

“Ethereal” Protocol Analyzer

PURPOSE

This exercise will familiarize you with the Ethereal protocol analyzer. Ethereal is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. Current versions of Ethereal for all supported systems can be downloaded from www.ethereal.com. Upon completion of this exercise, you will be able to:

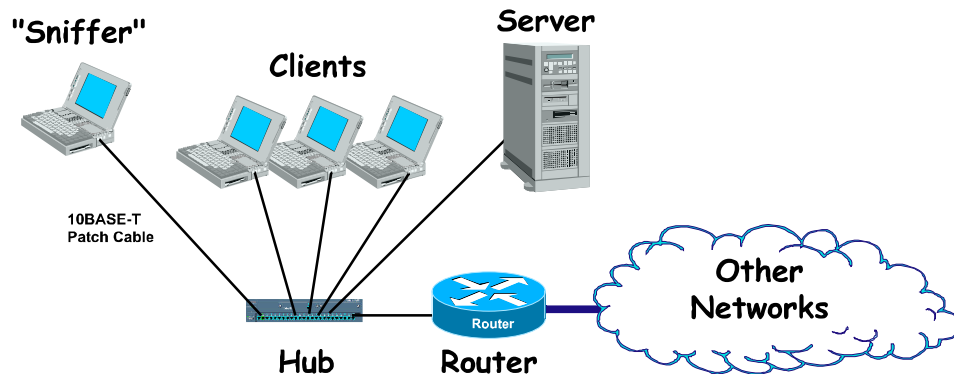
- Install and run the Ethereal and WinPcap software.
- Capture data from a “live” network.
- Create and Use filters to modify captured and displayed data.

DISCUSSION

Monitoring the traffic on your own network is one of the first steps in network security. In contemporary non-switched LANs, all of the machines receive all of the traffic, but they ignore traffic destined for other machines and instead selectively process only traffic bearing their address or the broadcast address. A protocol analyzer, frequently called a *sniffer*, is a program that listens to and captures all network traffic, in what is known as *promiscuous* mode. This makes a sniffer an important security tool: It’s a tool that no network administrator should be without despite its often being associated with malicious intent. The ability to reconstruct packet flows and generate meaningful reports is what makes sniffers so valuable. In the networking world, the sniffer acts as your eyes and ears, looking and listening for both normal, and abnormal, traffic patterns.

Remember that most of the information which traverses a LAN is not encrypted. A sniffer, lays bare, the networked world before you. All of the network’s protocol headers and payloads can be captured and examined. This includes source and destination MAC addresses, IP addresses, and TCP/UDP ports. Files containing sensitive information may be captured while in transit. For those applications or protocols which submit credentials in plaintext form, such as HTTP, FTP, POP and Telnet, the sniffer can seriously compromise security. Even if credentials are encrypted, they can still be captured. Once captured, other tools may be used to crack the encryption given enough time and hints about the end systems.

OVERVIEW



Exercise Topology

The topology used in this exercise is depicted above. You will connect your laptop to an Ethernet 10BASE-T hub using an appropriate patch cable. Other equipment, including other students' laptops, routers, and servers, will also be connected to this hub. Using the Ethereal software, you will monitor, capture, and decode traffic passing thru the hub. This traffic includes frames to or from all other equipment directly connected to the hub. You can only view traffic from other networks if it is sent via the local hub.

To complete this exercise, you will do the following:

- Connect your laptop to the hub and confirm correct operation of the 10BASE-T link.
- Install the Ethereal and WinPcap software on your laptop.
- Capture, decode, and analyze traffic using Ethereal.
- Configure and apply capture and decode filters.

PROCEDURE

Task 1: Connect your laptop to the hub and confirm correct operation of the 10BASE-T link.

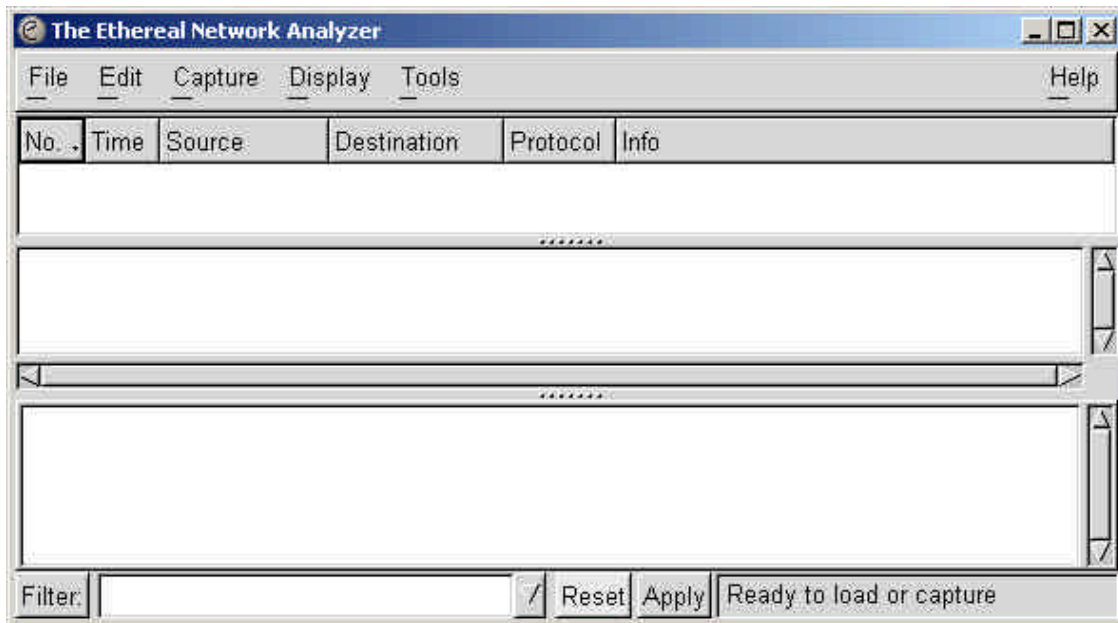
- Step 1: Connect a 10BASE-T patch cable to the Ethernet port on your laptop. Your laptop may have a built-in 10BASE-T port or may use a PC-card and "dongle." 10BASE-T cables and ports use an 8-position modular connector called an "RJ-45".
- Step 2: Connect the other end of the 10BASE-T patch cable to any port on the Ethernet hub. If you select a hub port which can have its polarity switched (the port will have a small switch next to it labeled MDI/MDI-X) make sure the switch is in the MDI position.
- Step 3: Power on your laptop and allow it to complete its boot cycle. (This process will vary depending your laptops configuration. This lab assumes that you already know how to operate your laptop.) A link indicator LED on the hub should illuminate if the 10BASE-T connection is operating correctly. If the LED fails to light, check your connections, then notify the instructor.

