HƯỚNG DẪN SỬ DỤNG PHẦN MỀM
ETHEREAL

Mục lục

1. Giới thiệu

Ethereal

Ethereal là phần mềm thu thập các gói tin truyền trên mạng, sau đó thực hiện phân tích để hiển thị khuôn dạng dữ liệu của từng gói tin dưới dạng tường minh nhất có thể.
Ethereal có thể được sử dụng như một thiết bị giám sát những gì được truyền đường dây mạng - tức là hoạt động giống như một chiếc Vôn kế trên đường dây điện.
Trước đây, những công cụ như vậy hoặc đắt tiền hoặc độc quyền nhưng *Ethereal* lại là phần mềm mã nguồn mở phân tích gói tin tốt nhất hiện nay. Phiên bản mới nhất của *Ethereal* có thể tải từ website

http://www.ethereal.com/download.html.

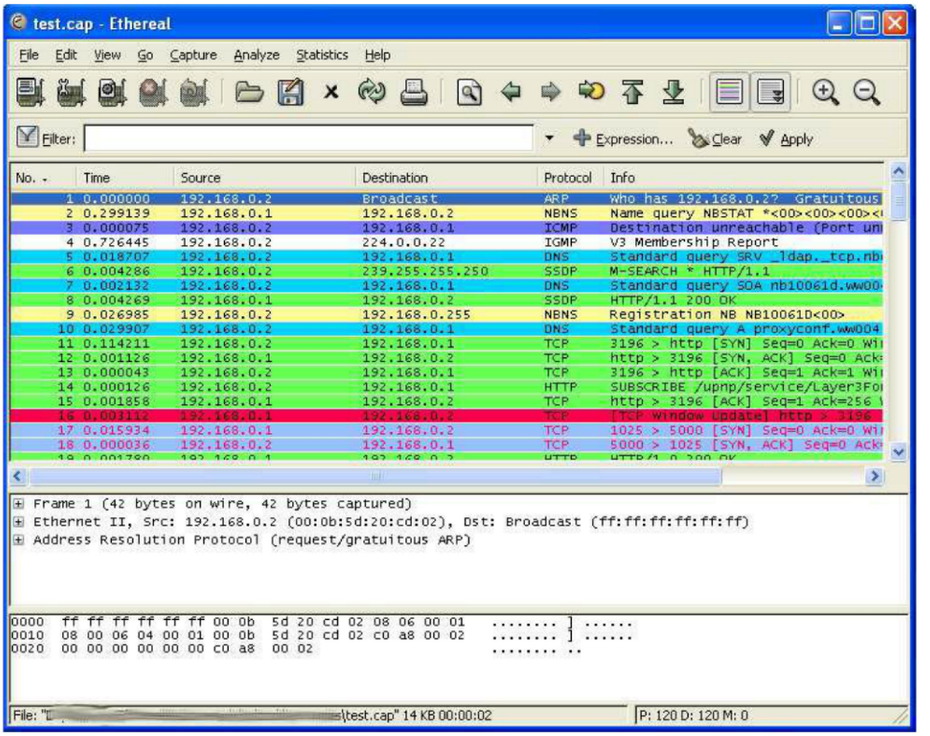
Mục đích sử dụng

- Người quản trị mạng khắc phục lỗi mạng
- Kĩ sư an ninh mạng xem xét các vấn đề bảo mật
- Người phát triển phân tích và gỡ rối hoạt động của các giao thức.
- Người dùng nghiên cứu bản chất giao thức mạng
- …

Tính năng

- Được cài đặt trên hai HĐH phổ biến là UNIX và Windows
- Thu thập ngay lập tức các gói tin lan tỏa đến card mạng
- Hiển thị các gói tin với những thông tin về giao thức chi tiết
- Có thể lưu giữ dữ liệu thu thập được vào file để sau này sử dụng lại
- Lọc gói tin theo nhiều tiêu chuẩn
- Tìm kiếm gói tin theo nhiều tiêu chuẩn
- Hiển thị màu sắc các gói tin dựa trên cơ chế lọc (để nhìn rõ hơn)
- Tạo nhiều thống kê khác nhau

Hình sau biểu diễn các gói tin *Ethereal* đã được thu thập và sẵn sàng để phân tích.



Ethereal được phát âm thế nào?

Ethereal có thể được phát âm theo 3 cách:

- E'thereal: trọng âm ở 'the' (xem thêm từ điển Anh-Việt)
- Ether-real
- E-the-real

Bạn có thể phát âm theo cách riêng của mình, miễn là bạn cảm thấy thoải mái. *Ethereal* User's Guide đưa ra cách phát âm chính thức là: "e-the-real".

2. Cài đặt *Ethereal*

File cài đặt chương trình cài đặt *Ethereal* (File *Ethereal*-setup-x.y.z.exe) có thể được tải về từ trang: http://www.Ethereal.com/download.html#releases

Các thành phần

- *Ethereal* GTK 1 hoặc 2: chương trình đồ họa phân tích giao thức mạng (*Ethereal* GTK2 được khuyến nghị vì sử dụng bộ công cụ hiện đại GTK2 GUI)

- GTK-Wimp: giả lập GTK2 windows
- Tethereal: chương trình phân tích giao thức mạng dựa trên dòng lệnh

Các công cụ

- Editcap: chương trình đọc file dữ liệu đã thu thập và ghi một số chọn lọc (hoặc tất cả) các gói tin sang một file dữ liệu khác.
- Text2Pcap: chương trình đọc mã ASCII và ghi dữ liệu vào một file.
- Mergecap: chương trình kết hợp nhiều file dữ liệu thành một file duy nhất.
- Capinfos: chương trình cung cấp thông tin về các file dữ liệu.

