Tribute to Wireshark

Why the Swiss army knife Wireshark isn´t enough any longer, ...and what to do instead!

Wireshark is fantastic expert tool for deep packet-level debugging!

But modern automotive networks, zonal E/E architectures and software-defined vehicles (SDV) are real-time, safety-critical, and schedule-driven.

Validating them is no longer about “can I decode this frame?”

It’s about “does every time-sensitive stream meet its latency/jitter/reliability guarantees under load and faults, across the whole car?”

That job demands time-synchronized, multi-point, stream-aware, standards-literate tooling.

Modern validation tools MUST do this; Wireshark doesn’t.

What changed?

from “packets on a bus” to “real-time distributed systems”

Validation now requires **system-level evidence** that these guarantees hold **end-to-end** and **over time**, not just proof a packet arrived. It needs to be done across all links and correlated throughout its time “on the wire”.

Zonal/SDV networks combine:

- **Time-Sensitive Networking (TSN)** features (802.1AS/gPTP, Qbv TAS, Qav/CBS, Qcc, Qci PSFP, Qbu/Qbv preemption, 802.1CB FRER, etc.)
- **Mixed-criticality traffic** (control loops, perception, diagnostics, over-the-air updates, infotainment)
- **Service-oriented stacks** (SOME/IP, DoIP) riding on **deterministic Ethernet**
- **Hard budgets** (e.g., <2 ms E2E for control; <50 µs hop latency variance; five-nines availability), legacy CAN communication, A²B communication – all correlated!

The (data) elephant in the room:

Modern vehicles **generate *huge* network traces**: multi-gig Ethernet backbones, dozens of cameras/sensors, continuous logging, and OTA/service traffic. Wireshark is brilliant for interactive, packet-level debugging on *megabyte-to-gigabyte* captures—but it doesn’t scale to *hundreds* of gigabytes or terabytes. Here’s why:

The math (linear, and brutal) on average PCs

- **Wireshark open/prep speed:** takes ~ **20 s per GB**
- **“Add one simple filter” cost:** × 1.7 (≈ **+70%** time on top)

Wireshark average times needed to open those files below*
(this is just to open NOT to analyse it!)

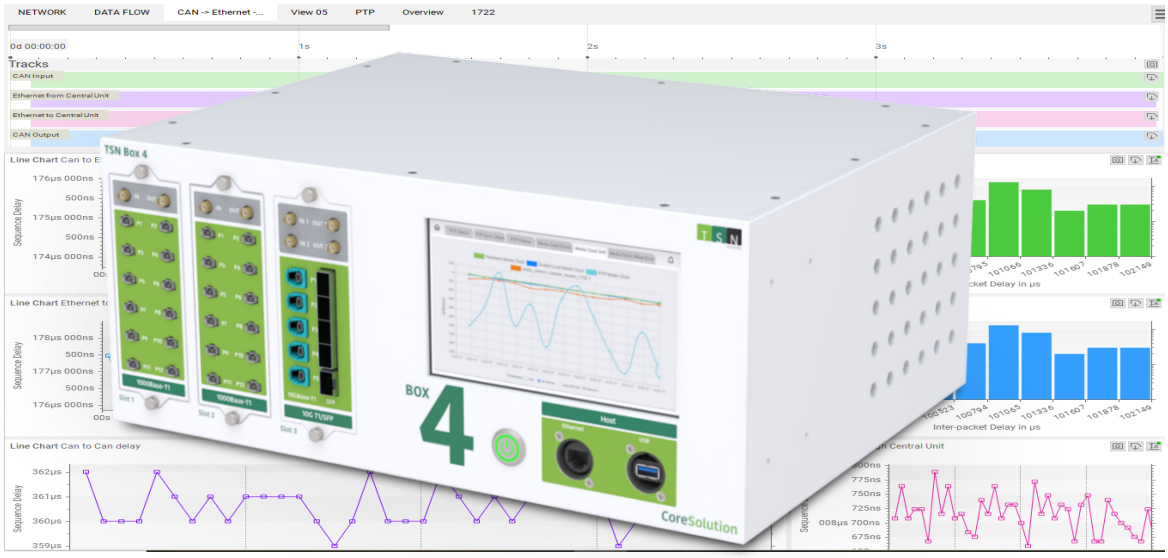
File sizes	Open only (20 s/GB)	With 1 simple filter (×1.7)
500 GB	2 h 46 m	4 h 43 m
1 TB (1000 GB)	5 h 33 m	9 h 27 m
4-min capture @ (~3 GB/s ≈ 720 GB)	4 h 00 m	6 h 48 m

These times are just to ingest/index data once. The numbers describe examples of data traces in SDV validation. *Any filter tweak or view change repeats big chunks of this cost during analysis*

**find more insights in the paper “Why Wireshark Collapses Under Modern Car Data Volumes” also posted on https://tsn.systems/en/downloads/#c1148*

TSN Systems CoreSolution 4

specially developed modern toolchain to handle data intense Zone Architecture and SDV Validation



- Integrated Analysis and Filtering (destructive and non-destructive)
- **All** Taps are directly attached to its super fast intenal **2 Terabit/s** PCIe Bus
- **All** Taps **are connected directly to Multi-Terabyte internal high-speed SSDs**
- **Real time processing** and **Real time analysis** is available during and after recording/tapping data
- **Multi Terabyte Project file sizes** can be reviewed and analyzed **instantaneously**
- Any **filter settings** or changes in **Analysers** can happen almost instantaneously and do NOT require long time-intensive data rescans
- The **Project file size** is only limited by the number and sizes of the built in SSDs
- Any modern PC with a Gigabit Ethernet Interface can be attached and run the TSN **CoreSolution Analyser software**
- **Up to 36 x 1Gb (18Taps)** and/or **up to 10 x 10Gb (4 Taps) T1 or T Ports** can be used simultaneously

Wireshark vs. CoreSolution 4 Fact Sheet

	Gigabytes	Load T. (s)	Filter Ch.	Time (s)	Time (h)	Tests	Time Mh	Time MM	Cost EU**	Cost World***
Wireshark	25	500	4	3400	2	100	194	1.22	12 056	4 861
CoreSolution	25	1	4	6.8	1	100	100	0.63	6 212	2 505
Wireshark	250	5 000	4	34 000	10	100	1044	6.53	64 756	26 111
CoreSolution	250	1	4	6.8	1	100	100	0.63	6212	2 505
Wireshark	1 000	20 000	4	136 000	39	100	3878	24.24	240 422	96 944
CoreSolution	1 000	1	4	6.8	1	100	100	0.63	6212	2 505

The table compares processing times for Wireshark versus TSN CoreSolution across 100 tests with file sizes of 25 GB, 250 GB, and 1 TB.

Each test assumes four filter changes plus one hour of analysis.

As file size increases, the time gap grows roughly linear:

* At 25 GB, Wireshark takes more than twice as long as CoreSolution.
  (If heavier filtering is required—e.g., 12 filters per test—the factor nearly doubles to ~4.)

* At 250 GB, the factor rises to **10 times more time spent.**

* At 1 TB, the gap widens to **40 times more time spent.**

Remember, we evaluate only the time factor here!
And this isn't a Wireshark-only issue—it affects the vast majority of test systems and toolchains out there as well a they share Wireshark´s monolithic analysis approach.

If you like to know more about other aspects beyond time spent as well you can find more insights in the paper "Why Wireshark Collapses Under Modern Car Data Volumes" also posted on https://tsn.systems/en/downloads/#c1148

** Cost is calculated on the basis of €62 per engineer (VDA)

***Cost is calculated on the basis of €25 per engineer