Installing and using Ethereal

Ethereal is a network analyzer. It works by reading network packets, decoding them, and present them in an easy to understand format. Ethereal is open source software that can be downloaded and used on many popular platforms such as Windows, UNIX, and Linux. Ethereal is a powerful networking tool that can be used by network professionals for such purposes as troubleshooting, analysis, and protocol development.

Steps on how to download Ethereal software:

To download Ethereal, follow these steps:

1. To download Ethereal, type www.ethreal.com in your web browser and click **Enter**.

2. When the site appears, click the **Download** link from the top or the left menu.

3. When the download window appears, choose the correct version depending on your computer's operating system. In this case, we are downloading Ethereal on Windows XP machine. Therefore, we will choose **Main site** under the **Windows 98/ME/2000/XP/2003 Installers** section in the HTTP row.

4. If you wish to capture live network packets, download and install the WinPcap packet capture driver. The recommended WinPcap version at the time of this writing is 3.0, which supports multiprocessor machines and Windows XP. The Winpcap packet will appear as:

   WinPcap_3_0.exe

   Note: *If you have an older version of WinPcap installed, you must un-install it before installing the current version.*

   Note: *If you do not have WinPcap installed you will be able to open saved capture files, but you will not be able to capture live network traffic.*

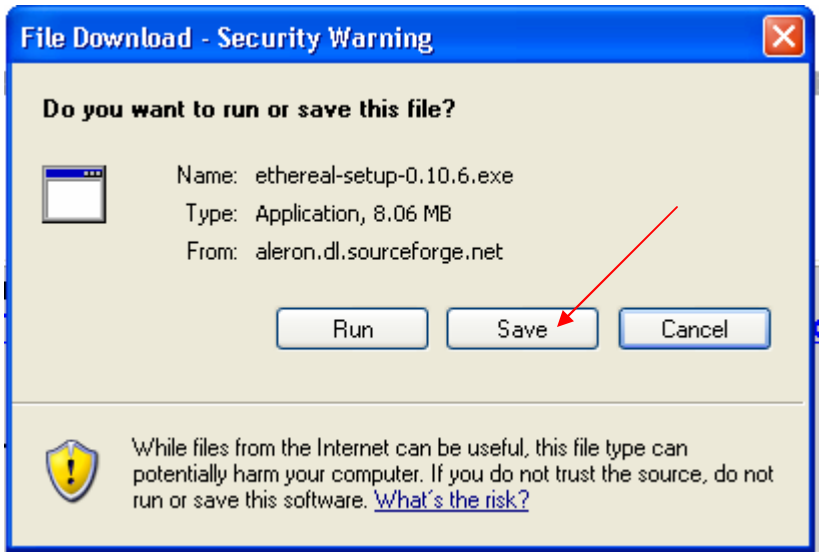
5. To download and install Ethereal, click the **ethereal-setup-*x.y.z*.exe** package. At the time of this writing, the latest version of ethereal is:

   ethereal-setup-0.10.6.exe

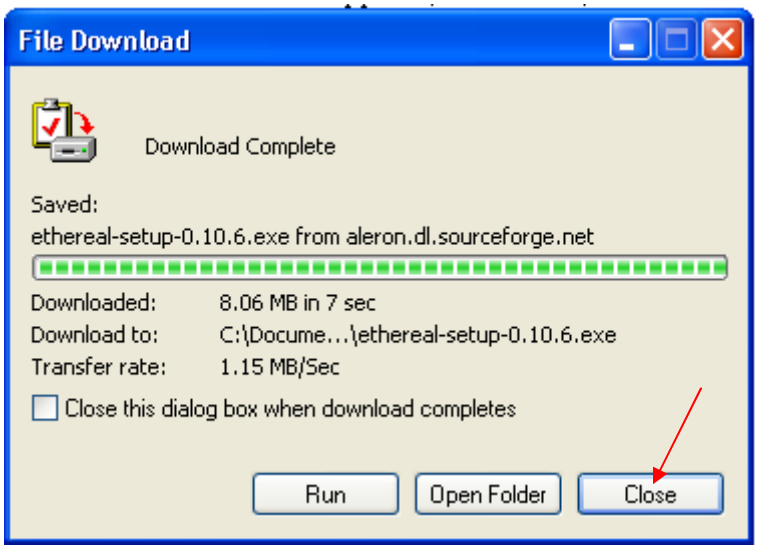
6. After you click on the ethereal package, you will be asked to select a mirror. Select the following mirror:

New York, New York	North America	8263 kb

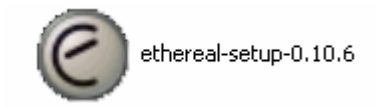
7. When the **File Download** screen appears, click **Save**, and choose to which location you want to save the file.



8. After the download is complete, click **Close** from the **File Download** screen.



9. To install ethereal, double click the ethereal icon from the location where you have downloaded it to.



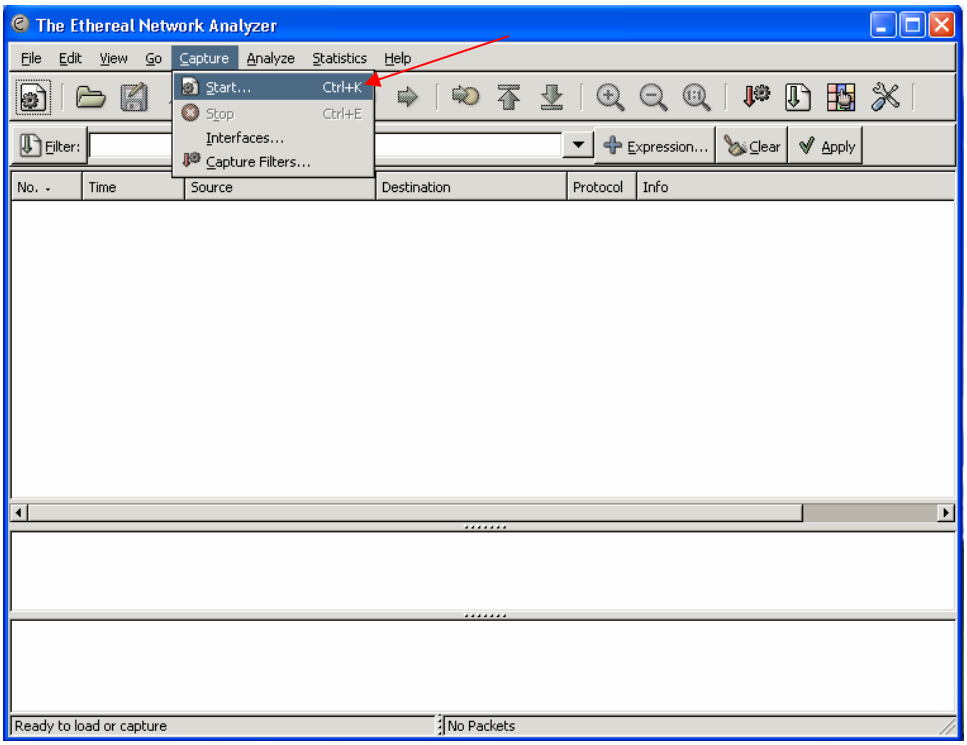
10. When the Open File screen appears, click Run, and follow the rest of the installation process.

Capturing Live Network Data:

To capture live network data using ethereal, follow these steps:

1. To start ethereal, simply click the ethereal icon from the desktop or click **Start** > **Programs** > **Ethereal**.

2. After you started Ethereal, select **Start...** from the **Capture** menu (or use the corresponding item in the "Main" toolbar), this brings up the **Capture Options** dialog box.



Note: *If you are not sure which options to choose in the* **Capture Options** *dialog box, just try keeping the defaults as this should work well in many cases.*

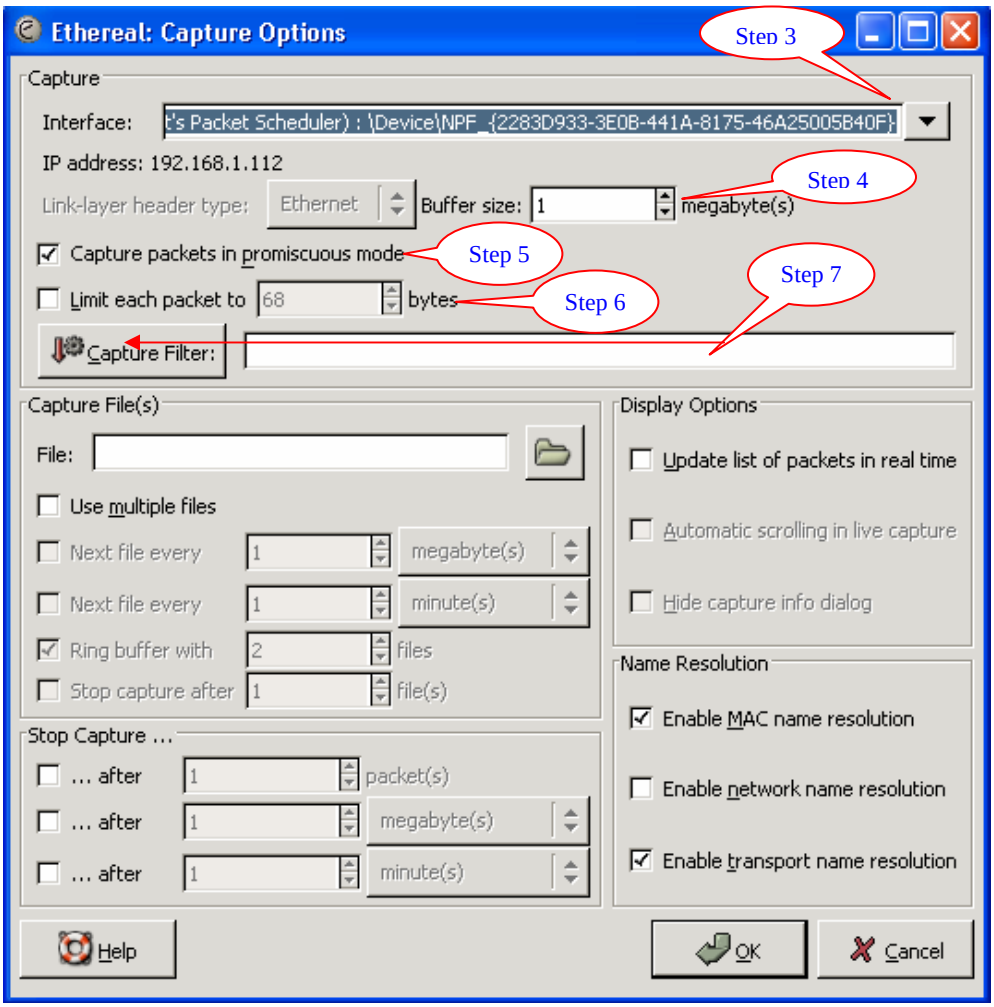
3. When the **Capture Options** dialog box appears, select the interface you want to capture on from the **Interface** dropdown menu. You can only capture on one interface, and you can only capture on interfaces that Ethereal has found on the system.
4. In the **Buffer size** text box, enter the buffer size to be used while capturing. This is the size of the kernel buffer which will keep the captured packets, until they are written to disk. If you encounter packet drops, try increasing this value.

5. Click the **Capture packets in promiscuous mode** option if you want to capture all packets on your LAN segment. If you do not specify this, Ethereal will only capture the packets going to or from your computer (not all packets on your LAN segment).

Note: *On a switched network, unicast traffic between two ports will not necessarily appear on other ports - only broadcast and multicast traffic will be sent to all ports. This means that even if you selected the promiscous mode, if you are connected to a switched network, you may not be able to see all trafic on your LAN segment.*

6. The **Limit each packet to** option can be used to specify the maximam amount of data that will captured for each packet in bytes. By default, this option is 68, which will be sufficient for most protocols.

7. The text box next to the **Capture filter** button can be used to specify a capture filter. By default, this option is empty, where no filters are selected. You could also click the **Capture filter** button to bring up the **Capture filter** dialog box, where you could create or select a previously created filter. To learn more about capture filters, refer to the **Capture Filter** section of this document.



8. In the **Capture File(s)** section, type the path name for the file you want to use as the capture file in the **File** text box. Or browse for the file using the button to the right of the **File** text box. If the field is left blank, the capture data will be stored in a temporary file.

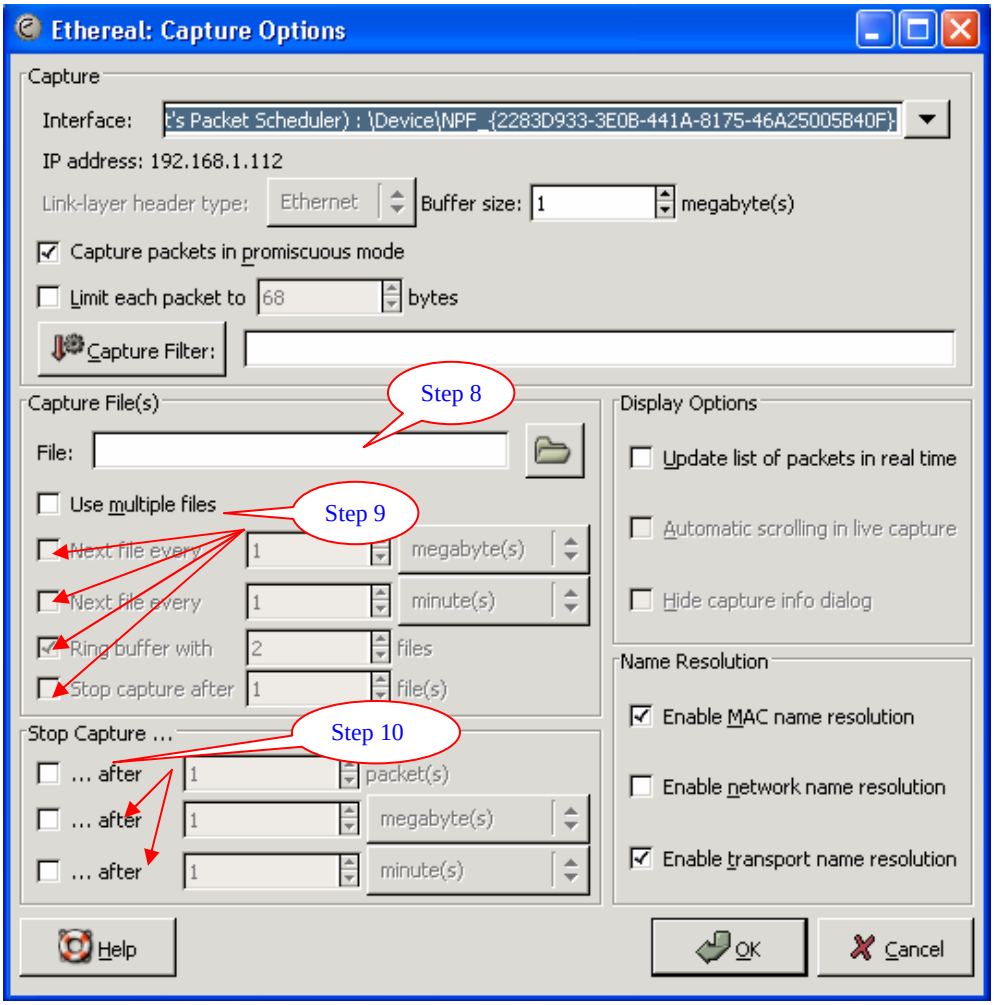
9. Instead of using a single capture file only, you could als use the **Use multiple files** option to use more than one file as the capture file. Ethereal will automaticaly swithch to a new file if a certain condition is met. Once you click the **Use multiple files** optionThe following are the conditions you can use to swithch to the next file:

   a- **Next file every n megabyte(s)**: Switch to the next file after the given number of byte(s)/kilobyte(s)/megabyte(s)/gigabyte(s) have been captured.
   b- **Next file every n minute(s)**: Switch to the next file after the given number of second(s)/minutes(s)/hours(s)/days(s) have elapsed.
   c- **Ring buffer with n files**: Form a ring buffer of the capture files, with the given number of files.
   d- **Stop capture after n file(s)**: Stop capturing after switching to the next file the given number of times.

