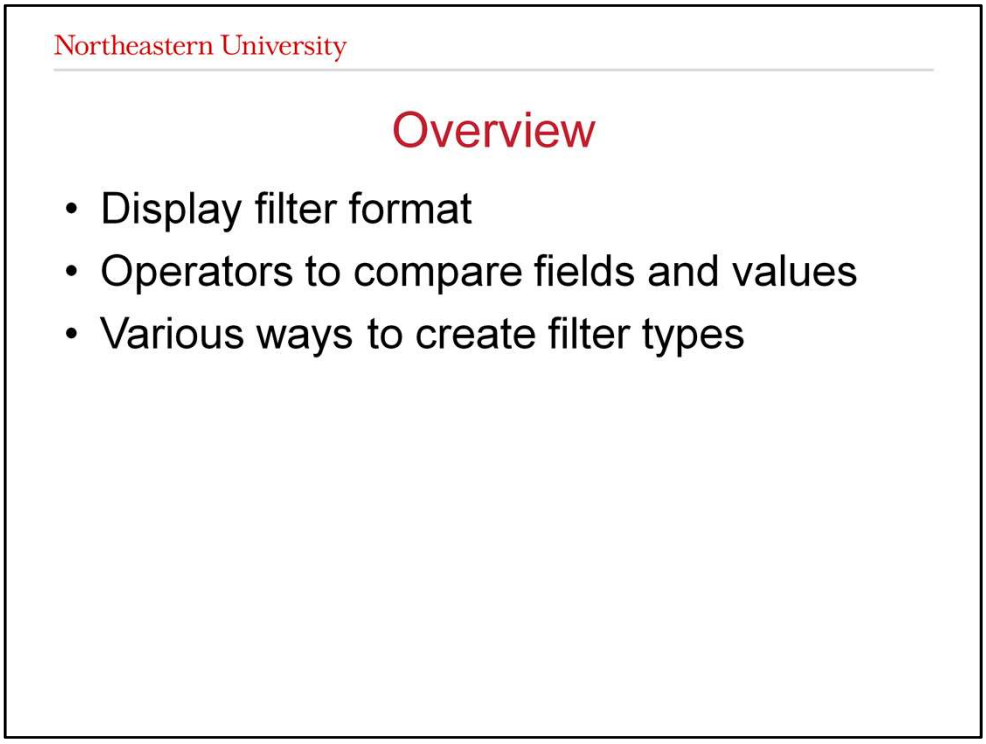

Northeastern

Northeastern University

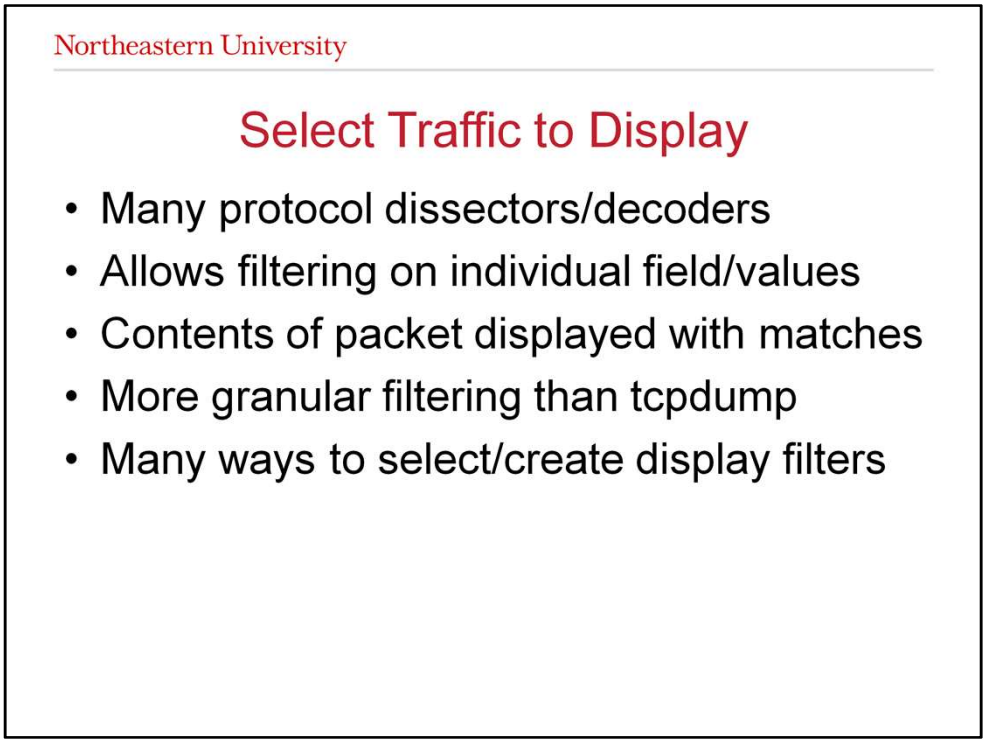
Wireshark Display Filters

This slide intentionally left blank.



Wireshark capture filters (same as Berkley Packet Filters) and display filters are different. Capture filters are used when collecting packets, or frames, from the physical medium. Display filters are used when you have a collection of captured packets and you want to display packets with a specific characteristic.

