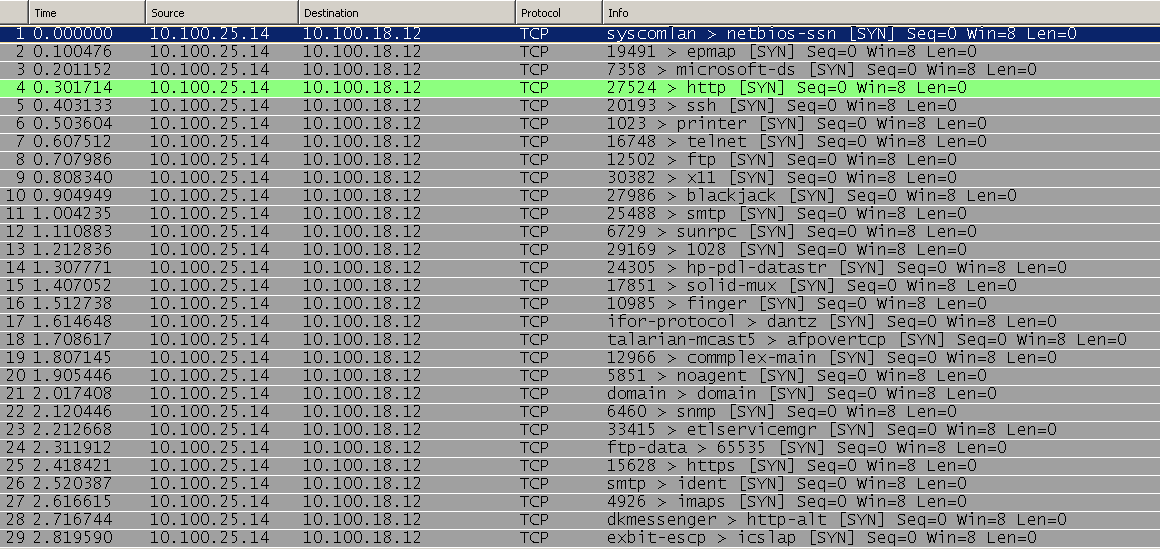
**A Simple Port Scan (quét cổng ở dạng đơn giản)**

Một trong các chương trình quét port nhanh và phổ biến nhất là : nmap

Mục tiêu của người tấn công:

* tìm các port mở
* xác định các tunnel bí mật

Chúng ta có thể nhận dạng việc quét cổng bằng cách đặt máy “nghe” trên máy chủ cần bảo vệ để theo dõi.

[](http://www.guru.net.vn/ct.ashx?id=253e84d1-26fb-407b-952e-9385396e16cb&url=http://docs.google.com/File?id=dg34rcvn_73ctcgc3dv_b)

Hình 3.3-2: A port scan shows multiple connection attempts on various ports.

Như trên hình có thể nhận ra rằng có những kết nối rất đáng nghi ngờ giữa máy 10.100.25.14 (local machine) và máy 10.100.18.12 (remote computer).

Log file cho thấy máy tính từ xa (remote computer) gửi gói tin đến rất nhiều cổng khác nhau trên máy local ví dụ cổng 21,1028…

Nhưng đặc biệt là những cổng nhạy cảm như telnet (22), microsoft-ds, FTP (21), và SMTP (25) những cổng này được gửi số lượng gói tin lớn hơn vì đây là những cổng có khả năng xâm nhập cao do lỗi của những ứng dụng sử dụng cổng này. Các gói tin đó có thể là các đoạn mã khai thác.

**Blaster Worm (Sâu Blaster)**

**Hiện tượng:** Máy tính phía client hiển thị của sổ thông báo shutdown máy trong vòng 60s. Các thông báo này xuất hiện liên tục.