Các chức năng khác

- Start Menu ShortCuts: thêm shortcuts vào Start Menu
- Desktop Icon: thêm biểu tượng *Ethereal* vào màn hình Desktop
- Quick Launch Icon: thêm biểu tượng *Ethereal* vào thanh Explorer Quick launch

Chương trình WinPCap

WinPCap là chương trình dùng để thu thập tức thì các luồng dữ liệu trong mạng. Nếu chưa cài đặt WinPcap, bạn chỉ có thể sử dụng *Ethereal* để mở các file thu thập dữ liệu có sẵn. Vì vậy, *Ethereal* và WinPcap thường được cài đặt cùng nhau.

Tuy nhiên, kể từ phiên bản *Ethereal* 0.10.12, bộ cài WinPcap đã được tích hợp vào bộ cài *Ethereal* nên bạn không cần phải tải về và cài đặt hai gói phần mềm riêng biệt nữa

Thông tin thêm về WinPcap:

- http://wiki.Ethereal.com/WinPcap
- http://www.winpcap.org

3. Giao diện người dùng

Giới thiệu

Sau khi cài đặt thành công, chúng ta bắt đầu nghiên cứu giao diện cũng như cách sử dụng của chương trình Ethreal :

- Giao diện người dùng *Ethereal*
- Cách bắt các gói tin
- Cách xem các gói tin
- Cách lọc gói tin

Cửa sổ chính

Cửa sổ chính của *Ethereal* cũng giống như trong các chương trình máy tính khác. Dưới đây là giao diện mà người dùng thường gặp sau khi các gói tin được bắt và hiển thị:

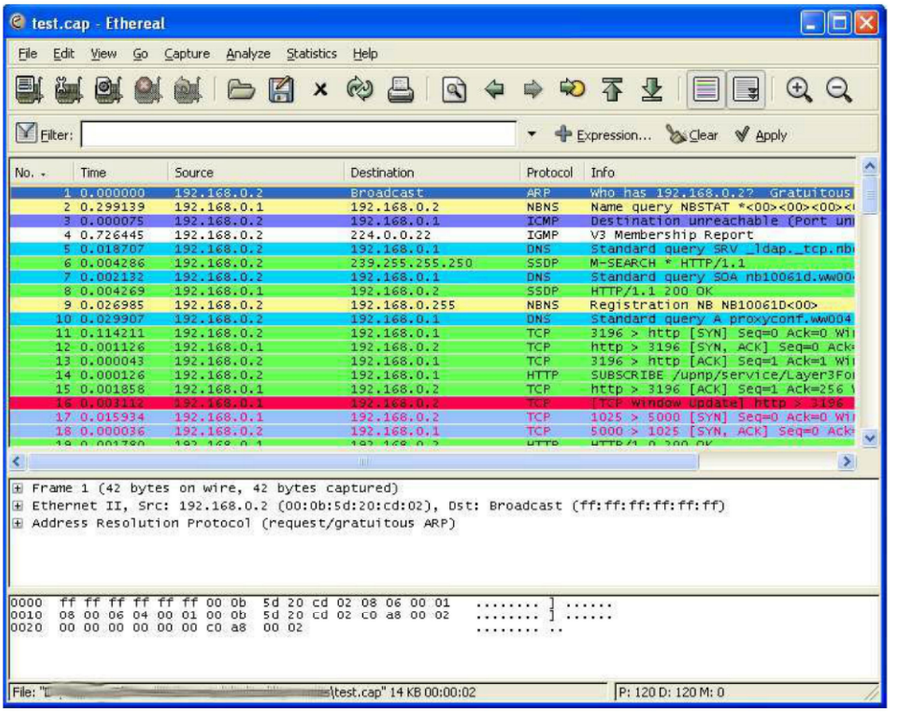
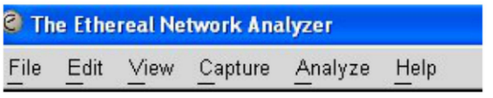


Figure 1 – Giao diện tổng quát của chương trình

Bố cục của cửa sổ chính có thể được chỉnh lại bằng cách thiết lập Preference.

Thanh Menu



- File: chứa các lệnh mở hay kết hợp các file dữ liệu thu thập, lệnh lưu/ in/ kết xuất toàn bộ hoặc một phần file dữ liệu thu thập, lệnh đóng chương trình *Ethereal*.
- Edit: chứa các lệnh tìm gói tin, tham chiếu thời gian hoặc đánh dấu một hay nhiều gói tin, thiết lập các tùy chọn.
- View: chứa lệnh điều khiển việc hiển thị dữ liệu thu được, bao gồm việc tô màu các gói tin, phóng to cỡ font, biểu diễn gói tin trong cửa số riêng, mở rộng hoặc thu hẹp cây chi tiết gói tin…

- Capture: chứa lệnh bắt đầu hoặc kết thúc việc thu thập các gói tin và lệnh hiệu chỉnh bộ lọc.
- Analyze: chứa các lệnh thao tác trên bộ lọc hiển thị, cho phép hoặc không cho phép phân tích chi tiết các giao thức, định cấu hình bộ giải mã cho người dùng và "lần" theo vết của một luồng TCP.
- Statistics: chứa các lệnh hiển thị các kết quả thống kê khác nhau, bao gồm bảng tóm tắt của các gói tin đã được bắt, hiển thị cấu trúc phan tầng các giao thức.
- Help: giúp đỡ người dùng sử dụng các chức năng cơ bản, xem danh sách các giao thức được hỗ trợ, các trang hướng dẫn, các trang web, và hộp thoại About như thường lệ.