Display filters have many formats including comparison of fields, values, specific operators, and text matches such as “contains” and “matches.” This lecture will cover various methods Wireshark provides to assist in making display filters and analyzing the specific traffic. These methods are a useful starting point to learn how to create these types of filters.



A protocol decoder is software that analyzes a protocol similar to how an application using that protocol would. The protocol must be understood, followed, and values must be associated with their respective fields.

Display Filter Format

- Indicator of protocol or field
  - dns
  - ftp.response
- Indicator of a condition
  - ip.fragment.overlap
  - udp.checksum_bad
- Field name – comparison – value
  - ip.src == 192.168.11.65
  - ipv6.fragment.offset > 0
- Field offset:range – comparison – hex
  - ip[0:2] == 45:00

Northeastern University

Comparison Operators

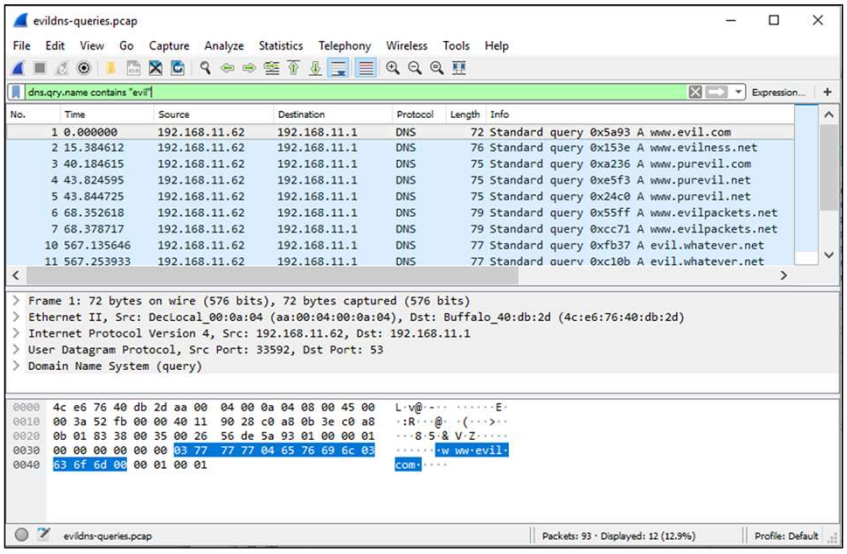
Comparison	Operator
Equal	==
Not equal	!=
Greater than	>
Less than	<
Greater than or equal	>=
Less than or equal	<=
Contains	contains
Regular expression	matches

Comparison	Operator
And	&&
Or	||
Not	!

See http://www.wireshark.org/docs for a full list of operators described within the User's Guide.