Task 2: Install the WinPcap and Ethereal software on your laptop.

- Step 1: Login to your laptop using the account credentials previously configured for this workshop. (This procedure varies depending on what Windows OS version you are using.)
- Step 2: Navigate in your Network Neighborhood (or My Network Places) to the “Apps” software installation share located in the “SCG” workgroup on the workshop server “Summit” and open the Ethereal folder. Use the username and password given to you by the instructor.
<\\Summit\Apps\Ethereal>
- Step 3: Launch the WinPcap installer, named “WinPcap_2_3.exe”. Follow the on-screen instructions to install the required packet capture driver. If you had an older version of WinPcap already installed, reboot your computer before advancing to the next step. Otherwise continue directly to step 4.
- Step 4: Launch the Ethereal installer, named “Ethereal-Setup-0.9.3-1.exe”. Follow the on-screen instructions to install the analyzer software in the default location. Feel free to explore the installation options, but be careful not to deselect any of the default settings.

Task 3: Capture and decode traffic using Ethereal

- Step 1: The Ethereal installer created program shortcuts under Start Menu: Programs: Ethereal. Launch Ethereal by using the Ethereal shortcut.

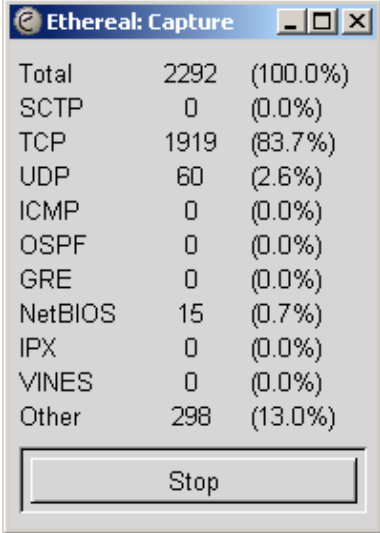


Ethereal Window

- Step 2: Note the major features of the Ethereal window. The menu bar (File, Edit, Capture, Display, Tools, Help) contains pull-down menus which control Ethereal’s operation.

The main window contains three panes (upper, middle, lower) to display captured data. The bottom line holds controls for setting and applying filters.

- Step 3: Choose “Start...” from the Capture menu to bring up the Capture Options window. Briefly examine the options presented in this window, but leave the default settings. Click “OK” to begin capture.



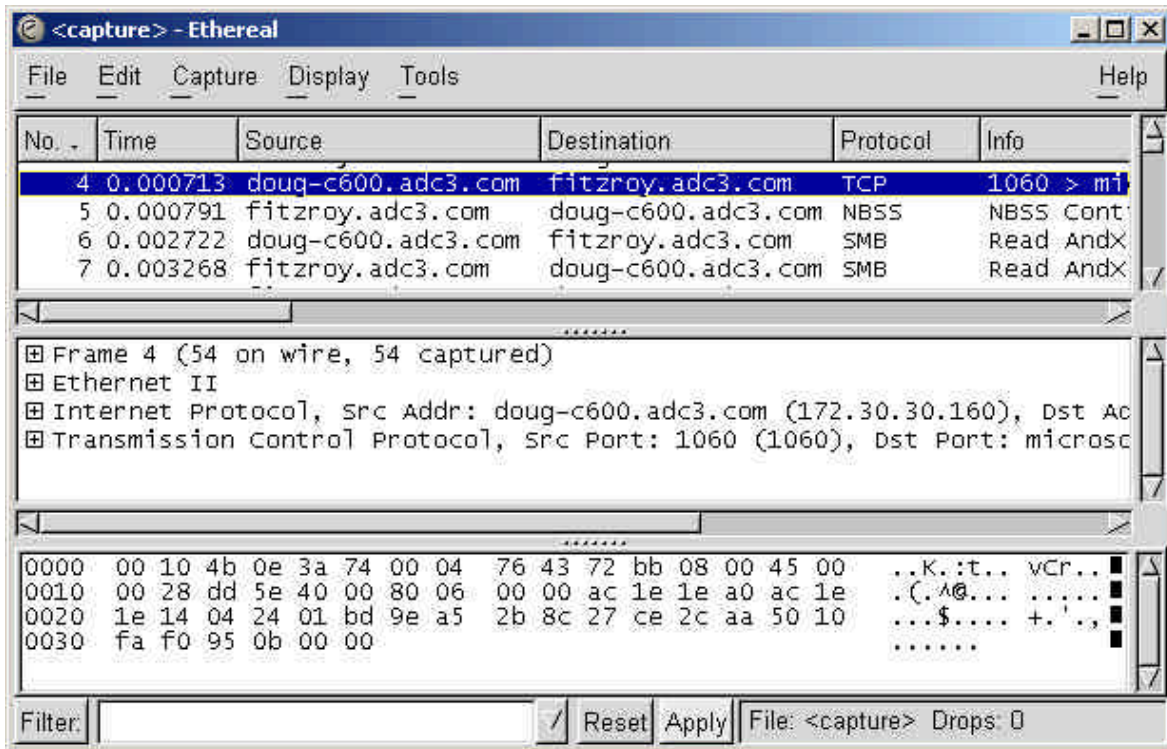
The screenshot shows a window titled "Ethereal: Capture" with a table of statistics and a "Stop" button at the bottom.