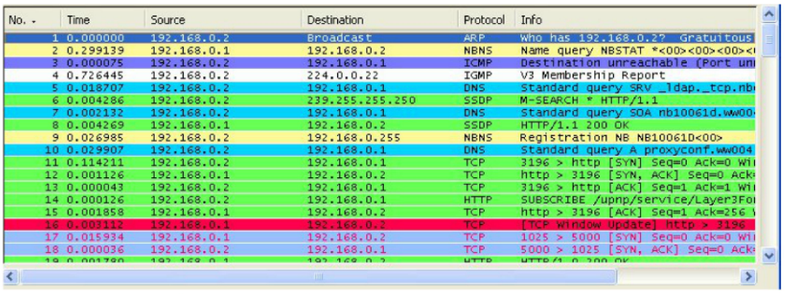
Thanh công cụ chính (Main Toolbar)

Thanh công cụ chính có các nút lệnh giúp người sử dụng nhanh chóng ra các lệnh cần thiết

Thanh lọc (Filter Toolbar)

Thanh công cụ lọc cung cấp các thao tác trực tiếp trên bộ lọc hiển thị đang được sử dụng.

Ô liệt kê gói tin (Packet List Pane)



Ô liệt kê gói tin hiển thị tóm tắt về mỗi gói tin bắt được.

Mỗi dòng trong danh sách ứng với một gói tin trong file dữ liệu thu thập. Nếu chọn một dòng trong ô này, ô Packet Details và Packet Bytes sẽ hiển thị thông tin chi tiết về gói tin tương ứng.

Khi phân tích một gói tin, *Ethereal* sẽ lấy thông tin từ bộ phân tích giao thức và đặt vào các cột. Vì thông tin về giao thức ở tầng cao sẽ ghi đè lên thông tin của giao thức ở tầng thấp nên bạn sẽ chỉ nhìn thấy thông tin giao thức tầng cao nhất có thể.

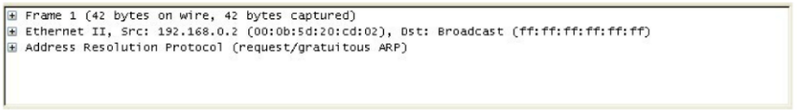
Ví dụ, giả sử một gói tin TCP nằm bên trong gói tin IP, gói tin IP lại nằm bên trong frame Ethernet. Bộ phân tích Ethernet ghi dữ liệu của mình (chẳng hạn địa chỉ card mạng), sau đó bộ

phân tích IP ghi đè bằng dữ liệu IP (ví dụ địa chỉ IP), và cuối cùng bộ phân tích TCP sẽ ghi đè lên thông tin về IP..
Có rất nhiều cột thông tin khác nhau và có thể chọn hiển thị cột nào bằng cách thiết lập tùy chọn (Preference settings).

The default columns will show:

- **No.** The number of the packet in the capture file. This number won't change, even if a display filter is used.
- **Time** The timestamp of the packet. The presentation format of this timestamp can be changed, see Section 6.9, "Time display formats and time references".
- **Source** The address where this packet is coming from.
- **Destination** The address where this packet is going to.
- **Protocol** The protocol name in a short (perhaps abbreviated) version.
- **Info** Additional information about the packet content

Ô chi tiết gói tin (Packet Details Pane)

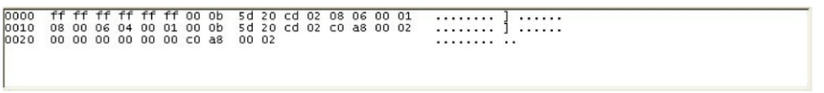


Ô chi tiết gói tin hiển thị chi tiết gói tin được chọn ở ô liệt kê gói tin.
Giao thức và các trường của gói tin được biểu diễn dưới dạng cây, có thể dễ dàng mở rộng hoặc thu gọn lại.

Some protocol fields are specially displayed.

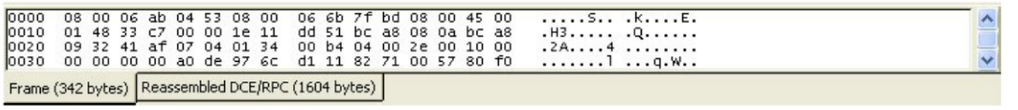
- **Generated fields** Ethereal itself will generate additional protocol fields which are surrounded by brackets. The information in these fields is derived from the known context to other packets in the capture file. For example, Ethereal is doing a sequence/acknowledge analysis of each TCP stream, which is displayed in the [SEQ/ACK analysis] fields of the TCP protocol.
- **Links** If Ethereal detected a relationship to another packet in the capture file, it will generate a link to that packet. Links are underlined and displayed in blue. If double-clicked, Ethereal jumps to the corresponding packet

Ô mã nhị phân gói tin (Packet Bytes Pane)



Ô mã nhị phân hiển thị dữ liệu biểu diễn dưới dạng cơ số 16 của gói tin được chọn (là gói tin được chọn trong ô gói tin chi tiết).