Northeastern University

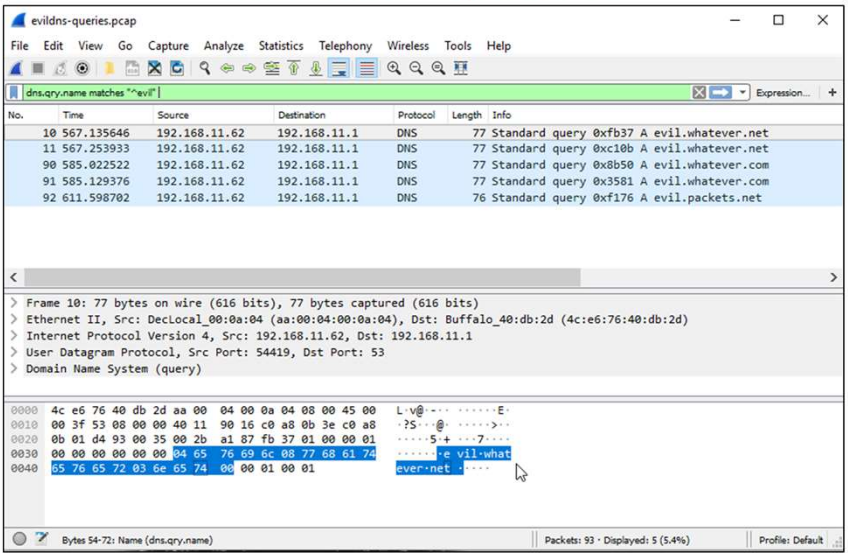
Contains Operator



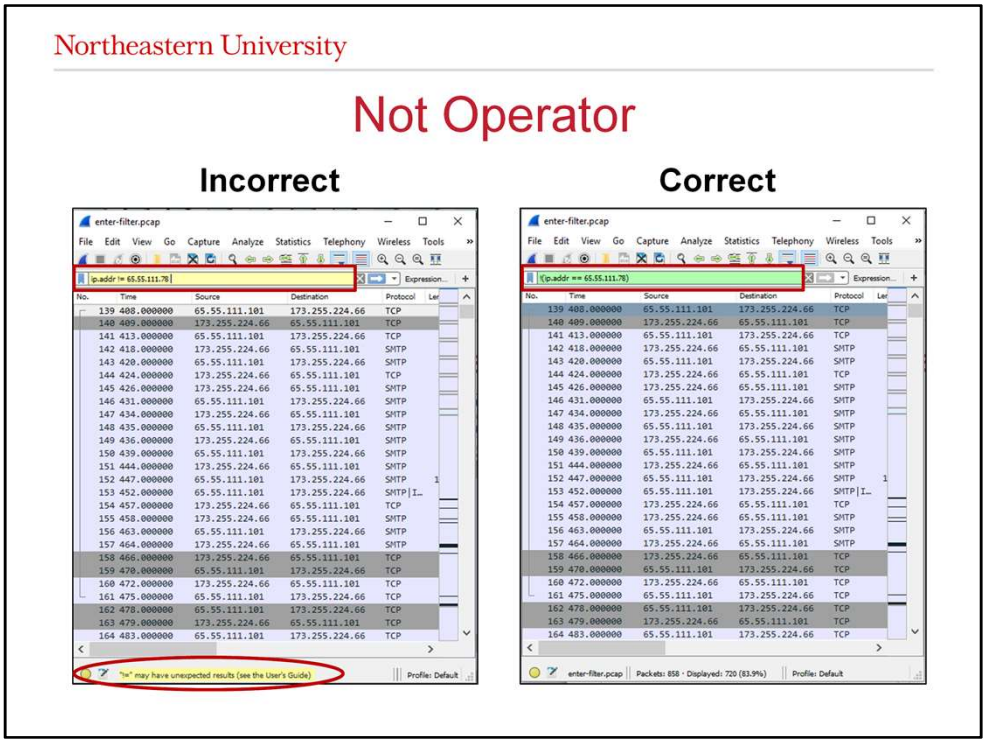
The “contains” comparison operator can be used to find a particular value in a specified field. The filter “dns.qry.name contains evil” reviews the query name field in DNS record packets looking for the occurrence of a specific string, which is “evil” in this case. This display filter will identify all records found with this string.

Northeastern University

Matches Operator



The “matches” operator allows some basic regular expression syntax uses to specify more complex content. Due to a lack of documentation, experimentation is recommended for this operator before drawing conclusions. The “^” operator is used in regular expressions to denote the beginning of a line.



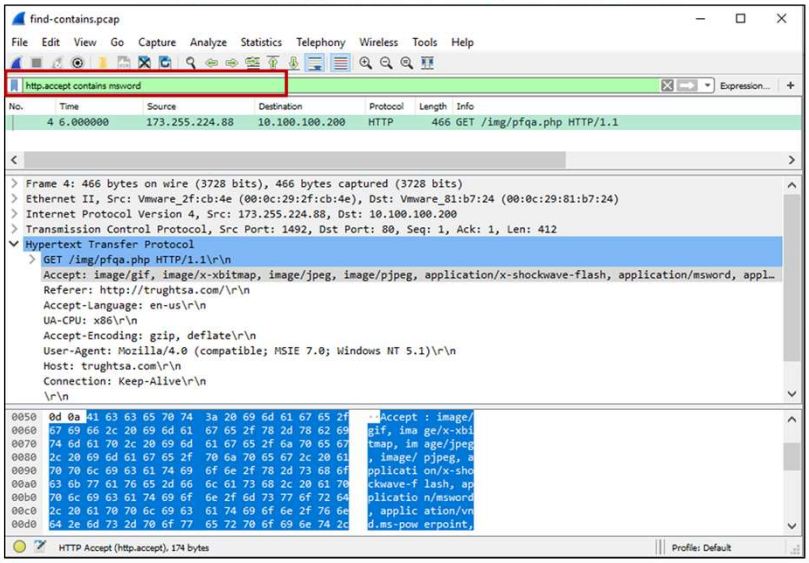
The “not” or “!” operator negates a specific condition. Although this seems straightforward, the “!=“ operator has a couple caveats that are mentioned in the documentation. The first example is an incorrect filter because Wireshark interprets this as finding any packets that must have an IP address of 65.55.111.78. This will expose all records in the capture, because of the disparate source and destination IP addresses. This will result in all captures because there are two IPs to consider.

Also note, there is a feature within Wireshark that assists analysts in understanding what the application is attempting to do and the results that come from the particular search. Green backgrounds appear when the correct syntax is entered, red when the incorrect syntax is entered, and yellow backgrounds signify when Wireshark cautions you that the results may be unexpected, as noted in the slide above.

The proper expression to exclude an IP address is “!(ip.addr == 65.55.111.78)” which indicates that we are searching for no occurrences when the ip.addr filed has a specific value. The point is to be aware of this issue, especially if a field is found in the source and destination packets.