Protocol	Count	Percentage
Total	2292	(100.0%)
SCTP	0	(0.0%)
TCP	1919	(83.7%)
UDP	60	(2.6%)
ICMP	0	(0.0%)
OSPF	0	(0.0%)
GRE	0	(0.0%)
NetBIOS	15	(0.7%)
IPX	0	(0.0%)
VINES	0	(0.0%)
Other	298	(13.0%)

Stop

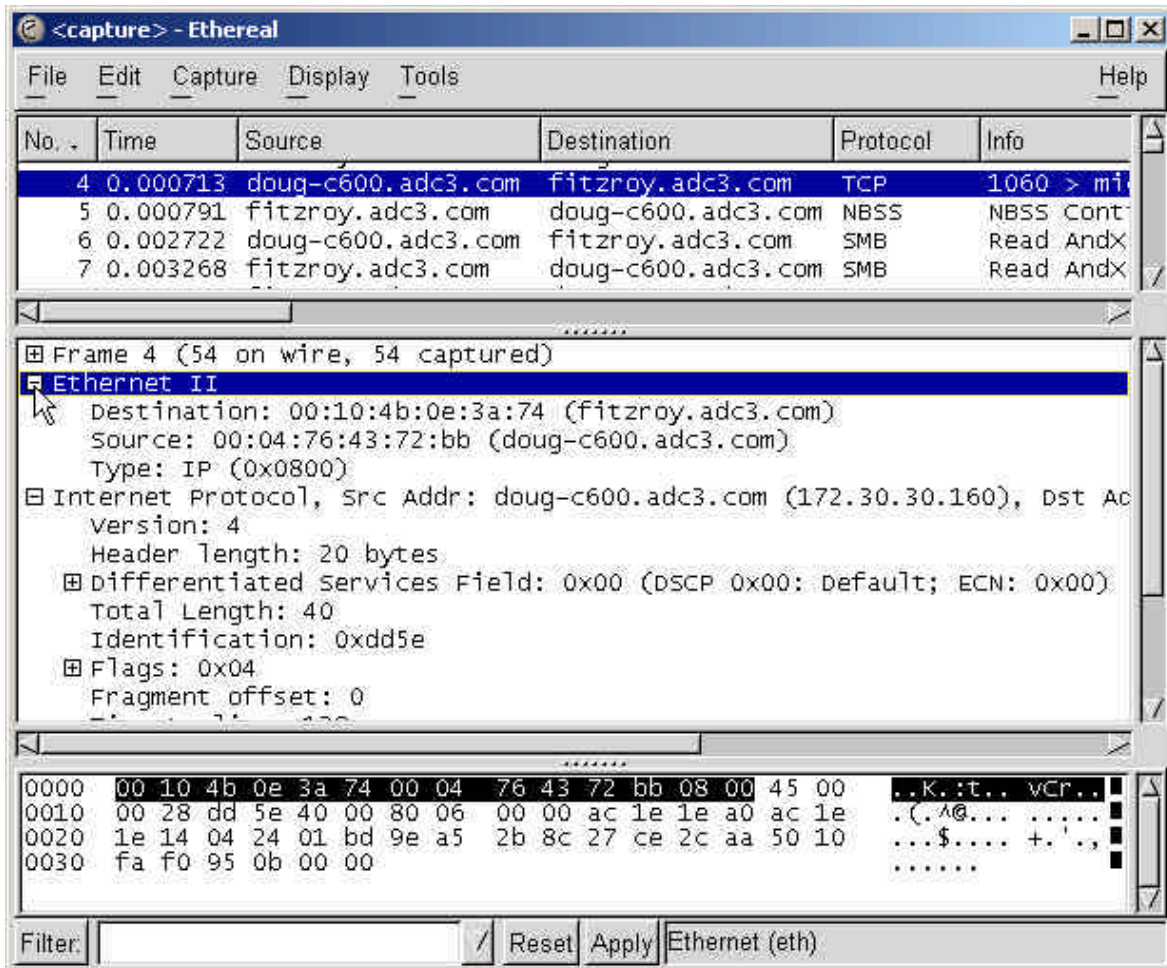
Ethereal Capture Window

- Step 4: The Ethereal Capture window appears showing a running total of various packet types captured. After about 2-3 minutes, stop capturing by clicking the “Stop” button



<capture>- Ethereal Window

Step 5: Examine the data displayed in the resulting “<capture>-Ethereal” window. The upper pane shows a one-line summary of each captured frame. Clicking on any frame in this pane will display its decode and hex data in the middle and lower panes. Select any TCP or SMB packet that interests you. If there are no interesting packets, just pick one. If you have no frames at all, notify the instructor.