Cột bên trái ghi vị trí tương đối (offset) của dữ liệu trong gói tin, cột ở giữa là dữ liệu được biểu diễn dưới dạng cơ số 16 và cột bên phải là kí tự ASCII tương ứng (hoặc dấu chấm ('.') nếu kí tự không hiển thị được).
Tùy thuộc vào dữ liệu gói tin, đôi khi ô này chứa nhiều trang, chẳng hạn như khi *Ethereal* ráp nhiều gói tin lại thành một khối dữ liệu duy nhất. Trong trường hợp này, một vài tab sẽ xuất hiện ở đáy của ô để có thể lựa chọn các trang cần xem.



Thanh trạng thái (Statusbar)

Thanh trạng thái biểu diễn một số thông tin thêm về trạng thái hiện tại của chương trình và các dữ liệu thu thập được. Thông thường phần bên trái sẽ hiển thị thông tin liên quan đến ngữ cảnh (tên, kích thước của file dữ liệu thu thập, thời gian thực hiện thu thập), trong khi phần bên phải hiển thị số lượng gói tin hiện đã thu thập được.
Các chú thích viết tắt:

- P: số gói tin bắt được
- D: số gói tin đang được hiển thị
- M: số gói tin được đánh dấu

4. Thu thập tức thì dữ liệu trong mạng

4.1 Giới thiệu

Thu thập tức thì dữ liệu trong mạng là một trong những tính năng chủ yếu của *Ethereal*. *Ethereal* cung cấp các chức năng sau:

- Thu thập thông tin từ các kiểu kiến trúc phần cứng mạng khác nhau (Ethernet, Token Ring, ATM,…).
- Chấm dứt việc thu thập thông tin khi một trong số các chỉ tiêu sau đạt được: độ lớn dữ liệu thu thập, thời gian thu thập hay tổng số gói tin bắt được.
- Hiển thị các gói tin đã được phân tích trong khi vẫn tiếp tục thu thập thông tin.
- Lọc gói tin, giảm độ lớn của dữ liệu.
- Ghi ra nhiều file khác nhau. Có thể lựa chọn để ghi dữ liệu thu được lần lượt và theo thứ tự xoay tròn vào các file và giữ lại x file cuối cùng. Điều này cực kỳ có ích khi cần thu thập dữ liệu trong thời gian dài.

Tuy nhiên, các tính năng sau chưa có trong *Ethereal*:

- Bắt thông tin đồng thời từ nhiều card mạng khác nhau (tuy nhiên, có thể chạy nhiều chương trình *Ethereal* ứng với các card mạng khác nhau cùng lúc và sau đó kết hợp – các file dữ liệu được thu thập lại).
- Chấm dứt việc bắt thông tin (hay thực hiện một hành động nào đó) dựa trên dữ liệu được thu thập.

Các thao tác thực hiện việc thu thập dữ liệu (khởi động/ dừng/ khởi động lại) được chọn từ menu **Capture** trên thanh Menu.

4.2. Start Capturing

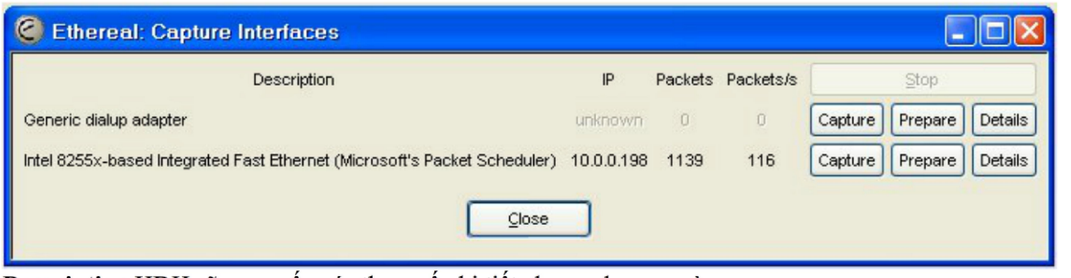
Để thu thập gói tin trong Ethereal, chúng ta có thể sử dụng một trong các phương thức sau:

- Nhấn vào biểu tượng  trên thanh công cụ. Quá trình thu thập có thể được khởi tạo sau khi bấm vào nút "Capture" trong hộp hội thoại.
- Nhấn vào biểu tượng  trên thanh công cụ để đặt các tham số tùy chọn.
- Nếu đã đặt hết các tham số, có thể ấn vào nút  trên thanh công cụ để bắt đầu quá trình thu thập..
- Nếu biết được tên của card mạng được , bạn có thể khởi tạo Ethereal bằng cách đánh lệnh ethereal -i eth0 -k

  Lệnh này khởi tạo chương trình Ethereal thu thập các gói tin đến được card eth0.

4.3. Hộp hội thoại "Capture Interfaces"

Khi chọn "Interfaces..." từ menu Capture, xuất hiện hộp hội thoại "Capture Interfaces" như minh họa trên Hình ??.



Description HĐH sẽ cung cấp các tham số chi tiết cho card mạng này.

