

Packet Capture Instructions: ETHEREAL

Table of Contents:

Introduction.....	1
Before you begin.....	1
Ethereal packet sniffer	2
Obtaining the programs.....	2
Installing WinPcap.....	2
Installing Ethereal	3
Configuring	5
Creating a Filter	6
Capturing test data	9
Sending your Packet Capture.....	13
If you need help	13

Introduction

This document describes the exact steps necessary to create a “packet capture” that will be used to assist the Technical Support department in discovering how our software is performing in your environment. If you have previous knowledge on using “Ethernet sniffers” you may not need all the data described here, but we ask that you follow these steps *exactly* so that the data provided by the capture will be useful for diagnostics. If you are not the network administrator, or do not have a sufficient technological background to understand such terms as “MAC address” or “Packet Sniffer”, we suggest that you delegate the performance of the packet capture to a qualified network technician.

Before you begin

In order to perform all the steps detailed in this document, you will need to make sure you have all of the following:

- ___ Administrator credentials for the workstations and servers involved in the test
- ___ CONSOLE access to the server used for the test
- ___ CONSOLE access to the workstation used for the test
- ___ Internet Access***

****This is only required to obtain the Ethereal distribution archive and supporting files.*

Important Note: a Terminal Server/Citrix session, VNC session or PC Anywhere session to the server or workstations involved is *not* the same as CONSOLE access! In order to perform the packet capture without inadvertently “cluttering” the capture with the data involved in a remote session, you must follow the steps below from the CONSOLE of each machine. We are aware that in many situations, the Server is located in a server room and the workstation is physically far from it. If this is the case, and you cannot find someone to assist you in performing the test, you may use a remote-control software package, but make sure the remote console is NOT located on the same machine as the source for your testing (i.e. Workstation 1-Test machine, Workstation 2-Remote server console). If you configure the filters as we detail below, in most cases, the remote-control packet traffic (screen updates, mouse and keyboard data etc.) will not be included in the capture.

Ethereal packet sniffer

[Ethereal](#) is a freely distributable packet sniffer software package that runs on Windows and Unix derivatives. It is available for free from a number of places on the Internet and is [Open Source](#) software released under the [GNU](#) General Public License.

Obtaining the programs

Though it is possible to obtain the two distribution archives that are required for Ethereal to work in a windows environment, we have provided a direct link to an archive that contains all the needed files for a working Ethereal setup here****:

http://www.cnenet.com/ethereal/Ethereal_0.9.12-WinPcap_3.0.zip

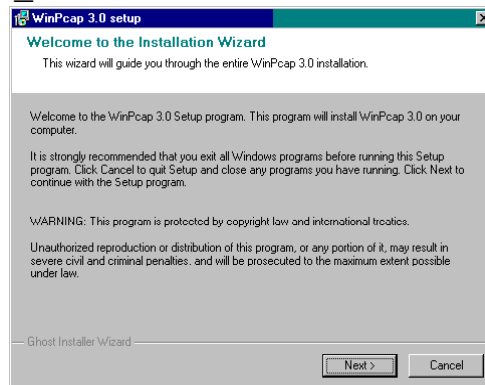
**** The CNENET.COM address is soon to change to a www.softwaremetering.com address!

⊕ **TIP** If you prefer to obtain the files directly from their sources, their respective websites are available here:
Ethereal can be obtained from this link: <http://www.ethereal.com>
WinPcap can be obtained from this link: <http://winpcap.polito.it>.

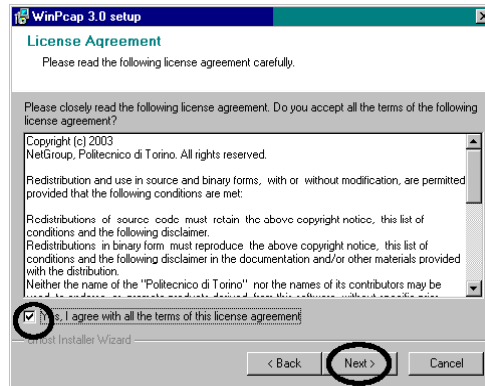
Installing WinPcap

In order for Ethereal to work, you must first install the WinPcap program. This is a low level driver that allows Ethereal to talk to your Ethernet card.

