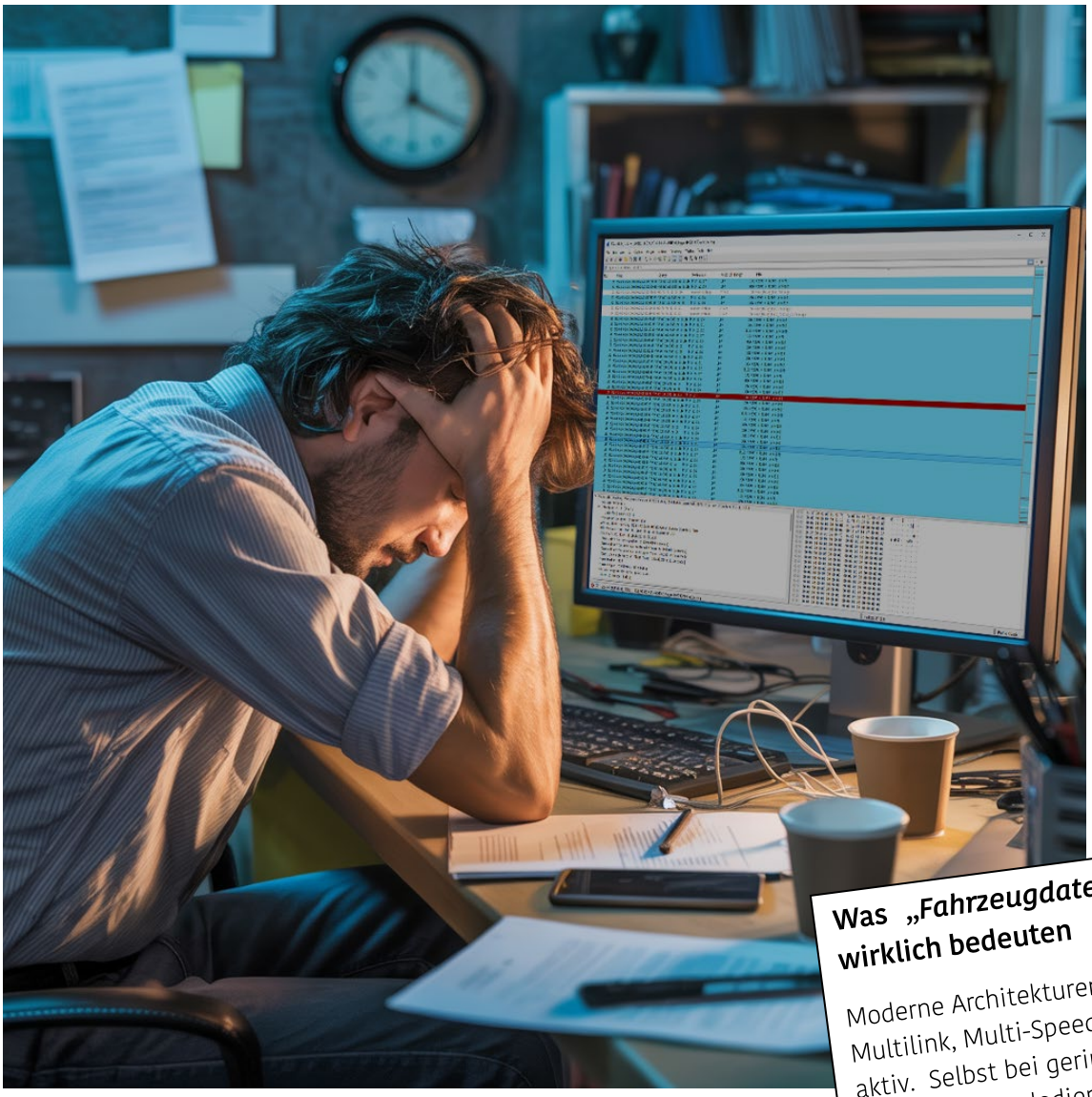

Was „Fahrzeugdaten“ heute wirklich bedeuten

Moderne Architekturen sind Multilink, Multi-Speed und immer aktiv. Selbst bei geringer Auslastung explodiert das Volumen, wenn mehrere Verbindungen gleichzeitig laufen.

„Anklicken. Warten. Wiederholen.”

Warum Wireshark unter der Last moderner Fahrzeugdatenmengen zusammenbricht

Moderne Fahrzeuge generieren Datenverkehr im Umfang eines Rechenzentrums. Bei diesen Volumina verwandelt der Single-File- und Packet-by-Packet-Workflow von Wireshark jede grundlegende Aktion in stundenlange Ausfallzeiten … noch bevor die Analyse überhaupt beginnt.

Die Mathematik dazu ist klar, brutal und unmöglich zu ignorieren.

Das Warten (auch bekannt als „Ihr Tag ist vorbei“)

Zeit zum Öffnen von Standard-„.pcapng“-Dateien anhand der gemessenen Ladezeiten von Standard-PCs:

- 2 GB (~16,5 Mio. Pakete) → 40 s
- 4 GB (~33 Mio. Pakete) → ~ 80 s (~ linear)
- Einen einfachen Filter hinzufügen → ~ +70 % Zeit

Das sind ~ 20 s/GB nur für das Öffnen und Vorbereiten einer Datei.

