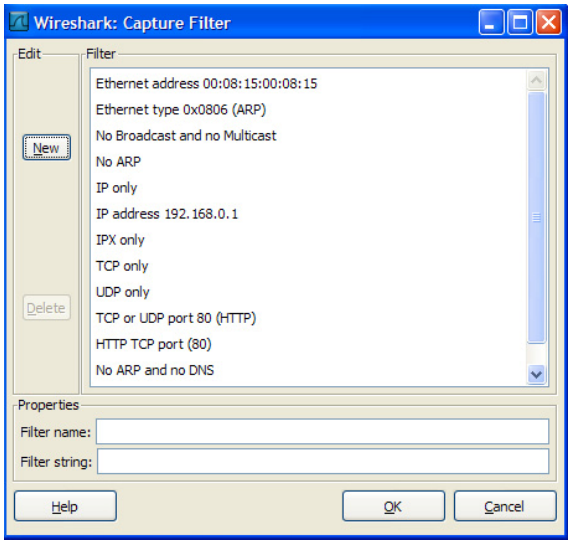
Capture Filters

Capture filters are used when we want to limit the number of packets that we are capturing. For example we may want to capture only ARP traffic or HTTP traffic or traffic coming only from our interface card.

To open the default list of capture filters in Wireshark, go to: Capture > Capture Filters... or you could also use the corresponding button on the toolbar.



List of Default Filters

1.1 Syntax of common capture filters

[src|dst] host <ip-address|host-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.	
src host 192.168.1.1	Packets coming from 192.168.1.1
dst host 134.91.90.77	Packets going to 134.91.90.77
host 134.91.90.77	Packets coming from and going to 134.91.90.77
src host www.neu.edu.cn	Packets coming from www.neu.edu.cn

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.	
ether src host 00:01:FF:22:B1:32	Packets coming from 00:01:FF:22:B1:32
ether dst host 00:01:FF:22:B1:32	Packets going to 00:01:FF:22:B1:32
ether host 00:01:FF:22:B1:32	Packets coming from and going to 00:01:FF:22:B1:32

[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**.	
port 80	Packets coming from and going to port 80, independent if it uses TCP or UDP
tcp dst port 80	Packets going to TCP-Port 80
udp port 4987	Packets coming from and going to UDP-Port 4987

1.2 Logical operators used in Capture Filters

Examples for logical expressions:	
ip and less 80	IP-Packets equal or less than 80 Bytes
ether proto \ip && len > 512	Ethernet-Packets transporting IP-Packets, which are bigger than 512 Bytes
dst host 192.168.1.1 **&& port** 80	Packets which have as destination 192.168.1.1 and are transmitted over port 80

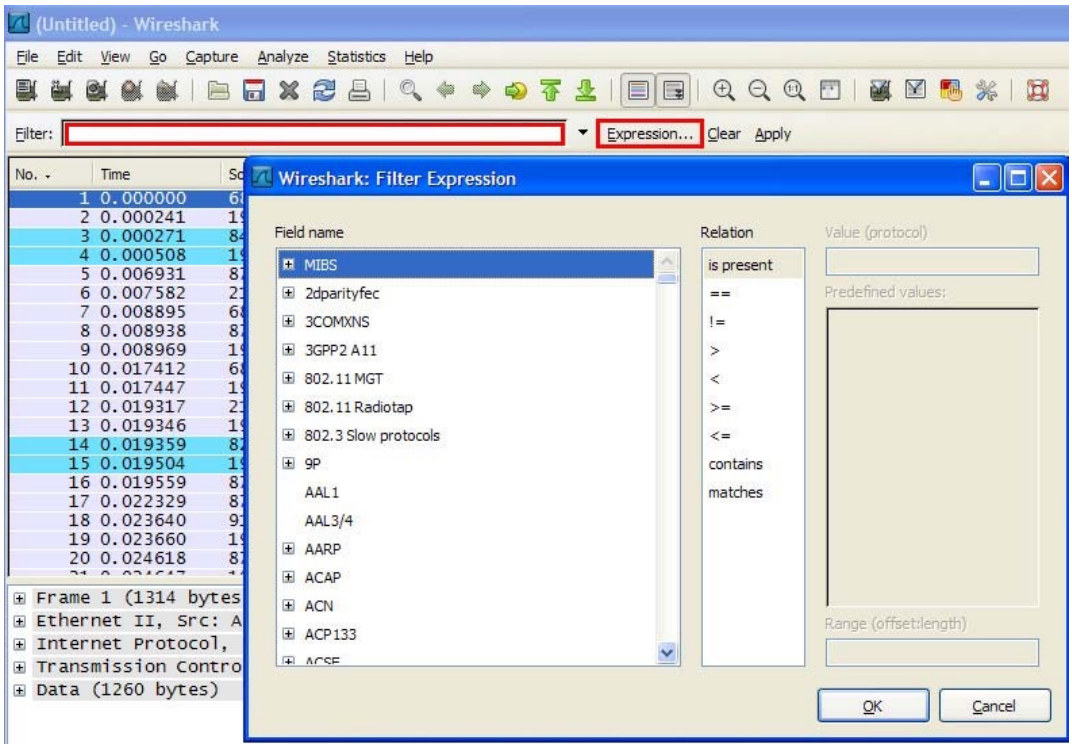
Logical Operators:	
&&	Logical AND between 2 expressions
||	Logical OR between 2 expressions
!	NOT operator
General declaration of logical output for Capture Filters *(Everyting in square brackets “[ ]” means it is optional)	
[**not**] **primitive** (**and** | **or**) [**not**] **primitive**	
[**!**] **primitive** (**&&** | ||) [**!**] **primitive**	

