Wireshark v2 Review

Laura Chappell, Wireshark University

In Wireshark version 2, Gerald Combs and the exceptional Wireshark development team have done an amazing job streamlining and improving many of the tasks that I undertake when troubleshooting or performing network forensics.

Many peopxle have no idea that this Wireshark version has been in development for almost 2 years. In order to support the November 12th Introduction to Wireshark webinar, I put together a list of some of my favorite improvements and features in this new version.

- USBPcap – yes – you can capture traffic to and from your USB drive. Visit http://desowin.org/usbpcap/ for more details on USBPcap.
- Androiddump – interface to capture on Android devices.
- Qt application framework – replaced GTK+ and provides a better user experience,
- especially on Windows and Mac OS X (Mac users finally have a native install).
- Related packet feature – depicting the relationship between requests/replies and data/ACKs.
- Intelligent scrollbar – miniature coloring system that helps you quickly locate issues in the trace file - very cool!
- Conversations window and Endpoints windows are now configurable – define the tabs you'd like to see.
- Expert filterable – right-click on any expert indication to quickly apply them as a filter in the main packet window.
- New Wireless toolbar – updated and streamlined.
- New Wireless menu item – includes Bluetooth and WLAN features.
- Export Objects > TFTP – another quick way to export transferred data to a file.
- Edit > Configuration Profiles - includes hyperlink to profile directory (lots of other hyperlink additions throughout Wireshark 2 as well).

- Faster display of columns – use right-click on a column heading to view available columns (much faster process now).

- Better starting TCP preference settings - calculate conversation timestamps is now on by default, for example.

- SSL dissector improved

- Language support – translated into Chinese, English, French, German, Polish, Italian, and Japanese so far (see https://www.transifex.com/wireshark/wireshark/ for translation status).

- TCP Stream Graphs – change directions, change graph, too many improvements to list.

- IO Graph – more control over graphed.

- HTTP2 statistics – new and necessary.

- UDP Multicast Streams statistics – improved control.

- Many graph and statistic windows can be kept open even after trace file closed – this is great for comparing trace file information.

- List of ports in display filters (for example "Non-HTTP and non-SMTP to/from 192.0.2.1" ip.addr == 192.0.2.1 and not tcp.port in {80 25} is a new sample filter using the port listing feature {80 25})

- Background dissection – allows for smoother Wireshark operations when opening a trace file.

Kudos to the Wireshark development team and Gerald for a job well done!

Laura Chappell
Wireshark University