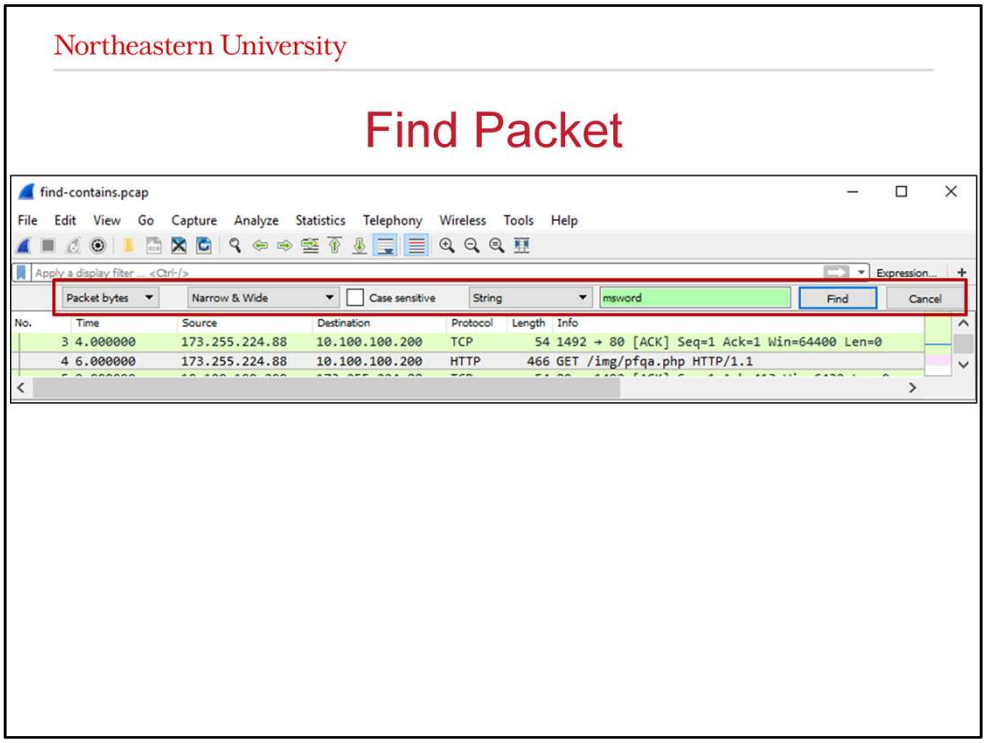
Northeastern University

Contains vs. Find Packet



Some students wonder what the difference might be between the “contains” operator and the “Find Packet” option of the Edit Menu. The contains operator allows you to do more focused granular searches on a particular field or protocol.

Above, we are searching for “msword” if the text is in an HTTP Accept header. All discovered records will be displayed.

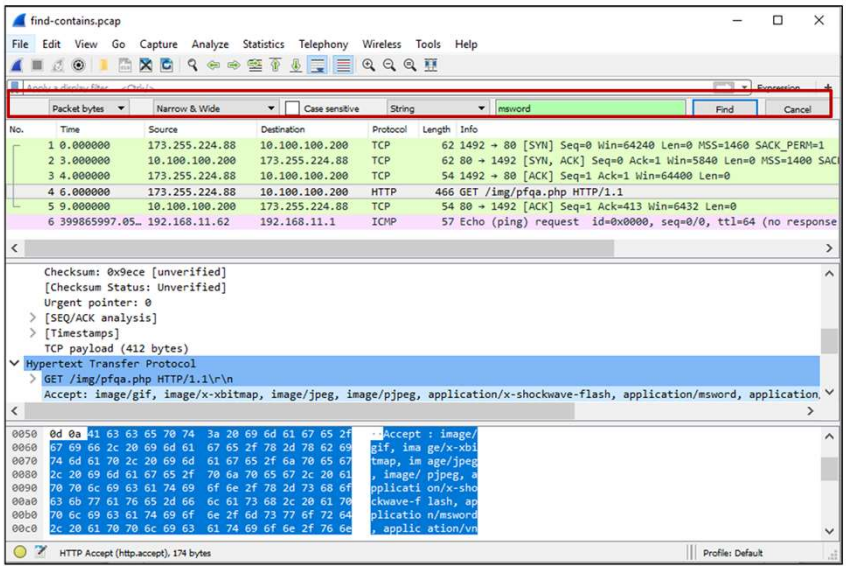


The Edit Menu has a “Find Packet…” option that allows you to search for packets based on some string or hex value. This search is typically completed on a value in the packet bytes, although it can be on the packet list or packet details panes. When a match is found, the result(s) is highlighted – but still leaving all other records displayed, while the contains results displays only matching records.

You need to complete additional “Find Next” searches to find additional packets. This is a generic search as we look for the string value of “msword” anywhere in the packet payload, not just the HTTP Accept header.

Northeastern University

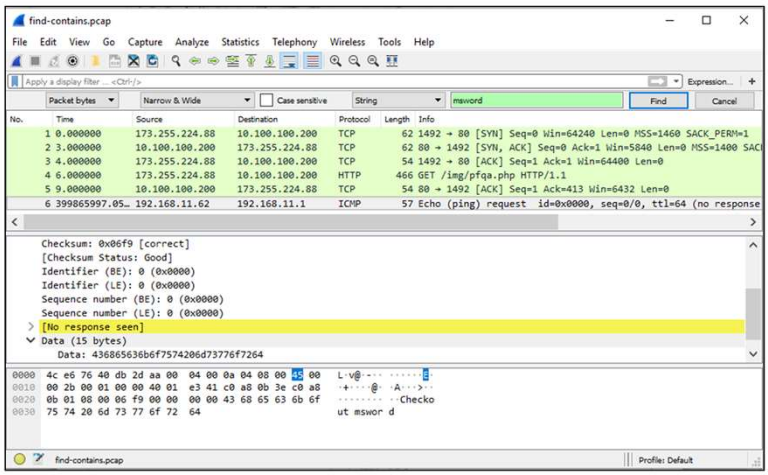
First Match



In this example, record 4 contains the first match of the string “msword.” It is is the HTTP Accept header as desired. This record is selected by either the “Find Packet” or “contains” searches that we performed.