**Thông tin chúng ta có:**

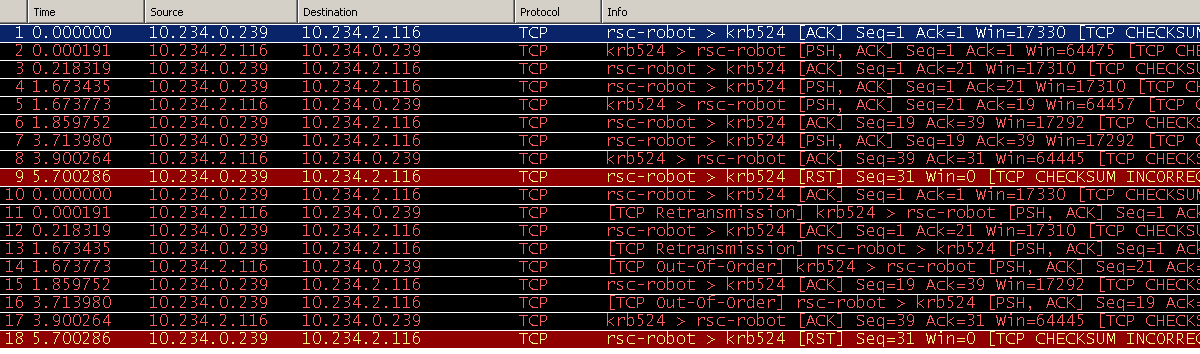
* máy tính client đã cài chương trình diệt virus mới nhất tại thời điểm đó

**Tiến hành:**

Cài đặt Wireshark trên máy có virus.

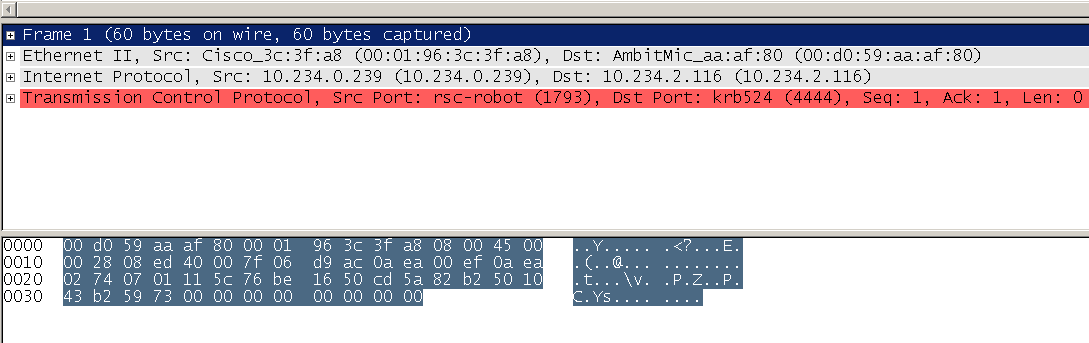
**Phân tích:**

Màn hình Wireshark đã thể hiện các hành vi có nguy hại đến máy tính của virus Blaster, được thể hiện bằng màu đỏ, đen.

[](http://www.guru.net.vn/ct.ashx?id=253e84d1-26fb-407b-952e-9385396e16cb&url=http://docs.google.com/File?id=dg34rcvn_74drzbrdgc_b)

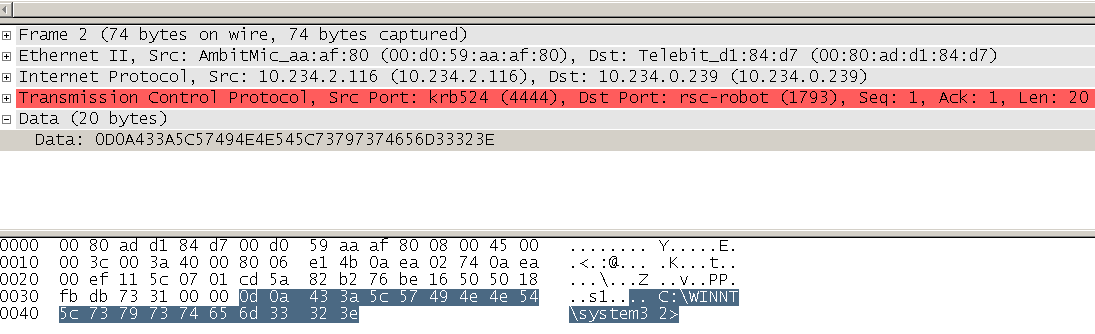
Hình 3.3-9: We shouldn’t see this level of network activity with only the timer running on this machine.

