SharkFest '17 Europe

TCP Analysis

When Things get complicated…

Jasper Bongertz

PACKET-FOO

10 November 2017

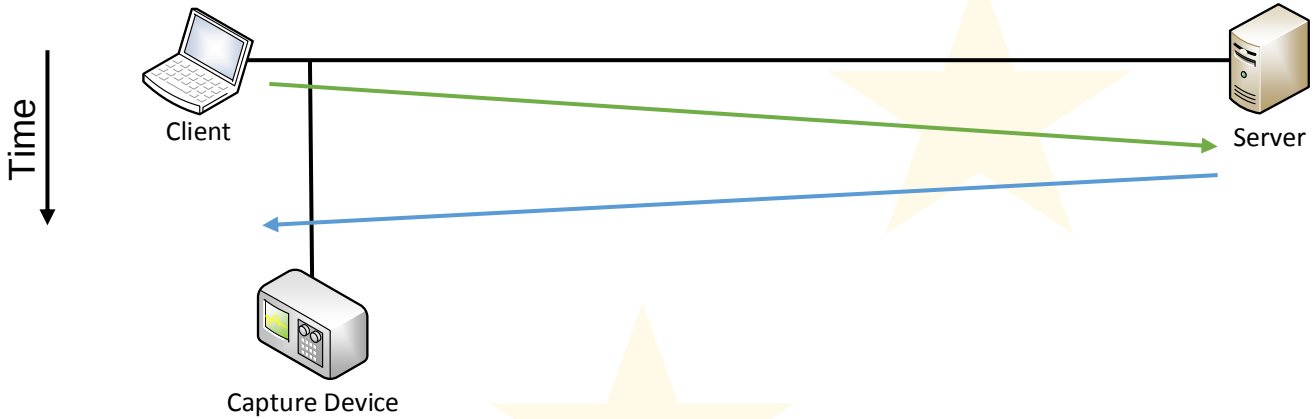
About me?

- 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

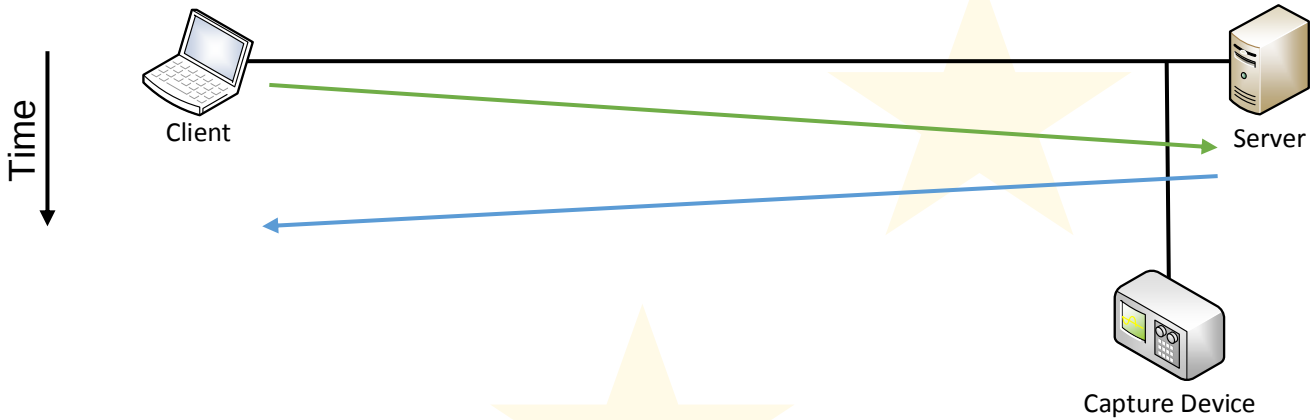
TCP Analysis - Challenges

- Capture Quality („Precision“)
  - See my „Network Capture Playbook“ series at https://blog.packet-foo.com
- Capture Location
  - Client
  - Server
  - Somewhere in the middle