Northeastern University

Second Match



The second match is an ICMP packet that has the string “msword” in the payload. Using the “Find Packet” option when you want to examine each individual record separately that contains the match, although you don’t care about the context in the payload – just that the string exists.

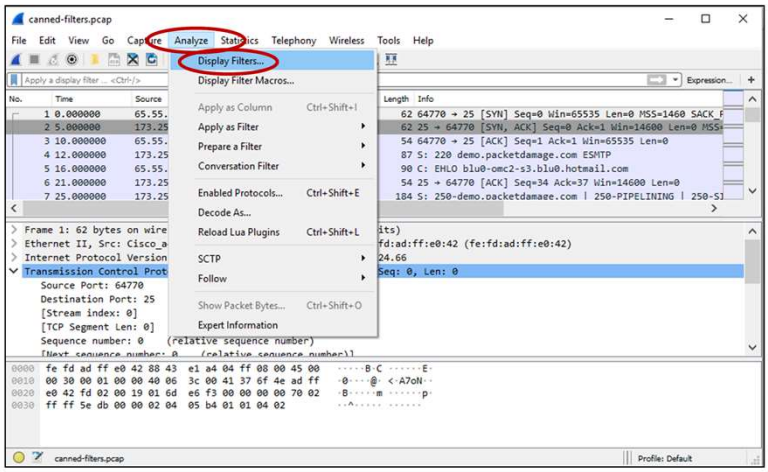
It’s important that you select the correct option, “contains” or “Find Packet,” depending on your purpose for the search.

Create/Select Display Filters

- Use canned default filters
- Manually enter in “Filter:” input
- Use “Expression…” to display menu
- Right-click “Apply as Filter”
  - Packet list, packet details entry
  - Statistics output fields

Northeastern University

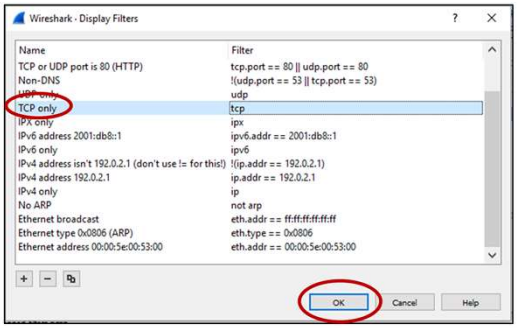
Canned Filters



Some of the most common and simple display filters are available as default or canned filters. These can be accessed by navigating to Analyze > Display Filters menu/selection or by clicking the Filter button to the left of the filter entry.

Northeastern University

Sample Canned Display Filters

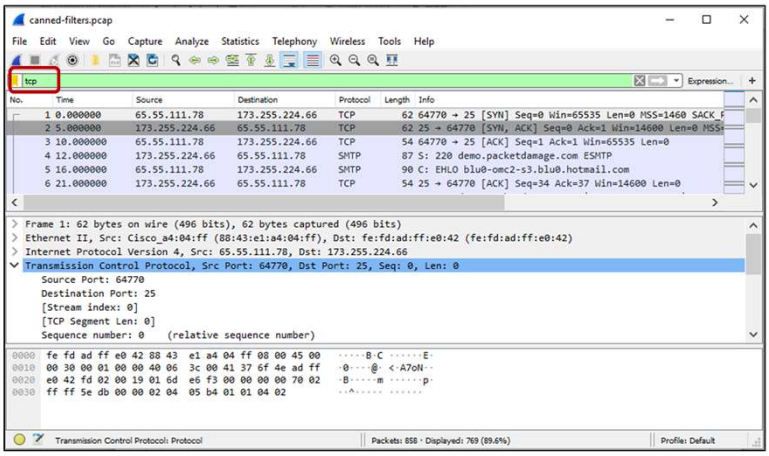


There are some very basic supplied filters. Suppose you want to see only TCP traffic. You could select the “TCP only” filter and select OK. The actual display filter that will appear in the Filter box after you select OK will be “tcp.”

The filters that appear are contained in the file ./wireshark/dfilters found in the user’s home directory.