   Note: *When working with large files (ex. Serveral 100 MB's) you will face a very slow process. Therefore if you plan to do long term capture or capture from a high trafic network it is a good idea to use the multiple file options. This will sepread the job over several smaller files that are easyer to work with.*

10. In the **Stop Capture…** section, you could stop capturing packets when a certain condition is met. The following is a list of condition options can be used to stopcapturing packets:

   a- **... after n packet(s)**: Stop capturing after the given number of packets have been captured.
   b- **... after n megabytes(s)**: Stop capturing after the given number of byte(s)/kilobyte(s)/megabyte(s)/gigabyte(s) have been captured.
      Note: *This option is greyed out, if the **Use multiple files** check box is selected.*
   c- **... after n minute(s)**: Stop capturing after the given number of second(s)/minutes(s)/hours(s)/days(s) have elapsed.

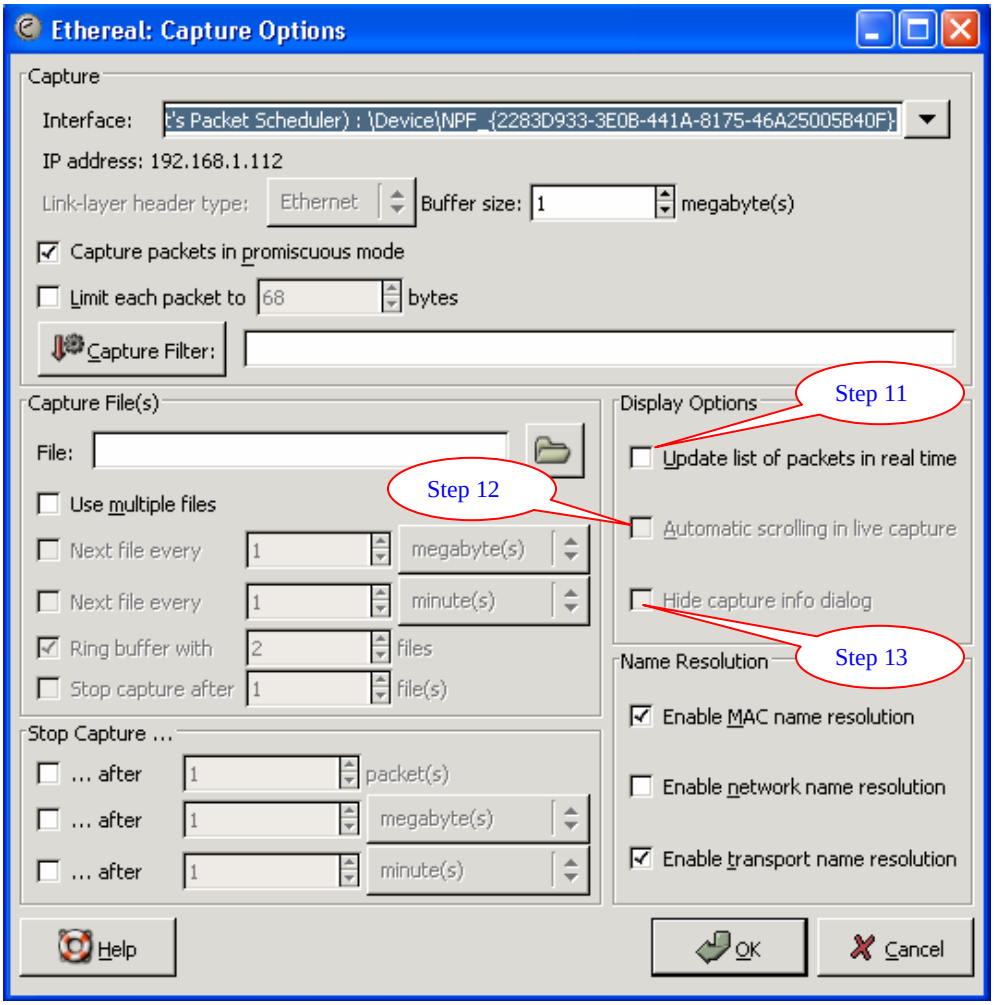


11. In the **Disply Options** section, you can use the **Update list of packets in real time** option to update the packet list pane in real time. If this option is not selected, no packets will be displayed until you stop the capture.

    Note: *If this option is checked, it will disable the* **Use multiple files** *option.*

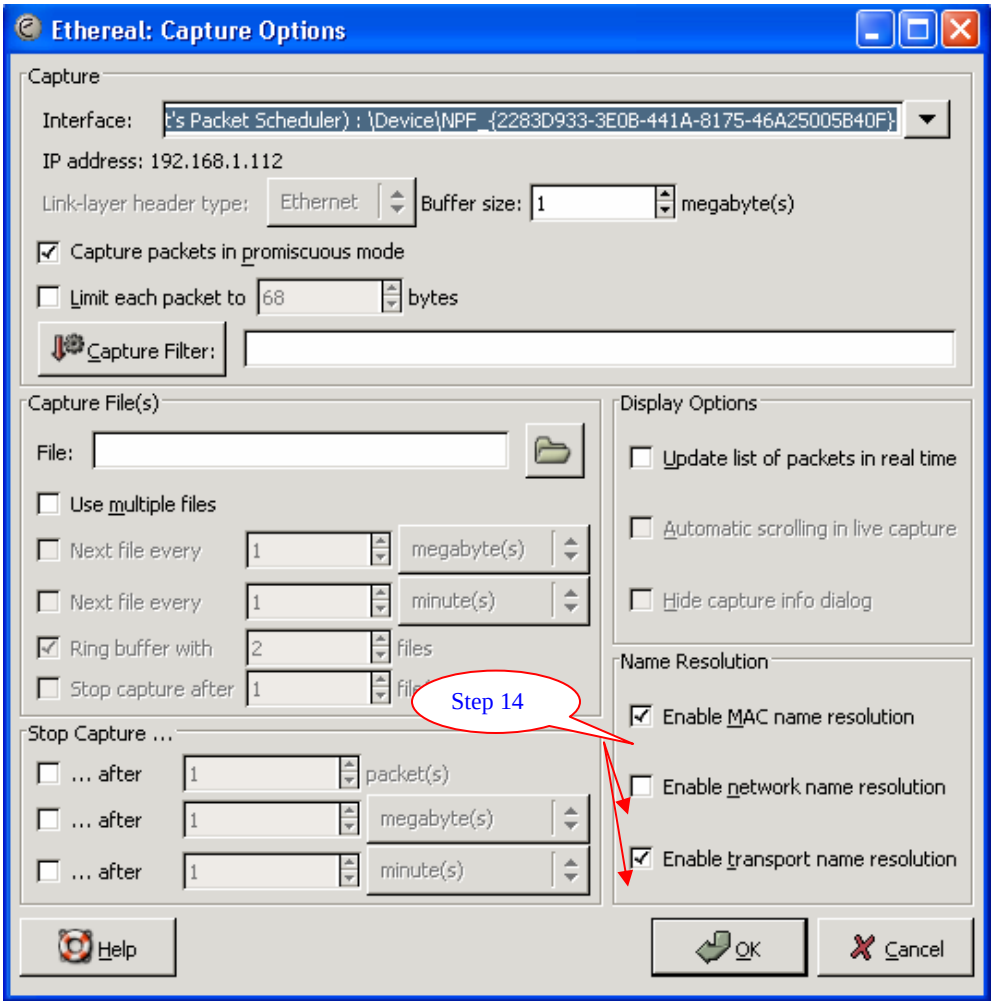
12. Once you select the **Update list of packets in real time** option, you can also select the **Automatic scrolling in live capture** option to scroll the packet list pane as new packets come in, so you are always looking at the last packet. If you do not specify this, Ethereal simply adds new packets onto the end of the list, but does not scroll the packet list pane.

13. Once you select the **Update list of packets in real time** option, you can also select the **Hide capture info dialog** option and the following capture info dialog will be hidden.



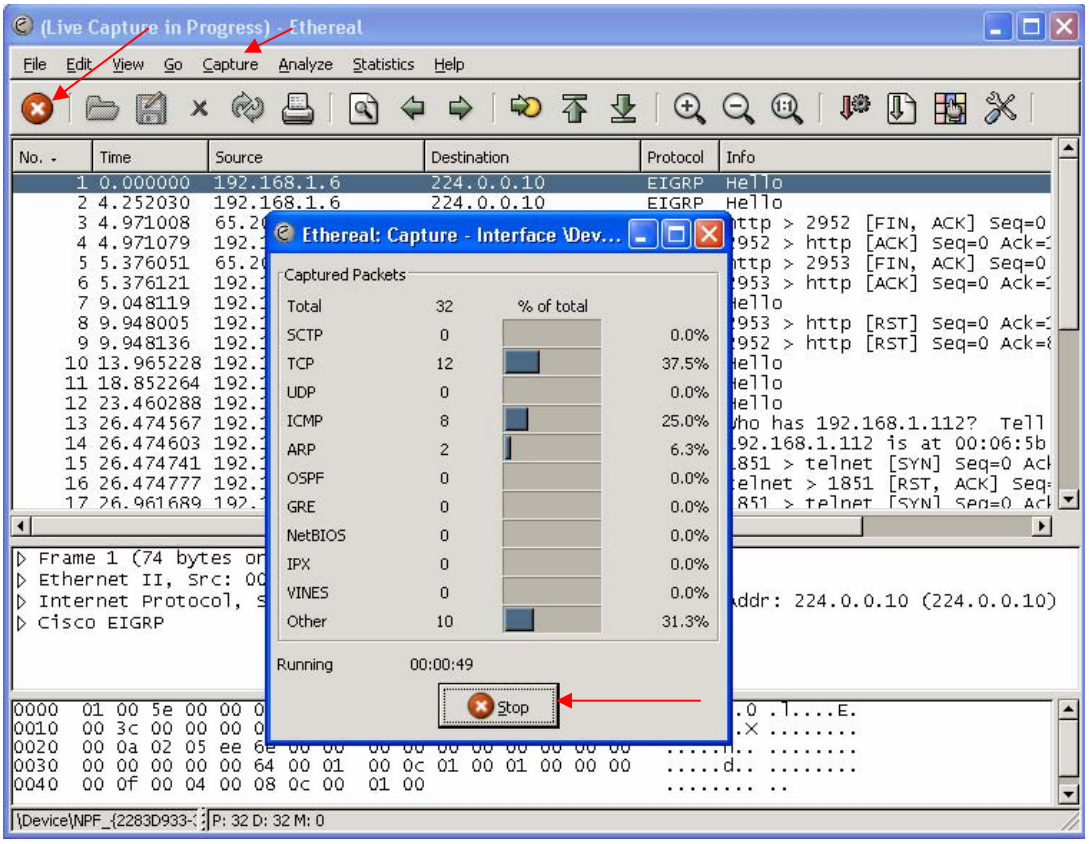
14. In the **Name Resolution** section, you could select the following options:

    a- **Enable MAC name resolution**: This option allows you to control whether or not Ethereal translates MAC addresses into names.
    b- **Enable network name resolution**: This option allows you to control whether or not Ethereal translates network addresses into names.
    c- **Enable transport name resolution**: This option allows you to control whether or not Ethereal translates transport addresses into protocols.



15. After setting the options you desired, click **OK** to start capturing packets, or **Cancel** to cancel the capture.

16. If you start a capture, Ethereal pops up a dialog box that shows you the progress of the capture. The capture will automaticly stop if one of the previously set conditions is met. However, there are other way to manualy stop the capture process. You can also stop capturing by using one of these methods:
    - a- Using the Stop button from the **Capture Info dialog box** .
      Note: *The Capture Info dialog box might be hidden, if the option* **Hide capture info dialog** *is used.*
    - b- Using the menu item **Capture** > **Stop** or the corresponding stop capture toolbar icon .
      Note: *These options are only available, if the option* **Update list of packets in real time** *is used.*
    - c- Pressing **Ctrl+E**.



Viewing Packets:

After capturing some packets or opening an already captured packet file, you will notice that the Ethereal packet viewing window consists of three panes. These panes are the **Packet List**, **Packet Details**, and **Packet Bytes** pane. To quickly view information about a specific packet, click on the packet once and the packet will be displayed in Packet Details pane and Packet Byte pane.

Packet List Pane:

The **Packet List** pane contains a list of all the captured packets, time captured, source IP address, destination IP address, protocol, and information.
There are also many other useful options available in the **Packet List** pane. To use these options, simply right click the desired packet and select one of the available options.

The following is a list of all the available options in the **Packet List** pane:

- **Follow TCP Stream**: It allows you to view all the data on a TCP stream between a pair of nodes. This menu item brings up a separate window and displays all the TCP segments captured that are on the same TCP

connection as a selected packet. This menu item is also available from the **Analyze** menu bar item.

- Decode As... : This menu item allows the user to force Ethereal to decode certain packets as a particular protocol. It lets you temporarily divert specific protocol dissections. This might be useful for example, if you do some uncommon things on your network. This menu item is also available from the **Analyze** menu bar item.

- Display Filters...: It allows you to specify and manage display filters. This menu item brings up a dialog box that allows you to create and edit display filters. You can name filters, and you can save them for future use. This menu item is also available from the **Analyze** menu bar item.

- Mark Packet: It allows you to mark a packet. This menu item is also available from the **Analyze** menu bar item.

- Time Reference: It allows you to set and work with time references. After setting a time reference, you could easly go from one time reference to another. This menu item is also available in the **Edit** menu bar item.

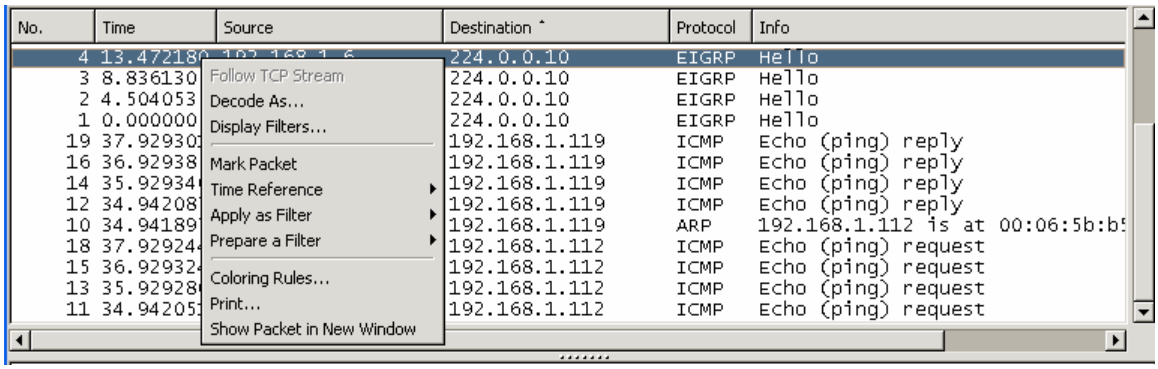
- Apply as Filter: These menu items will change the current display filter and apply the changed filter immediately. Depending on the chosen menu item, the current display filter string will be replaced or appended to by the selected protocol field in the packet details pane. This menu item is also available in the **Analyze** menu bar item.

