SharkFest '17 Europe

Hands-On TCP Analysis

Packets, Sequences & Fun

Jasper Bongertz

PACKET-FOO

08 November 2017

About me?

- Working for Airbus
- Wireshark community
  - Blog: blog.packet-foo.com
  - Twitter: @packetjay
  - Q&A: https://ask.wireshark.org
  - Sharkfest (obviously)
- Creator of TraceWrangler
  - https://www.tracewrangler.com

Rules of Engagement

- This session is
  - No slides (well, five…)
  - Beginner Level
  - Highly interactive
- You don‘t need to have the right answers
  - It‘s good if you do, but better if you don‘t

Let's dive into some PCAPs...

No.	IF	Source	Destination	Protocol	Info	Lengtl	Delta Time	Relative Ti
1	0	192.168.0.1	192.168.0.101	TCP	1404 → 80 [SYN] Seq=3727963648 Win=16384 Len=0 MSS=1460 SACK…	62	0.000000	0.000000
2	0	192.168.0.1	192.168.0.101	TCP	[TCP Retransmission] 1404 → 80 [SYN] Seq=3727963648 Win=1638…	62	2.922719	2.922719
3	0	192.168.0.101	192.168.0.1	TCP	80 → 1404 [SYN, ACK] Seq=2050753024 Ack=3727963649 Win=0 Len…	60	0.002056	2.924775
4	0	192.168.0.1	192.168.0.101	TCP	1404 → 80 [ACK] Seq=3727963649 Ack=2050753025 Win=17520 [TCP…	54	0.000018	2.924793
5	0	192.168.0.101	192.168.0.1	TCP	[TCP ZeroWindow] 80 → 1404 [ACK] Seq=2050753025 Ack=37279636…	60	0.001672	2.926465
6	0	192.168.0.101	192.168.0.1	TCP	[TCP Window Update] 80 → 1404 [ACK] Seq=2050753025 Ack=37279…	60	1.306026	4.232491
7	0	192.168.0.1	192.168.0.101	TCP	1404 → 80 [PSH, ACK] Seq=3727963649 Ack=2050753025 Win=17520…	434	0.000011	4.232502
8	0	192.168.0.101	192.168.0.1	TCP	80 → 1404 [ACK] Seq=2050753025 Ack=3727964029 Win=1818 Len=0	60	0.009203	4.241705
9	0	192.168.0.101	192.168.0.1	TCP	80 → 1404 [PSH, ACK] Seq=2050753025 Ack=3727964029 Win=2048 …	60	0.011729	4.253434
10	0	192.168.0.101	192.168.0.1	TCP	80 → 1404 [PSH, ACK] Seq=2050753026 Ack=3727964029 Win=2048 …	310	0.069505	4.322939
11	0	192.168.0.1	192.168.0.101	TCP	1404 → 80 [ACK] Seq=3727964029 Ack=2050753282 Win=17263 [TCP…	54	0.000015	4.322954
12	0	192.168.0.101	192.168.0.1	TCP	80 → 1404 [FIN, ACK] Seq=2050753282 Ack=3727964029 Win=2048 …	60	0.002096	4.325050
13	0	192.168.0.1	192.168.0.101	TCP	1404 → 80 [ACK] Seq=3727964029 Ack=2050753283 Win=17263 [TCP…	54	0.000013	4.325063
14	0	192.168.0.1	192.168.0.101	TCP	1404 → 80 [FIN, ACK] Seq=3727964029 Ack=2050753283 Win=17263…	54	0.001680	4.326743
15	0	192.168.0.101	192.168.0.1	TCP	80 → 1404 [ACK] Seq=2050753283 Ack=3727964030 Win=2048 Len=0	60	0.001958	4.328701

Mail: jasper@packet-foo.com
Web: blog.packet-foo.com
Twitter: @packetjay