Northeastern University

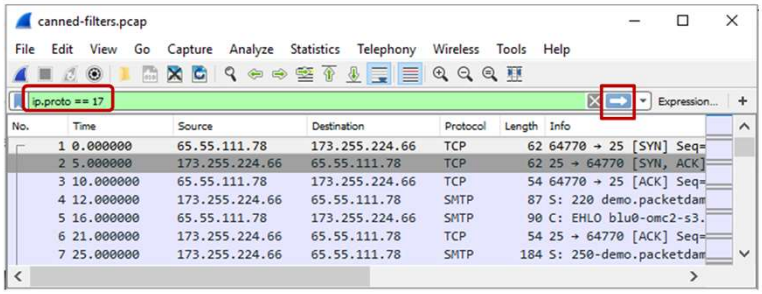
Filter Results



As you can see, the actual display filter is “tcp.” This selects all the TCP records only.

Northeastern University

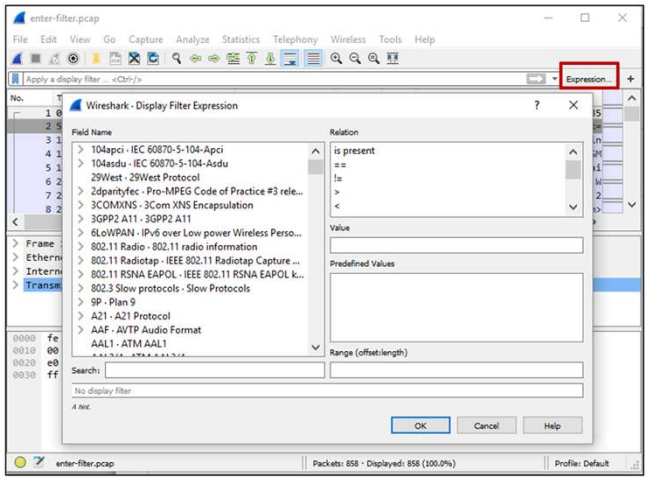
Create a Filter



Wireshark allows you to create your own filters, once you are comfortable wit the Wireshark options and choices. You may find it relevant to create your own display filters. If you know you want to see UDP records only, for instance, you may create a filter for protocol 17 – UDP. Once applied, only UDP records will be displayed.

Northeastern University

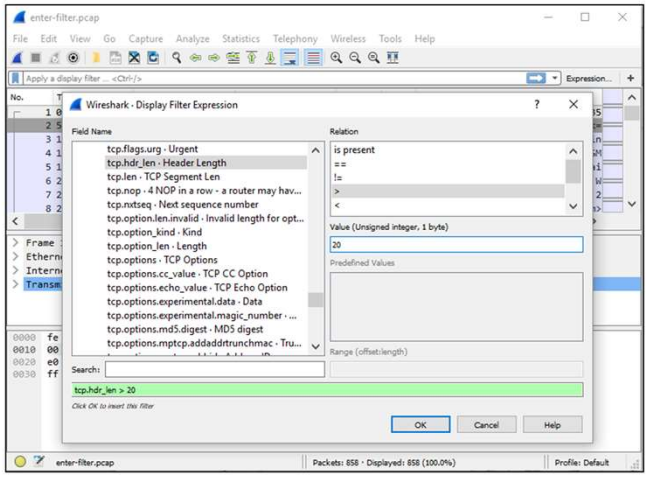
Expression Menu



There is an “Expression” button to the right of the filter entry. When this option is selected, a menu of many different types of protocols should appear. The menu shows the available Wireshark dissectors and permits you to use and view the same fields and conditions that the dissectors do.

Northeastern University

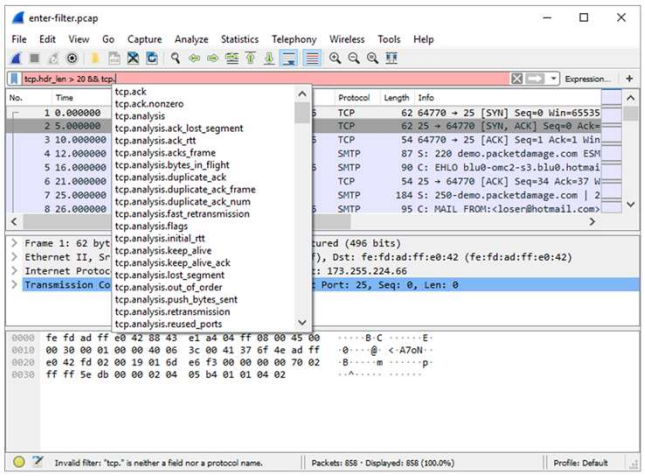
Filter Expression Menu



Once you find the search you'd like to search for a given value, Wireshark brings up a menu to assist in selecting a relation and value. Wireshark knows the appropriate relations that apply to chosen fields and will only show values that pertain to a particular field.

Northeastern University

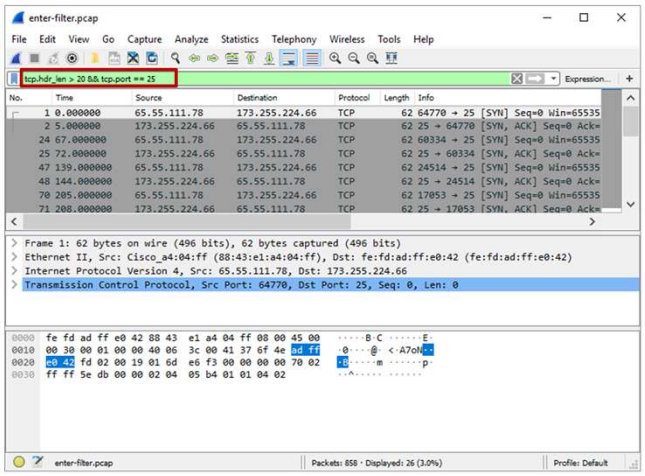
Auto-Complete Function



Wireshark does have an “auto-complete” feature which allows you to begin entering a value in the “Filter…” filed but will also show you the latest run searches and filters used.

