




100 WIRESHARK TIPS

@laurachappell


These tweets were released on Twitter (@laurachappell) from June 18-November 5, 2013.

- #Wireshark Tip 1:** Turn OFF TCP pref for reassembly when working HTTP - see the Response Code in correct packet.
- #Wireshark Tip 2:** Use groups to find sets of words - frame matches "(attachment|tar|exe|zip)"
- #Wireshark Tip 3:** Graph http.time in Wireshark 1.10 - Cool!
- #Wireshark Tip 4:** Look for "data" in Statistics | Protocol Hierarchy when you suspect malicious traffic.
- #Wireshark Tip 5:** In 1.10, right-click on an item in the Expert Info window | Internet Search. Nice!
- #Wireshark Tip 6:** Filter on tcp.analysis.flags && !tcp.analysis.window_update – click Save to make it a button.
- #Wireshark Tip 7:** Edit/remove Filter Expression buttons through Preferences | Filter Expressions.
- #Wireshark Tip 8:** Disable IP, TCP, UDP checksum validation – task offload very common
- #Wireshark Tip 9:** Select Help | About Wireshark | Folders to find your personal configs/profiles.
- #Wireshark Tip 10:** Right click on TCP Stream field and Apply as Column for spaghetti TCP traffic
- #Wireshark Tip 11:** Right-Click on No. column heading to left-align – get it away from Time column
- #Wireshark Tip 12:** Add an http.host column when analyzing web browsing sessions
- #Wireshark Tip 13:** Select "Classic" in Wireshark 1.10 profiles to use brighter color palette.
- #Wireshark Tip 15:** Capture at the client to obtain RTT and performance from the client's perspective.
- #Wireshark Tip 16:** Apply a IO graph line based on Bad TCP coloring rule string to correlate TCP/thruput probs.
- #Wireshark Tip 17:** Increase Filter Display max. list entries to 30 in User Preferences.
- #Wireshark Tip 18:** Increase "Open Recent" max list entries to 30 in User Preferences.
- #Wireshark Tip 19:** Toggle Bytes pane with View | Packet Bytes – more room is nice.
- #Wireshark Tip 20:** Clear recent files with File | Open Recent | Clear the recent file list.
- #Wireshark Tip 21:** I always disable the Bad Checksum coloring rule.
- #Wireshark Tip 22:** Enable Calculate Conversation Timestamps (TCP Pref) to track TCP delta times.






100 WIRESHARK TIPS @laurachappell

- #Wireshark Tip 23:** After #Wireshark Tip 22, add a tcp.time_delta column and sort high to low.
- #Wireshark Tip 24:** Coloring Rule: http.response.code > 399 to highlight errors.
- #Wireshark Tip 25:** Coloring rule: Bad TCP Con Options - tcp.hdr_len < 28 && tcp.flags.syn == 1.
- #Wireshark Tip 26:** I always set View | Time Display Format | Secs. Since Prev. Displayed Packet.
- #Wireshark Tip 27:** Use Prefs | Filter Exp. to reorder your Filter Exp. buttons.
- #Wireshark Tip 28:** I use "|" name and "frame" string to create Filter Exp. button separator.
- #Wireshark Tip 29:**  Stats | TCP Stream Gr | Time-Seq Gr (tcptrace) - top grey line is available rec. window space – pic.twitter.com/7wifRtFURu
- #Wireshark Tip 30:** I always add a tcp.stream column to quickly catch new connections being established -
- #Wireshark Tip 31:** Wireshark 1.10 has an http.time field in responses - turn off TCP pref 4 reassembly first.
- #Wireshark Tip 32:** Those grey lines dipping down in Time Seq. graph (tcptrace) are duplicate ACKs
- #Wireshark Tip 33:** Select Help > About Wireshark > Folders > personal config dir > profiles!
- #Wireshark Tip 34:** Update Wireshark from an earlier vers? Might need to disable IP checksum validation
- #Wireshark Tip 35:** Click Internals > Supported Protocols (slow!) to find protocols/apps dissected by Wireshark.
- #Wireshark Tip 36:** Edit | Prefs | Name Resolution - add path to GeoIP dir (see bit.ly/1cjd23a for database).
- #Wireshark Tip 37:** HTTP over some other port (not 80)? Edit | Preferences | Protocols | HTTP -add to the port list.
- #Wireshark Tip 38:** I always right-click the No. column header to change alignment to left - cleaner view.
- #Wireshark Tip 39:** Fast way to set protocol prefs. Right-click on the protocol in the detail window - Protocol Prefs!
- #Wireshark Tip 40:** The display filter "a && b || c" is processed as "a && (b || c)" - go figure! See Aug 7 tweets.
- #Wireshark Tip 41:** Use wlan.fc.retry == 1 to locate WLAN retries.
- #Wireshark Tip 42:** Export field info - add as column, File | Export Packet Dissections (packet summary line only)
- #Wireshark Tip 43:** Use Editcap to split big traces into file sets - use File | File Sets to view
- #Wireshark Tip 44:** Wireshark 1.10 Status Bar includes percentage info when you apply a display filter.
- #Wireshark Tip 45:** Use the filter/coloring rule string/button sip.Status-Code > 300 to detect SIP errors.
- #Wireshark Tip 46:** Filter on tcp.analysis.retransmissions to see standard/fast retransmissions.
- #Wireshark Tip 47:** Use CIDR format for a subnet display filter - for example, ip.addr==10.2.0.0/16.

