Instructions "How to apply capture filters to Wireshark".

Step 1: Download the capture filters from Analysis Solution web site. Select the Technical button, and look for Wireshark, Capture Filters.

http://www.analysissolution.com/

Step 2: Open the Capture Filter file. The easiest way is to cut and paste the page of capture filters to the **cfilter** file in Wireshark. The **cfilter** file can be found in a Wireshark folder that was created automatically during the Wireshark install. See Figure 1.1

Figure 1.1
C:\Documents and Settings**Your User Logon Name** (replace with your logon name)\Application Data\Wireshark

You will find the file cfilters. Open the file with Notepad. Cut and paste the new filters in the file. Save the file. Make sure that the file is saved with no extension.

The capture filters are from all layers of the OSI stack. This list is not complete to say the least, but an overview of various types. The idea is supply as many combinations of filters as possible and from this create your own that fit your environment. It can be a reminder of how a filter is built and taking it to the next step and applying your own patterns. For example IP address can be changes for what you want to capture. Keeping a copy of the cfilters file is a good idea just incase it's necessary to replace it if the need arises.

Please send you comments and suggestions to

Wireshark Ethereal Capture Filters Defined

The capture filters that we have put together were chosen from several categories. Starting with the MAC layer selecting filters that are used for general collection of data traffic. This is in no way a complete list of filters, but an introduction that can be used as a pattern to create other filters.

MAC FILTERS
Mac Address can be changed to what device you would like to collect.
Ethernet Source will collect on the OUI (Organizationally Unique Identifier). This can be used to capture traffic from a group that have the same manufacture. An example would be to capture all traffic from HP printers. By selecting the OUI for the printer you will capture only the source MAC OUI that you have selected.

IP Filters
IP will capture the source IP address. These can be changed to the preferred IP address that you wish to capture.
Host is just another way to capture source IP address.

Source Host will capture any source IP address that you put into the Filter String field.
Destination Host will capture any destination IP address that you put into the Filter String field.

BROADCAST & MULTICAST FILTERS
IP Multicast will capture IP multicast packets.
Ethernet Multicast will capture Ethernet multicast packets.
Broadcast will capture Ethernet broadcast packets.

SPECFIC ETHER TYPE
A variety of ether types that are commonly seen on the wire.

PROTOCOL & PORTS
A variety of ports and protocols that can be changed to capture any port you wish.

NETWORK & HOST TO HOST
Network Address is designed to capture the IP subnet address.