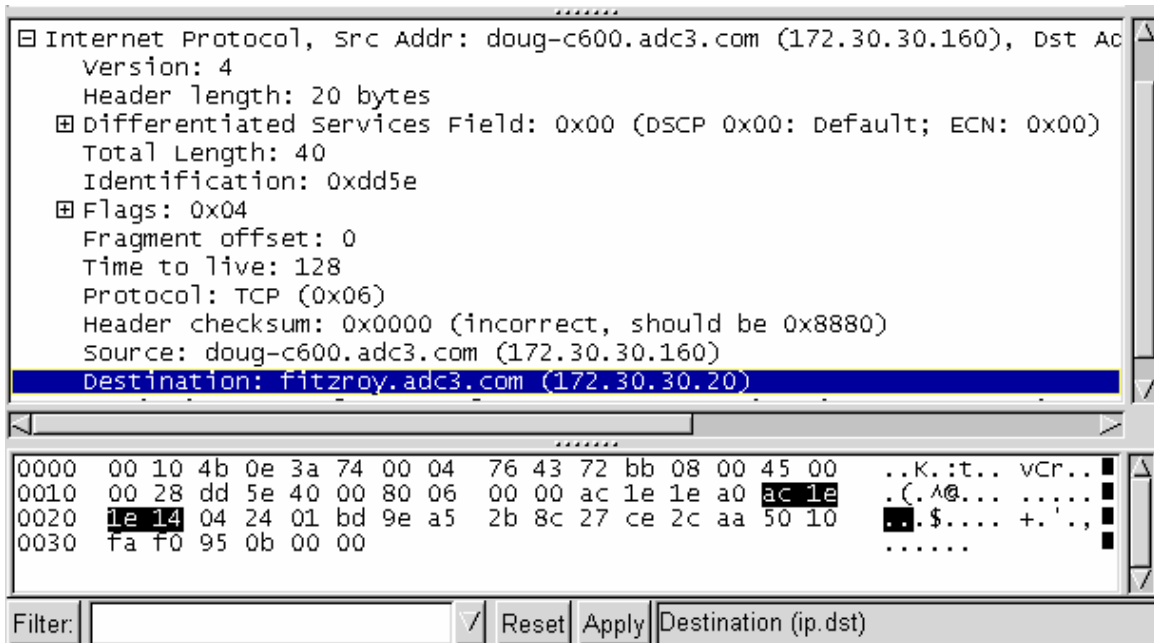


Expanded Decode in Decode Pane

- Step 6: Expand the data link decode information by clicking on the “+” next to the line containing the word “Ethernet”. Notice that the “+” turns into a “-”. Clicking on this icon toggles between expanded and collapsed displays.
- Step 7: In the middle decode pane, click on the word “Ethernet” to select the entire layer-2 header. Notice that the corresponding hex bytes automatically highlight in the lower hex pane.
- Step 8: Click on the “Destination:” field in the decode pane. Note that only the hex bytes corresponding to the destination MAC address highlight in the lower hex pane.

What station is this frame intended for?
 (Station name, MAC address) _____

Is this an Ethernet-II or an IEEE 802.3 frame? _____



Expanded IP Header in Decode Pane

Step 9: In the middle decode pane, Click on the “+” next to the word “Internet Protocol” to expand the IP decode. Then click on the word, “Internet”. Note that the bytes corresponding to the IPv4 header are highlighted in the lower hex pane.

How long is this packet header (in bytes) ? _____

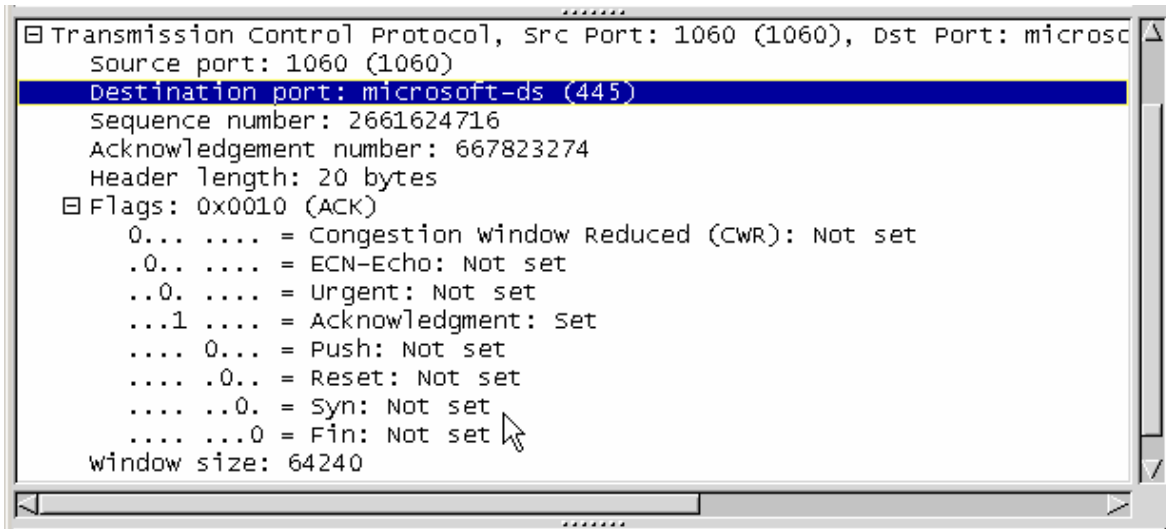
How long is this entire packet (in bytes) ? _____

Has this packet been fragmented? _____

What IP address is this packet intended for? _____

From what IP address did this packet originate? _____

Are the devices exchanging this packet capable of RFC-3168 IP Explicit Congestion Notification (ECN) ? _____



Expanded TCP Header in Decode Pane

Step 10: Expand the TCP header information.

