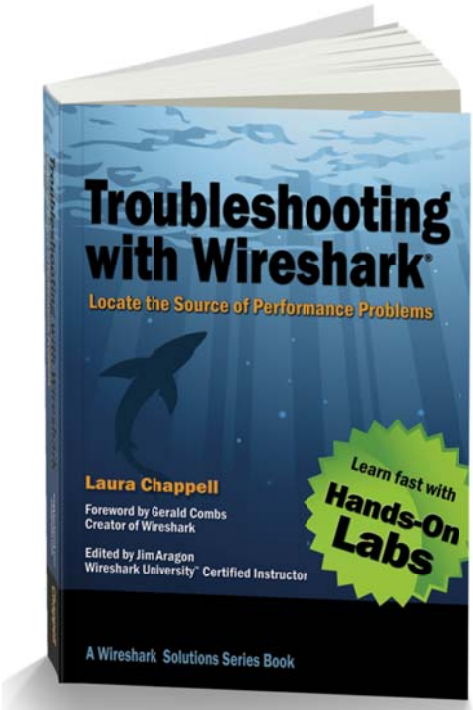

Troubleshooting Checklist

Based on the book *Troubleshooting with Wireshark*
Author: Laura Chappell, Founder of Wireshark University™
Foreword: Gerald Combs, Creator of Wireshark®
Editor: Jim Aragon, Wireshark University Certified Instructor™

Hardcopy ISBN: 9781893939974
www.wiresharkbook.com
info@wiresharkbook.com

About this Troubleshooting Checklist

I have a basic troubleshooting checklist (albeit in my head) that I run through each time I open a trace file. The order in which I go through the checklist may change depending on the troubleshooting issue (UDP-based application troubleshooting vs. TCP-based application troubleshooting, for example).

Consider expanding this checklist to suit your needs.

This Troubleshooting Checklist was created as a supplement for the book ***Troubleshooting with Wireshark*** (Copyright 2014; hardcopy ISBN: 9781893939974).

For more book supplements or information, visit www.wiresharkbook.com.

Let's get started…

Troubleshooting Checklist Sections

- ☐ Verify Trace File Integrity and Basic Communications
- ☐ Focus on Complaining User's Traffic
- ☐ Detect and Prioritize Delays
- ☐ Look for Throughput Issues
- ☐ Check Miscellaneous Traffic Characteristics
- ☐ TCP-Based Application: Determine TCP Connection Issues/Capabilities
- ☐ TCP-Based Application: Identify TCP Issues
- ☐ UDP-Based Application: Identify Communication Issues
- ☐ Spot Application Errors

Verify Trace File Integrity and Basic Communications

- ☐ Look for ACKed Unseen Segment (**`tcp.analysis.ack_lost_segment`** filter)
  [Switch oversubscribed?] See *ACKed Unseen Segment* starting on page 191 of *Troubleshooting with Wireshark, 1st Edition*.
- ☐ Verify traffic from the complaining user's machine is visible. If not…
  - Ensure the host is running.
  - Test the host's connectivity (Can it communicate with another host?).
  - Recheck capture location and process.
  - Consider a resolution problem. See *Chapter 4: Resolution Problems* starting on page 91 of *Troubleshooting with Wireshark, 1st Edition.*
- ☐ Verify resolution process completion
  - DNS queries/successful responses (consider cache use). See *Detect DNS Errors* starting on page 237 of *Troubleshooting with Wireshark, 1st Edition.*
  - ARP requests/responses (consider cache use). See *MAC Address Resolution – Local Target* and *MAC Address Resolution – Remote Target* on page 97 of *Troubleshooting with Wireshark, 1st Edition.*

Notes

Focus on Complaining User's Traffic

- ☐ Filter **on** related traffic (such as **`tcp.port==80 && ip.addr==10.2.2.2`**). See *Filter on a Host, Subnet or Conversation, Filter on an Applications Based on Port Number, Filter on Field Existence or Field Value* starting on page 42 of *Troubleshooting with Wireshark, 1st Edition.*
- ☐ Filter **out** unrelated traffic (such as **`!ip.addr==239.0.0.0/8`** or perhaps **`!bootp`**). See *Filter OUT Normal Traffic* starting on page 51 of *Troubleshooting with Wireshark, 1st Edition.*
- ☐ Export related traffic to a separate trace file (**File | Export Specified Packets**). See *Wireshark Lab 4: Extract and Save a Single Conversation* on page 91 of *Troubleshooting with Wireshark, 1st Edition.*

Notes

Detect and Prioritize Delays

- ☐ Sort and identify high delta times (**Edit | Preferences | Columns | Add | Delta time displayed**). See *Add/Sort a Delta Displayed Time Column* on page 116 of *Troubleshooting with Wireshark, 1st Edition.*
- ☐ Sort and identify high TCP delta times (**`tcp.time_delta`** column). See *Wireshark Lab 29: Add/Sort a TCP Delta Time Column* starting on page 123 of *Troubleshooting with Wireshark, 1st Edition.*
    - o If Expert Infos items are seen, examine the Errors, Warnings and Notes listings. See *Chapter 6: Identify Problems Using Wireshark's Expert* starting on page 151 of *Troubleshooting with Wireshark, 1st Edition.*
    - o Consider "acceptable delays" (such as delays before TCP FIN or RST packets). See *Do Not Focus on "Normal" or Acceptable Delays* starting on page 107 of *Troubleshooting with Wireshark, 1st Edition.*

