



# Display Filters

# Display Filters

## » What are display filters?

## » Display filter rules

- Only applied during or after capture
- Different syntax than capture filters
- Can be applied to other tools (flow graph, color filters, I/O graph, etc.)

## » Using display filters

- Found in main Capture window

# Display Filters

Filter: tcp.ack

Expression... Clear Apply Save

No.	Time	UTC	Source	Destination	Protocol	Info
355	0.005474000	2014-09-03 16:50:41.587278000	10.121.90.106	149.174.28.1	TCP	49614→80 [ACK] Seq=172
356	0.001120000	2014-09-03 16:50:41.588298000	10.121.90.106	68.67.152.71	TCP	49882→80 [SYN] Seq=0 w
358					CP	80→49882 [SYN, ACK] Se
359					CP	49882→80 [ACK] Seq=1 A
360					TTP	GET /getuid?http://cma
361					CP	80→49882 [ACK] Seq=1 A
362					TTP	HTTP/1.1 204 No Conter
363					CP	49881→80 [FIN, ACK] Se
364					CP	80→49881 [FIN, ACK] Se
365					CP	49881→80 [ACK] Seq=865
366					TTP	HTTP/1.1 200 OK
368					CP	49617→443 [ACK] Seq=90
370					CP	49882→80 [ACK] Seq=582
371					CP	80→62785 [FIN, ACK] Se
372					CP	62785→80 [ACK] Seq=1 A
400					CP	49805→2869 [RST, ACK]
401					CP	49804→2869 [RST, ACK]
405					CP	49806→2869 [RST, ACK]
406					CP	49803→2869 [RST, ACK]
407					CP	49809→2869 [RST, ACK]
410					CP	49808→2869 [RST, ACK]
411					CP	49807→2869 [RST, ACK]

Wireshark: Filter Expression - Profile: Classic

Field name

- TALI - Transport Adapter Layer Interface v1.0, RFC
- TANGO - Tango Dissector Using GIOP API
- TAPA - Trapeze Access Point Access Protocol
- TAPI - Microsoft Telephony API Service
- TC-NV - TwinCAT NV
- TCAP - Transaction Capabilities Application Part
- TCP - Transmission Control Protocol
  - tcp.ack - Acknowledgment number
  - tcp.ack.nonzero - Expert Info (The acknowledg
  - tcp.analysis - SEQ/ACK analysis (This frame ha
  - tcp.analysis.ack\_lost\_segment - Expert Info (AC
  - tcp.analysis.ack\_rtt - The RTT to ACK the segm
  - tcp.analysis.acks\_frame - This is an ACK to the

Relation

- is present
- ==
- !=
- >
- <
- >=
- <=

Value (Unsigned integer, 4 bytes)

Predefined values:

Range (offset:length)

OK Cancel

# Display Filters

## » How can I edit dfilters?

### » GUI

- You can add filter strings as needed—example: udp
- You can copy other strings and add them to the dialog box

### » Notepad

- You can add filter strings manually to the file
- You can make a copy of another dfilters file or the contents within one to your file

# Display Filters

Filter: tcp.ack Expression... Clear Apply Save

No.	Time	UTC	Source	Destination	Protocol
355	0.005474000	2014-09-03 16:50:41.587278000	10.121.90.106	149.174.28.1	TCP
356	0.001120000	2014-09-03 16:50:41.588398000	10.121.90.106	68.67.152.71	TCP
358	0.002739000	2014-09-03 16:50:41.591137000	68.67.152.71	10.121.90.10	TCP
359	0.000100000	2014-09-03 16:50:41.591237000	10.121.90.106	68.67.152.71	TCP
360	0.000420000	2014-09-03 16:50:41.591657000	10.121.90.106	68.67.152.71	HTTP
361	0.002806000	2014-09-03 16:50:41.591657000	10.121.90.10	10.121.90.10	TCP
362	0.001386000	2014-09-03 16:50:41.591657000	10.121.90.10	10.121.90.10	HTTP
363	0.000440000	2014-09-03 16:50:41.591657000	23.77.209.43	23.77.209.43	TCP
364	0.004643000	2014-09-03 16:50:41.591657000	10.121.90.10	10.121.90.10	TCP
365	0.000074000	2014-09-03 16:50:41.591657000	23.77.209.43	23.77.209.43	TCP
366	0.014261000	2014-09-03 16:50:41.591657000	10.121.90.10	10.121.90.10	HTTP
368	0.102078000	2014-09-03 16:50:41.591657000	173.194.123.	173.194.123.	TCP
370	0.090088000	2014-09-03 16:50:41.591657000	68.67.152.71	68.67.152.71	TCP
371	0.153156000	2014-09-03 16:50:41.591657000	10.121.90.10	10.121.90.10	TCP
372	0.000314000	2014-09-03 16:50:41.591657000	10.140.195.8	10.140.195.8	TCP
400	1.867391000	2014-09-03 16:50:41.591657000	10.121.90.13	10.121.90.13	TCP
401	0.000011000	2014-09-03 16:50:41.591657000	10.121.90.13	10.121.90.13	TCP
405	0.000142000	2014-09-03 16:50:41.591657000	10.121.90.13	10.121.90.13	TCP
406	0.000005000	2014-09-03 16:50:41.591657000	10.121.90.13	10.121.90.13	TCP
407	0.000049000	2014-09-03 16:50:41.591657000	10.121.90.13	10.121.90.13	TCP
410	0.000937000	2014-09-03 16:50:41.591657000	10.121.90.13	10.121.90.13	TCP
411	0.000006000	2014-09-03 16:50:41.591657000	10.121.90.13	10.121.90.13	TCP

Context menu options:

- Mark Packet (toggle)
- Ignore Packet (toggle)
- Set Time Reference (toggle)
- Time Shift...
- Edit Packet
- Packet Comment...
- Manually Resolve Address
- Apply as Filter
- Prepare a Filter
  - Selected
  - Not Selected
  - ... and Selected
  - ... or Selected
  - ... and not Selected
  - ... or not Selected
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow TCP Stream
- Follow UDP Stream
- Follow SSL Stream
- Copy
- Protocol Preferences
- Decode As...
- Print...
- Show Packet in New Window

Packet details for Frame 360:

- Frame 360: 635 bytes on wire (5080 bits) on interface 0
- Ethernet II, Src: 3c:97:0e:8f:d5:
- Internet Protocol Version 4, Src:
- Transmission Control Protocol, Sr
- Hypertext Transfer Protocol

# Questions?