Advanced TCP Troubleshooting

#sf24us

Jasper Bongertz
Head of CSIRT
G Data Advanced Analytics

About me

#sf24us

Working at G Data Advanced Analytics, Germany

- Principal Network Security Specialist
- Head of the CyberSecurity Incident Response Team (CSIRT)

Network analysis & forensics since 2003

- NetXRay, Sniffer Pro/Distributed, Clearsight
- Ethereal since... uh... version 0.9something

Creator of Tracewrangler

- www.tracewrangler.com or www.pcapwrangler.com

Topics

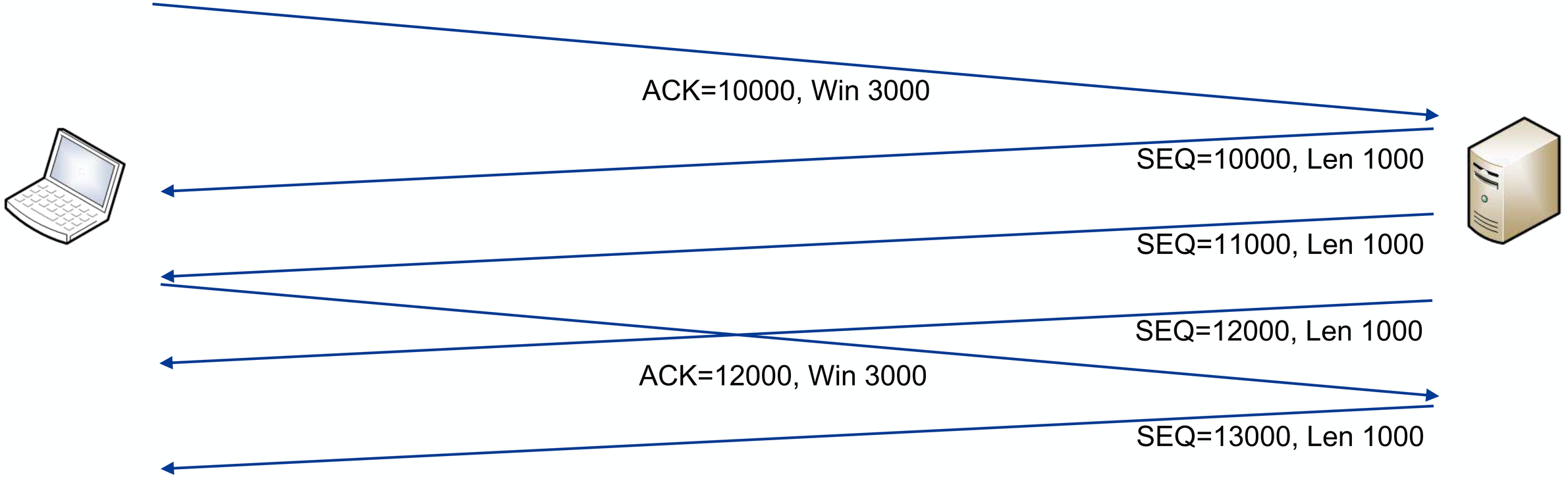
- Capture Location matters
- Round Trip Time Relevance
- Messages from the other side
- Retransmissions take time