- Prepare a Filter: These menu items will change the current display filter but won't apply the changed filter. Depending on the chosen menu item, the current display filter string will be replaced or appended to by the selected protocol field in the packet details pane. This menu item is also available in the **Analyze** menu bar item.

- Coloring Rules... : It allows you to colorize packets in the packet list pane. Also available in the **View** menu bar item.

- Print...: It allows you to print packets. Also available in the **File** menu bar item.

- Show Packet in New Window: It allows you to display the selected packet in another window. This option is very helpful, specialy when comparing two packets. Also available in the **View** menu bar item.



Packet Details Pane:

This pane shows the protocols and protocol fields of the packet selected in the **Packet List** pane. The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed as needed. This pane also contains a list of useful options available with a right mouse click.

The following is a list of all the available options in the **Packet Details List** pane:

- **Follow TCP Stream**: Same as the one in **Packet List** pane (listed above).

- **Follow TCP Stream**: Same as the one in **Packet List** pane (listed above).

- **Decode As...**: Same as the one in **Packet List** pane (listed above).

- **Display Filters...**: Same as the one in **Packet List** pane (listed above).

- **Resolve Name**: This menu item causes name resolution to be performed for the selected packet.

- **Go to Corresponding Packet**: If the selected field has a corresponding packet, go to it. An exapmle of corresponding packets will usually be a request/response packet pair.

- **Export Selected Packet Bytes...**: This option allows you to export raw packet bytes to a binary file.

- **Protocol Properties...**: The menu item takes you to the properties dialog and selects the page corresponding to the protocol if there are properties associated with the highlighted field.

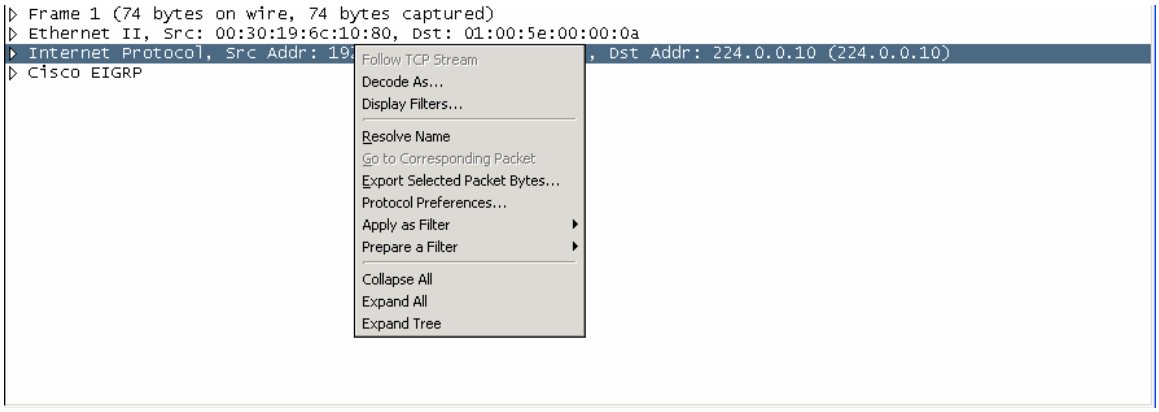
- **Apply as Filter**: Same as the one in **Packet List** pane (listed above).

- **Prepare a Filter**: Same as the one in **Packet List** pane (listed above).

- **Collapse All**: Ethereal keeps a list of all the protocol subtrees that are expanded, and uses it to ensure that the correct subtrees are expanded when you display a packet. This menu item collapses the tree view of all packets in the capture list.

- **Expand All**: This menu item expands all subtrees in all packets in the capture.

- **Expand Tree**: This menu item expands the currently selected subtree.



Packet Bytes Pane:

The **Packet Bytes** pane shows the data of the current packet, selected in the **Packet List** pane, in a hexdump style.

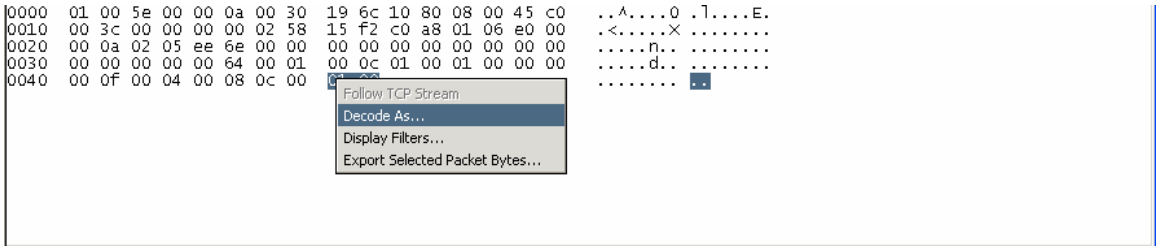
The following is a list of all the available options in the **Packet Bytes** pane:

- **Follow TCP Stream**: Same as the one in **Packet List** pane (listed above).

- **Decode As...**: Same as the one in **Packet List** pane (listed above).

- **Display Filters...**: Same as the one in **Packet List** pane (listed above).

- **Export Selected Packet Bytes…**: Same as the one in **Packet Details** pane (listed above).



Packet Range Frame:

The packet range frame is a part of various output related dialog boxes. It provides options to select which packets should be processed for the output function.

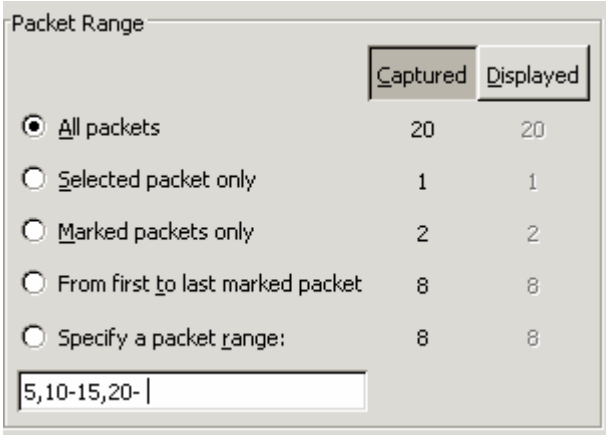
17. **All packets**: will process all packets.

18. **Selected packet only**: process only the selected (highlighted) packet.

19. **Marked packets only**: process only the marked packets. Note that this option is grayedout by default. To activate this option, you must mark the desired packets by right cklicking the packet and selecting **Mark Packet**.

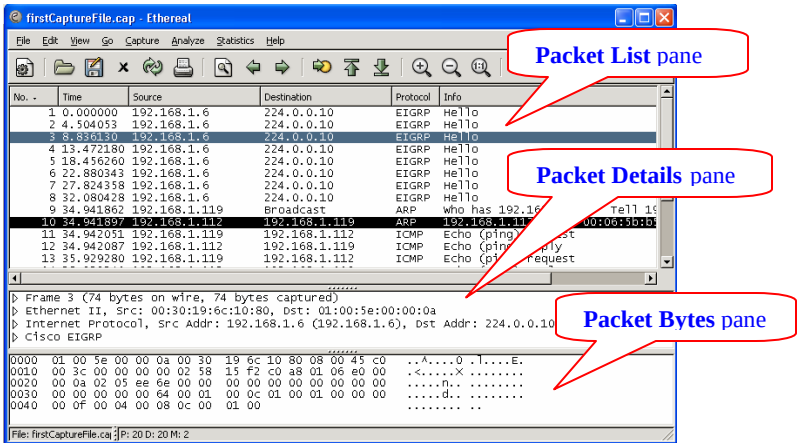
20. **From first to last marked packet**: process the packets from the first to the last marked one. Note that this option is grayedout by default. To activate this option, you must mark the desired first and last packets, by right clicking the packet and selecting **Mark Packet**.

21. **Specify a packet range**: process a user specified range of packets, e.g. specifying **5,10-15,20-** will process the packet number five, the packets from packet number ten to fifteen (inclusive) and every packet from number twenty to the end of the capture.



Packet Format Frame:

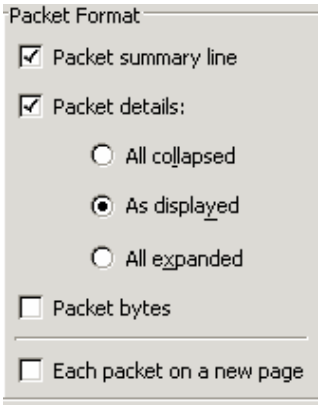
The packet format frame is a part of various output related dialog boxes. It provides options to select which parts of a packet should be used for the output function.



1. **Packet summary line** enable the output of the summary line, just as in the **Packet List** pane.

2. **Packet details** enable the output of the packet details tree.
   - **All collapsed** the info from the **Packet Details** pane in all collapsed state.
   - **As displayed** the info from the **Packet Details** pane in the current state.
   - **All expanded** the info from the **Packet Details** pane in all expanded state.
3. **Packet bytes** enable the output of the packet bytes, just as in the **Packet Bytes** pane.

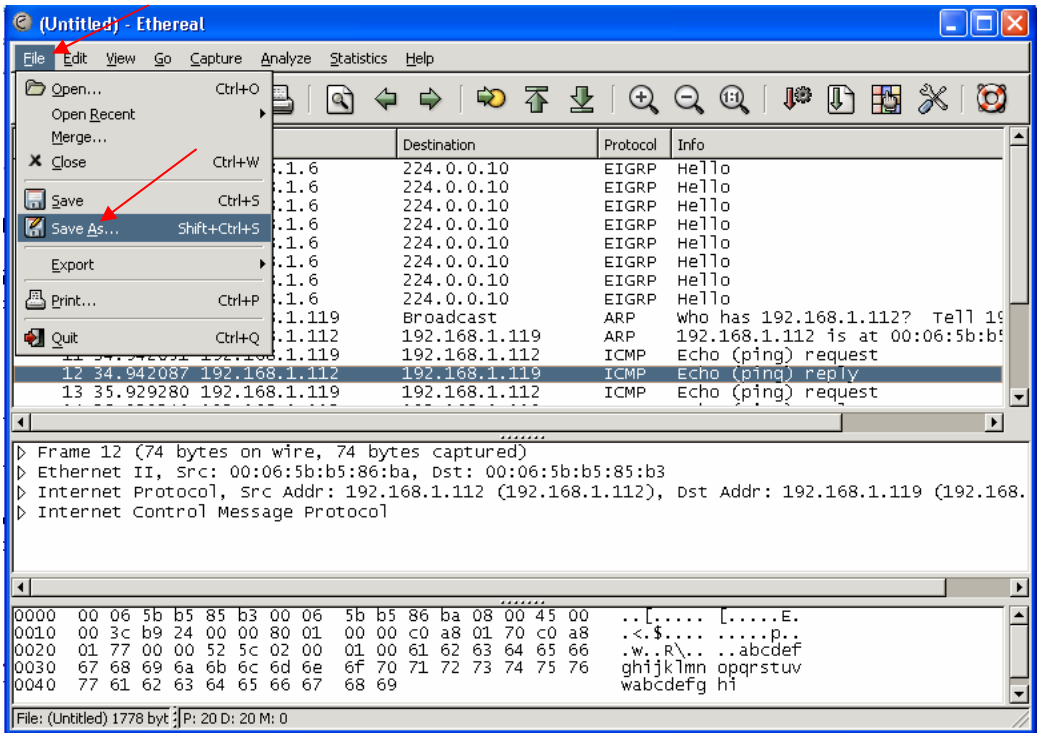
4. **Each packet on a new page** put each packet on a separate page (e.g. when saving/printing to a text file, this will put a form feed character between the packets). This option works as a combination with one of the above options. When this option is selected by itselfe, the **Ok** button is grayed out.



Saving, Opening, and Merging Capture File:

To learn how to use Ethereal's save and open capture file features, follow these steps:

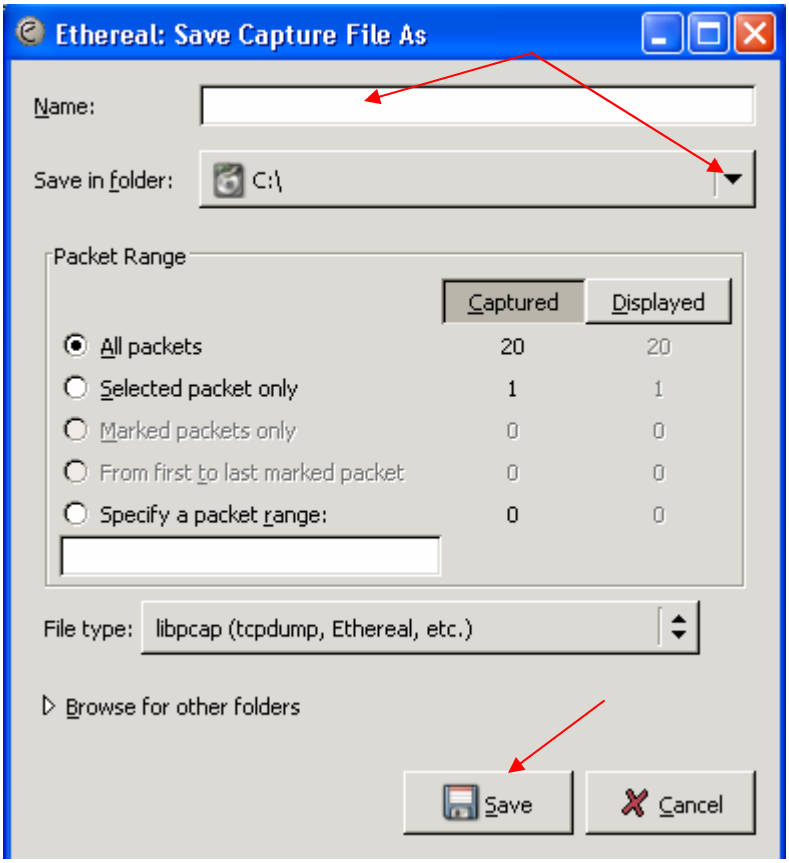
1. To save an ethereal capture file, click **File** > **Save As…** from the menu bar.



2. When the **Ethreal: Save Capture File As** window appears, type the desired file name in the **Name** text field, and find the location to save the file in from the **Save in folder**[1] dropdown menu. Click **Save** to save the file.

   Note: *You can save a file as a capture file by adding the* **.cap** *extention to the file name.*

[1] If the folder or directory you want is not present in the **Save in folder** dropdown menu, go to **step 3**.

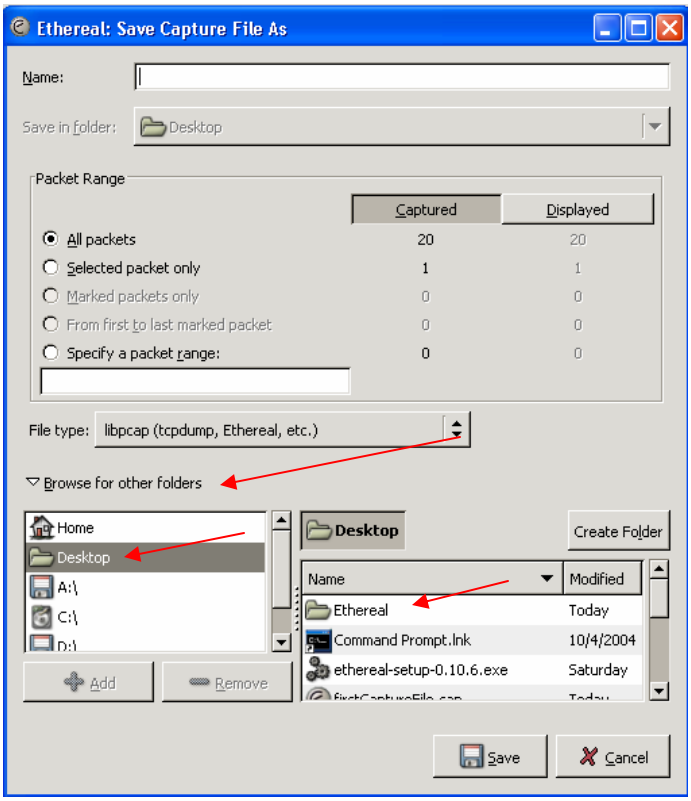


3. If the directory you want is not present in the **Save in folder** dropdown menu, click the **Browse for other folders** option. Choose the location you want to save the file in and click the **Add** button.

