

SHARKFEST '12

Wireshark Developer and User Conference

Wireshark 1.8
19 ~~16~~ Cool New Features
to Drool Over

Laura Chappell
Founder, Wireshark University
Founder, Chappell University

Just Released!



SHARKFEST '12

1

Note

- The video covering these new features should be online at www.wireshark.org and www.wiresharkbook.com...

SHARKFEST '12

2

Enhancements/Fixes!



Capture

1. multiple interfaces 
2. separate filters per interface – expand Options window

Packet info

3. DNS Transaction ID added to Info column
4. ignore TCP Timestamps in Summary (TCP Preference)

Expert Info




5. LEDs – learn the Expert button color coding faster
6. Fast Retransmissions and Retransmissions under Notes 
7. Window Update excluded from Bad TCP coloring rule 

3

SHARKFEST '12

Enhancements/Fixes!

Miscellaneous

8. Profiles > Create From 
9. IP header checksum disabled 
10. coloring rules - default placement at top 
11. GeoIP IPv6 support (CSV files at maxmind.com)
12. Time Shift feature

4

SHARKFEST '12

Enhancements/Fixes!

Miscellaneous

- 13. Flow Graph maintains Time column setting →
- 14. pcap-ng format is the default (if enabled) →
- 15. TCP Stream Index definition changed →
- 16. Decode As settings can be saved in a Profile →
- 17. File Export Changes

5

SHARKFEST '12

Enhancements/Fixes!

18. Display filters - save filter expressions

Try this one out – download the *sample profiles* at wiresharkbook.com and look at the one titled “laura’s config”



6

Enhancements/Fixes!

19. Packet and File Annotations (pcapng required)

Check this one out – download the new
pcapng trace file set from wiresharkbook.com

– all trace files are
annotated and
many have packet
annotations as well