Capture Location matters

1 - Client-Side-Trace.pcapng
1 - Server-Side-Trace.pcapng

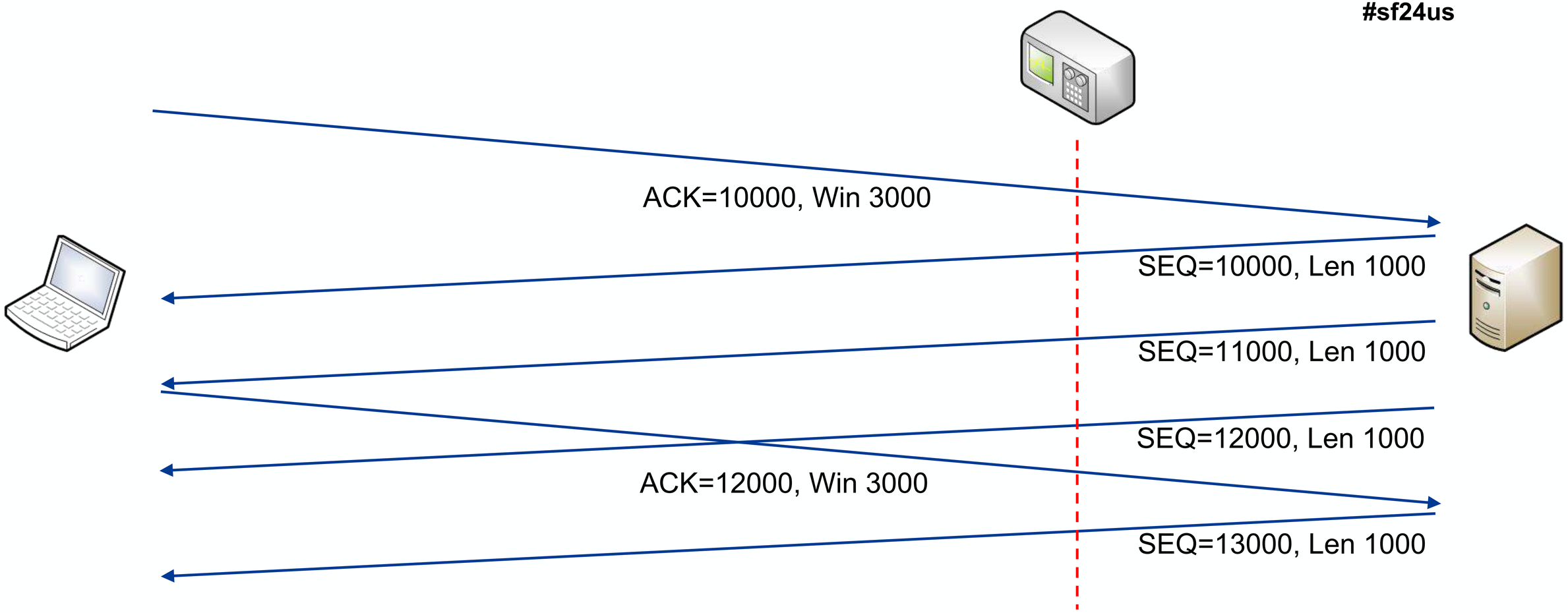
TCP Window Full?

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us



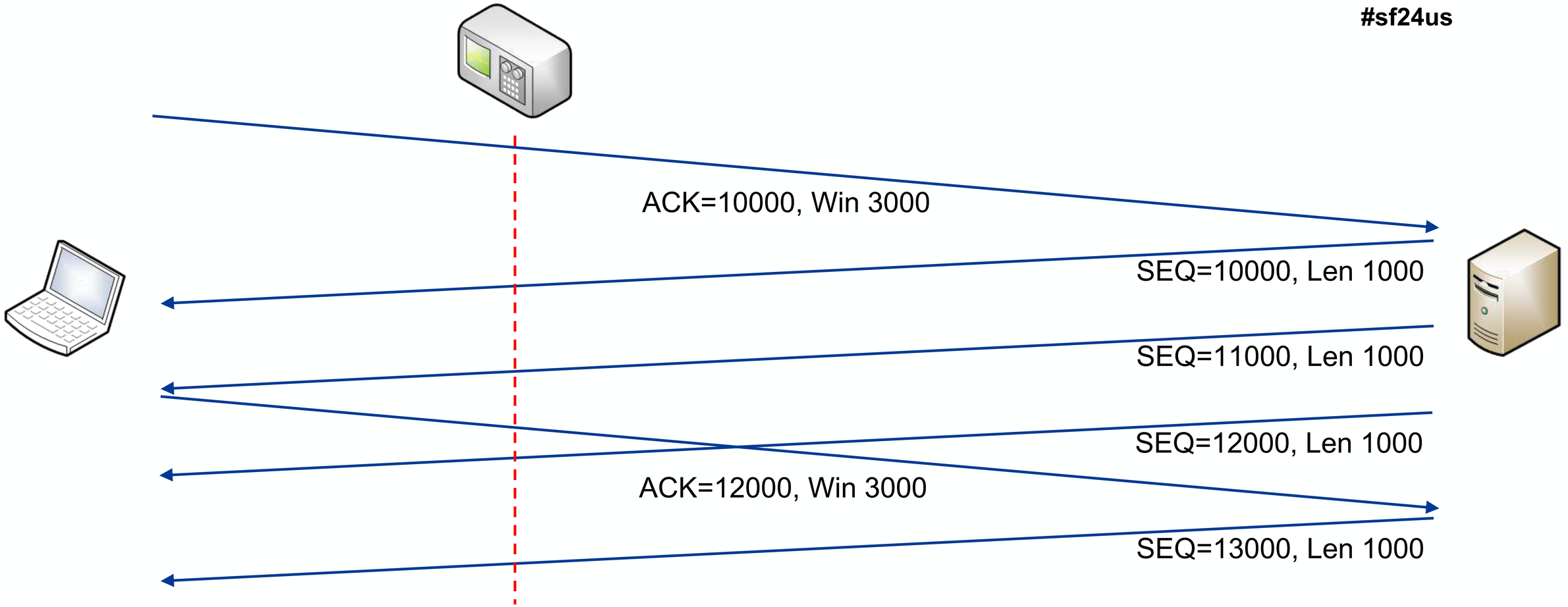
TCP Window Full?