100 WIRESHARK TIPS @laurachappell

- #Wireshark Tip 48:** Customize profiles - Right-click on a field and select Apply as Column on interesting field.
- #Wireshark Tip 49:** Wireshark 1.10.1 has an auto-update feature - also Help | Check for Updates is new.
- #Wireshark Tip 50:** Use Preferences | Filter Expressions to edit, reorder, disable, delete Filter Expression buttons.
- #Wireshark Tip 51:**  New TCP Time-Seq graph depicts SACK packets in blue. Nice! pic.twitter.com/9CpP92kBn3
- #Wireshark Tip 52:** Tshark subnet stats - tshark -q -z io,stat,3600,ip.addr==192.168.1.0/24 >stats.txt (manual stop)
- #Wireshark Tip 53:** Click and drag over areas to zoom in on TCP Stream Graphs. Click Home to revert.
- #Wireshark Tip 54:** When no dissector is available, right-click and follow the stream to look for commands, etc.
- #Wireshark Tip 55:** Statistics | Show Address Resolution (1.10.1) pulls all name resolution from trace file - nice!
- #Wireshark Tip 56:** Two great reasons to add a column: ability to sort and export column data.
- #Wireshark Tip 57:** Why is that packet colored that way? Expand the Frame section for the answer.
- #Wireshark Tip 58:** Use Editcap to split a single large trace file into a manageable file set.
- #Wireshark Tip 59:** Hate seeing "blackjack" and other dynamic client port values? Turn off transport name resolution.
- #Wireshark Tip 60:** My Golden Rule #1 - Capture as close to the client as you can be for the client perspective!
- #Wireshark Tip 61:** U don't need to load the whole trace of a DoS attack - a quick peek tells the story.
- #Wireshark Tip 62:** Right-click on the Profile column on the Status Bar to create a new custom profile!
- #Wireshark Tip 63:** Golden #Wireshark Tip for Network Forensics - open the Statistics | Protocol Hierarchy first.
- #Wireshark Tip 64:** If u use a capture filter and save to pcapng, capture filter info is in Stats | Summary! Nice!
- #Wireshark Tip 65:** See original packet+ retrans,-packet loss has not occurred yet-move Wireshark closer to sender.
- #Wireshark Tip 65:** Filter for SMB errors - smb.nt_status > 0. Make it a coloring rule too!
- #Wireshark Tip 66:** ARP storm detection can be enabled in ARP/RARP preferences (Edit | Preferences | Protocols).
- #Wireshark Tip 67:** Turn on Expert icons (last item) in Preferences | User Interface to learn Expert button colors.
- #Wireshark Tip 68:** Try http.request.uri contains "/profile_images/" filter and then cruise Twitter feeds. Funny.
- #Wireshark Tip 69:** http.request.method == "POST" will show all POST HTTP messages.
- #Wireshark Tip 70:** After defining an awesome display filter, click Save to make it a filter expression
- #Wireshark Tip 71:** File | Export Objects | HTTP (make sure TCP pref for reassembly is on). Also see NetworkMiner.
- #Wireshark Tip 72:** Statistics | HTTP | Packet Counter for HTTP Response Codes.

