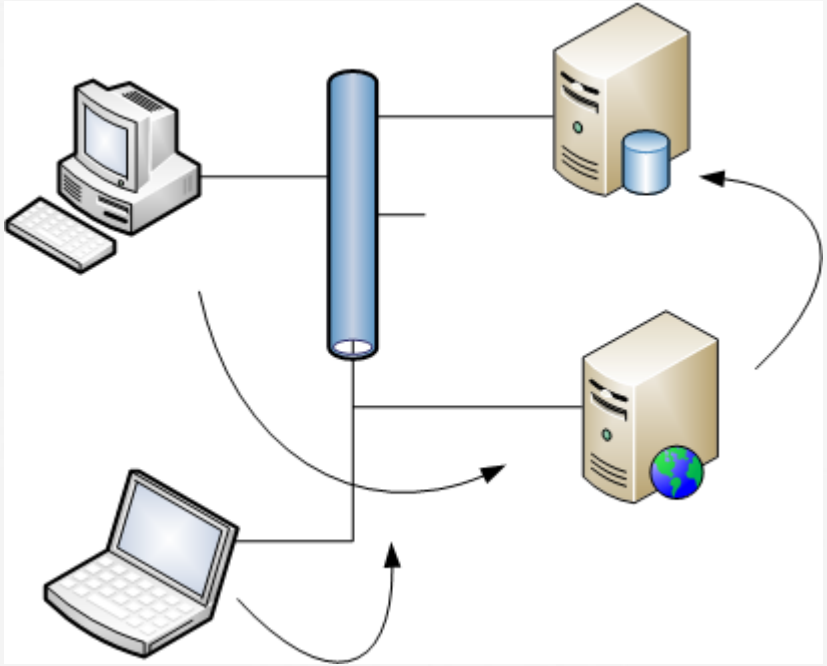
Analyzing an Issue with tshark

Analyzing an Issue with tshark

- Solving problems with tshark (command line)
- First, why use it?
  - Many people use command line for scripting purposes
  - Small footprint, flexible, and loads on multiple machine types (Windows, Linux, etc.)
- Types of issues
  - Network traffic
  - Failed service

Analyzing an Issue with tshark



Analyzing an Issue with tshark

- Solving problems with tshark (command line)
- Issue 1: Network Traffic
  - Delay coming form web server, not really a network issue, only manifested that way; Wireshark ruled it out
- Issue 2: Failed Service
  - Certificate problem caused this issue

Analyzing an Issue with tshark

```
k=2921 Win=35040 Len=0
 32.999887 173.194.123.8 -> 192.168.73.128 TLSv1 1052 Certificate
 32.999900 192.168.73.128 -> 173.194.123.8 TCP 54 54788 > https [ACK] Seq=173 Ac
k=3919 Win=37960 Len=0
 33.015769 192.168.73.128 -> 173.194.123.8 TLSv1 212 Client Key Exchange, Change
 Cipher Spec, Encrypted Handshake Message
 33.016118 173.194.123.8 -> 192.168.73.128 TCP 60 https > 54788 [ACK] Seq=3919 A
ck=331 Win=64240 Len=0
 33.022467 173.194.46.116 -> 192.168.73.128 TLSv1 182 Application Data
 33.022493 173.194.46.116 -> 192.168.73.128 TLSv1 87 Application Data
 33.022824 173.194.123.8 -> 192.168.73.128 TLSv1 349 New Session Ticket, Change
Cipher Spec, Encrypted Handshake Message, Application Data
 33.023005 192.168.73.128 -> 173.194.46.116 TCP 54 33806 > https [ACK] Seq=5953
Ack=259765 Win=65535 Len=0
 33.024124 192.168.73.128 -> 173.194.123.8 TLSv1 107 Application Data
 33.024247 192.168.73.128 -> 173.194.123.8 TLSv1 910 Application Data
 33.024315 173.194.123.8 -> 192.168.73.128 TCP 60 https > 54788 [ACK] Seq=4214 A
ck=384 Win=64240 Len=0
 33.024405 173.194.123.8 -> 192.168.73.128 TCP 60 https > 54788 [ACK] Seq=4214 A
ck=1240 Win=64240 Len=0
 33.076867 173.194.123.8 -> 192.168.73.128 TLSv1 333 Application Data
 33.077497 173.194.123.8 -> 192.168.73.128 TLSv1 1514 Application Data
 33.077511 192.168.73.128 -> 173.194.123.8 TCP 54 54788 > https [ACK] Seq=1240 A
ck=5953 Win=40880 Len=0
```

Questions?