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us



TCP Window Full?

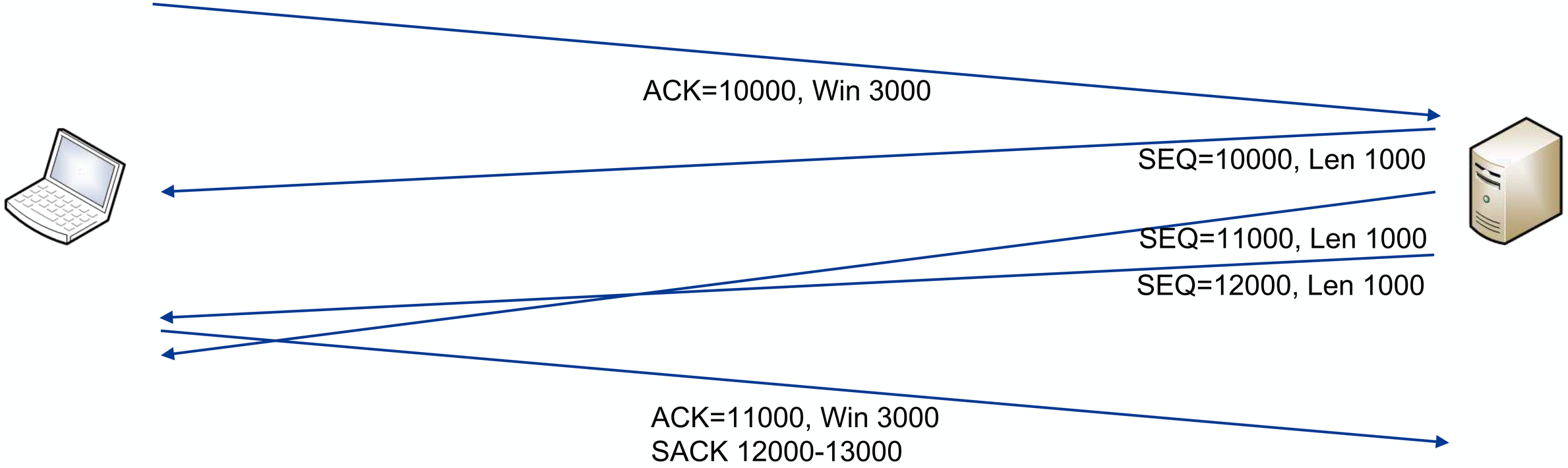
SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us



Round Trip Time Relevance

2 - RTT.pcapng

Packetloss?


