Wireshark In the Large Enterprise

Hansang Bae
Director – Product Architecture
Hansang.bae@riverbed.com

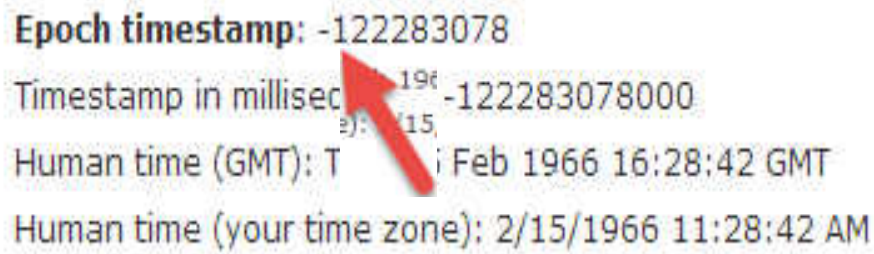
Due to an error in video recording, this session was not recorded. I will cover the trace files in separate recordings – give me a month. The last and most interesting trace will be covered in 2014!!!

Information

YouTube Channel with older sessions etc.

www.youtube.com/hansangb

ww



NET/NET = I'm older than epoch, the beginning of time

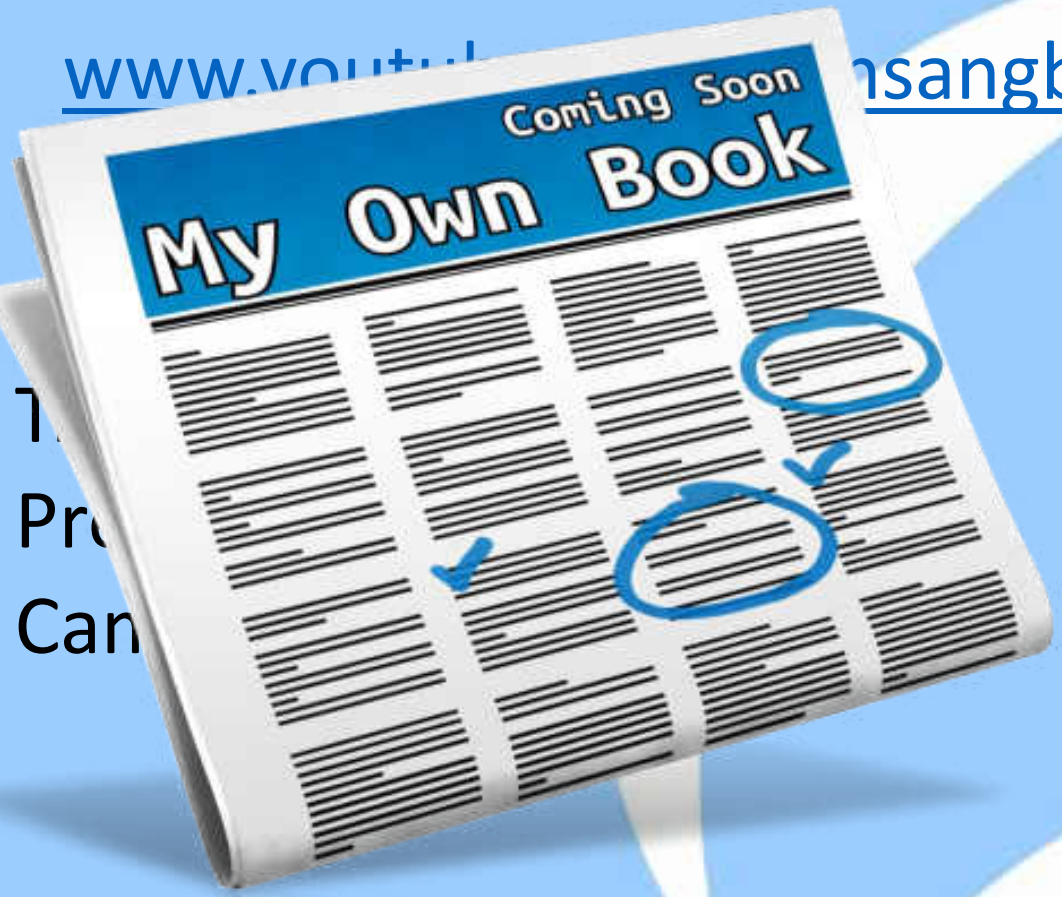
Q4 2014 Information (pester me - *PLEASE*)

YouTube Channel with older sessions etc.

www.youtu nsangb

ww

- T
- Pr
- Can



Slow Throughput, Not always…what you think.

- Old medical school saying: When you hear hooves beating, think horses and not zebras!
- Server SA reports extreme slowness during file transfers
  - What are the top issues that come to mind?
  - Server SA started a ping script and in it showed…..
- Lessons Learned:
  - Learn to recognize what should and should not change as you go through the trace files.
  - RFC1323 was not in play because they are on the same switch!
  - Take a few minutes to scan the trace files. Learn to trust your brain's ability to spot differences.
  - Know how protocols work so you can rule out red-herrings. This is what separates "techs" from "engineers"
  - Try not to filter. You might have missed the "arp" frames in this trace. This is different than capturing in "promiscuous" mode.

Training the Brain

SUNDAY

MONDAY

TUESDAY

WEDNESDAY

THURSDAY

FRIDAY

SATURDAY

Training the Brain

First signs of danger

- Be on the look out for excessive use of PSH
- The more PSH bits there are, the more chances that it will be chatty
- Previous topics (window size, etc.) still is in play.
- Buffer tearing
  - This is where the application uses PSH bits to set the amount of data “chunk” it is willing to release to the network.
  - It’s the way apps work, you can’t fight it.

Murder Conviction, No Body

- Rule out the usual suspects
  - Window size
  - Buffer tearing
  - RFC1323
- Recognize false positives
  - Sometimes you just have to assume.
- Know the RFCs/Protocols to identify things that are ABSOLUTELY wrong.