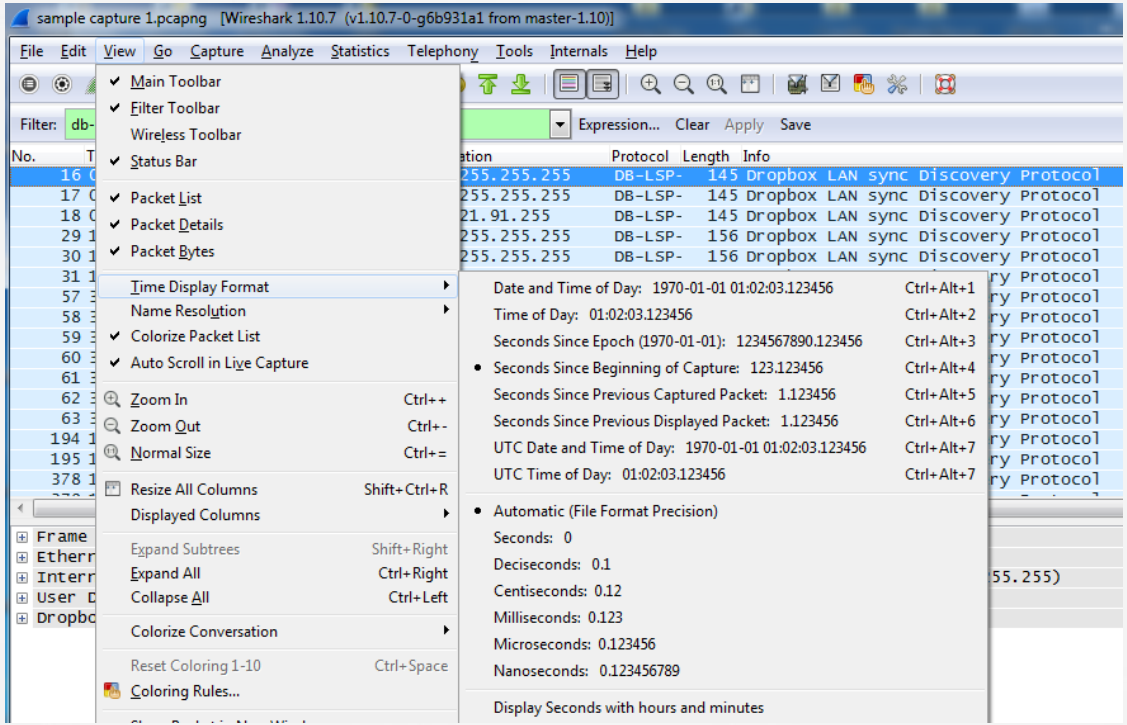
Timestamps & Time Values

Wireshark Timestamps

- **Timestamps**
  - Used to mark the capturing of your packets
  - Can be converted to different time formats for viewing
- **Time delta**
  - The time it takes to travel from source to destination and back again, used for troubleshooting latency issues

Wireshark Timestamps



Wireshark Timestamps

- **You can adjust the time format as follows:**
  - Absolute time and time of day when packet captured
  - Absolute time and time (no date) when packet captured (relative time)
  - Seconds since beginning of capture (relative time)
  - Seconds since previous captured packet (relative time)
  - Seconds since previous displayed packet (relative time)
  - Seconds since epoch (relative time)

Wireshark Timestamps

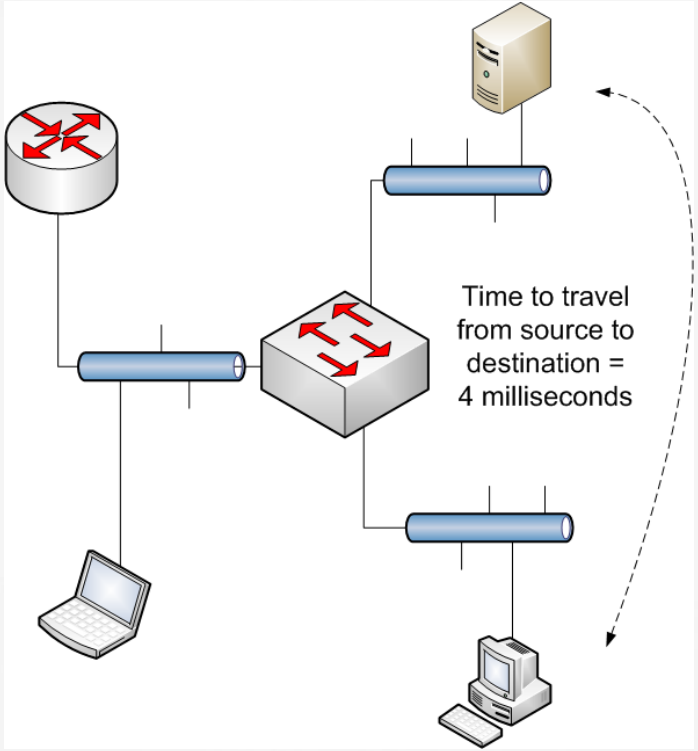
- Precision in the time value
  - Automatic
  - Specific settings

Wireshark Timestamps

Checking the delta

- When you need to find latency in your network
- Check application response time
- May require Wireshark on both source and destination hosts
- May require filtering of the data on both hosts

Network Lab



Questions?