# T2-9: Top 10 Tips and Tasks

Tuesday, April 1, 2008 – 3:45pm to 5:00pm

**Laura Chappell**
Founder | Wireshark University

**Betty DuBois**
Principal Consultant | DuBois Training & Consulting, LLC

**SHARK**FEST **'08**
Foothill College
March 31 - April 2, 2008

# Top 10

1. Prepare display filter (type in, right-click, expressions)
2. Building basic and advanced IO graphs (use calc feature)
3. Reassemble streams
4. Graph TCP Streams (IO, Sequence/ACK)
5. Graph HTTP Flows

# Top 10 (continued)

6. Add columns
7. Alter protocol configurations (especially TCP)
8. Create baselines (use yourself)
9. Place the analyzer properly
10. Capture to disk (ring buffer, stop triggers)

# Top 10 (continued)

11. Use ***tshark*** for command-line capture (with parameters)
12. Use ***edicap*** to split a large file
13. Use mergecap to merge files taken from different capture points – asymmetrical routing (mergecap)
14. Utilize *Expert Notes* and the filtering capabilities in the Analysis section of packets
15. Interpret the Expert information in the dissector code
16. Search for a string (not just a “data contains” filter)
17. Decode one application as another (“decode as”)

# Vista and Windows Server 2008 Notes

Both are capable of protocol and checksum offloading

Both use window scaling with a factor of 8 (16MB receive window)

Both use selective ACKs and SACK options

Neither use TCP Timestamps to set the Retransmission Timeout (RTO) or define the round-trip time (RTT)

Both allow three SYN and SYN ACK retransmissions (0 secs, 3 secs, 6 seconds and 12 seconds) before connection abandoned

Neither has TCP Keepalives enabled (application must request)

Both use Delayed ACKs (200ms max) RFC 1122

Both use Receive Window Auto-Tuning (measure bandwidth delay product and application retrieve rate)

Both have an updated Slow Start Algorithm to account for Delayed ACKs

WS08 only: Compound TCP to increase send window faster on high receive window/high BDP connections

# Thanks For Coming!

Enjoy the rest of the conference.



CACE TECHNOLOGIES

www.wiresharkU.com
WIRESHARK UNIVERSITY