2.0 Display Filters

Display filters allow you to concentrate on the packets you are interested in while hiding the currently uninteresting ones. They allow you to select packets by many different criteria.

Wireshark provides a simple but powerful display filter language. You can compare values in packets as well as combine expressions into more specific expressions.

We could define filters directly to the Display Filter Toolbar or choose a filter from the “Expression...” dialog box.



2.1 Syntax of Display Filters:

<protocol>.<element>.<sub-element> <operator> <value>

An element is an available field name for filtering for the selected protocol. We can take a look at them by expanding the field for any protocol in the “Filter Expression” dialog box.

Examples:

ip.addr eq 134.91.90.77 - displays all IP-Packets that have the address 134.91.90.77 as source or destination.

eth.src eq 00:01:FF:22:B1:32 - displays all Ethernet-Frames that have a source station with MAC 00:01:FF:22:B1:32

2.2 Common operators in Display Filters

Operator	Analogue	Meaning
eq	**==**	Equal
not	**!**	Not
ne	**!=**	Not Equal
gt	**>**	Greater Than
lt	**<**	Less Than
ge	**>=**	Greater then or Equal to
le	**<=**	Less than or Equal to

3.0 Exercises

Directions: Browse to http://www.neu.edu.cn from the Windows 7 machine and use Wireshark to capture the packets sent to your computer. Once you have opened at least 3 tabs on the www.neu.edu.cn site end your browse session and stop the capture. Create the filters listed below.

Create a lab report that includes screen shots of both the filter and the number of packets captured. Begin each exercise by removing any previously applied filter.

Part 1
Create filters that display only those packets that:

1. use the TCP protocol.
2. use the HTTP protocol.
3. request HTTP information from http://www.neu.edu.cn
4. are sent to your computer.
5. are sent to the server at http://www.neu.edu.cn
6. are sent between your computer and to the server at www.ibm.com and use the HTTP protocol.
7. are sent to port 80.
8. transmit a standard DNS name query.

Part 2
For the following exercises first apply the filter you created in the exercise above:

1. Which protocol is used by all packets?
2. What are the source port values for these packets? (Select at least two different packets before answering this question).
3. Which Transport Control Protocol flags are set?
4. Review an HTTP packet. Were you able to locate an HTTP request method? If so, which one is specified?
5. What is the HTTP request version?
6. What version of the Internet Protocol is being used?
7. What is the IP header length in bytes?
8. Which IP flags are set?
9. What is the IP Time-to-Live value in seconds?

Part 3
Browse to http://www.neu.edu.cn from the Windows 7 machine and use Wireshark to capture the packets sent to your computer. Once you have opened at least 3 tabs on the www.neu.edu.cn site end your browse session and stop the capture.

Apply a capture filter that:

1. Sets web server as the source ip address.
2. Captures only HTTP Traffic.
3. Sets Windows 7 machine as the source ip address.
4. How do the captures compare?