ACK=10000, Win 3000
SEQ=10000, Len 1000
SEQ=11000, Len 1000
SEQ=12000, Len 1000
ACK=11000, Win 3000
SACK 12000-13000

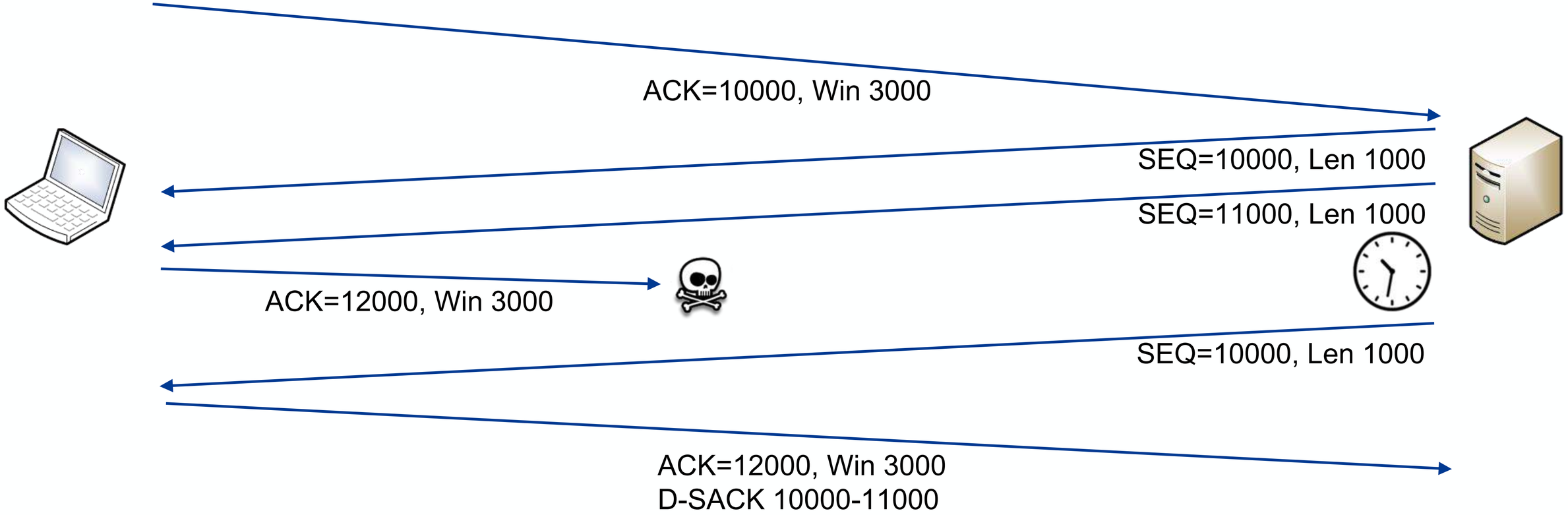
Messages from the other side

3 – D-SACK Example.pcapng

Hey, TMI!