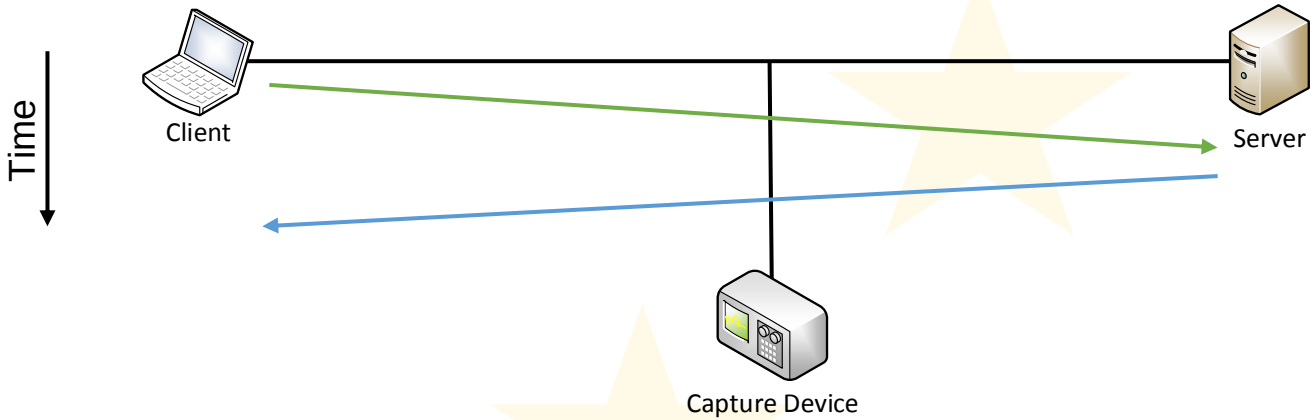
Capture Location - @Client



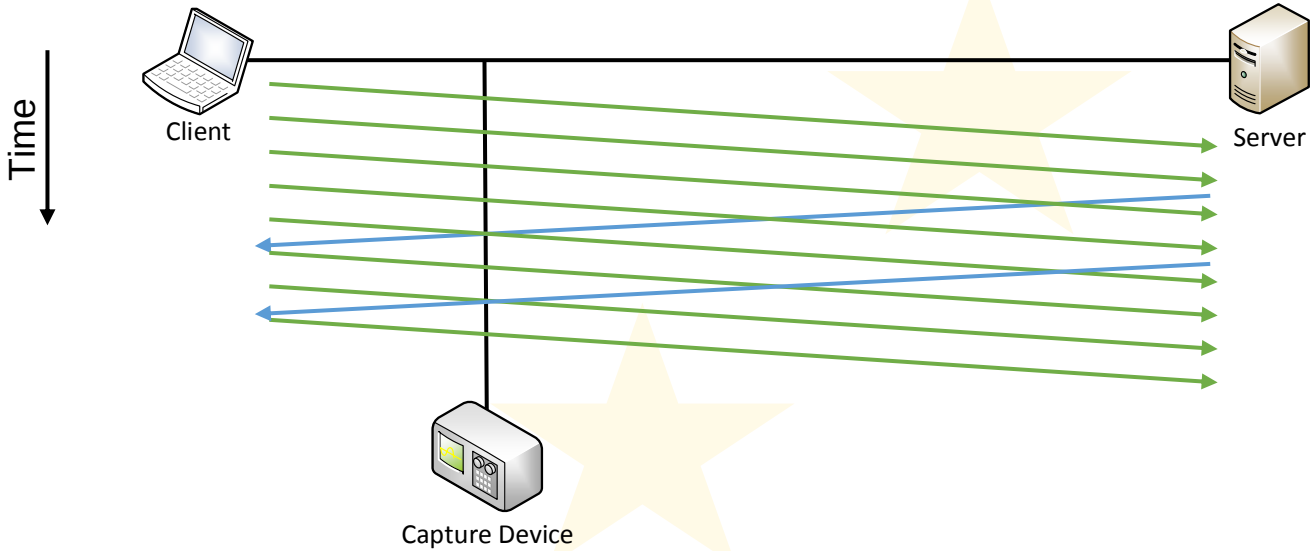
Capture Location - @Client



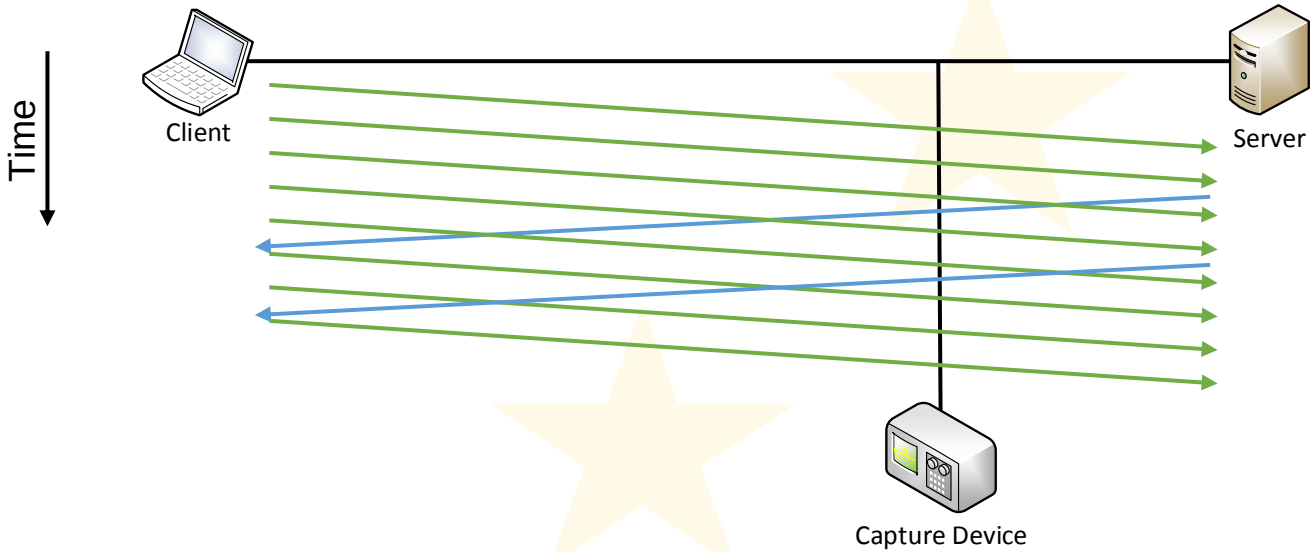
Capture Location - @Client



Capture Location - Effects



Capture Location - Effects



Some Guidelines

- Watch out for iRTT
  - Only available when the handshake is in the trace
- Isolate TCP connections
  - 5-Tuple
  - Stream Index
- Know your capture location
  - If you don't, determine it from the trace if possible

Let's dive into some PCAPs...

No.	IF	Source	Destination	Protocol	Info	Lengtl	Delta Time	Re
74716	0	192.168.0.1	10.10.10.1	TCP	49161 → 1494 [ACK] Seq=10233220 Ack=541211962 Win=4051 Len=0	64	0.203048	28
74717	0	10.10.10.1	192.168.0.1	TCP	1494 → 49161 [PSH, ACK] Seq=541211962 Ack=10233220 Win=62933…	72	0.000665	28
74718	0	10.10.10.1	192.168.0.1	TCP	1494 → 49161 [PSH, ACK] Seq=541211980 Ack=10233220 Win=62933…	1514	0.013098	28
74719	0	10.10.10.1	192.168.0.1	TCP	1494 → 49161 [PSH, ACK] Seq=541213440 Ack=10233220 Win=62933…	1512	0.000013	28
74720	0	192.168.0.1	10.10.10.1	TCP	49161 → 1494 [ACK] Seq=10233220 Ack=541214898 Win=1115 Len=0	64	0.001113	28
74721	0	10.10.10.1	192.168.0.1	TCP	[TCP Window Full] 1494 → 49161 [ACK] Seq=541214898 Ack=10233…	1169	4.997794	28