What Destination port is this segment intended for? _____

Is the Destination port a “well-known” port value? _____

From what Source port did this segment originate? _____

Is the Source port a “well-known” port value? _____

What are the settings of the Ack, Syn, and Fin flags? _____

Step 11: If you’ve selected a frame containing Server Message Block (SMB) data, click on the SMB decode line. Note the corresponding hex highlighted in the lower hex pane. Also note the ASCII representation in the lower right pane. If this SMB payload contains ASCII text, you will be able to read the plaintext data. However, if the SMB payload is non-ASCII, the payload will appear as a series of random characters.

Most word processors save documents using ASCII text with various embedded control characters to control formatting. The same is true of most Email clients. Were you to capture someone’s MS-Word file transfer, or someone’s Email submission using POP3 or SMTP, the resulting capture would be readable in the ASCII display! Can you now understand why many companies “discourage” the unauthorized use of *sniffers* on their networks?

Task 4: Configure and apply capture filters.

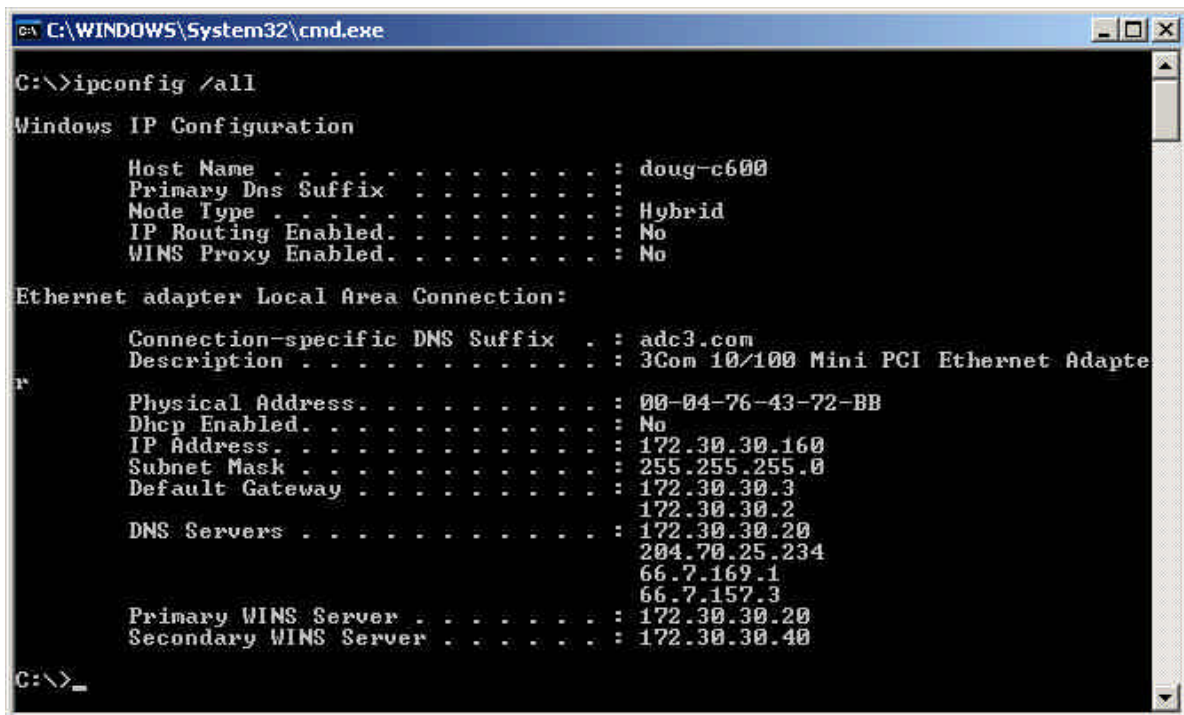
Protocol analyzers typically store captured data in a capture buffer which is part of RAM memory. Because RAM memory is limited, the capture buffer can be quickly filled when promiscuously monitoring an active LAN. You may configure the analyzer to either stop capturing when the buffer becomes full, or to overwrite the oldest data. But the best way to utilize the capture buffer involves capturing only the frames that are relevant to your current task. This is accomplished through the use of *capture filters*.

Capture filters affect what frames are allowed to enter your capture buffer. By selectively filling the buffer with only relevant frames, better use of the limited space is possible. Capture filters are defined and applied in Ethereal using the “Capture Filters...” item located under the “Edit” menu and the “Filters” setting in the “Ethereal: Capture Options: window which appears just prior to capturing traffic. Unfortunately, capture filters in Ethereal are somewhat cumbersome to configure as compared to commercial tools like NAI’s Sniffer Pro or Novell’s LANalyzer.

Ethereal Packet capturing is performed with the pcap library. The capture filter syntax follows the rules of the pcap library derived from the Unix utility “*tcpdump*.” This syntax is different from the display filter syntax. A reference to TCPDUMP can be found at www.ethereal.com/tcpdump.8.html or in the workshop at <http://www.scg.lab/Apps/Ethereal/docs/tcpdump.8.html> . Because this workshop will tend to use Display filters more heavily than Capture filters, we’ll only pursue one example for a capture filter. Follow the steps below to create a capture filter which will capture traffic to or from your station only.

Step 1: In order to create a filter which will capture traffic to or from your laptop only, you need to supply some unique information about your computer. Because your IP address will change in subsequent exercises, we need a more lasting identification. Your Ethernet MAC address, which is burned into your NIC, will uniquely identify your machine until you change NICs. You can learn your Ethernet address using built-in Windows utilities. The process will vary depending on your operating system. If you are running Windows NT, 2000, or XP, you will use the *ipconfig* utility from the command line. If you are running Windows 9x or ME, you will use the GUI-based *winipcfg* utility.