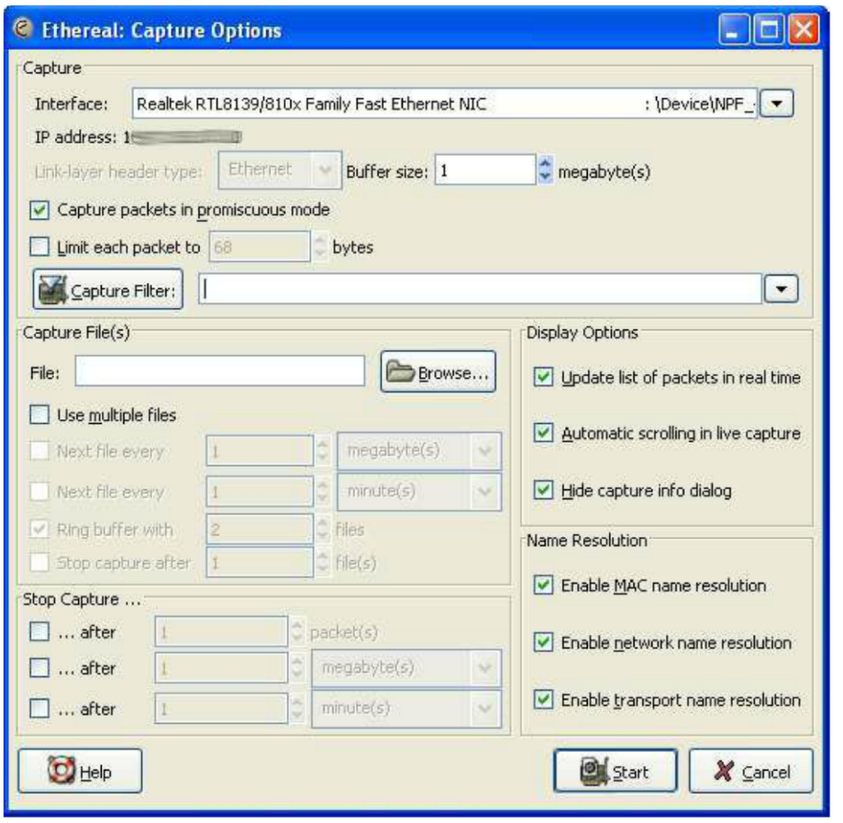
IP Là địa chỉ IP ứng với card mạng. Nếu không xác định được địa chỉ IP (chẳng hạn do không có DHCP server) thì sẽ là unknown. Nếu máy tính có hai địa chỉ IP, thì chỉ một trong hai địa chỉ được hiển thị (nhưng không xác định được là địa chỉ nào).

Packets Số lượng các packet bắt được kể từ khi mở Hộp hội thoại.

Packets/s Số lượng packet bắt được trong giây cuối cùng.
Stop Dừng quá trình thu thập.
Capture Bắt đầu quá trình thu thập với cấu hình từ lần thu thập trước.
Prepare : Mở hộp hội thoại Capture Options trên card mạng được lựa chọn.
Close Đóng hộp hội thoại.

4.2 Các tùy chọn (Menu Capture/ Options).

Khi khởi động việc bắt dữ liệu, *Ethereal* có thể sẽ hiển thị một hộp thoại tùy chọn (Capture Options). Nếu không chắc về một tuỳ chọn nào đó, hãy để chế độ mặc định. Trong nhiều trường hợp điều đó sẽ không ảnh hưởng nhiều đến kết quả hiển thị.



Khung Capture:

- Interface: chọn card mạng bạn sử dụng.
- IP address: địa chỉ IP ứng với card mạng.

- Link-layer header type: Trong nhiều trường hợp hãy để mặc định.
- Buffer size: Nhập kích cỡ bộ đệm sử dụng khi bắt dữ liệu.
- Capture packets in promiscuous mode: Tắt chế độ này nếu bạn chỉ muốn bắt các dữ liệu đến hoặc đi từ máy tính của bạn.
- Limit each packet to n bytes: Kích cỡ dữ liệu lớn nhất của mỗi gói tin.
- Capture Filter: thiết lập bộ lọc.

Khung Caputure File(s)

- File: tên file được sử dụng để ghi lại dữ liệu thu thập.
- Use multiple files: Thay vì dùng một file duy nhất, *Ethereal* sẽ tự động chuyển sang file mới nếu một điều kiện nào đó được thỏa mãn.
- Next file every n megabyte(s): Chuyển sang file mới sau khi thu thập được byte(s)/kilobyte(s)/megabyte(s)/gigabyte(s) nào đó.
- Next file every n minute(s): Chuyển sang file mới sau mỗi khoảng thời gian là một giây/ phút/ giờ/ ngày nào đó.
- Ring buffer with n files: Tạo một vòng lần lượt các file dữ liệu thu thập, sau khi đã ghi vào file cuối cùng sẽ quay lại ghi đè vào file đầu tiên.
- Stop capture after n file(s): Dừng việc bắt dữ liệu sau khi đã ghi đủ vào n file.

Khung Stop Capture :

- …after n packet(s): Ngừng việc bắt dữ liệu sau khi đã thu thập được một số lượng nào đó các gói tin.
- …after n megabyte(s): Ngừng việc bắt dữ liệu sau khi đã thu thập được một số lượng nào đó dữ liệu.
- …after n minute(s): Ngừng việc thu thập dữ liệu sau một số giây/ phút/ giờ/ ngày.

Display Options Frame:

- Update list of packets in real time: Yêu cầu *Ethereal* cập nhật ô liệt kê gói tin trong thời gian thực. Nếu không có lựa chọn này, *Ethereal* sẽ chỉ hiển thị các gói tin sau khi ngừng quá trình thu thập dữ liệu.
- Automatic scrolling in live capture: Tùy chọn này cho phép *Ethereal* cuộn ô liệt kê gói tin khi có thêm gói tin mới, để người sử dụng luôn luôn nhìn thấy gói tin mới nhất.
- Hide capture info dialog: Nếu được chọn, hộp thoại hiển thị thông tin thu thảo dữ liệu sẽ được ẩn đi.