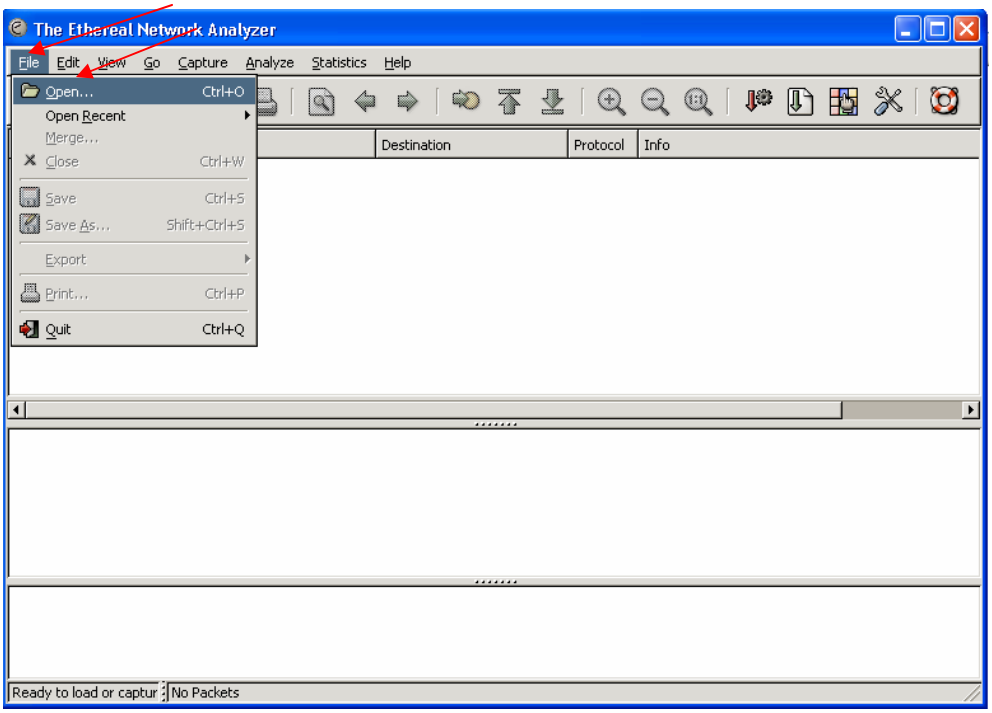
   For example, if you want to save the file in a folder called Ethereal located on desktop, click Desktop from the bottom left box and on the bottom right box click Ethreal. Then click **Add** to add this location to the **Save in folder** dropdown menu.

   Once you finished adding the new location, click the **Browse for other folders** option again, and select the new location form the **Save in folder** menu. Click **Save** to save the file.

   Note: *To delet a folder or directory from the **Save in folder** dropdown menu, repeat step 3 and click the **Remove** button instead of **Add**.*



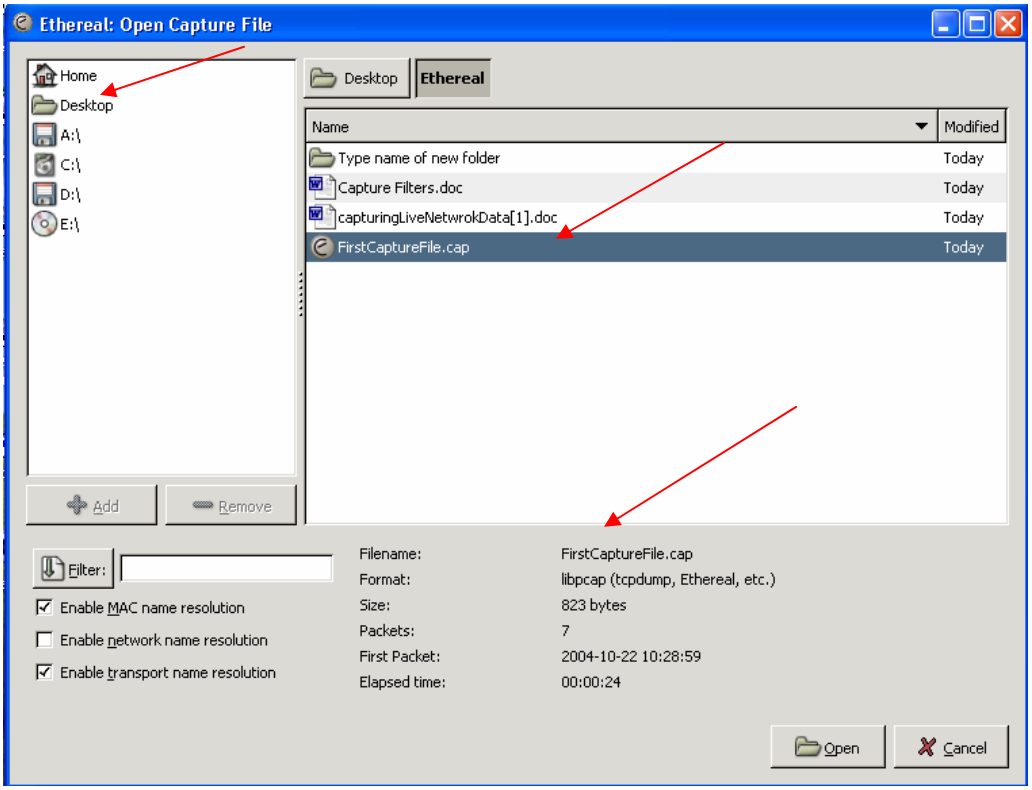
4. To open a capture file that has already been saved on the computer, click **File > Open…**.



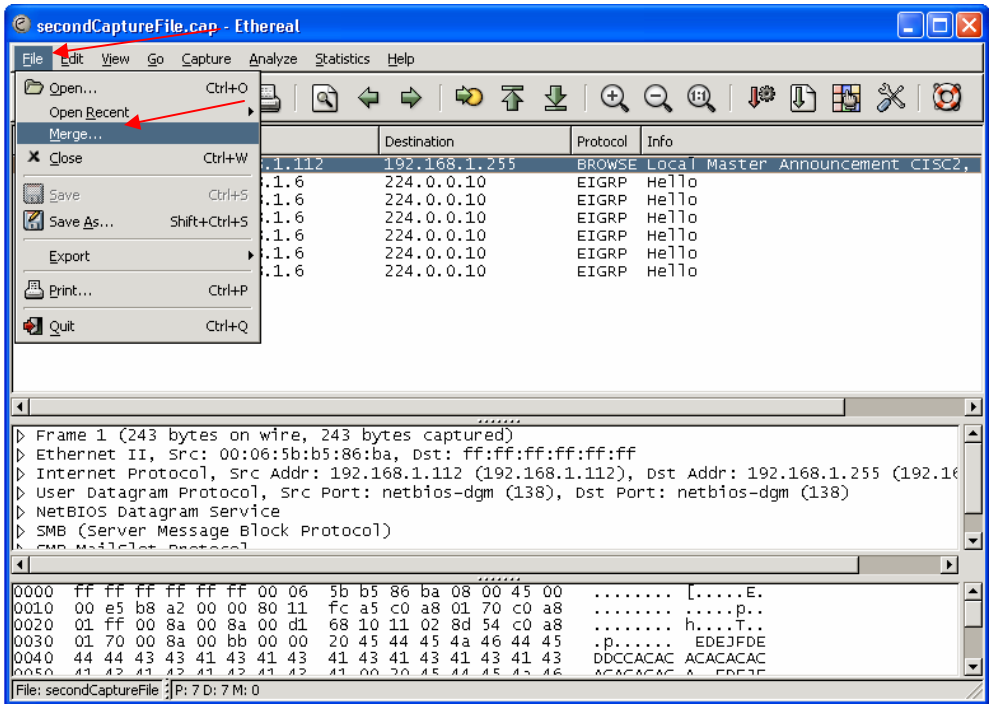
5. When you click **Open…**, the **Ethereal: Open Capture File** screen will appear. Double click the desired directory form the left of the screen and from the right side double click capture file. If the file is stored inside a folder, double click the folder to view its content, then double click the file.

Note: *To view important information about the capture file before opening it, click of the file once and view the bottom of the screen.*

Note: *Ethereal can read capture files from a large number of other packet capture programs as well.*



6. To merge two capture files, open one of the files in Ethereal and click **File > Merge…** from the menu items.

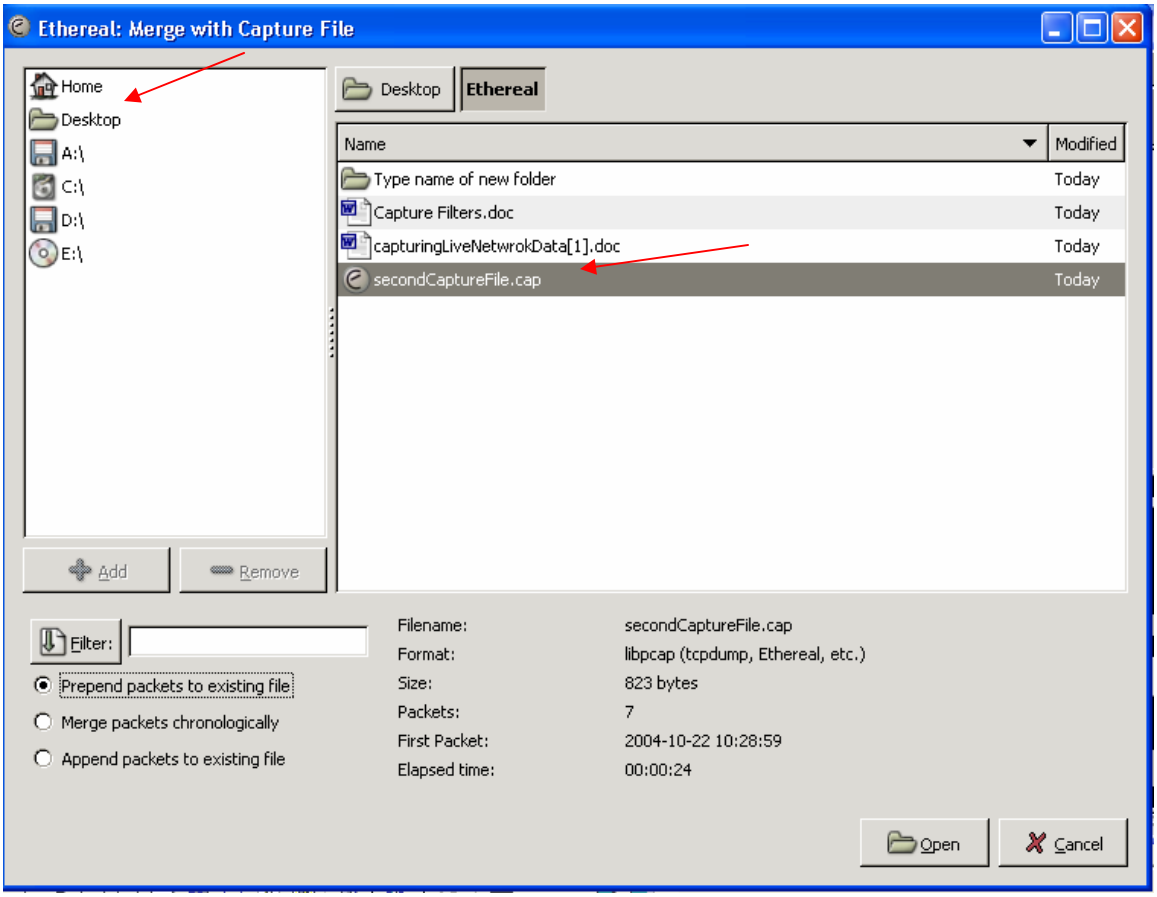


7. When the **Ethereal: Merge with Capture File** screen apperas, browse for the other capture file you want to merge and single click it.

There are three different formats you can choose from to merge files. To choose a specific format, select one of the radio buttons located at the bottom of the screen:

a- **Prepend packets to existing file:** Prepend the packets from the selected file before the currently loaded packets.
b- **Merge packets chronologically:** Merge both the packets from the selected and currently loaded file in chronological order.
c- **Append packets to existing file:** Append the packets from the selected file after the currently loaded packets.

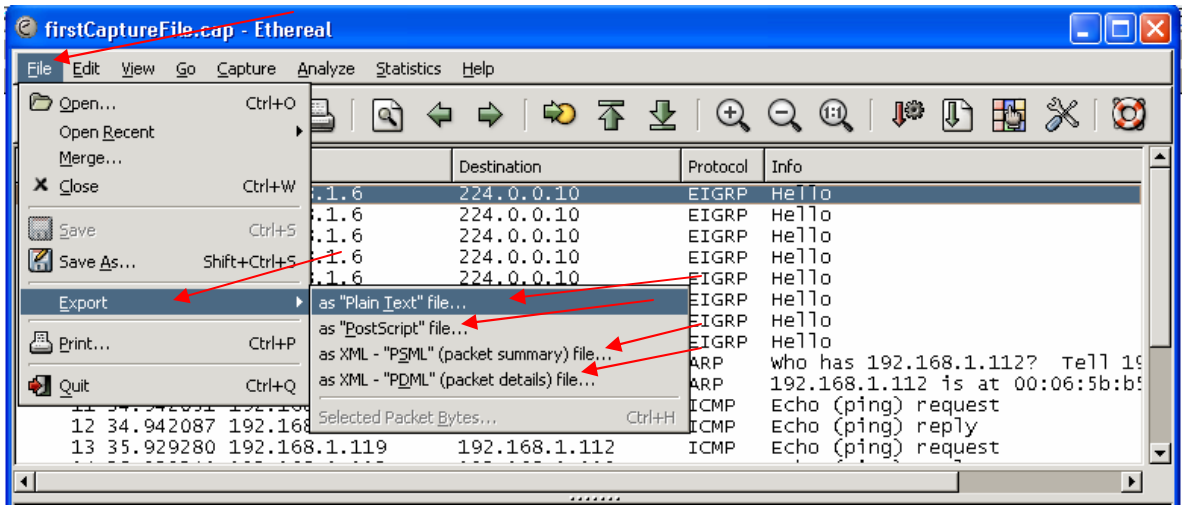
Once you finish, click **Open** and the files will be merged.



Note: *You can also use drag-and-drop to drop multiple files on the main window. Ethereal will try to merge the packets in chronological order from the dropped files into a newly created temporary file.*

Exporting Packet Data:

Ethereal can be used to export packet data in many ways and formats. An ethereal packet data can be exported as a plain text file, postscript file, PSML file, or as a PDML file. You can see these options when you click **File > Export** from the main menu.