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

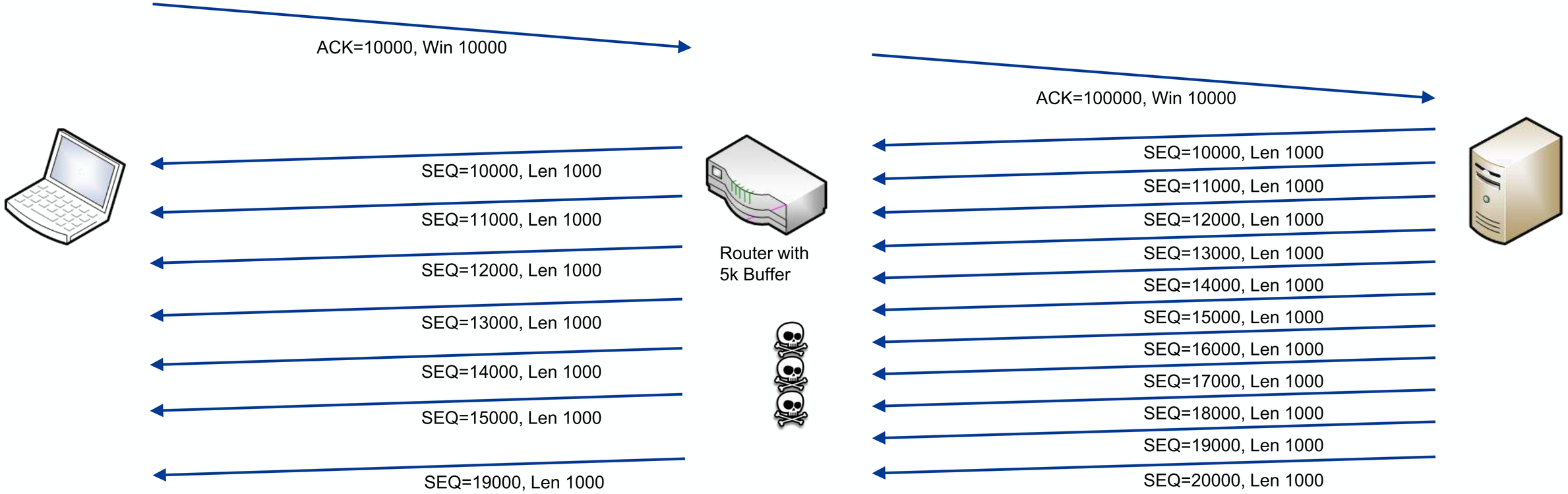


Retransmissions take time

4 - FTP with 87 MBit Throughput.pcapng

Buffer Bloat

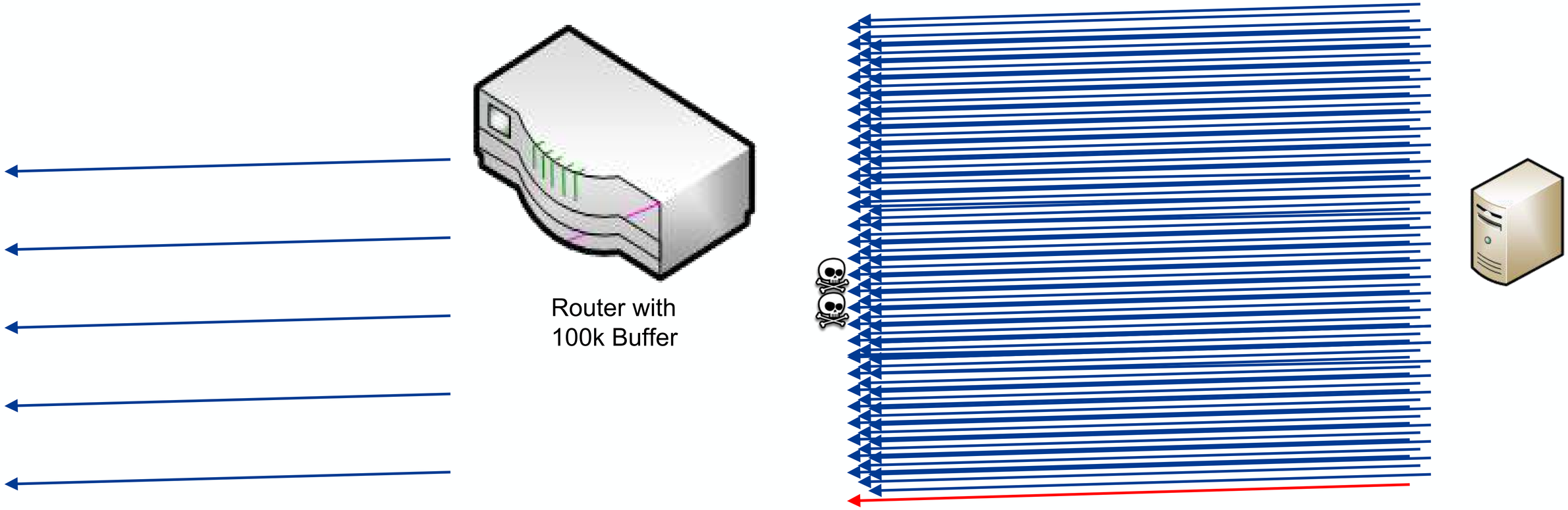
SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

