



# 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

The screenshot shows the Wireshark 1.10.7 interface. The 'View' menu is open, displaying the 'Time Display Format' submenu. The main window shows a packet capture list with columns for No., Time, Protocol, Length, and Info. The filter is set to 'db-'. The packet list shows several entries for 'DB-LSP' with a length of 145 or 156 bytes, identified as 'Discovery Protocol'.

No.	Time	Protocol	Length	Info
16	0.000000	DB-LSP	145	Dropbox LAN sync Discovery Protocol
17	0.000000	DB-LSP	145	Dropbox LAN sync Discovery Protocol
18	0.000000	DB-LSP	145	Dropbox LAN sync Discovery Protocol
21	91.255	DB-LSP	145	Dropbox LAN sync Discovery Protocol
29	1.255	DB-LSP	156	Dropbox LAN sync Discovery Protocol
30	1.255	DB-LSP	156	Dropbox LAN sync Discovery Protocol

**Time Display Format Submenu:**

- Date and Time of Day: 1970-01-01 01:02:03.123456 (Ctrl+Alt+1)
- Time of Day: 01:02:03.123456 (Ctrl+Alt+2)
- Seconds Since Epoch (1970-01-01): 1234567890.123456 (Ctrl+Alt+3)
- Seconds Since Beginning of Capture: 123.123456 (Ctrl+Alt+4)
- Seconds Since Previous Captured Packet: 1.123456 (Ctrl+Alt+5)
- Seconds Since Previous Displayed Packet: 1.123456 (Ctrl+Alt+6)
- UTC Date and Time of Day: 1970-01-01 01:02:03.123456 (Ctrl+Alt+7)
- UTC Time of Day: 01:02:03.123456 (Ctrl+Alt+7)
- Automatic (File Format Precision)
  - Seconds: 0
  - Deciseconds: 0.1
  - Centiseconds: 0.12
  - Milliseconds: 0.123
  - Microseconds: 0.123456
  - Nanoseconds: 0.123456789
- Display Seconds with hours and minutes

# 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

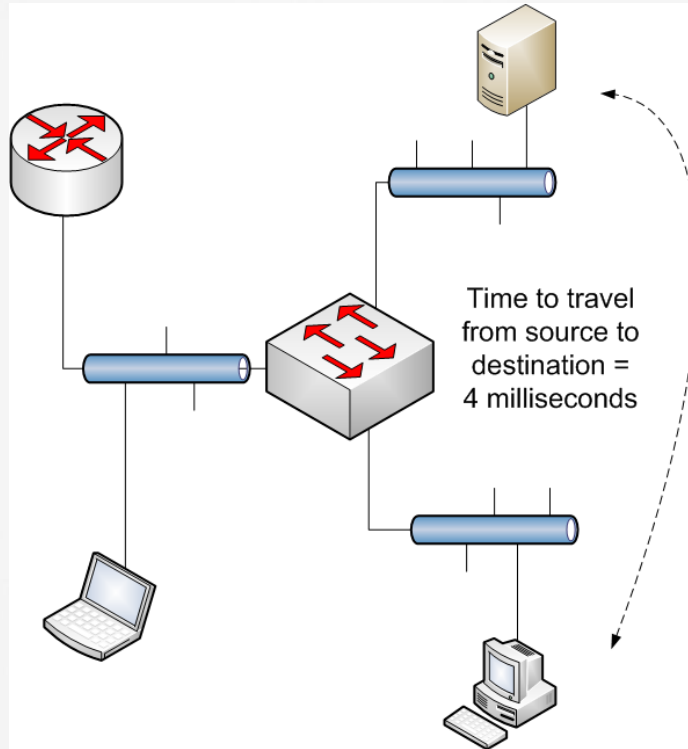
- Automatic
- Specific settings

# 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?