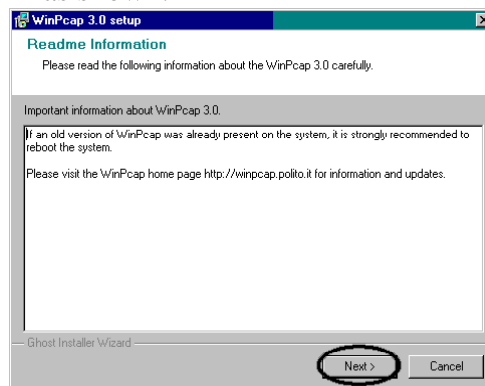
Step 1: Run the archive WinPcap_3_0.exe. You will see the following requestor:



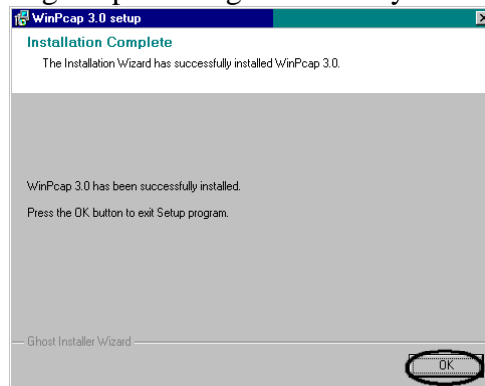
Step 2: Click Next, and you will see the following License agreement. You must select the check box and then click next to continue as shown:



Step 3: A series of files will be copied to your machine. After they have been copied, you will be presented with an informational window. Click NEXT as shown:



Step4: This window will appear showing Pcap as being successfully installed:

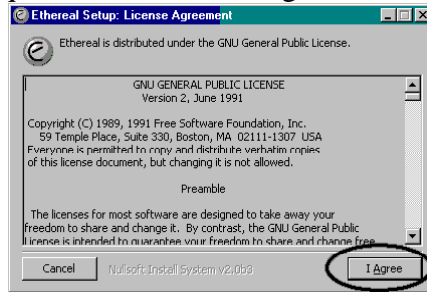


Step 5: WinPcap is now installed. Now move on to installing Ethereal.

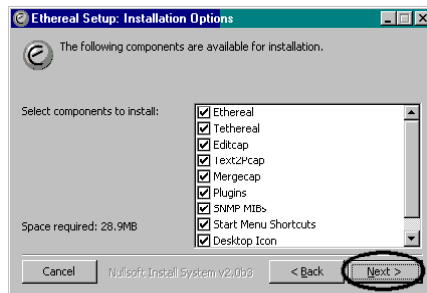
Installing Ethereal

TIP Ethereal will *not* work on a Windows system without the WinPcap! Please make sure it is installed before you install Ethereal!

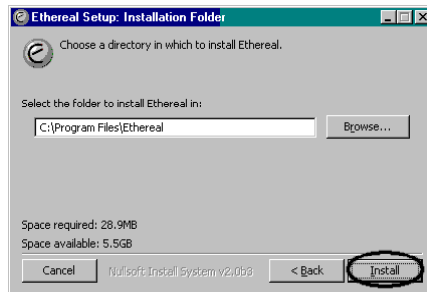
Step1: Locate the distribution archive and launch the file “ethereal-setup-0.9.12.exe” Once launched, you will see the following requestor. Click the “I agree” button to continue as shown circled here:



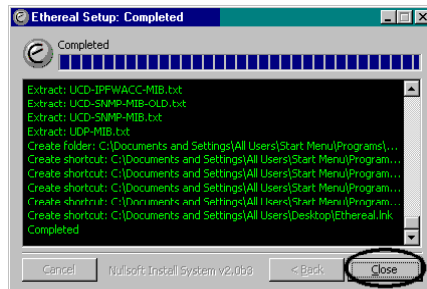
Step 2: You will then be presented with a requestor offering selections of the various components of Ethereal. Leave the settings unchanged and click the “Next” button shown circled here:



Step 3: The next requestor asks where you want Ethereal to reside. Leave the directory as shown and click the “install” button shown circled here:



Step 4: The files will then be decompressed and copied to your local hard drive. When the files are done copying, click the “Close” button shown circled here:

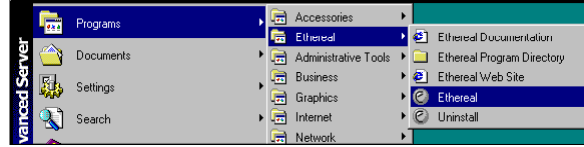


Ethereal is now installed on your system.

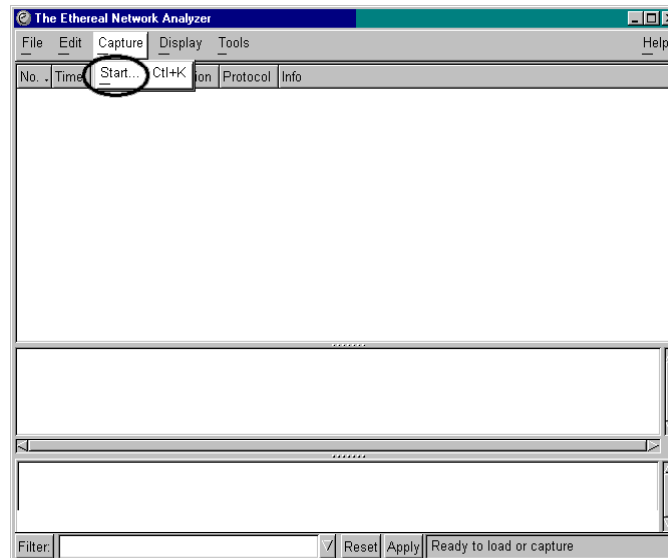
Configuring

Before you can effectively use Ethereal, it is important that we configure some settings so it will produce useful results. Follow these steps to configure Ethereal:

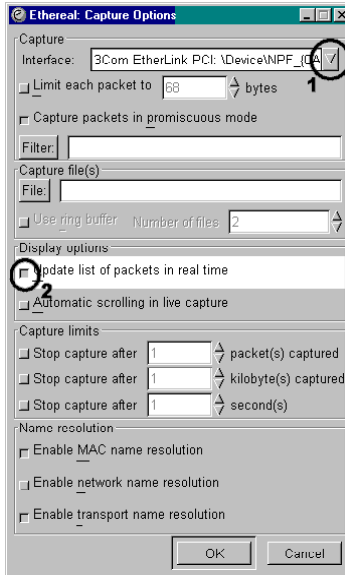
Step 1: Start the Ethereal from the administrative Tools menu as shown:



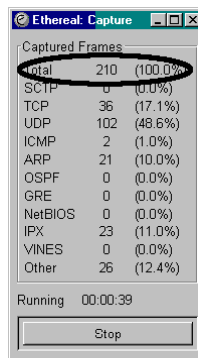
Step 2: When Ethereal starts, you will be presented with the main screen of the program. To begin, select the CAPTURE pull down menu, then select the START item as shown here:



Step 3: The Ethereal Capture Options requestor will open. From here you will choose the Ethernet board from which you wish to capture (circle 1), and turn on real-time update so you can see the data as it is captured (circle 2):



Step 4: Click OK. Ethereal will open this window and start to show traffic being captured by incrementing counters such as the one circled here:



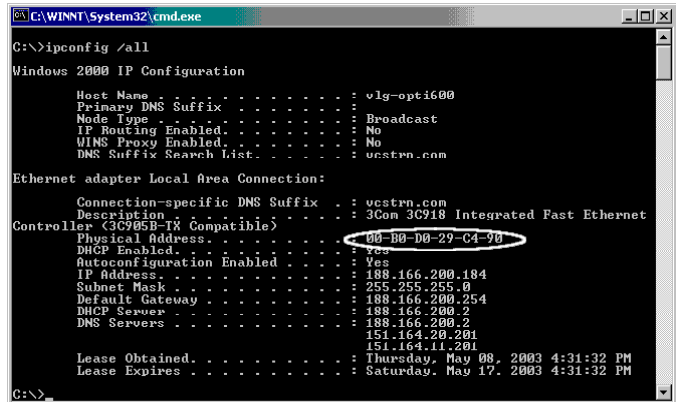
Step 5: Click Stop. You have now configured and tested Ethereal.

Creating a Filter

In order to keep the “clutter” down and keep the capture focused on relevant data, it is important that we set up a filter that instructs Ethereal to ignore any packets from machines not involved in the test. We do this by creating a filter using the MAC addresses of the two stations that *are* involved in test. Usually, you will need the MAC addresses of the server and the workstation involved in the test. If Ethereal is running on a 3rd machine, you will need to use the MAC address from each machine who’s traffic you want to include in your capture.

TIP Remember that Ethernet switches *by design* do *not* echo traffic to all ports! If you plan to capture packet data between two machines from a 3rd machine, **all** machines should be connected with a HUB (or the switch you use must have a “sniffer port” option). If you do not know how to set your switch to “sniffer” operation, using a hub is the simplest solution.

Step 1: Obtain the MAC addresses from the windows machines that are to be included in the test. To do this, open a DOS shell and type "IPCONFIG /ALL". Record the MAC address (titled Physical Address) shown circled here:



```
C:\WINNT\System32\cmd.exe
C:\>ipconfig /all
Windows 2000 IP Configuration

Host Name . . . . . : vlg-opti600
Primary DNS Suffix . . . . . :
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : vcstrn.com

Ethernet adapter Local Area Connection:

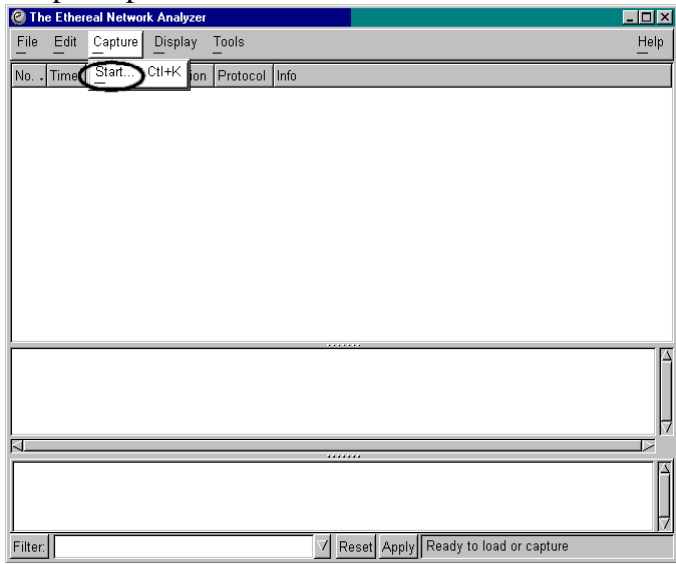
Connection-specific DNS Suffix . . : vcstrn.com
Description . . . . . : 3Com 3C918 Integrated Fast Ethernet
Controller (3C995B-PA Compatible) . . . :
Physical Address. . . . . : 00-B0-D0-29-C4-90
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address. . . . . : 188.166.200.184
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 188.166.200.254
DHCP Server . . . . . : 188.166.200.2
DNS Servers . . . . . : 188.166.200.2
                          151.164.20.201
                          151.164.11.201
Lease Obtained. . . . . : Thursday, May 08, 2003 4:31:32 PM
Lease Expires . . . . . : Saturday, May 17, 2003 4:31:32 PM

C:\>
```