Northeastern University

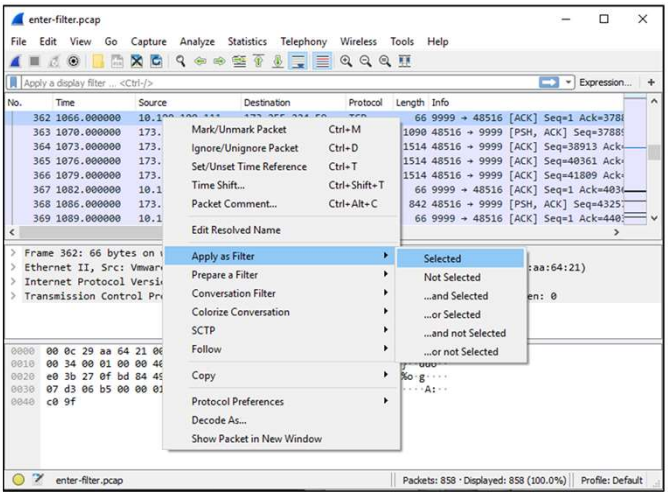
Filter Result



Here is the result of the auto-complete assisted filter. This selects all records with TCP options. Wireshark provided assistance with the selecting the ".port" notation while we supplied the "== 25" condition.

Northeastern University

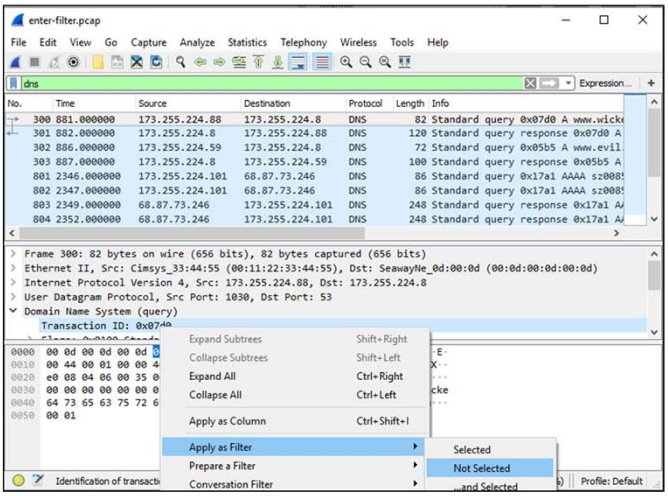
Apply as Filter (Packet Pane Record)



Another Wireshark filter is the “Apply as Filter” menu option that appears when you right-click on a record or particular field/value. An “Apply as Filter” option allows you to create a simple or complex condition to select of not select based on the column in the record where arrow might be when you right click.

Northeastern University

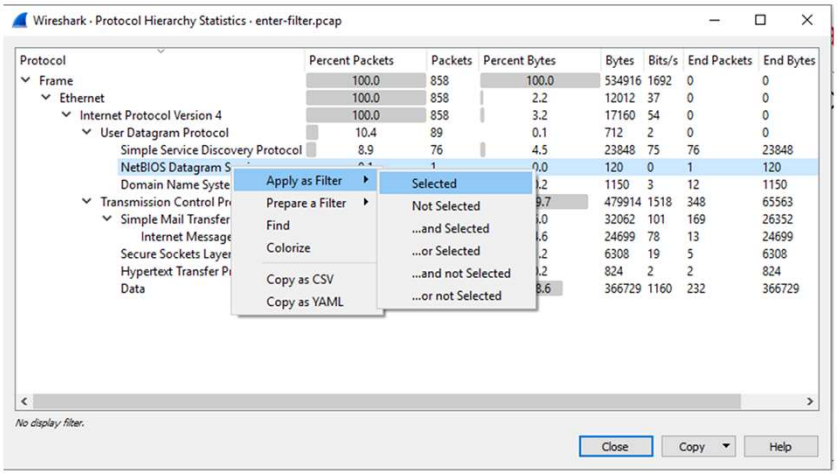
Apply as Filter (Field and Value)



This screenshot shows the “Apply as Filter” option when we’re looking for all packets/records that don’t meet the option that we’ve selected.

