SharkFest'22 US
Kansas City, MO
July 9-14

#sf22us

Troubleshooting Fundamentals

Hansang Bae
zscaler, inc.

Hello!

SharkFest'22 US
Kansas City, MO
July 9-14

#sf22us

My name is Indigo Montoya..

You killed my father, prepare to die!

Hello!

My name is ***Hansang Bae***

https://youtube.com/hansangb

Trace Files: https://bit.ly/HSB-Sharkfest

Email: hbae@protonmail.com

Fundamentals

- Fundamentals
  - More fundamental
- Fundamentals
  - More fundamental
- It's more art than science
- Sorry, there's no compression algorithm for experience.

WIRESHARK™
UNIVERSITY

Capturing strategy

- Capturing SYN-SYN/ACK is important. But may not be an option
- Don't do full packet capture if it's encrypted and lack the key. But not all "snaplen" is the same
- Demarcation between transactions
    - Use ping with different packet size
    - ping as a calculator

Location, Location, Location

- Where are you capturing from? It matters (giant pkts)
    - https://blog.packet-foo.com/2015/08/frame-bytes-vs-frame-file-headers/
- Snaplen can confuse some tools and throw off any BW calculations. Know your tool limitations
- You may never know. Depend on circumstantial evidence.
    - You're trying to get a murder conviction w/o a body
- Use MAC addresses, TTL, VLAN tags, syn vs syn-ack vs ack, serialization delay
- Use "naked ack" if you can. Be careful of delayed ack/OS.