Substep a: If you are running Windows NT, 2000, or XP, open a Command Window by selecting “Run...” from the Windows “Start” menu. Type the string *cmd* then press Enter. (If you are running Windows 9x or ME, skip to substep c.)



```
C:\WINDOWS\System32\cmd.exe
C:\>ipconfig /all
Windows IP Configuration

    Host Name . . . . . : doug-c600
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . : adc3.com
    Description . . . . . : 3Com 10/100 Mini PCI Ethernet Adapte
    Physical Address. . . . . : 00-04-76-43-72-BB
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 172.30.30.160
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.30.30.3
                                172.30.30.2
    DNS Servers . . . . . : 172.30.30.20
                                204.70.25.234
                                66.7.169.1
                                66.7.157.3
    Primary WINS Server . . . . . : 172.30.30.20
    Secondary WINS Server . . . . . : 172.30.30.40

C:\>_
```

Command line window: ipconfig utility

Substep b: In the command window that appears type *ipconfig /all* then press Enter. You should see a display similar to that pictured above. After noting your Physical Address in the space below, type the command *exit* to close the command window. Skip substeps c and d below which are for Win9x/ME machines.

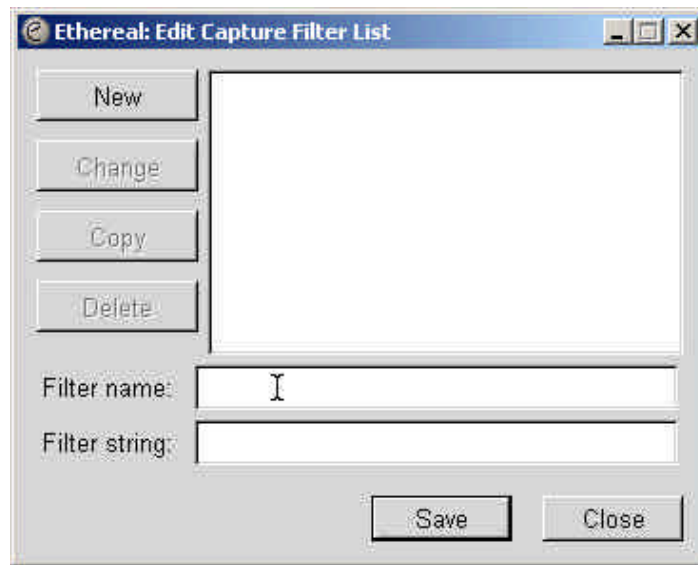
What is the Physical Address used by your station? _____

Substep c: If you are running Windows 9x (95, 98) or Windows ME, launch the WinIPcfg utility by selecting "Run..." from the Windows "Start" menu. Type the string *winipcfg* then press Enter.

Substep d: In the IP Configuration window that appears, select your Ethernet adapter from the pull down menu. Click on the More info button and take note of the Physical address displayed. You can close the WinIPcfg utility.

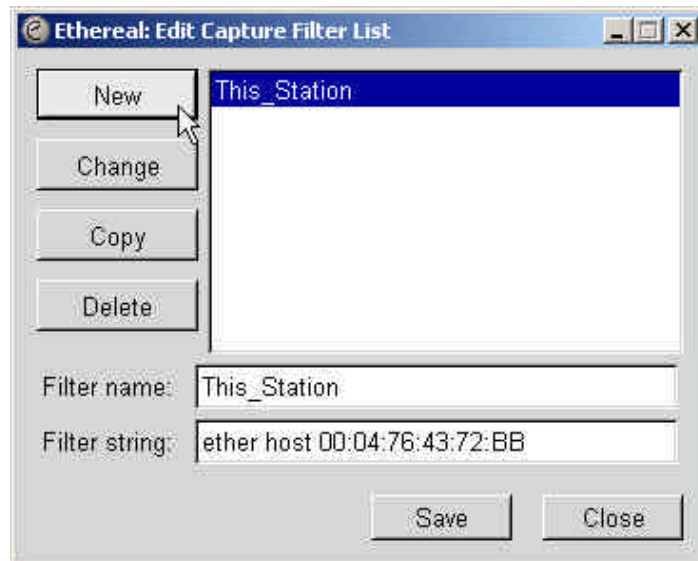
What is the Physical Address used by your station? _____

Step 2: Return to the Ethereal window and select the "Capture Filters..." item from the "Edit" menu. A window titled, "Ethereal: Edit Capture Filter List" should appear.



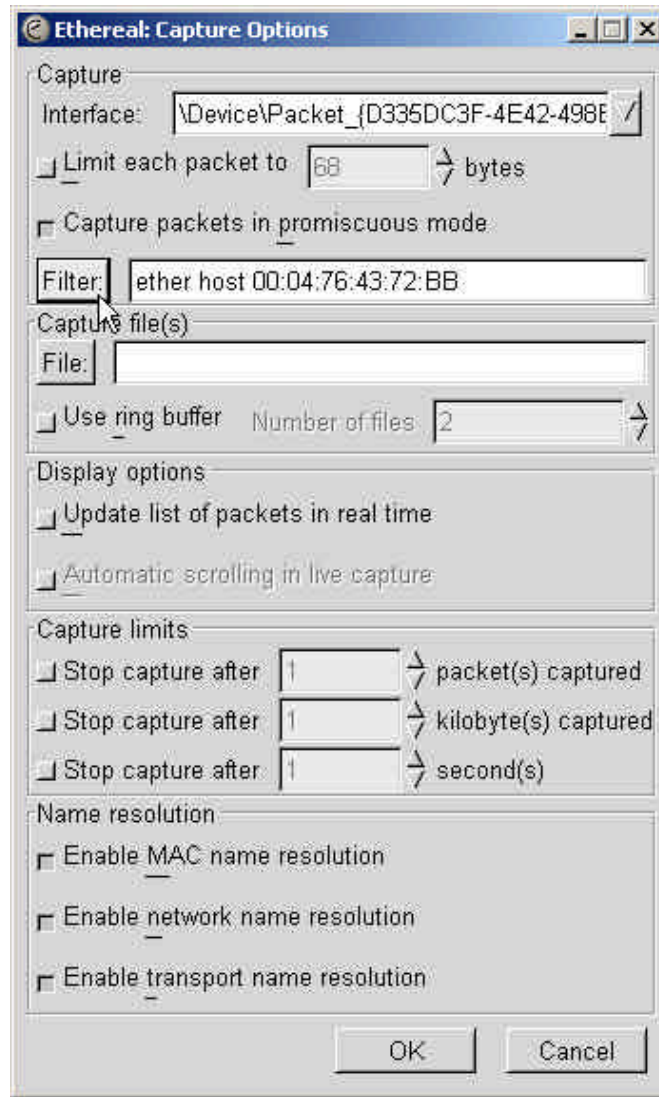
Ethereal: Edit Capture Filter List window

