SharkFest'17 US

Using Wireshark to Solve Real Problems for Real People

Step-by-Step Real-World Case Studies in Packet Analysis

Kary Rogers
Director, Staff Engineering | Riverbed Technology

SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017

SharkFest'17 US

Packet A(nalysis)-Team

Helping strangers on the Internet

Kary Rogers
PacketBomb.com

Slow Network Tput for the First 6.5 Seconds

- Post on /r/networking
- Rack of 7 Dell PowerEdge servers
- 1Gbps TOR switch
- Low throughput
- Initial delay of 6.5 seconds
- Troubleshooting for over a month
- Where‘s the pcap?

6.5 Second Delay Take Aways

- Learn the basics of packet analysis
- Add TCP seq numbers to columns
- Have a delta column
- Set a Time reference
- Learn TCP/IP basics
  - PMTUD
  - MTU probing - /proc/sys/net/ipv4/tcp_mtu_probing

Slow FTP Upload

- Replaced Fortigate firewall with new Checkpoint
- Video team complains of slow FTP upload to London
- NetEng team generally doesn‘t deal with many perf issues
- ~5Mbps now, was ~20Mbps before
- To the pcaps!

Slow FTP Upload Take Aways

- Always look at RTT
- Latency is a huge factor for some apps/protocols
- PSH bit can be a buffer size indicator
- Bytes in flight should reach BDP

Slow Web Proxy

- Web proxy isn‘t giving expected performance – same as without
- UI says it was a cache hit
- Lab testing environment

Slow Web Proxy Take Aways

- Always look at RTT
- Tcptrace stream graph is your friend
- Scratch the itch – be thorough
- Work through the layers – don‘t forget layer 2

Contact

- kary@packetbomb.com
- @packetbomb
- Packetbomb.com