Name Resolution Frame:

- Enable MAC name resolution: Giải mã địa chỉ MAC trong quá trình thu thập.
- Enable network name resolution: Giải mã địa chỉ mạng trong quá trình thu thập.
- Enable transport name resolution: Giải mã địa chỉ tầng giao vận trong quá trình thu thập.

4.5 Bộ lọc

Có thể điền biểu thức lọc vào trường Filter của hộp thoại Capture Options. Biểu thức có thể được xem là tổ hợp của các biểu thức nguyên thủy (primitive) kết nối với nhau theo các phép toán AND OR hoặc NOT.

Khuôn dạng tổng quát của biểu thức: [not] **primitive** [and|or [not] **primitive …**]

Ví dụ 1: Bắt thông tin ứng dụng telnet đến hoặc đi từ một host cụ thể nào đó:

tcp port 23 and host 10.0.0.5

Ví dụ 2: Bắt thông tin telnet không xuất phát từ địa chỉ IP 10.0.05:

tcp port 23 and not host 10.0.0.5

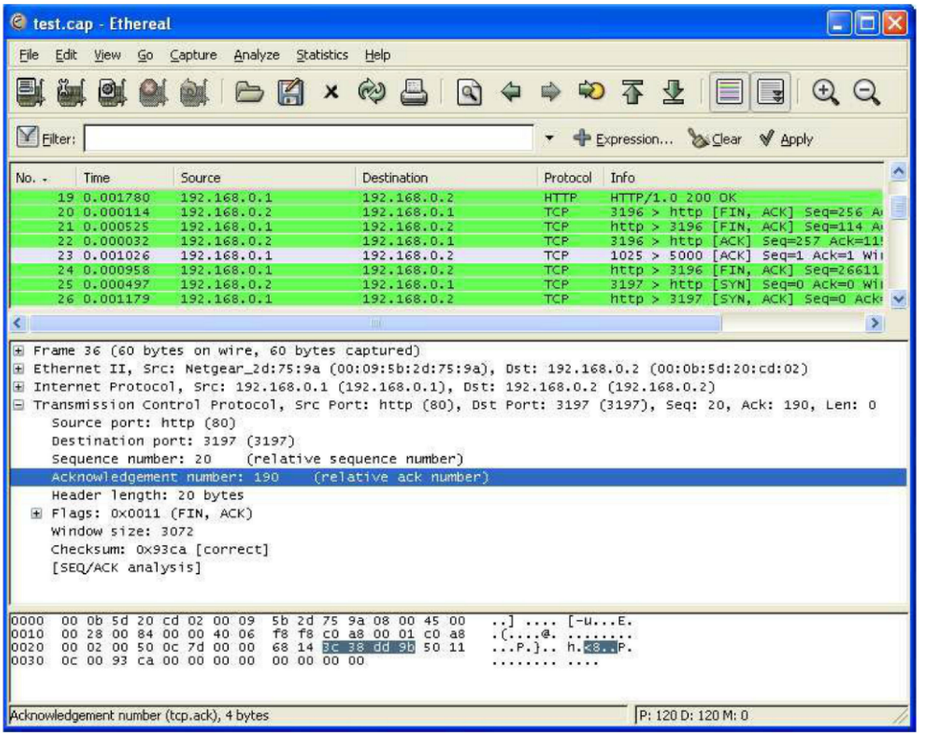
Dưới đây là các biểu thức nguyên thủy thường được sử dụng:

- **[src|dst] host <host>:** lọc dựa trên tên hoặc địa chỉ IP của máy tính. Nếu có thêm từ khóa src (hoặc dst) thì chúng ta chỉ lấy những gói tin có địa chỉ gửi (hoặc địa chỉ nhận) là host. Nếu không có hai từ khóa này, hệ thống sẽ thu giữ tất cả gói tin có địa chỉ gửi hoặc nhận là host.
- **ether [src|dst] host <ehost>:** lọc dựa trên địa chỉ của Ethernet host. Từ khóa src và dst giống như trên.
- **gateway host <host>:** lọc các gói tin sử dụng host như một gateway (router). Có nghĩa là địa chỉ Ethernet là địa chỉ của host nhưng địa chỉ IP không phải là địa chỉ của host.
- **[src|dst] net <net> [{mask <mask>}|{len <len>}]** Lọc theo địa chỉ subnet của mạng. Từ khóa src hoặc dst chỉ ra rằng chỉ cần lấy gói tin gửi từ (hoặc đến) một mạng cụ thể nào đó. Có thể bạn phải chỉ ra mặt nạ mạng hoặc tiền tố CIDR trong trường hợp bạn địa chỉ subnet khác subnet trên máy tính cài Ethereal.
- **[tcp|udp] [src|dst] port <port>:** lọc theo cổng của TCP và UDP.
- **less|greater <length>:** lọc các gói tin theo một độ dài cho trước.
- **ip|ether proto <protocol>:** lọc dựa trên các giao thức cho trước thuộc tâng Ethernet hoặc tầng IP.