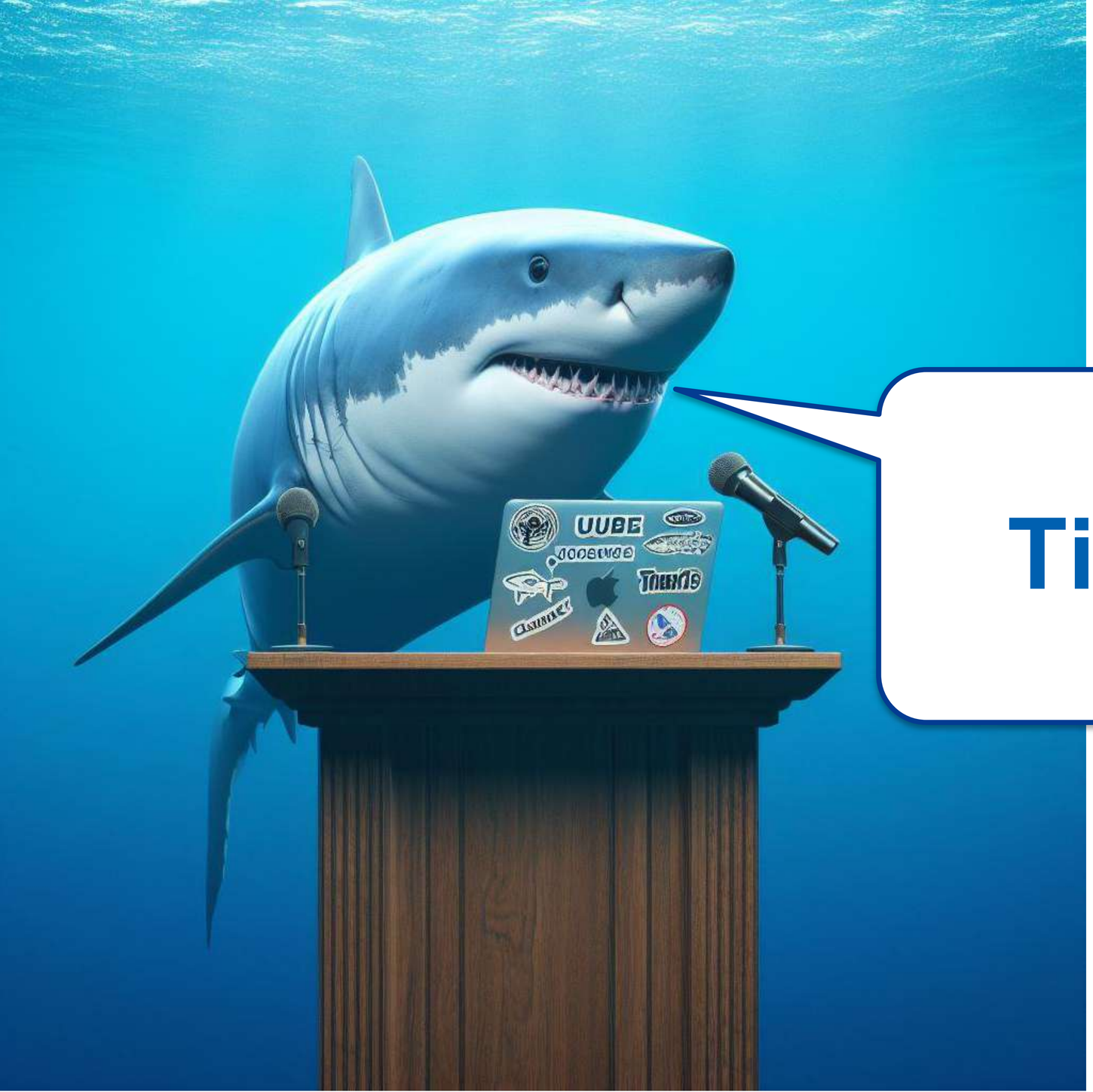


Bloat – Bigger Buffer?

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us





SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

Time for Q & A