- Step 3: Type the name, *This_Station* in the “Filter name:” field. Then type the filter string *ether host xx:xx:xx:xx:xx:xx* in the “Filter string:” field, substituting your Ethernet (Physical) address for the xx pattern.



Capture Filter for “This_Station”

- Step 4: Click on the “New” button to transfer your newly defined filter to the filters list pane. Then click “Save” and “Close”.
- Step 5: Capture data using your new capture filter. Choose “Start” from the “Capture” menu.



Activating a Capture Filter

Step 6: In the “Ethereal: Capture Options” window, activate your newly created filter by clicking on the Filter button. Select the “This_Station” filter in the filters list pane. Click OK to accept the selected filter, then OK to begin capture. Capture traffic for several minutes then click Stop. Observe the captured frames. Do they match your expectations regarding source and destination based on your filter selection? If you get an error message upon starting capture, check your filter syntax for typos or missing parameters.

Task 5: Configure and apply decode filters.

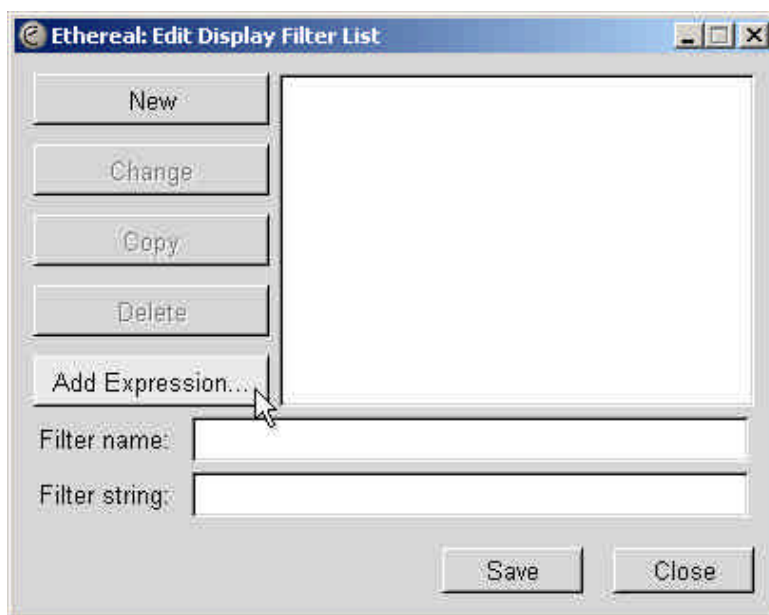
Even when using capture filters, the amount of captured data can be overwhelming. When trying to analyze the data, frequently it's helpful to look at a capture from several different angles. Sometimes patterns can be more easily spotted by focusing on only a portion of traffic, such as that between a particular pair of stations, or a particular protocol type, and temporarily eliminate other distracting traffic. Display filters allow you to suppress certain captured traffic from being displayed on your screen, and allowing other traffic to show.

While a capture filter affects what frames are initially captured, a display filter determines which captured frames are displayed. By selectively displaying only portions of the traffic at a time, it's easier to spot trends and analyze faults. Yet, if an analysis requires more than one perspective, you still have the relevant data captured and can simply apply a different display filter without having to recapture data. This "post processing" of the captured data is more forgiving than a capture filter for that reason. If capture buffer space allows, it's frequently helpful to capture all traffic, and simply use decode filters later to look at only what you're interested in.

The display filters in Ethereal are *extremely* powerful. In Ethereal, text rules are strung together similar to the strings used in its capture filters. As mentioned earlier, the decode filter syntax differs slightly from the capture filter syntax. Fortunately, Ethereal now has a built-in helper window to assist in creating display filters.