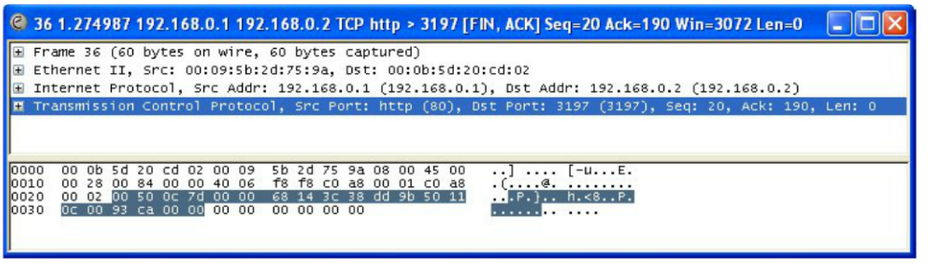
5. Làm việc với các gói tin bắt được

5.1 Xem các gói tin đã bắt

Sau khi bạn đã bắt được một số gói tin, hay khi mở file dữ liệu thu thập, chúng ta có thể chọn và xem từng gói tin được hiển thị trong ô liệt kê các gói tin bằng cách nhấn chuột vào. Chi tiết về gói tin sẽ hiển thị ở các ô phía dưới – theo dạng cây và dạng nhị phân. Có thể mở rộng cây hiển thị gói tin bằng cách ấn vào dấu (+), khi đó các thông tin chi tiết hơn về giao thức sẽ hiện ra trên màn hình.



Ngoài ra, bạn có thể xem gói tin trong từng cửa sổ riêng. Điều này cho phép bạn dễ dàng so sánh hai hay nhiều các gói tin. Để xem như vậy, nhấn chuột phải vào gói tin và chọn Show Packet in New Window.

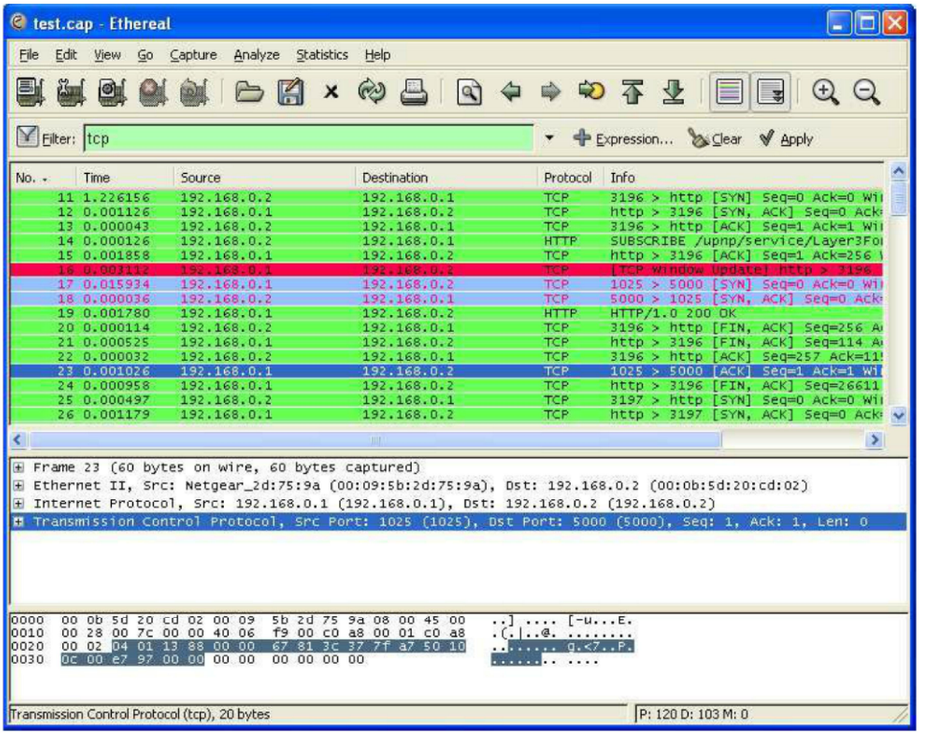


Lọc các gói tin khi đang xem

Bộ lọc hiển thị cho phép bạn tập trung vào những gói tin bạn quan tâm và ẩn đi các gói tin khác. Bạn có thể chọn các gói tin dựa trên:

- Giao thức
- Sự xuất hiện một trường
- Giá trị của trường

- So sánh giữa các trường
- … và nhiều hơn thế!



Bạn cũng có thể lọc trên nhiều trường khác nữa bằng cách chọn hộp thoại Add Expression… Chẳng hạn, để thu hẹp danh sách gói tin thành những gói tin đi hoặc đến địa chỉ IP 192.168.0.1, ta dùng biểu diễn **ip.addr = = 192.168.0.1.**

Tạo các biểu thức lọc hiển thị

Ethereal cung cấp ngôn ngữ lọc hiển thị đơn giản nhưng rất hiệu quả. Bạn có thể so sánh giá trị giữa các gói tin cũng như kết hợp các biểu thức thành những phép lọc phức tạp. Các bảng sau cung cấp nhiều thông tin để bạn sử dụng.