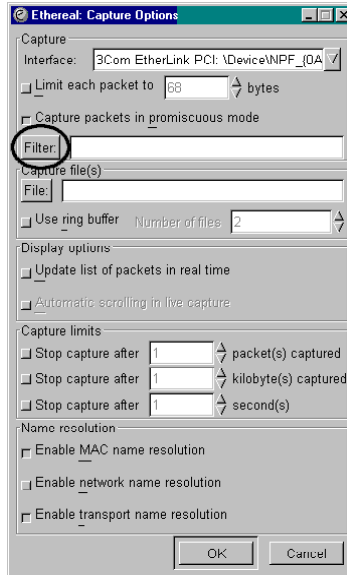
TIP The MAC address shown in the example above (00-B0-D0-29-C4-90) is from the specific Ethernet board in our test machine here. IT WILL NOT WORK for you! You must fetch unique MAC addresses from your own machines!

Repeat this step for each machine that is to be included in the test.

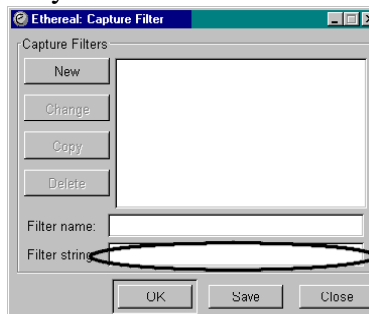
Step 2: On Ethereal, select the Capture pull down menu and choose the START item shown circled here:



Step 3: In the resulting window, select the filter item shown circled here:



Step 4: You will be presented with a window where you may enter the filter using a syntax that is valid for tcpdump and/or WinPcap. The field where you enter the data is shown circled here:



You will enter the MAC addresses of the machines involved in the test the using the following syntax:

`"ether host [MAC] and ether host [MAC]"`

An example of the syntax with real MAC addresses would look like this:

`"ether host 00:b0:d0:d8:97:d6 and ether host 00:b0:d0:29:c4:90"`

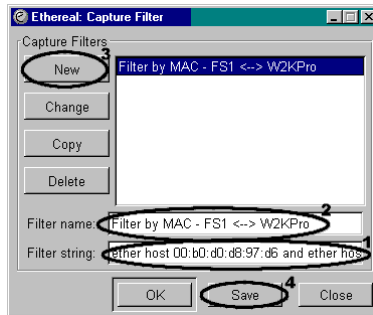
TIP If you prefer, it is possible to use the IP address to create the filter rather than the MAC address. The syntax for IP address filter is:

`"host [IP] and [IP]"`

An example with a real IP addresses would look like this:

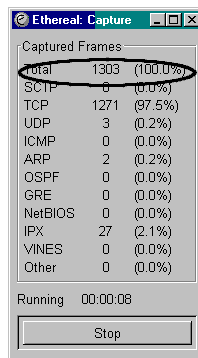
`"host 192.168.0.1 and 192.168.0.4"`

Step 5: Enter the appropriate data into the fields shown here as directed:



1. Filter String: Enter the MAC addresses in the format shown.
2. Filter Name: Enter a *useful* description here so you may easily identify this filter.
3. New: Click this button to add your new filter to the list of available filters.
4. Save: Click this to save your new filter.

Step 6: Once your filter is defined, click OK. The following requestor will appear:

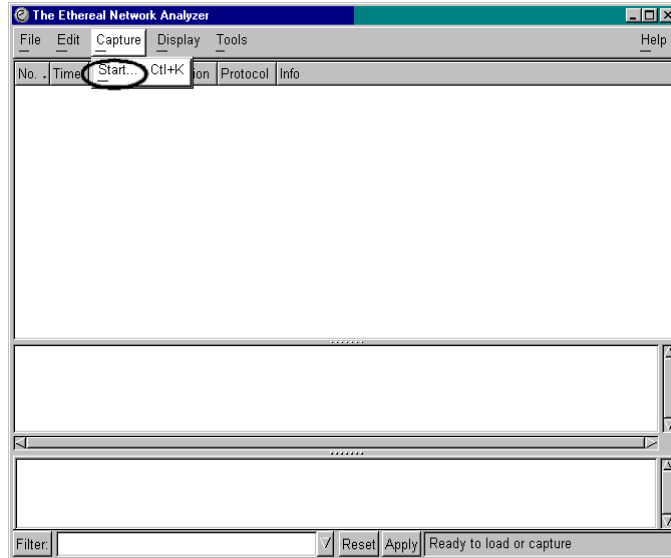


Step 7: Try pinging the test workstation and watch the “Total” field to see that it is incrementing. If it is, then you have configured the capture filter correctly. Click stop.

Capturing test data

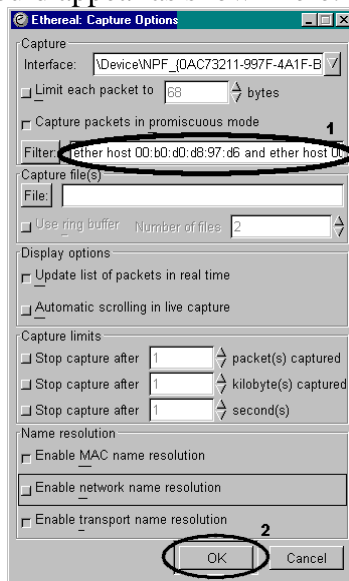
To capture test data, you will need to generate traffic from the test workstation to the server. This is usually done from the workstation under test, not the server. To keep the capture as “clean” as possible, try to generate JUST the traffic necessary to the diagnostic during the capture period. Running Terminal Server sessions, VNC, web surfing, pinging, telnet sessions etc. will create extra events that will complicate (and possibly obscure) the test data. So, when testing, please do not perform any network operations other than what is called for by the test. To capture test data, follow the steps detailed here:

Step 1: To begin the packet capture, select the “Capture” pull down menu, then select the “Start” Item as shown here:

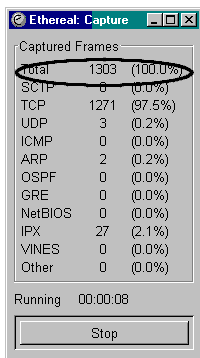


NOTE: The test itself will vary depending on what the Support Technician has asked you to generate. If you are unsure of what you should be capturing here, please contact tech support as listed in the “If You Need Help” section.

Step 2: The capture definition window should appear as shown here:



Step 3: Make sure the Capture Filter you defined earlier is displayed in the Filter field detail in Circle 1 above. Click the OK button (circle #2) and the packet capture will begin. When the testing begins, you should see the total capture fields start to increment as shown here:

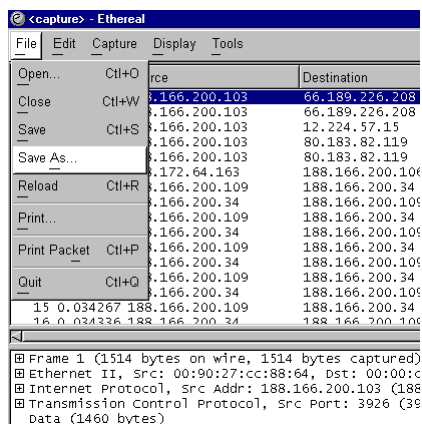


Step 4: Check to be sure the “Total” field shows more than zero frames (circled above).

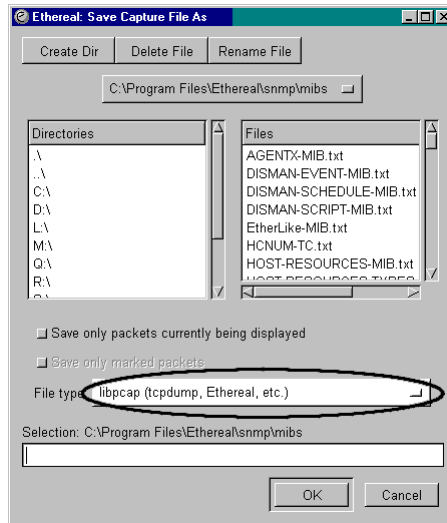
NOTE: If the Total Captured Frames is ZERO, then you need to check your settings and attempt the capture again! A Zero-length capture file cannot be used for analysis!

