Hansang Bae
A-7: Wireshark in the Large Enterprise

Director, Citi (f.k.a Citigroup)

hansang@gmail.com

This session came about due to feedback from 2011 Trace file (deepdive.zip)

https://www.box.com/s/24c25c3109ec54777c2e
A7- Wireshark in the Large Enterprise

- Interview the right user
  - Often times, you will find that problem statements are inaccurate after it has been filtered by several users/departments.
  - Stick to the “chief complaint” and focus on the problem.
- Be liberal in what you capture; be strict in what you analyze
- Develop a “pre-flight” checklist and go through it all the time.
  - My favorite technique?
    - Use relative sequence numbers
    - Must add a delta column
    - Add a LENGTH field
    - Use “tcp.analysis.flags” and “Apply as a column”
    - Add Cumulative Bytes, and use Time Reference markers
    - Use multiple profiles to convenience (real/relative seq, etc.)
    - Always sort by delta column
A user presents with slow application experience.
  - Rule out the usual suspects (duplex mismatch)

• Be liberal in what you capture; be strict in what you analyze

• Be judicious because you can’t analyze everything. Only experience will tell you what the “right” filter is.

• This is a simple problem, but without the right capture filter, it would have been nearly impossible to solve.
A7- Wireshark in the Large Enterprise

- A remote location is experiencing BGP timeouts.
- Operations is having response time issues with the router
  - Rule out the usual suspects “sho proc cpu | excl 0.00”, “sho proc cpu history”, “sho proc cpu sorted”
- If someone told you bgp is dropping and the router is sluggish, what would you suspect?
- But surprisingly, no one was complaining.
A7- Wireshark in the Large Enterprise

• An application takes forever to load.
• Usual problems are?
• What can we fix?
• What can’t we fix (quickly)?
Our interface to the SaaS vendor is slowing down.
SaaS brings unique challenges of its own.
Everything past your network diameter becomes a “cloud”
Packet capture placement can become tricky.
You have to learn how to coax the information from incomplete trace files.
Use Occam’s Razor!