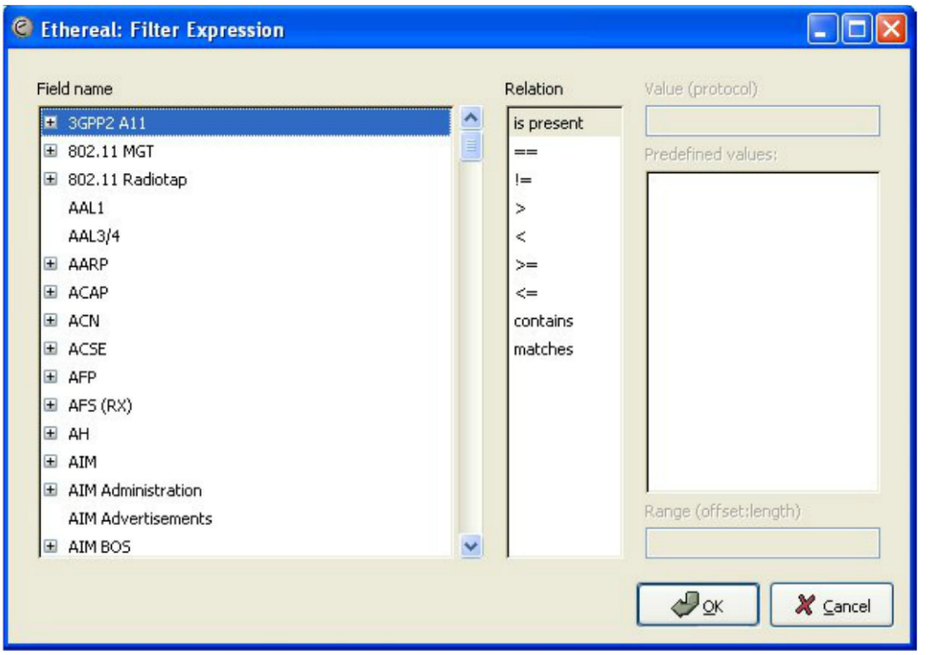
Bảng các toán tử so sánh:

Viết tắt tiếng Anh	Cú pháp của C	Mô tả và ví dụ
eq	==	**Equal** ip.addr==10.0.0.5
ne	!=	**Not equal** ip.addr!=10.0.0.5
gt	>	**Greater than** frame.pkt_len > 10
lt	<	**Less than** frame.pkt_len < 128
ge	>=	**Greater than or equal to** frame.pkt_len ge 0x100
le	<=	**Less than or equal to** frame.pkt_len <= 0x20

Kiểu	Ví dụ
Số nguyên dương (8-bit, 16-bit, 24-bit, 32-bit)	ip.len le 1500 (cơ số 10) ip.len le 02734 (cơ số 8) ip.len le 0x436 (cơ số 16)
Số nguyên có dấu (8-bit, 16-bit, 24-bit, 32-bit)	
Boolean	**tcp.flags.syn** = = true chỉ khi cờ SYN được bật trong tiêu đề TCP.
Ethernet address (6 bytes)	eth.addr == ff:ff:ff:ff:ff:ff
IPv4 address	ip.addr == 192.168.0.1

Hộp thoại các biểu thức lọc (Filter Expression Dialog box)

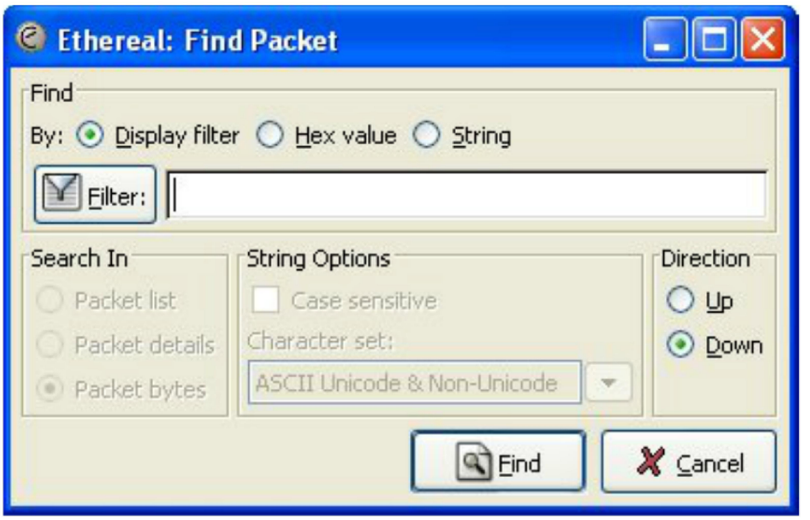
Khi bạn đã quen với hệ thống lọc của *Ethereal* và biết được nhãn nào bạn cần dùng thì việc tạo một chuỗi biểu thức lọc là rất đơn giản. Tuy nhiên nếu bạn mới làm quen với *Ethereal* hoặc bạn phải làm việc với một giao thức hơi lạ nào đó, bạn có thể sẽ gặp khó khăn. Hộp thoại biểu thức lọc (Filter Expression dialog box) sẽ giúp bạn trong trường hợp này.



- **Field name:** Liệt kê các trường giao thức trong cây.
- **Relation:** Chọn quan hệ bạn mong muốn. Quan hệ is present là true nếu trường bạn chọn có trong gói tin. Các quan hệ khác cần thêm dữ liệu giá trị (Value).
- **Value:** Điền giá trị thích hợp cho biểu thức.
- **Predefined values:** Một số trường giao thức đã định nghĩa sẵn các giá trị. Bạn chỉ việc chọn một trong số các giá trị đó.

Tìm kiếm các gói tin

Bạn có thể dễ dàng tìm kiếm các gói tin bằng cách chọn **Find Packet…** trong menu **Edit**.



- **Display filter**: Điền chuỗi lọc hiển thị. Ví dụ để tìm thủ tục bắt tay (handshaking) từ host 192.168.0.1, sử dụng chuỗi sau: ip.addr = = 192.168.0.1 and tcp.flags.syn.
- **Hex Value**: Tìm một chuỗi byte nào đó trong dữ liệu gói tin. Ví dụ, dùng "00:00" để tìm gói tin tiếp theo chứa hai byte không.
- **String**: Tìm một chuỗi trong dữ liệu gói tin, với nhiều tùy chọn khác nhau.