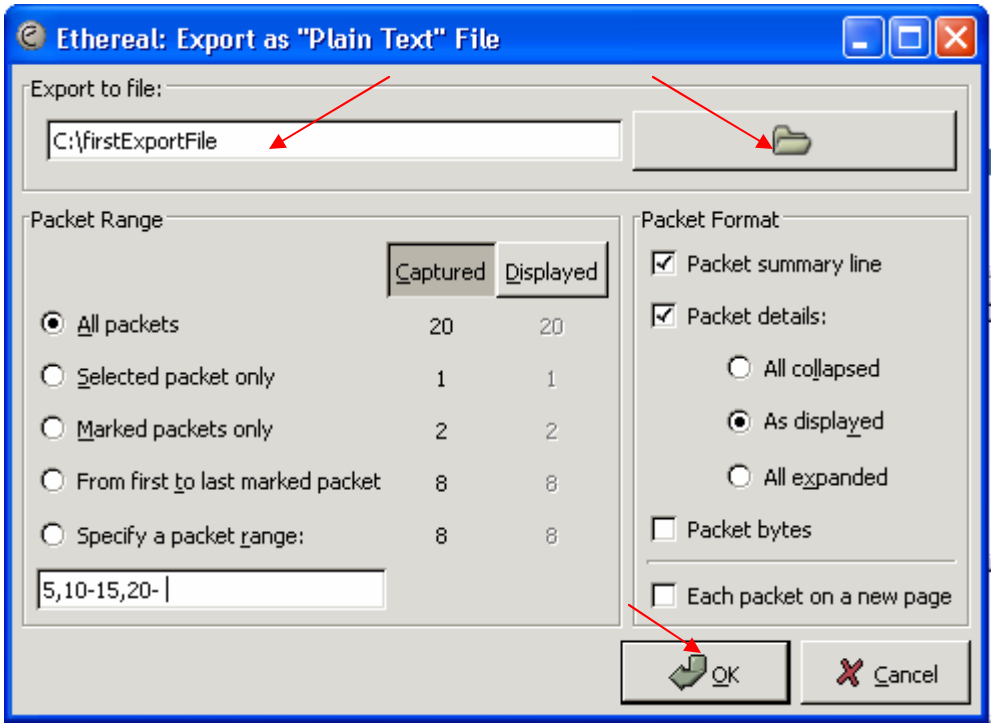


To learn the different ways and how to export packet data in ethereal, refer to the following sections:

<u>Exporting Packet Data as Plain Text File:</u>

1. To export a packet data as plain text, click **File > Export > as "Plain Text" file…**.

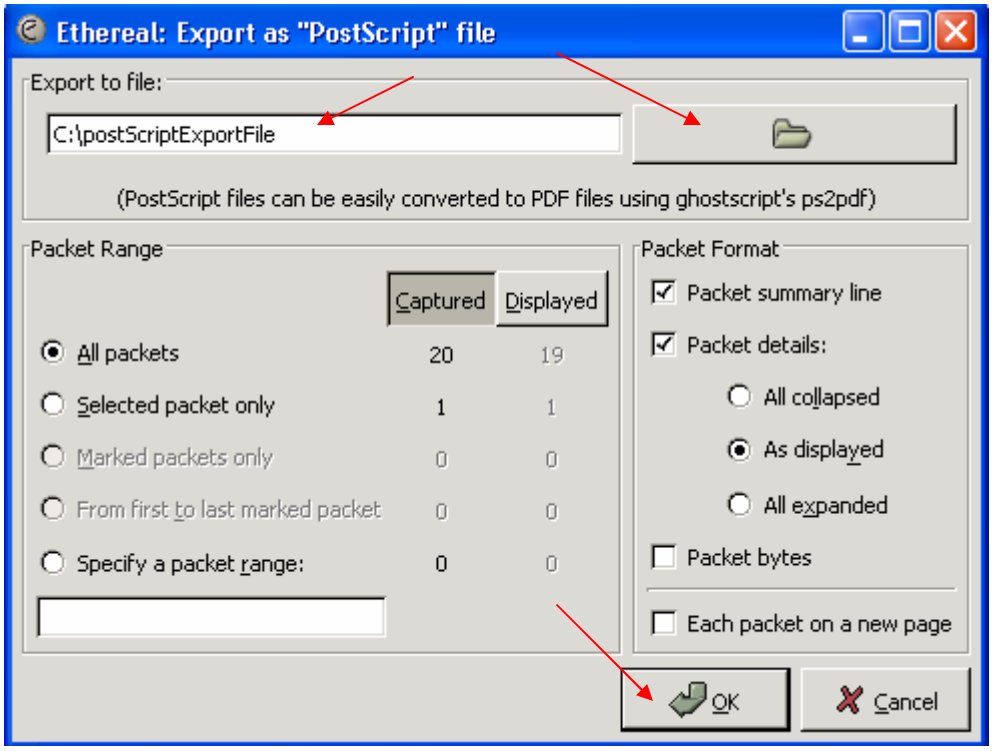
2. Next, the **Export as "Plain Text" File** screen appears. In the **Export to file** textbox, type the destination to where you want to export the packet data, or click the button to the right of this textbox and browse for the location to export. For more information on the **Packet Range** and **Packet Format** options, refer to the **Packet Range and Format Frames** section. Once you are done, click **OK** to export the file.



Exporting Packet Data as Postscript File:

1. To export a packet data as postscript file, click **File > Export > as "PostScript" file…**.

2. Next, the **Export as "PostScript" File** screen appears. In the **Export to file** textbox, type the destination to where you want to export the packet data, or click the button to the right of this textbox and browse for the location to export. For more information on the **Packet Range** and **Packet Format** options, refer to the **Packet Range and Format Frames** section. Once you are done, click **OK** to export the file.



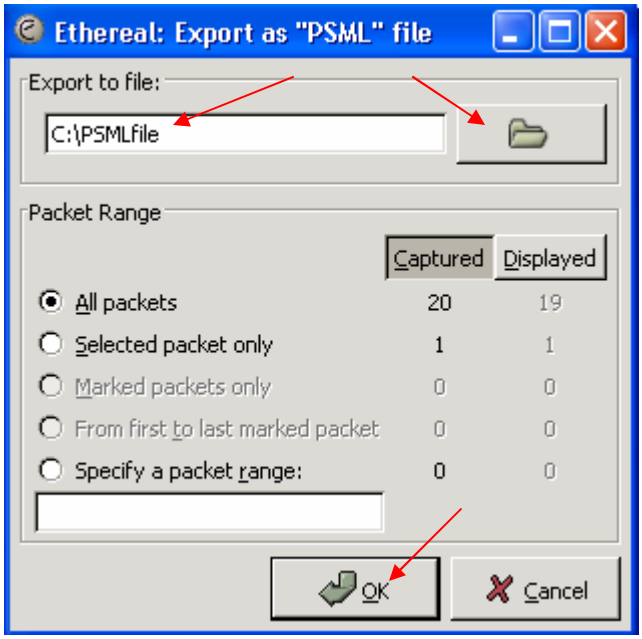
Exporting Packet Data as PSML File:

This is an XML based format including only the packet summary.

1. To export a packet data as postscript file, click **File > Export > XML - "PSML" (packet summary) file….**

2. Next, the **Export as "PSML" File** screen appears. In the **Export to file** textbox, type the destination to where you want to export the packet data, or click the button to the right of this textbox and browse for the location to export. For more information on the **Packet Range** options, refer to the **Packet Range and Format Frames** section. Once you are done, click **OK** to export the file.

   Note: *There's no such thing as a packet details frame for PSML export, as the packet format is defined by the PSML specification.*



Exporting Packet Data as PDML File:

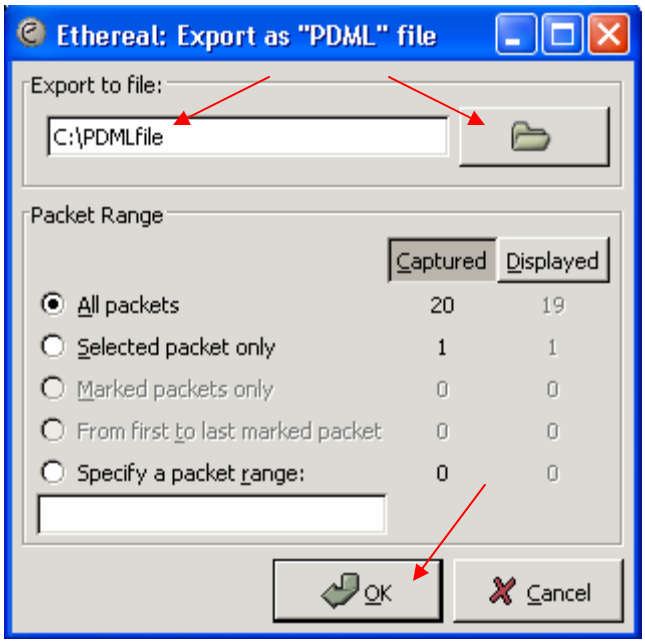
This is an XML based format including the packet details.

1. To export a packet data as postscript file, click **File > Export > XML - "PDML" (packet details) file….**

2. Next, the **Export as "PDML" File** screen appears. In the **Export to file** textbox, type the destination to where you want to export the packet data, or click the button to the right of this textbox and browse for the location to export. For more information on the **Packet Range** options, refer to the **Packet Range and Format Frames** section. Once you are done, click **OK** to export the file.

   Note: *Ther is no such thing as a packet details frame for PDML export, as the packet format is defined by the PDML specification.*

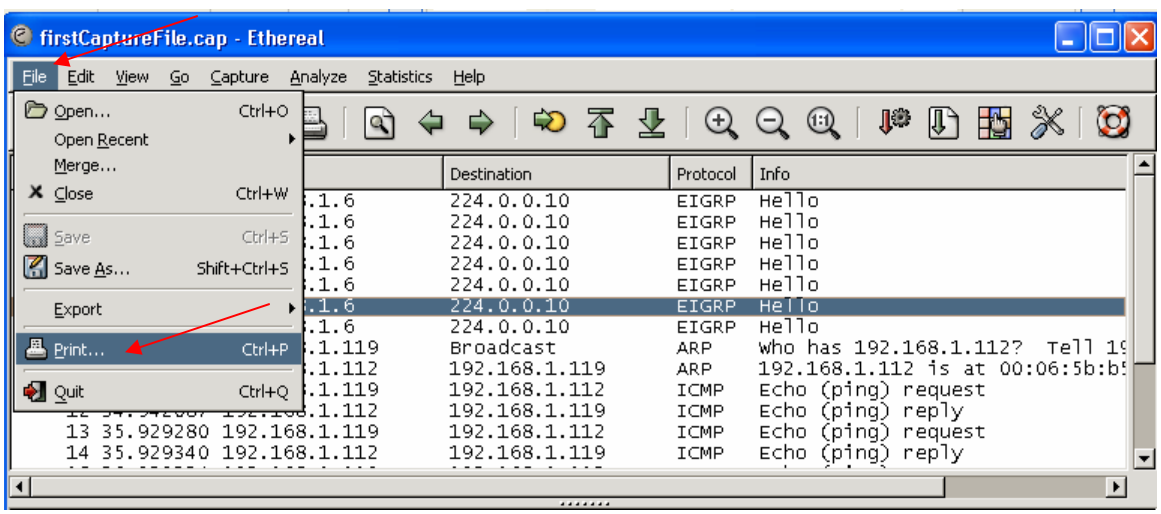
   Note: *The PDML specification is not officially released and Ethereal's implementation of it is still in an early beta state, so please expect changes in future Ethereal versions.*



Printing Packets:

To print packets in Ethereal, follow these steps:

1. To print a packet, click **File** > **Print…** from the main menu.

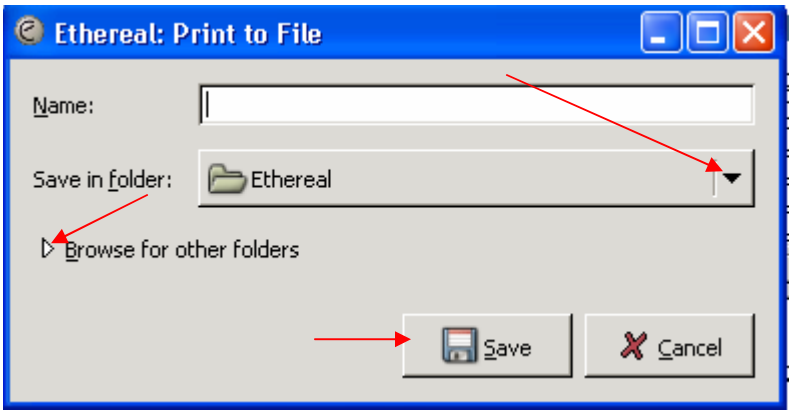


2. When the **Print** screen appears, in the **Printer** section, select one of the following:

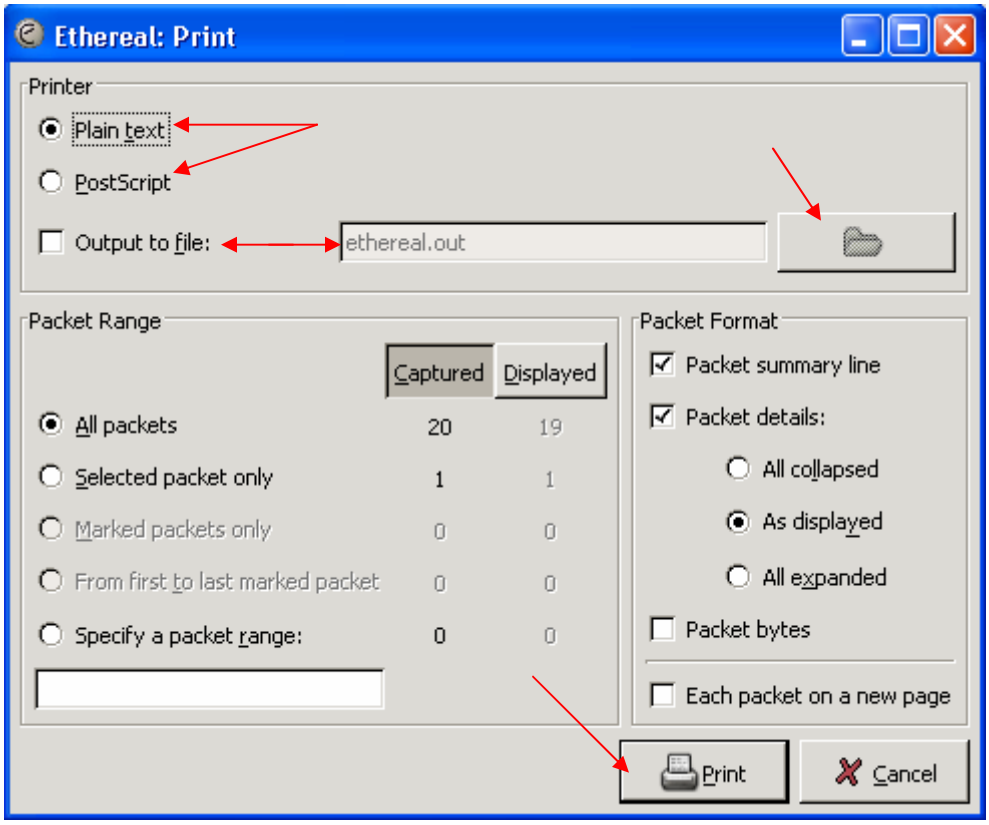
   a- **Plain Text**: The packet will be printed in plain text.

b- **PostScipt**: The packet will be printed as postscritp. This option is useful to generate a better print output on PostScript aware printers.

c- **Output to file:** This option could be used as a combination with any of the two options above. Prints the output to the file specified in text box next to this option. You can also use the browse button to select the file to print the output to. When you click the browse button, the **Print to File** screen appears. Type the file name in the **Name** textbox. You can choose a location from the **Save in folder** dropdown menu or you can browse for a specific place using the **Browse for other folders** option. Click **Save** when done.