☐ Measure path latency (Round Trip Time) using delta times in TCP handshake. See *Wireshark Lab 31: Obtain the Round Trip Time (RTT) Using the TCP Handshake* starting on page 128 of *Troubleshooting with Wireshark, 1st Edition.*

- o Capturing at client: measure delta from TCP SYN to SYN/ACK - see *Filter for SYN and SYN/ACK Packets (Packets 1 and 2 of the TCP Handshake)* starting on page 129 of *Troubleshooting with Wireshark, 1st Edition.*
- o Capturing at server: measure delta from SYN/ACK to ACK - see *Filter for SYN/ACK and ACK Packets (Packets 2 and 3 of the TCP Handshake)* starting on page 130 of *Troubleshooting with Wireshark, 1st Edition.*
- o Capturing in the infrastructure: measure delta from SYN to ACK[1] - see *Filter for SYN and ACK Packets (Packets 1 and 3 of the TCP Handshake)* starting on page 130 of *Troubleshooting with Wireshark, 1st Edition.*

- ☐ Measure server response time
    - o TCP-based application: measure from ACK to response, not request to ACK. See *Identify High HTTP Response Time* and *Identify High SMB Response Time* starting on page 139 of *Troubleshooting with Wireshark, 1st Edition.*
    - o Use Wireshark's response time function if possible (such as **`dns.time`**, **`smb.time`**, and **`http.time`**). See *Identify High DNS Response Time, Identify High HTTP Response Time,* and *Identify High SMB Response Time* starting on page 135 of *Troubleshooting with Wireshark, 1st Edition.*
- ☐ Measure client latency
    - o How long did it take for the client to make the next request?
    - o Consider "acceptable delays" (such as a delay before an HTTP GET). See *Do Not Focus on "Normal" or Acceptable Delays* starting on page 107 of *Troubleshooting with Wireshark, 1st Edition.*

Notes

---

[1] This trick was brought up by Jasper Bongertz at the Sharkfest conference.

Look for Throughput Issues

- ☐ Build the Golden Graph (IO Graph with "Bad TCP" on Graph 2). See *Correlate Drops in Throughput with TCP Problems (the "Golden Graph")* starting on page 280 of *Troubleshooting with Wireshark, 1st Edition*.
- ☐ Click on low throughput points to jump to problem spots in the trace file.
- ☐ Look at traffic characteristics at low throughput points.
- ☐ Consider using an Advanced IO Graph to detect delays (such as **`tcp.time_delta`**). See *Chapter 10: Graph Time Delays* starting on page 283 of *Troubleshooting with Wireshark, 1st Edition*.

Notes

Check Miscellaneous Traffic Characteristics

- ☐ Check packet sizes during file transfer (Length column). See *Detect Consistently Low Throughput due to Low Packet Sizes* starting on page 275 of *Troubleshooting with Wireshark, 1st Edition.*
- ☐ Check IP DSCP for prioritization.
- ☐ Check 802.11 Retry bit setting (**`wlan.fc.retry == 1`**). See *Wireshark Lab 98: Filter on WLAN Retries and Examine Signal Strength* starting on page 326 of *Troubleshooting with Wireshark, 1st Edition.*
- ☐ Check for ICMP messages.
- ☐ Check for IP fragmentation.

Notes

TCP-Based Application: Determine TCP Connection Issues/Capabilities

- ☐ Look for unsuccessful TCP handshakes.
  - SYN, no answer (See *Wireshark Lab 20: No Response to TCP Connection Request* starting on page 101 of *Troubleshooting with Wireshark, 1st Edition*.)
  - SYN, RST/ACK
- ☐ Examine the TCP handshake Options area.
  - Check MSS values.
  - Check for Window Scaling and Scale Factor. (See *Lab 9: Create a Button to Detect Missing TCP Functionality* starting on page 53 of *Troubleshooting with Wireshark, 1st Edition*.)
  - Check for Selective ACK (SACK). (See *Lab 52: Determine if Selective ACK (SACK) is in Use* starting on page 172 of *Troubleshooting with Wireshark, 1st Edition*.)
  - Check for TCP Timestamps (especially on high-speed links).

Notes

TCP-Based Application: Identify TCP Issues

- ☐ Launch the Expert Infos window. See *Chapter 6: Identify Problems Using Wireshark's Expert* starting on page 151 of *Troubleshooting with Wireshark, 1st Edition.*
  - Consider number of errors, warnings and notes
  - Consider impact of each item
- ☐ Check the Calculated window size field values (**`tcp.window_size`**). See *Lab 7: Filter on the Calculated Window Size Field to Locate Buffer Problems* starting on page 48 of *Troubleshooting with Wireshark, 1st Edition.*
- ☐ Examine unexpected TCP RSTs.

Notes

UDP-Based Application: Identify Communication Issues

- ☐ Look for unsuccessful requests.
  - Request, no answer
- ☐ Look for repeated requests.

Notes

Spot Application Errors

☐ Filter for application error response codes (such as **`sip.Status-Code >= 400`**).
See *Chapter 7: Identify Application Errors*, starting on page 235 of *Troubleshooting with Wireshark, 1st Edition.*

Notes