Try to place the start and stop of the capture as close to the beginning and ending of the test as possible. When the test is complete, click STOP.

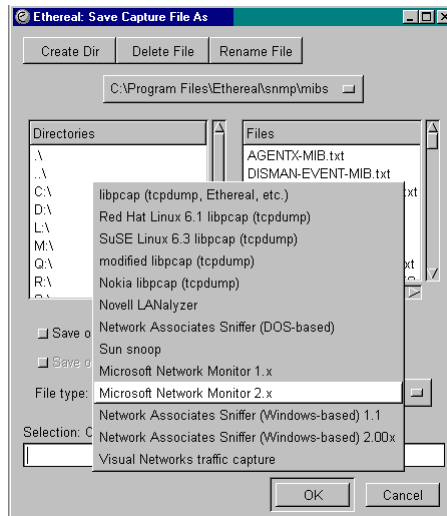
Step 5: Now that we have a capture of test data, you need to save this data to the disk. To save the data, select the “File” menu and then choose the “Save As” item as shown here:



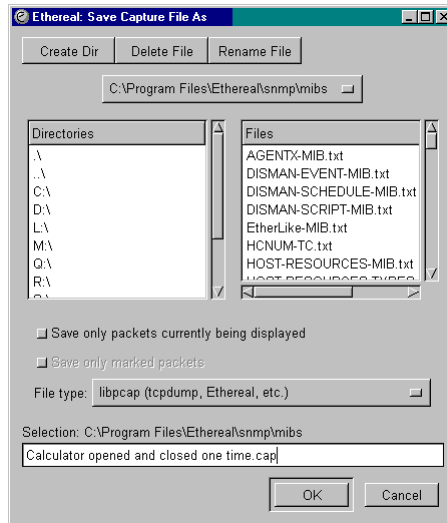
Step 6: In the resulting requestor, click “File Type” as indicated here:



Step 7: Change the File type to “Microsoft Network Monitor 2.x” as shown here:



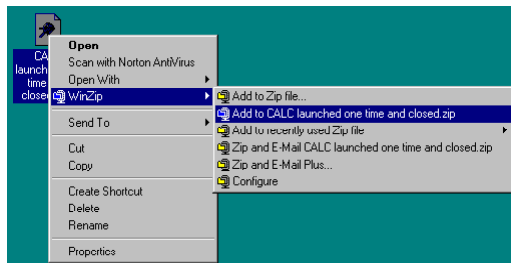
Step 8: Name the file as verbosely as is needed to convey the nature of the capture. If multiple tests are performed, please describe what test the capture represents and place a file extension of “.CAP”.



Sending your Packet Capture

Once you have successfully captured the data from your test, it needs to be sent to us for analysis. To save your capture data, follow these steps:

Step 1: In order to insure the integrity of the file, the file *must* be ZIPped before sending it to us! This is **very important** to make sure the file is not damaged, truncated or altered while in transit. ZIP the ".cap" file (or files) into an archive with a descriptive name such as that shown here:



Step 2: Once you have the zipped file on your desktop, send it to the address listed in the “**If you need help**” section listed below. Please include all relevant details about the problem that the capture is supposed to illustrate.

If you need help

We understand that doing a packet capture can be complex and we are happy to offer to help you create one. If you are unsure about any of the instructions included here, or if you need assistance in performing a packet capture, please contact our support department using the following methods:

Via Email: support@softwaremetering.com

Via Phone: (512) 372-8991 x611

Via Fax: (512) 372-8969

Thank you for your cooperation!

--The Tech Support Team