To learn more about the **Packet Range** and **Packet Format** options, refer to the **Packet Range and Format Frames** section. After making the desired selections, click **Print**.



Capture Filters:

A capture filter takes the form of a series of primitive expressions connected by conjuctions (**and/or**) and optionally preceded by **not**:

```
[not] primitive [and|or [not] primitive ...]
```

Exapmle1: A capture filter for telnet that captures traffic to and from a particular host:

```
tcp port 23 and host <host IP address>
```

Example2: Capturing all telnet traffic not from a particular host

```
tcp port 23 and not host <host IP address>
```

A primitive is simply one of the following:

a- [src|dst] host <host IP address or name> This primitive allows you to filter on a host IP address or name. You can optionally precede the primitive with the

keyword **src|dst** to specify that you are only interested in source or destination addresses. If these are not present, packets where the specified address appears as either the source or the destination address will be selected.

b- **ether [src|dst] host <ehost>** This primitive allows you to filter on Ethernet host addresses. You can optionally include the keyword **src|dst** between the keywords **ether** and **host** to specify that you are only interested in source or destination addresses. If these are not present, packets where the specified address appears in either the source or destination address will be selected.

c- **gateway host <host>** This primitive allows you to filter on packets that used **host** as a gateway. That is, where the Ethernet source or destination was **host** but neither the source nor destination IP address was **host**.

d- **[src|dst] net <net> [{mask <mask>}|{len <len>}]** This primitive allows you to filter on network numbers. You can optionally precede this primitive with the keyword **src|dst** to specify that you are only interested in a source or destination network. If neither of these are present, packets will be selected that have the specified network in either the source or destination address. In addition, you can specify either the netmask or the CIDR prefix for the network if they are different from your own.

e- **[tcp|udp] [src|dst] port <port>** This primitive allows you to filter on TCP and UDP port numbers. You can optionally precede this primitive with the keywords **src|dst** and **tcp|udp** which allow you to specify that you are only interested in source or destination ports and TCP or UDP packets respectively. The keywords **tcp|udp** must appear before **src|dst**. If these are not specified, packets will be selected for both the TCP and UDP protocols and when the specified address appears in either the source or destination port field.

f- **less|greater <length>** This primitive allows you to filter on packets whose length was less than or equal to the specified length, or greater than or equal to the specified length, respectively.

g- **ip|ether proto <protocol>** This primitive allows you to filter on the specified protocol at either the Ethernet layer or the IP layer.

h- **ether|ip broadcast|multicast** This primitive allows you to filter on either Ethernet or IP broadcasts or multicasts.

i- **<expr> relop <expr>** This primitive allows you to create complex filter expressions that select bytes or ranges of bytes in packets.

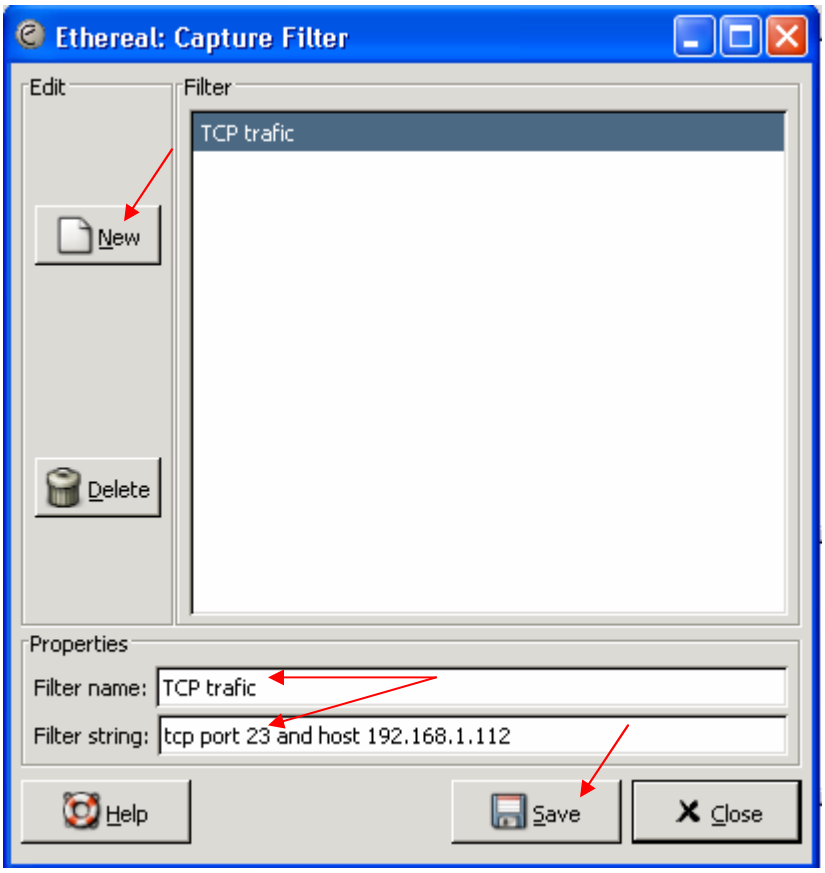
<u>Defining and Saving Capture Filters</u>

You can define capture filters with Ethereal and give them labels for later use. This can save time in remembering and retyping some of the more complex filters you use.

To define a new filter or edit an existing filter, follow these steps:

1. From the main menu bar, click **Capture** > **Capture Filters**.

2. When the **Capture Filter** box appears, Click **New**, and type the capture filter name in the **Filter name** text box. Type the filter string in the **Filter string** textbox. Click **Save** to save the filter string you created, and click **Close**.



Display Filters:

Ethereal provides a powerful display filter language. You can compare values in packets as well as combine expressions into more specific expressions. Display filters help the user by showing only those packets where the specified field in the display filter exists. For example, the filter string **tcp** will show all packets containing the tcp protocol.

For a complete list of all filter fields, click **Help** (from main menu bar) > **Supported Protocols** > **Display Filter Fields** tab.

You can build display filters that compare values using a number of different comparison operators.

Note: *You can use English and C-like terms in the same way, they can even be mixed in a filter string!*

Display Filter comparison operators

English	C-like	Description and example
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`

You can combine filter expressions in Ethereal using the logical operators.

Display Filter Logical Operations

English	C-like	Description and example
and	&&	**Logical AND** `ip.addr==10.0.0.5 and tcp.flags.fin`
or	||	**Logical OR** `ip.addr==10.0.0.5 or ip.addr==192.1.1.1`
xor	^^	**Logical XOR** `tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == 0.6.29`
not	!	**Logical NOT** `not llc`

[...]		**Substring Operator**
		
		Ethereal allows you to select subsequences of a sequence in rather elaborate ways. After a label you can place a pair of brackes [] containing a comma separated list of range specifiers.
		
		`eth.src[0:3] == 00:00:83`
		
		The example above uses the n:m format to specify a single range. In this case n is the beginning offset and m is the length of the range being specified.
		
		`eth.src[1-2] == 00:83`
		
		The example above uses the n-m format to specify a single range. In this case n is the beginning offset and m is the ending offset.
		
		`eth.src[:4] == 00:00:83:00`
		
		The example above uses the :m format, which takes everything from the beginning of a sequence to offset m. It is equivalent to 0:m
		
		`eth.src[4:] == 20:20`
		
		The example above uses the n: format, which takes everything from offset n to the end of the sequence.
		
		`eth.src[2] == 83`
		
		The example above uses the n format to specify a single range. In this case

English	C-like	Description and example

		the element in the sequence at offset n is selected. This is equivalent to n:1.
		
		`eth.src[0:3,1-2,:4,4:,2] ==`
		`00:00:83:00:83:00:00:83:00:20:20:83`
		
		Ethereal allows you to string together single ranges in a comma separated list to form compound ranges as shown above.

Note: *Often people use a filter string to display something like* ***ip.addr == 1.2.3.4*** *which will display all packets containing the IP address 1.2.3.4. Then they use* ***ip.addr != 1.2.3.4*** *to see all packets not containing the IP address 1.2.3.4 in it. Unfortunately, this does* ***not*** *do the expected. that expression will even be true for packets where either source or destination IP address equals 1.2.3.4.*

Defining and Saving Display Filters

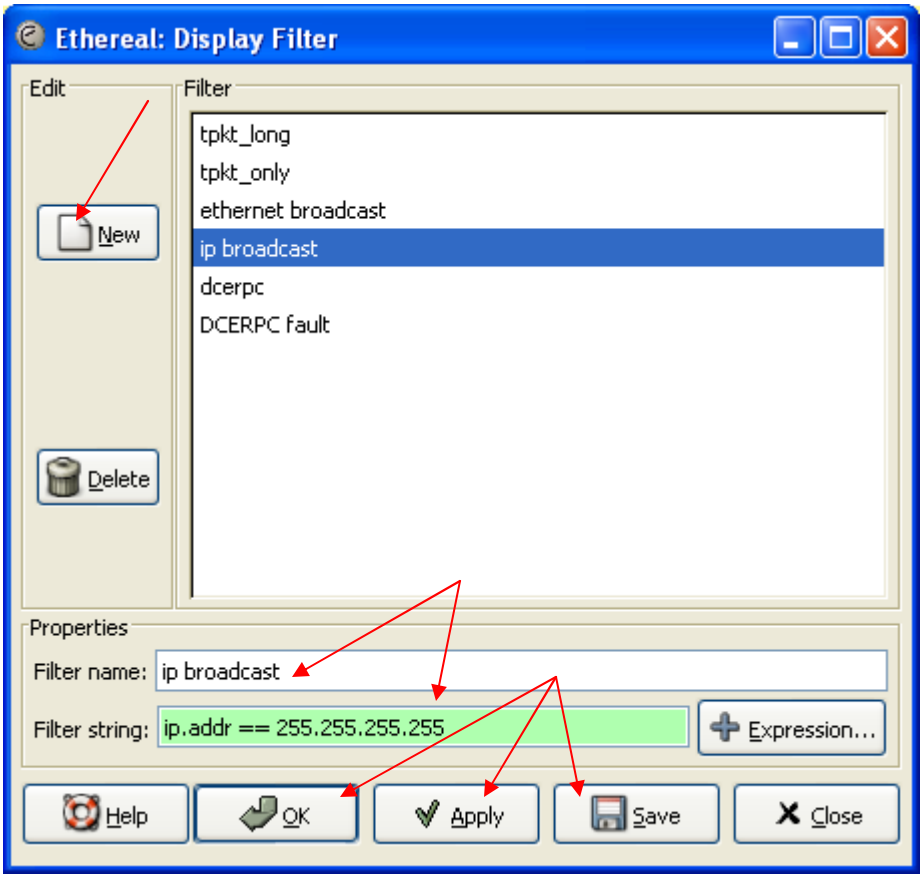
You can define filters with Ethereal and give them labels for later use. This can save time in remembering and retyping some of the more complex filters you use.

To define a new filter or edit an existing filter, follow these steps:

3. From the main menu bar, click **Analyze > Display Filter**.

4. When the **Display Filter** box appears, Click **New**, and type the display filter name in the **Filter name** text box. Type the filter string in the **Filter string** textbox. Click **Save** to save the filter string you created. Click **Apply** to apply the created filter to the captured packets, and click **Ok**. Now you will only see those packets that you specified in your filter.

   Note: *It is easyer for for new users to use the* ***Expression…*** *button to help them write a filter strings. The* ***Expression…*** *button will bring the* ***Filter expression*** *box up, which is explained in the next section.*

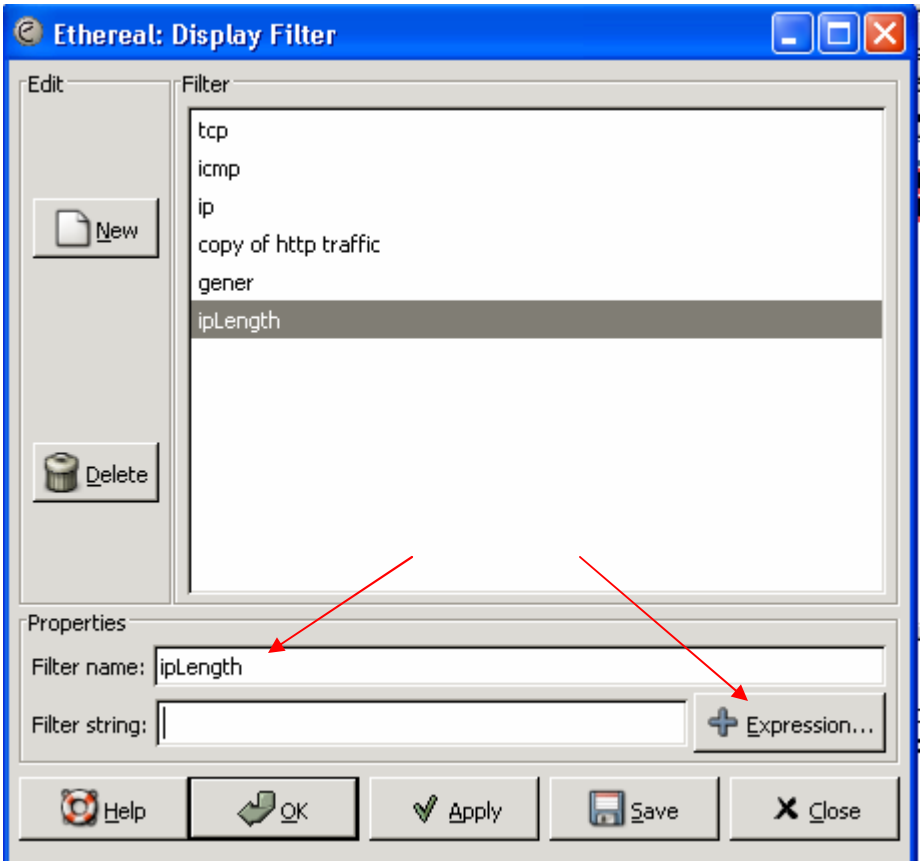


The Filter Expression Dialog Box

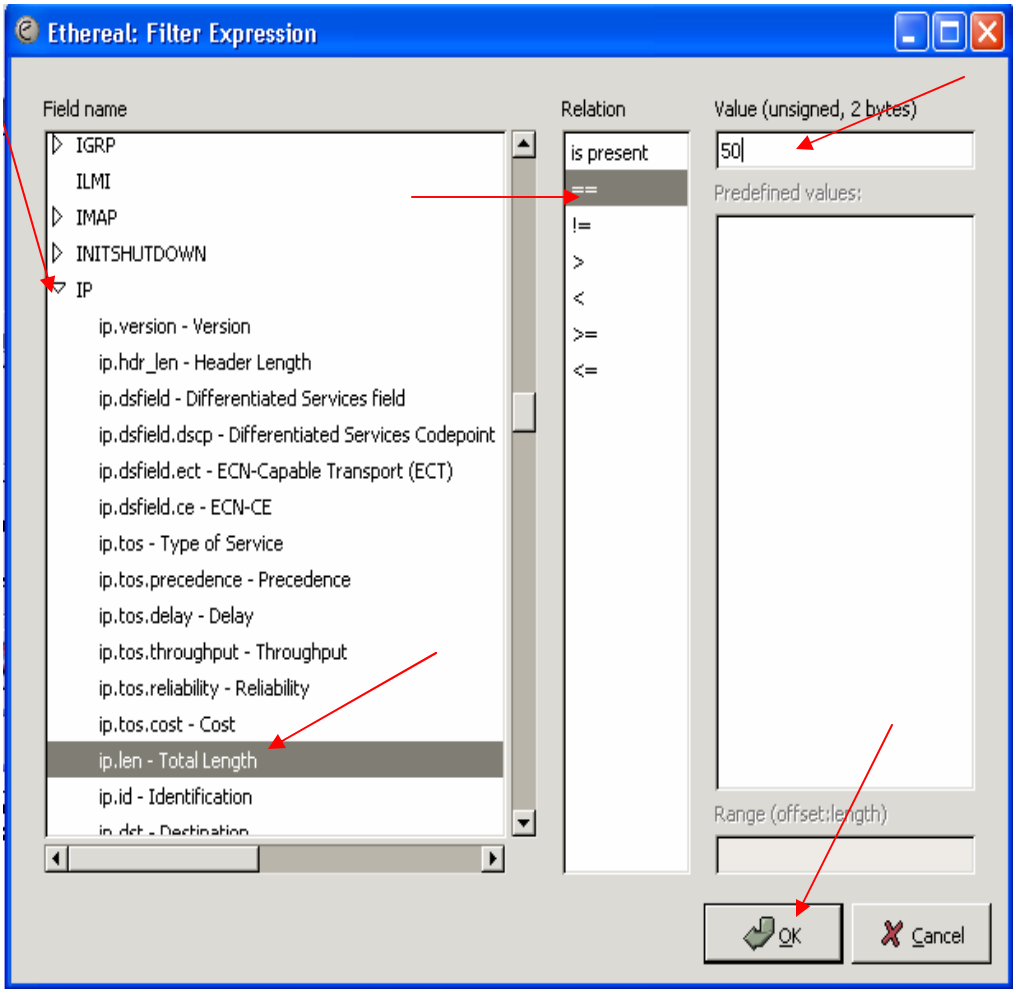
The **Filter Expression** dialog box is an excellent way to learn how to write Ethereal display filter strings. The **Filter Expression** dialog box makes it specialy easyer for new Ethereal users to write display filter trings. Follow these steps to use the **Filter Expression** dialog box:

5. From the main menu bar, click **Analyze > Display Filter**.

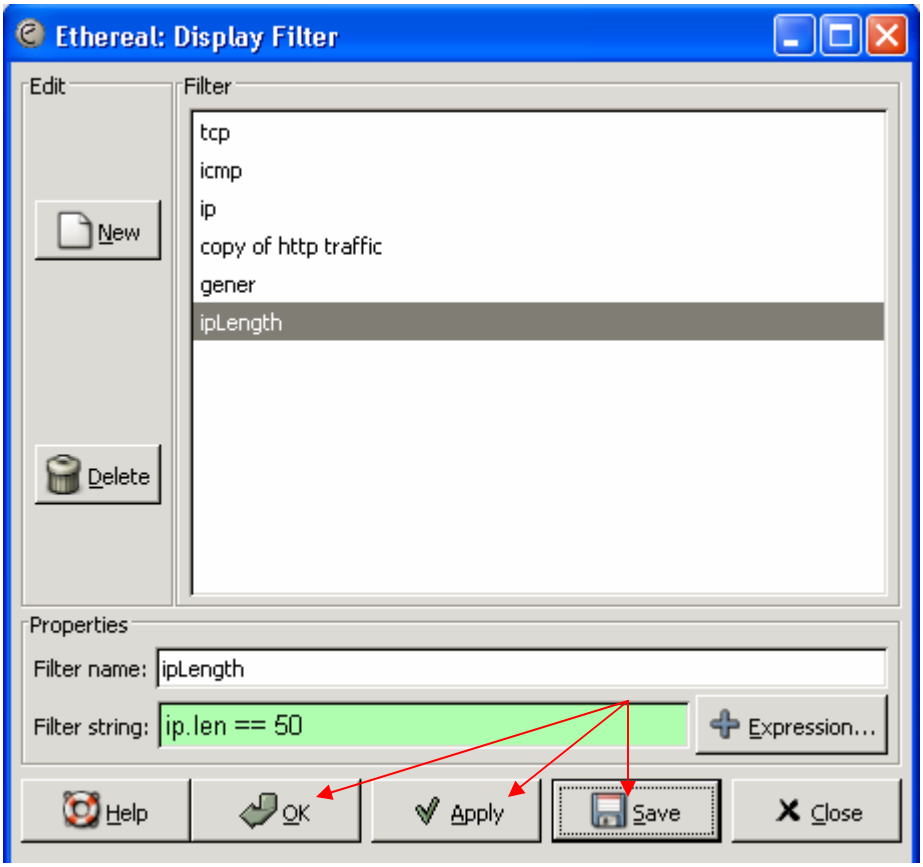
6. When the **Display Filter** box appears, Click **New**, and type the display filter name in the **Filter name** text box. Click **Expression…**



7. When **Filter Expression** box appears, click the arrow head that points to the desired **Filed name**. When the Filed name list appears, select an option by clicking on it once. Select the desired **Relation**, and type in the desired **Value**. When done, click **Ok**.



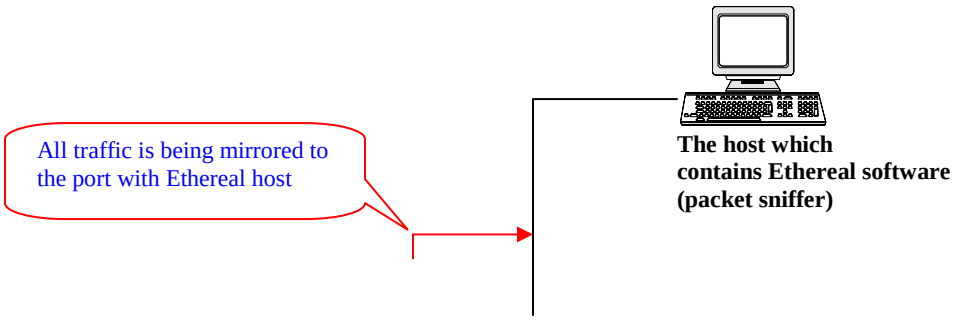
8. After you click Ok, you will be taken back to the **Display Filter** box. Make sure you have the correct filter name and filter string. Click **Save** to save the filter string you created. Click **Apply** to apply the created filter to the captured packets, and click **Ok**. Now you will only see those packets that you specified in your filter.

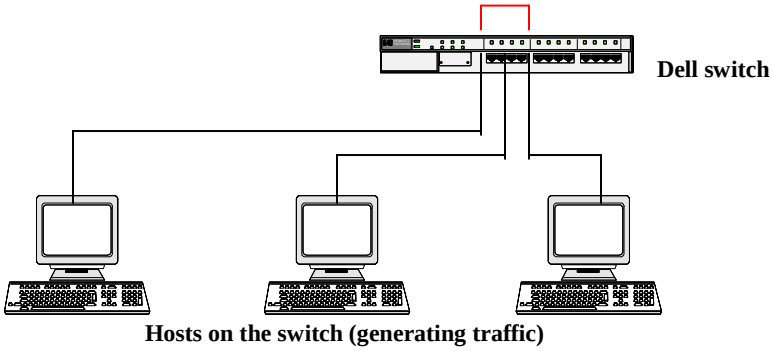


Detecting Network Packets:

Instead of detecting packets on a single computer, you can also use Ethereal to detect packets on an entire network. To do this, mirror all the ports on a switch to one specific port and connect the host which contains the Ethereal software to the port, which you mirrored all other ports to. This way, traffic from all the hosts connected to this switch will be duplicated and sent to the port with the Ethereal host. However, when I tested this scenario in lab 149 in ISAT, the big size of traffic on the switch caused an overflow on the port which I mirrored to. To better understand this scenario, please refer to figure **(A)**.

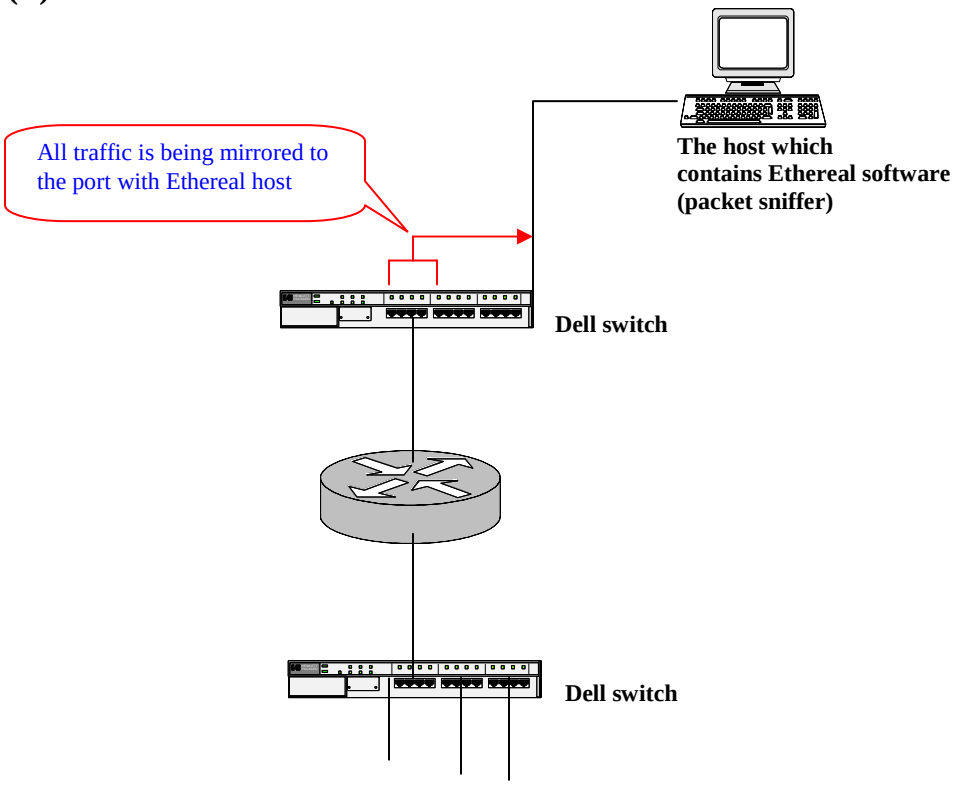
Figure (A)

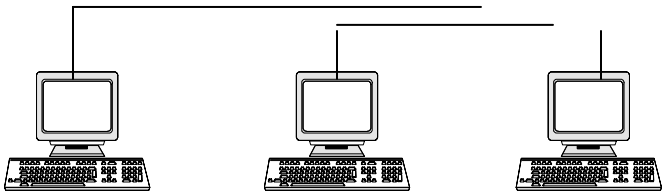




Another approach to detect network packets without experiencing overflow in the destination port in the switch is to connect a router to the switch and then mirror the router port on the switch to the port that connects to the Ethereal host. By doing so, all the traffic of the router will be duplicated to the switch port which is connected to the Ethereal host. Therefore, any traffic that involves the router will be detected by the Ethereal host. To better understand this scenario, please refer to figure **(B)**.

Figure (B)





Hosts on the switch (generating traffic)

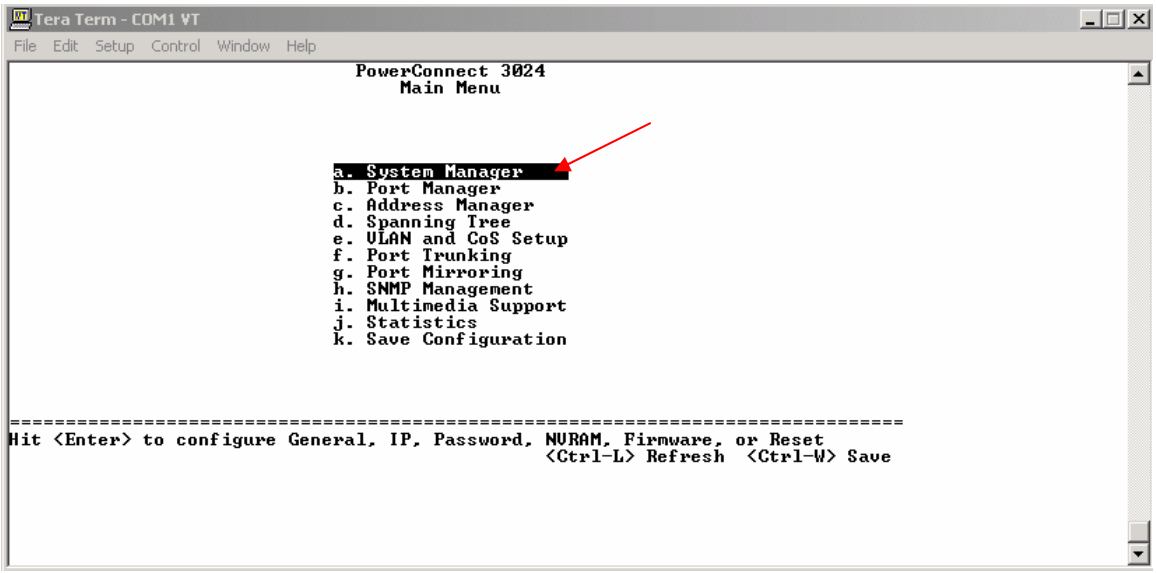
Mirroring Traffic on a Dell Power Connect 3024 Switch

Follow these steps to configure **3024 Dell Power Connect** to mirror traffic to a specific host:

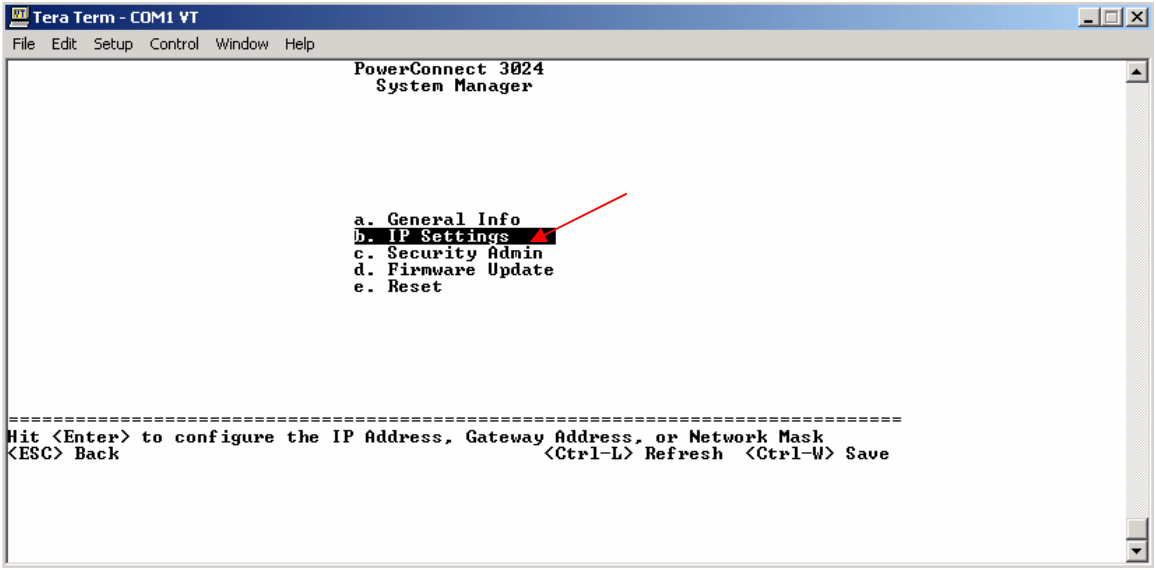
1. Connect the Dell switch to a PC using a blue console cable. Connect the nine-pin-female end of the console cable to the **console** port on the Dell switch, and the other end of the console cable to **Com1** or **Com2** on the PC.

2. On the PC, start a terminal emulator such as **Tera Term** to establish a console connection to the switch. For more information about Tera Term, please refer to the ***Configuration Guide for PIX 515E Firewall*** document chapter 2.