100 WIRESHARK TIPS @laurachappell

- #Wireshark Tip 73:** Click a field in Packet Detail window - look at Status Bar for field filter name.
- #Wireshark Tip 74:** Detect multicast bursts - Statistics | UDP Multicast Streams.
- #Wireshark Tip 75:** SMB error filter - `smb.nt_status > 0 || smb2.nt_status > 0`.
- #Wireshark Tip 76:** SIP error filter - `sip.Status-Code > 399`.
- #Wireshark Tip 77:** NFS error filter - `nfs.status2 > 0 || nfs.status3 > 0`.
- #Wireshark Tip 78:** Filter for SMB delays over 1 second - `smb.time > 1`.
- #Wireshark Tip 79:** `LoWin Size-(tcp.window_size>0 && tcp.window_size<1320) && tcp.flags.reset==0 && tcp.flags.fin==0`.
- #Wireshark Tip 80:**  Turn the Bad TCP coloring rule into a button. pic.twitter.com/0tF5WvCgkL
- #Wireshark Tip 81:**  Customized profile directories contain plain text files that you can edit. pic.twitter.com/dvwSsDXM9K
- #Wireshark Tip 82:**  Create, edit, share Filter Expression buttons via preferences file. pic.twitter.com/SwNaQdBGUZ
- #Wireshark Tip 83:**  Locating missing TCP options with a simple button. pic.twitter.com/cjaWJcu33u
- #Wireshark Tip 84:**  Find slow response to TCP SYNs (high path latency) with this simple filter. pic.twitter.com/XagkmjkzJH
- #Wireshark Tip 85:** Right click on any column heading and select Edit Column Details to rename.
- #Wireshark Tip 86:** Statistics | Comment Summary to see trace file/packet comments with basic trace details.
- #Wireshark Tip 87:** Capture options now offers kibibytes, mebibytes, and gibibytes... wish NIST site (1.usa.gov/15Gvmmw) available <gov shutdown>.
- #Wireshark Tip 88:** Export all Calc. Window Size info by right-clicking on field, Apply as Column, Exp. Packet Dissections | Summary to .csv.
- #Wireshark Tip 89:** Need lots of sample trace files? Download book supplements from bit.ly/10Klfzf.
- #Wireshark Tip 90:** Change Time column precision with View | Time Display Format | select precision.
- #Wireshark Tip 91:** Use Edit | Preferences | Filter Expressions to edit/reorder your filter buttons. Click away from edit area before saving.
- #Wireshark Tip 92:** Use `http.request.uri contains ".exe"` to find folks downloading .exe files.
- #Wireshark Tip 93:** You must save a file in .pcapng format to save packet and trace file comments.
- #Wireshark Tip 94:** Statistics | Conversations | UDP/TCP, uncheck Name Resolution to view port numbers, not names.
- #Wireshark Tip 95:** TCP Time-Sequence graph can be launched from Statistics | Conversations | TCP window now - nice!

100 WIRESHARK TIPS @laurachappell

- #Wireshark Tip 96:** Did you know a low window size can stop communications? See [http-download-good.pcapng](http://download-good.pcapng) from www.wiresharkbook.com site.
- #Wireshark Tip 97:** Statistics | Conversations | IPv4/IPv6 - click 2x on Bytes to find most active hosts.
- #Wireshark Tip 98:** SYN flood from many IP addresses? Make an IP TTL column and review to see if you have 1 or more sources.
- #Wireshark Tip 99:** Add an ip.dsfield.dscp column to look for DiffServ values in traffic.
- #Wireshark Tip 100:** Filter on ip.flags.mf==1 || ip.frag_offset > 0 to find IP fragments (yuck).

About Laura Chappell, Network Analyst, Instructor, and Wireshark® Evangelist

Laura Chappell is a highly-energetic speaker and author of numerous industry titles on network analysis, troubleshooting, and security. Nicknamed “Glenda, the Good Witch,” Laura has presented to thousands of State, Federal and international law enforcement officers, judicial members, engineers, network administrators, technicians and developers on the subject of “tapping into networks.” She focuses on troubleshooting, optimization, security and application analysis.

Ms. Chappell is the Founder of Chappell University (www.chappellU.com) which develops and delivers onsite and online training in the areas of network protocols, network forensics and network analysis tools.

In 2007, Ms. Chappell founded Wireshark University (www.wiresharkU.com), the worldwide premiere educational firm focused on teaching the art of wiretapping/communications interception, network forensics, TCP/IP analysis, network troubleshooting and network security.

Laura’s network analysis, troubleshooting and security training is available online through the All Access Pass at www.chappellU.com and through customized online/onsite analysis and training.