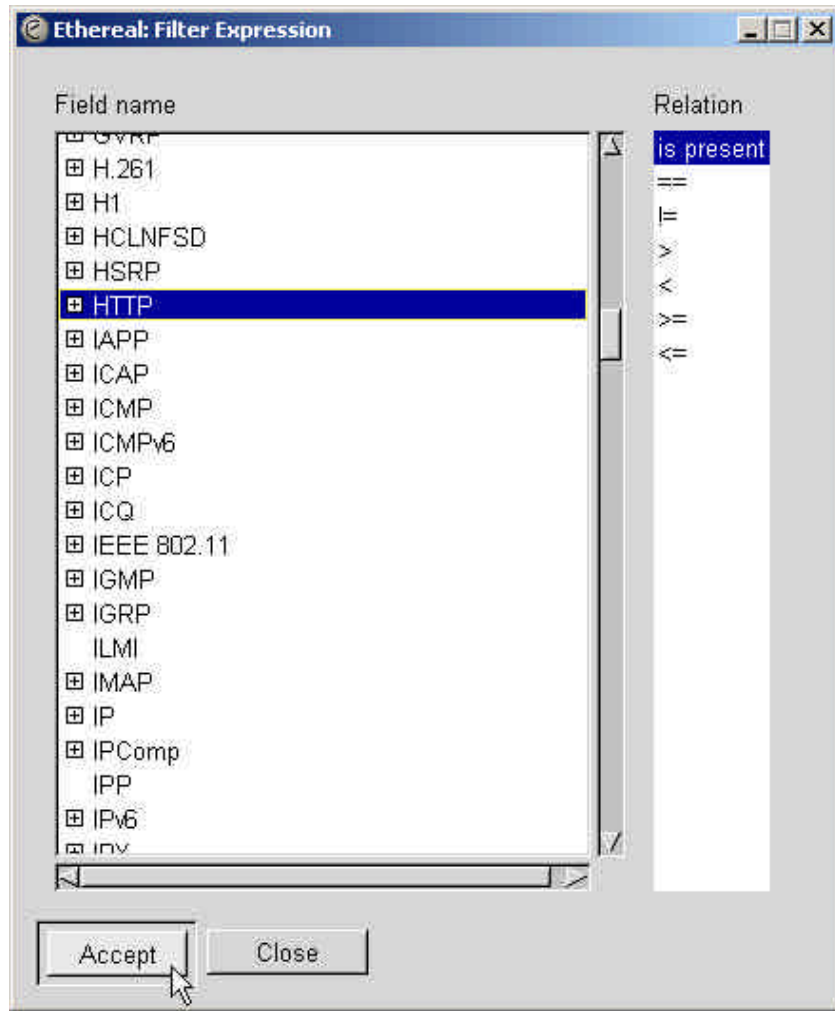
A reference to display filters formats can be found at www.ethereal.com/ethereal.1.html or in the workshop at <http://www.scg.lab/tools/ethereal/docs/ethereal.1.html>. A hyper-linked index is at the bottom of the document. Use the following steps to configure one example display filter. Others will be created in later exercises.

Step 1: Select the "Display Filters..." item from the "Edit" menu. A window titled, "Ethereal: Edit Display Filter List" should appear.



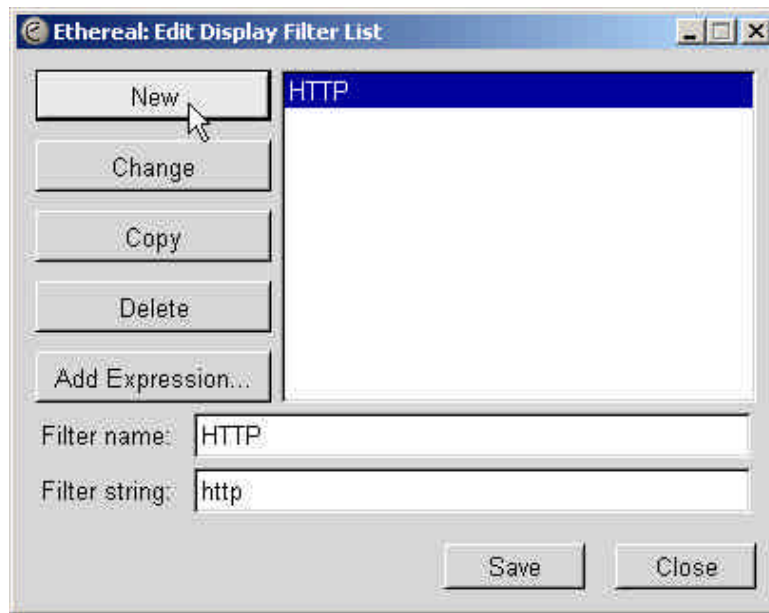
Ethereal: Edit Capture Filter List window

Step 2: Click on the “Add Expression...” button to open the Ethereal: Filter Expression window.



Ethereal: Filter Expression window

Step 3: Note the extensive list of display filter options. As an example, create a filter to display only HTTP by scrolling down and selecting the “HTTP” and accepting the default relation “is Present”. Then click “Accept”.



“http” Filter Expression added

- Step 4: Note that the filter string “http” has been added. Type the name, *HTTP* in the “Filter name:” field. Then click “New” followed by “Save” followed by “Close”
- Step 5: Return to the main Ethereal window and begin a new capture. Select the Capture filter, *This_Station* , which you created earlier. Begin capturing traffic.
- Step 6: Launch your web browser (Internet Explorer or Netscape Navigator, for example) and open the web page, <http://www.scg.lab/> . Once the page has loaded, minimize your browser window.
- Step 7: Return to Ethereal and stop capture. Once your capture window has finished loading, take a moment to note the traffic. It should only contain traffic to or from your station. Next observe the variety of traffic which may include SMB, ARP, DNS, and other protocols.
- Step 8: Apply the decode filter you created earlier by clicking on the “Filter:” button located at the bottom left corner of the capture window. Select the “HTTP” filter in the resulting “Ethereal: Display Filter” window. Click “Apply” then “OK”. Note the resulting display contains only HTTP traffic.

QUESTIONS AND ANALYSIS

Question 1: Briefly describe three ways in which a protocol analyzer might be a useful tool to a network administrator. How might the tool be used by a hacker?

Question 2: Protocol analyzers include both capture and decode filtering functions. Describe the difference between the two filter types and applications for each.

Question 3: What effect on a standard protocol analyzer might there be if LAN switches were deployed for physical connectivity instead of standard hubs?