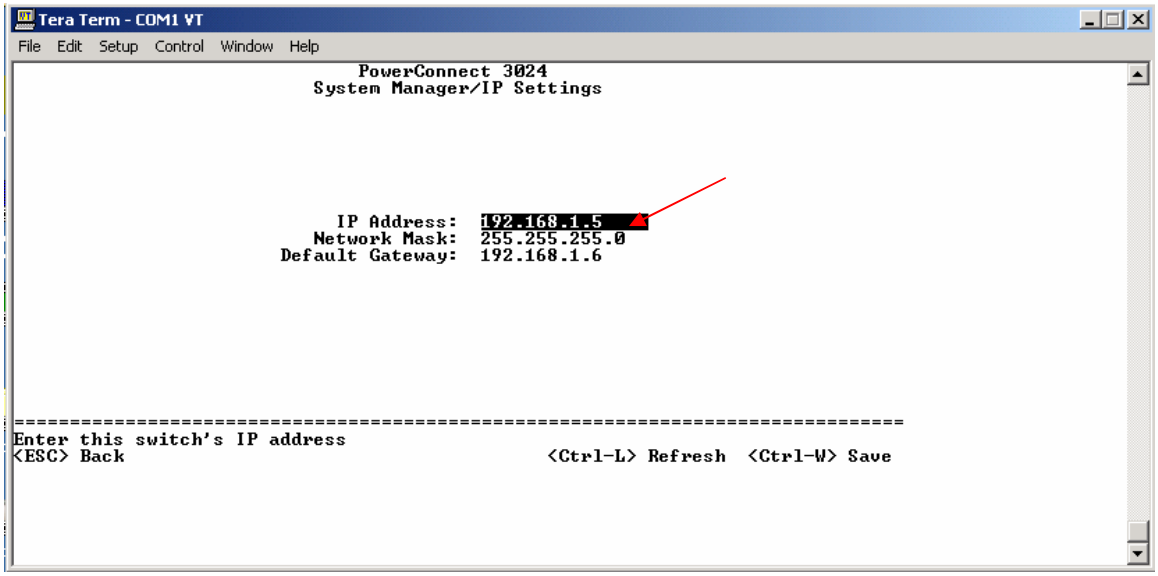
3. Once you establish a console connection to the switch, click Enter and the **Main Menu** will appear. Form the **Main Menu**, select **a. System Management** option.



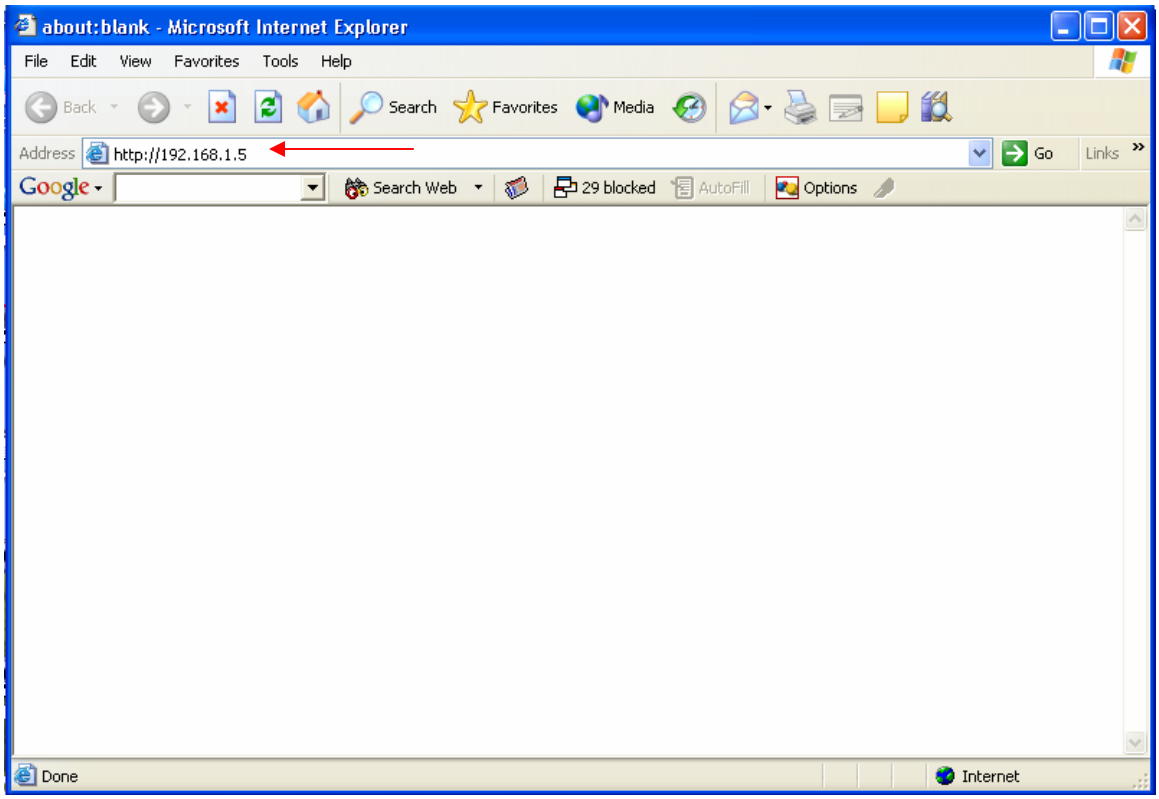
4. When the System Manager screen appears, select **b. IP Settings** option.



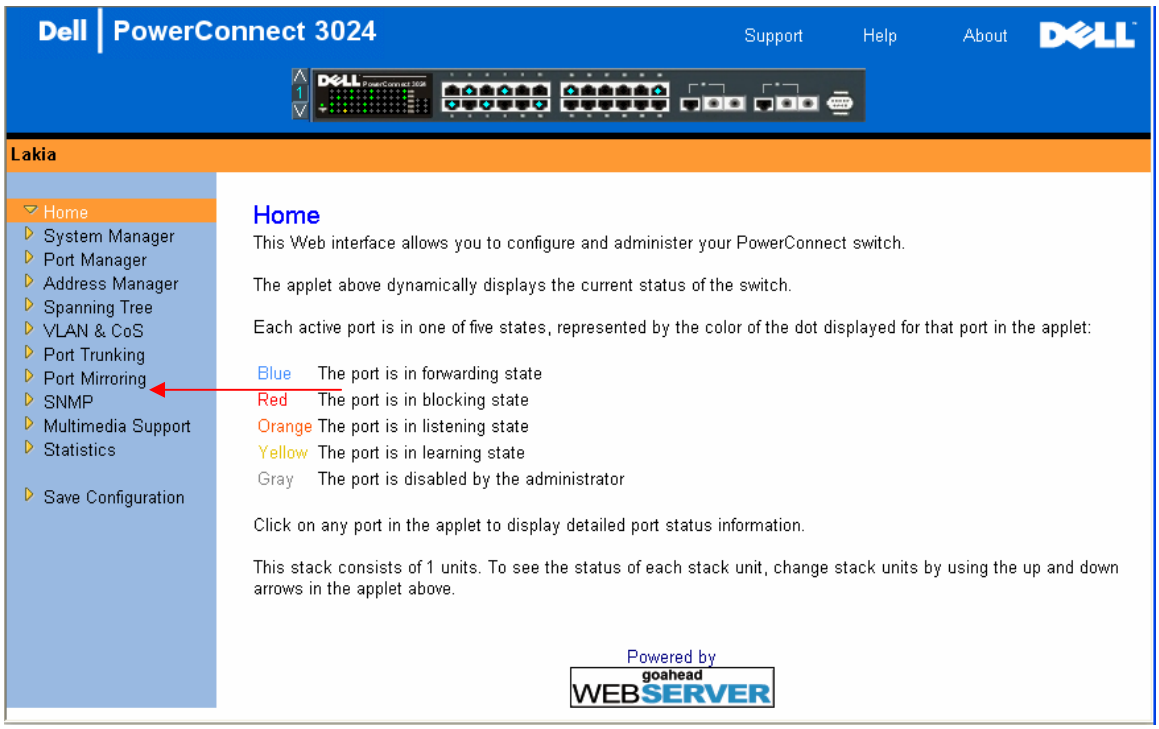
5. When the IP Settings screen appears, write down the switch IP address.



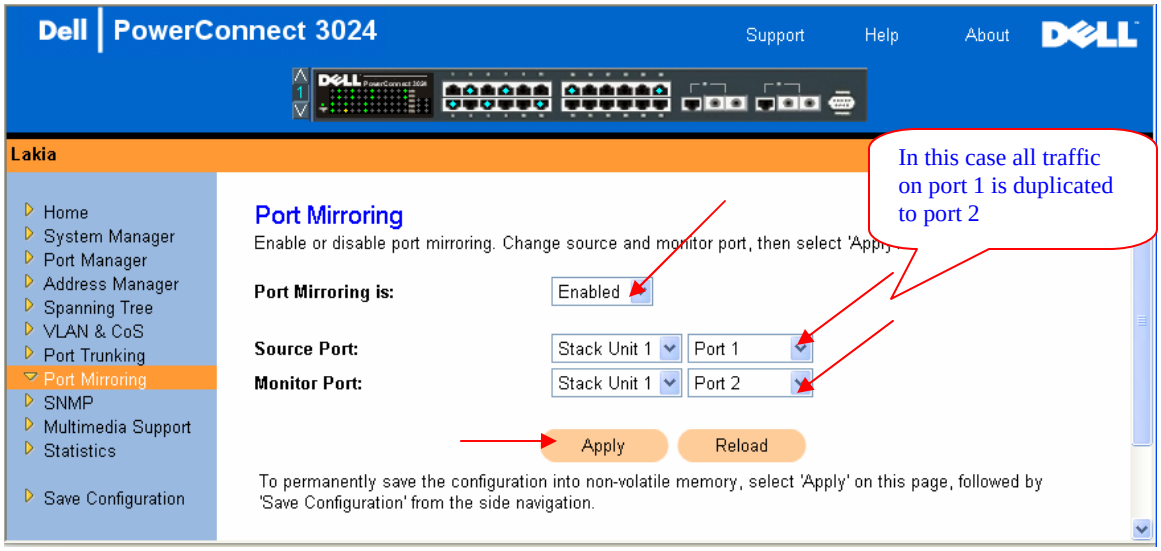
6. After obtaining the switch IP address, you can finish the rest of the configuration process using the graphical user interface. To get access to the graphical user interface of the switch, launch a web browser on one of the hosts connected to the switch. When the browser comes up, type **http://<IP of the switch>** in the address field, and hit **Enter**.



7. After you his **Enter**, the graphical user interface of the switch will appear. Click **Port Mirroring**.



8. When the **Port Mirroring** screen appears, make sure to select **Enabled** option from the **Port Mirroring is:** dropdown menu. There are two dropdown menus for each of the **Source Port** and **Monitor Port** options. Leave the first dropdown menu as is for both. From the second dropdown menu for **Source Port**, select the port from which all traffic will be mirrored to the monitor port. From the second dropdown menu for **Monitor Port**, select the port that receives a copy of all traffic that the source port receives. To make these changes permanent, click **Apply**.



9. After enabling port mirroring on the switch, connect the router to the switch port selected as **Source Port** in the previous step, and connect the Ethereal host to the port selected as **Monitor Port** in the previous step. Now all the traffic from the router port on the switch is duplicated to the Ethereal host port on the switch.

The Menu:

The Ethereal menu sits on top of the Ethereal window. Menu items will be grayed out if the corresponding feature isn't available. For example, you cannot save a capture file if you didn't capture or load any data before

Figure The Menu

It contains the following items:

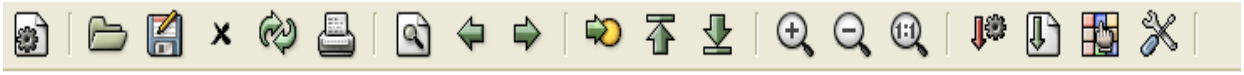
Menu Item	Description

File	This menu contains tems to open and merge capture files, save / print / export capture files in whole or in part, and to quit from Ethereal.
Edit	This menu contains items to find a packet, time reference or mark one or more packets, set your preferences, (cut, copy, and paste are not presently implemented).
View	This menu controls the display of the captured data, including the colorization of packets, zooming the font, show a packet in a separate window, expand and collapse trees in packet details, ...
Go	This menu contains items to go to a specific packet.
Capture	This menu allows you to start and stop captures and to edit capture filters.
Analyze	This menu contains items to manipulate display filters, enable or disable the dissection of protocols, configure user specified decodes and follow a TCP stream.
Statistics	This menu contains menu-items to display various statistic windows, including a summary of the packets that have been captured, display protocol hierarchy statistics and much more.
Help	This menu contains items to help the user, like access to some basic help, a list of the supported protocols, manual pages, online access to some of the webpages, and the usual about dialog.

The Main toolbar:

The main toolbar provides quick access to frequently used items from the menu. This toolbar cannot be customized by the user, but it can be hidden using the View menu, if the space on the screen is needed to show even more packet data. As you use the toolbar, only the items useful in the current program state will be available. The others will be greyed out.

Figure The "Main" toolbar



Main toolbar items

Toolbar Icon	Toolbar Item	Corresponding Menu Item	Description
	Start Capture...	Capture/Start...	This item brings up the Capture Options dialog box and allows you to start capturing packets. If
	Stop Capture	Capture/Stop	This item stops the currently running live capture process. If a live capture is in progress, and you are using "Update List of Packets in Realtime", otherwise the Start Capture icon is shown.
	Open...	File/Open...	This item brings up the file open dialog box that allows you to load a capture file for viewing.
	Save As...	File/Save As...	This item allows you to save the current capture file to whatever file you would like. It pops up the Save Capture File As dialog box. If you currently have a temporary capture file, the Save icon will be shown instead.
	Close	File/Close	This item closes the current capture. If you have not saved the capture, you will be asked to save it first.
	Reload	View/Reload	This item allows you to reload the current capture file.

Toolbar Icon	Toolbar Item	Corresponding Menu Item	Description
	Print...	File/Print...	This item allows you to print all (or some of) the packets in the capture file. It pops up the Ethereal Print dialog box.
	Find Packet...	Edit/Find Packet...	This item brings up a dialog box that allows you to find a packet.
	Find Previous	Edit/Find Previous	This item tries to find the previous packet, matching the settings from "Find Packet...".
	Find Next	Edit/Find Next	This item tries to find the next packet, matching the settings from "Find Packet...".
	Go to Packet...	Go/Go to Packet...	This item brings up a dialog box that allows you to specify a packet number to go to that packet.
	Go To First Packet	Go/First Packet	This item jumps to the first packet of the capture file.
	Go To Last Packet	Go/Last Packet	This item jumps to the last packet of the capture file.
	Zoom In	View/Zoom In	Zoom into the packet data (increase the font size).
	Zoom Out	View/Zoom Out	Zoom out of the packet data (decrease the font size).
	Normal Size	View/Normal Size	Set zoom level back to 100%.
	Capture Filters...	Capture/Capture Filters...	This item brings up a dialog box that allows you to create and edit capture filters. You can name filters, and you can save them for future use.
	Display Filters...	Analyze/Display Filters...	This item brings up a dialog box that allows you to create and edit display filters. You can name filters, and you can save them for future use.
	Coloring Rules...	View/Coloring Rules...	This item brings up a dialog box that allows you color packets in the packet list pane according to filter expressions you choose. It can be very useful for spotting certain types of packets.

Toolbar Icon	Toolbar Item	Corresponding Menu Item	Description
	Preferences...	Edit/Preferences	This item brings up a dialog box that allows you to set preferences for many parameters that control Ethereal. You can also save your preferences so Ethereal will use them the next time you start it.