74722	0	192.168.0.1	10.10.10.1	TCP	[TCP ZeroWindow] 49161 → 1494 [ACK] Seq=10233220 Ack=5412160…	64	0.174049	28
74723	0	10.10.10.1	192.168.0.1	TCP	[TCP ZeroWindowProbe] 1494 → 49161 [ACK] Seq=541216013 Ack=1…	60	0.415964	28
74724	0	192.168.0.1	10.10.10.1	TCP	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 49161 → 1494 [ACK]…	64	0.000900	28
74725	0	10.10.10.1	192.168.0.1	TCP	[TCP ZeroWindowProbe] 1494 → 49161 [ACK] Seq=541216013 Ack=1…	60	0.839138	28
74726	0	192.168.0.1	10.10.10.1	TCP	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 49161 → 1494 [ACK]…	64	0.000882	28
74727	0	10.10.10.1	192.168.0.1	TCP	[TCP ZeroWindowProbe] 1494 → 49161 [ACK] Seq=541216013 Ack=1…	60	1.684226	28
74728	0	192.168.0.1	10.10.10.1	TCP	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 49161 → 1494 [ACK]…	64	0.000866	28
74729	0	10.10.10.1	192.168.0.1	TCP	[TCP ZeroWindowProbe] 1494 → 49161 [ACK] Seq=541216013 Ack=1…	60	3.356345	28
74730	0	192.168.0.1	10.10.10.1	TCP	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 49161 → 1494 [ACK]…	64	0.004764	28
74731	0	10.10.10.1	192.168.0.1	TCP	[TCP ZeroWindowProbe] 1494 → 49161 [ACK] Seq=541216013 Ack=1…	60	6.712657	28
74732	0	192.168.0.1	10.10.10.1	TCP	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 49161 → 1494 [ACK]	64	0.000885	28

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