Northeastern University

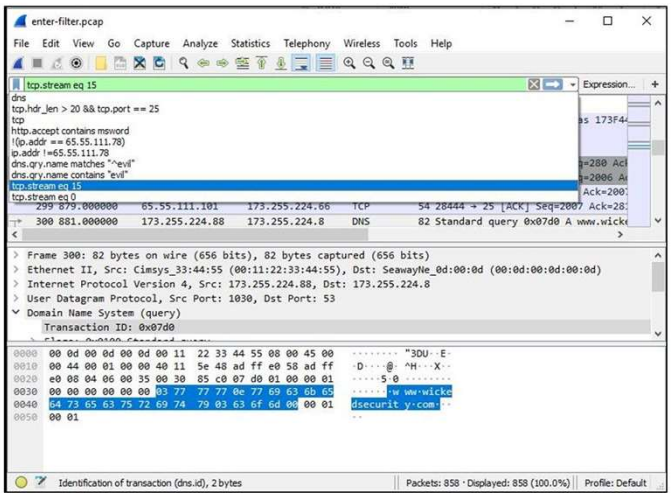
Apply as Filter (Statistics Output)



This Wireshark option can also be supplied to the Statistics menu option. This will allow analysts to identify a particular protocol to narrow in on for analysis and investigation (NetBIOS in this case).

Northeastern University

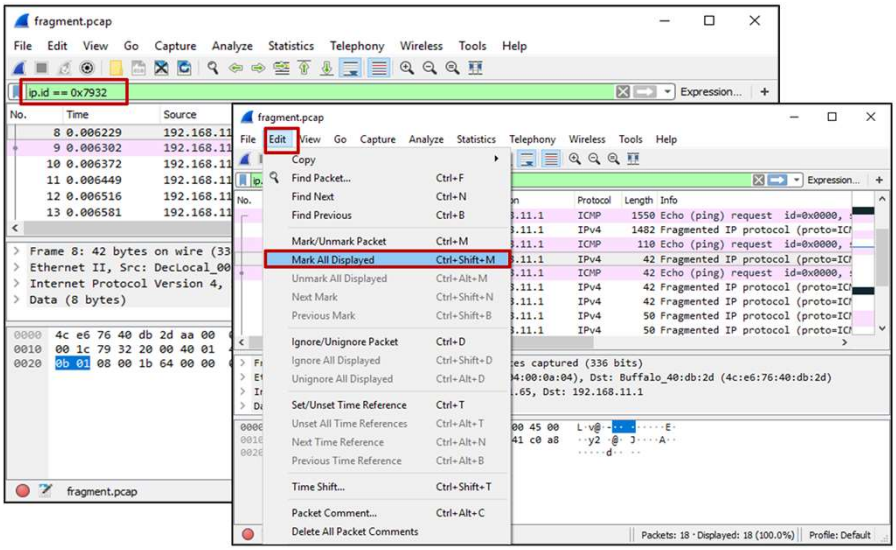
Previous Filters



A time-saving feature of Wireshark is that it saves all searches and queries that have been run. These display filters are stored in .wireshark/recent_common file associated with Wireshark users. You will find recently used pcap files listed in there too. Both display filter and pcap lists have a limited number of entries and the last one is deleted to make room for a new one when the limit is reached.

Northeastern University

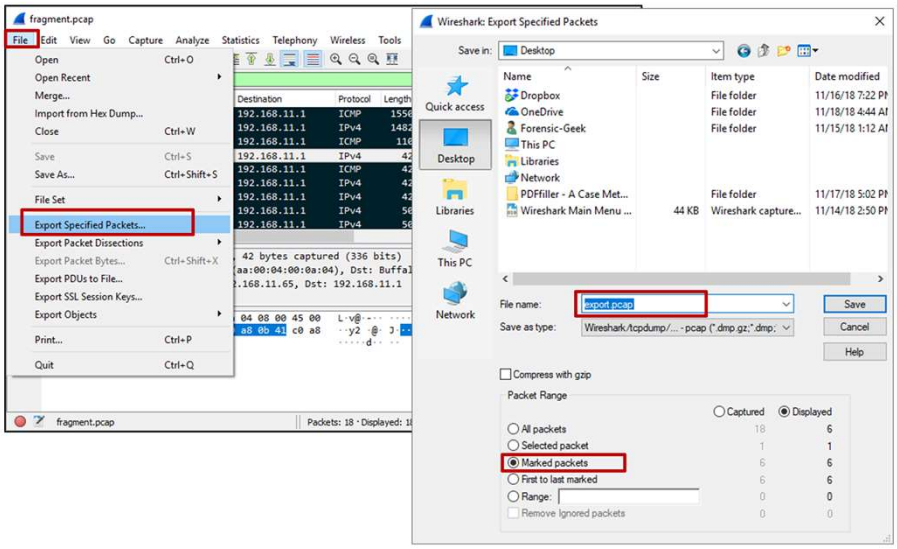
Save Packets to a New PCAP



There may be times when you want to create a new tcpdump pcap file where I either select or omit records from a current pcap file. Sometimes it is easy to specify a BPF field and value – sometimes not so much.

Northeastern University

Designate Packets and File Name



Save the marked records by selecting File > Export Specified Packets as seen in the upper left display. Save the packets to a file name that is manually entered and only save the marked packets in the lower right display. This is not the default option. You can then process these packets with other external libpcap input tools.

Display Filter Review

- Find packets with a specific trait
- Easier and more granular than BPF
- Many ways to create filters
- Don’t confuse with capture filters


Northeastern