Một trong các kinh nghiệm để phát hiện virus là xem dữ liệu các gói tin ở dạng thô (raw), rất có thể sẽ có những thông tin hữu ích.

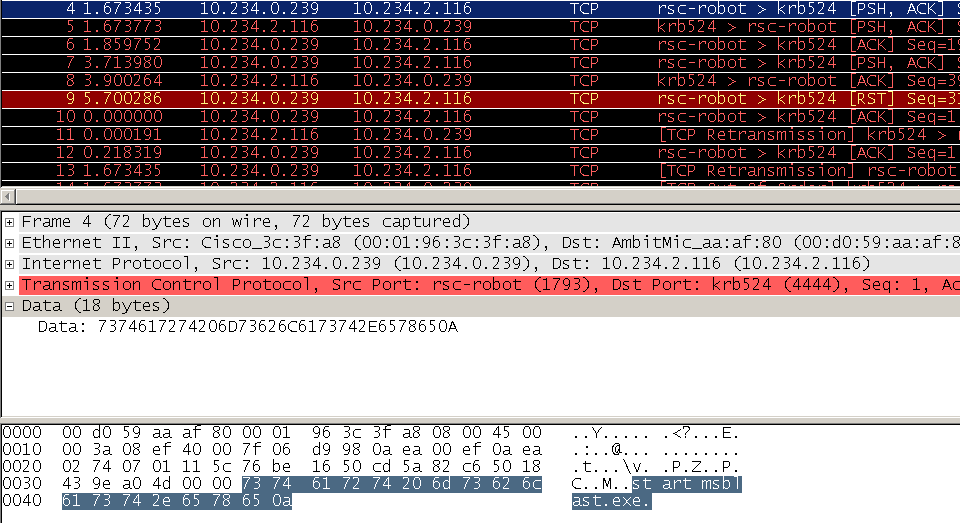
[](http://www.guru.net.vn/ct.ashx?id=253e84d1-26fb-407b-952e-9385396e16cb&url=http://docs.google.com/File?id=dg34rcvn_75c4wd7vdz_b)

Hình 3.3-10: No useful information can be discerned from packet 1.

Sau khi tìm một số gói tin thì thấy có gói tin mang lại thông tin hữu ích.

Hình 3.3-11, chúng ta thấy có địa chỉ trỏ đến thư mục C:\WINNT\System32. Thư mục này là một trong những thư mục quan trong nhấ[](http://www.guru.net.vn/ct.ashx?id=253e84d1-26fb-407b-952e-9385396e16cb&url=http://docs.google.com/File?id=dg34rcvn_76t6c3vfgs_b)t của hệ điều hành Windows.

Hình 3.3-11: The reference to C:\WINNT\System32 means something might be accessing our system files.

Tiếp tục tìm thông tin theo cách trên, phát hiện ra tên chương trình của sâu Blaster như ở hình 3.3-12.[](http://www.guru.net.vn/ct.ashx?id=253e84d1-26fb-407b-952e-9385396e16cb&url=http://docs.google.com/File?id=dg34rcvn_77ds489ghx_b)

Hình 3.3-12: Packet 4 shows a reference to msblast.exe.

Khi đã xác định được ví trí file của virus ta sẽ có nhiều cách giải quyết theo các mục đích khác nhau. Đối với người dùng thông thường thì tắt tiến trình có tên đó sau đó xóa các file virus đó đi…

Trong khuôn khổ tiểu luận chúng tôi đã nêu ra một số vấn đề cơ bản có thể xử lý bằng cách sử dụng Wireshark và kỹ năng phân tích gói tin.

Ngoài ra còn có rất nhiều tình huống khác và các tình huống nâng cao hơn tuy nhiên chúng tôi không đề cập ở đây.

Các vấn đề khác bạn đọc có thể tham khảo thêm qua tài liệu chúng tôi nêu ở phần phụ lục.