SHARKFEST '12

Wireshark Developer and User Conference

Jasper Bongertz

Senior Consultant, Fast Lane GmbH

Network Analysis, IT Security, Virtualization

Preflight Check

- My default column configuration:
  - No, Source, Destination, Protocol, Info, Size, Cummulative Bytes
  - Delta Time Displayed, Relative Time, Absolute Time
- TCP decode settings
  - Disable TCP stream reassembly
  - Relative Sequence numbers, Track bytes in flight
- Color settings
  - Set to indicate interesting stuff

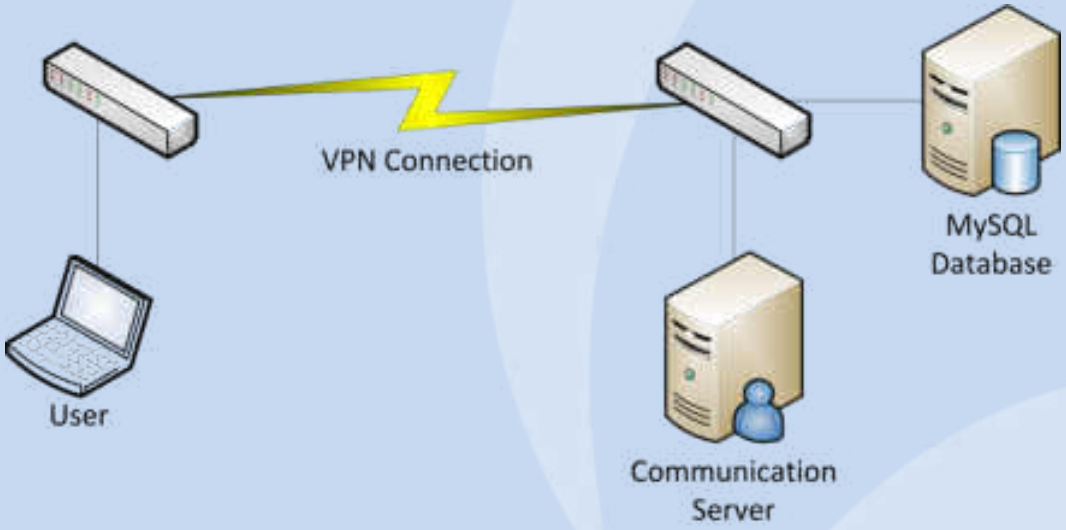
A word on PCAPng

- With Wireshark 1.8, PCAPng becomes the new default file format
  - installing over existing configurations might keep the old setting!
- PCAPng advantages:
  - Capture on multiple interfaces
  - File and frame comments
  - Store name resolution info with the file
  - Store statistical information, like dropped frame count

Case 01 – „Let's talk... Not!"

Case 01 – „Let‘s Talk... Not!“

- **Scenario**: Determine why a communication server doesn‘t send notification messages
  - Some sort of Growl/Snarl messaging system



Case 02 – „Industrial TCP... Yuck!“

Case 02 – „Industrial TCP... Yuck!“

- **Scenario**: Determine what is happening with the communication between a server and a ModBus device
  - Server talking to a device adjusting a huge cooling system
- Trace was provided by the customer
  - Communication is basically point to point, so no network diagram needed
  - But the network structure was pretty... chaotic...

Case 03 – Citrix vs. Thin Client

Case 03 – Citrix vs. Thin Client

- **Scenario**: users complain about bad Citrix Remote Desktop performance
  - A.k.a. ICA Protocol, Metaframe, XenApp
  - Customer had deployed thin client devices for the users
  - Screen froze for almost a minute in one case

Case 03 – Analyzing Citrix

- ICA protocol documentation is not publicly available
- There are some analyzers that can more or less decode it
  - Clearsight, Sniffer Pro, maybe others
  - Unfortunately, their decodes are pretty unreliable
- Analyzing Citrix in Wireshark is limited to
  - Decoding and verifying packet priority tagging
  - TCP behavior

Case 03 – Analyzing Citrix

- Let‘s take a look...

Case 04 – Filer Trouble

Case 04 - Filer Trouble

- Customer sends trace files
  - Filer seems to slow down sometimes
  - Customer had already worked through some of the files
  - Guess what the vendor said?
- Let‘s see...

Thank you !