

## Hands-On TCP Analysis

Jasper Bongertz, @packetjay

**Where:** Sharkfest 2017

**When:** 20th of June, 2:45pm – 4pm

### Session Summary

In this session, you'll work through a series of short but interesting sample TCP traces that will be distributed to participants prior to the beginning of the conference, giving you a chance to work and familiarize yourself with them before the group walkthrough, review and Q&A.

### PCAP Hints

In general you should look for trouble in the capture files provided. Try to find things that look like something is not working correctly, and check what the impact may be. Try to find an explanation why the behavior observed in the packets could have happened. Maybe even find who's causing the problem and how to fix it.

If you have questions or things that aren't clear, write them down and ask them during the presentation at Sharkfest 2017 or in the Q&A at the end.

### Specific hints

1. **Sample01.pcapng:** The TCP handshake looks like there's a problem. What looks different compared to a normal handshake?
2. **Sample02.pcapng:** The connection looks unsuccessful. Is this just an unstable connection?
3. **Sample03.pcapng:** Client and server can communicate, but sometimes there seems to be a problem connecting to the server. Can you verify that, and why doesn't it always work?
4. **Sample04.pcapng:** Accessing a web page seems broken. Is it the browser, the web server, or something else that's causing problems?
5. **Sample05.pcapng:** Is this a TCP problem? Can you tell what caused the connection to behave that way?