Skalieren Sie das nun hoch:

Zeit zum Öffnen einer 500-GB-Datei mit Wireshark:

500 GB (~ 2,4 - 5 min durch Antippen mehrerer Links in einem SDV-Netzwerk)

- Nur öffnen: 500 × 20 s = 10.000 s → **2 Stunden 46 Min.**
- Mit einem einfachen Filter: 10.000 s × 1,7 → **4 Stunden 43 Min.**

Zeit zum Öffnen einer 1-TB-Datei mit Wireshark:

1 TB (~ 5–10 Minuten für das Antippen mehrerer Links in einem SDV-Netzwerk)

- Nur öffnen: 1000 × 20 s = 20.000 s → **5 Stunden 41 Min.**
- Mit einem einfachen Filter: 20.000 s × 1,7 → **9 Stunden 40 Min.**

Dies ist nur die Zeit, die zum ***Öffnen einer*** *Testdatei benötigt wird!*

Wir reden hier also über den ersten Import-/Indizierungsdurchlauf. Eine Ansicht anpassen, einen Filter ändern, einen Zeitschnitt erneut scannen ...und ein großer Teil dieser Zeit-Kosten fällt wieder an.

Jede Änderung heist: „Anklicken. Warten. Wiederholen.“

... aber selbst wenn man sich die Zeit dafür nimmt ...

In einer modernen zonalen Architektur eines SDV (Software-Defined Vehicle) erfordert die Validierung mehrere Messonden (Taps) im gesamten Netzwerk, um Zeitstempel zu erfassen und die Testdaten zu korrelieren.

Daten strömen mit mehreren Gigabyte pro Sekunde ein und bringen zwei Hauptherausforderungen mit sich: die Synchronisierung mehrerer Datentaps auf eine gemeinsame Referenzuhr und die Möglichkeit die Daten in einen Standard-PC, schnell genug einzulesen um Paketverluste zu verhindern – insbesondere bei Lastspitzen..

Warum Wireshark (und die meisten anderen Analysemethoden) hier ins Straucheln gerät – und letztlich scheitert

Monolithisches Dateidenken in einer verteilten Welt

Wireshark glänzt bei interaktiven, kleineren Traces:
… eine Netzwerkkarte, ein Span-Port, ein Labortest, ein paar Minuten.

Moderne Fahrzeuge verfügen jedoch über Dutzende von gleichzeitigen Verbindungen mit Hunderten Millionen von Paketen pro Minute. Wenn man all das in ein einziges riesiges PCAPNG stopft, konzentriert sich alles auf einen einzigen I/O- und Indizierungsengpass. Ein PC&NIC sind dafür NICHT ausgelegt.

Erst GUI, dann Indexierung

Die Stärke von Wireshark ist die reichhaltige Benutzeroberfläche auf Paketebene. Seine Schwäche bei großem Umfang besteht darin, dass jede „einfache" Aktion zu einer Lawine an Nacharbeit führt:

- Datei öffnen → Header lesen, Indizes erstellen
- Filter anwenden → Millionen bis Milliarden von Paketen neu bewerten
- Zeitsprung → suchen, Status neu erstellen
- Dekodierungsoptionen ändern → erneut enorme Datenmengen durchsuchen

Wenn jeder dieser Schritte mehrere Stunden dauert, ist der Workflow nicht mehr interaktiv, sondern eine nervenaufreibende und zeitfressende Stapelverarbeitung.

Alles auf Paketebene

Vollständige, bitgenaue Dekodierung für jedes Paket über jeden Link zu jedem Zeitpunkt ist großartig für Root-Cause-Analysen im menschlichen Maßstab.
Im Flottenmaßstab ist das standardmäßig verschwenderisch. Die meisten Fragen brauchen nicht jedes Byte jedes Frames; anfangs zählen Sitzungs/Flow-Fakten, Counter oder Anomalien.

Zuerst den neuralgischen Punkt finden und erst dann tiefer eintauchen!
Paket zuerst bedeutet, dass Sie im Voraus die maximale Rechen- und E/A-Gebühr zahlen, die Sie in der Praxis NIEMALS benötigen.

Die Erfassung ist der einfache Teil

Bei geschätzten ~ 2-3 GB/s benötigen Sie bereits eine Multi-10-GbE-Protokollierung, um Schritt zu halten. Aber nicht nur die Speicherkapazität ist ein echter Engpass, sondern auch die Analyse. Bei Wireshark wird die Analysephase durch Single-Node Parsing, serialisierte GUI-Workflows und Re-Indexierungskosten gedrosselt.

Die Mathematik ist linear. Der Aufwand ist exponentiell.

Das lineare Gesetz des Schmerzes

Wie oben erwähnt, skaliert die Ladezeit ungefähr linear mit der Größe (~ 20 s/GB Basis, +70 % für einen Filter), d. h. eine Verdopplung der Trace-Größe verdoppelt die Wartezeit, in der „nichts passiert".

Die Anzahl der erforderlichen erneuten Öffnungen/Scans steigt jedoch mit der Teamgröße, den gestellten Fragen und den Hypothesenänderungen – sodass der Schmerz sogar noch schneller als linear zunimmt.

Faustregel:

Minuten/Erfassung × GB/s × 20 s/GB × Filtermultiplikatoren = verlorene Stunden.

„Aber wir können doch einfach vorfiltern … oder?"

Vorfiltern setzt voraus, dass Sie bereits wissen, was Sie behalten möchten.

Bei der Validierung, Integration und Feldtriage ist dies jedoch oft nicht der Fall. Das Ergebnis ist entweder:

- Überfilterung → der Fehler wird übersehen oder
- Unterfilterung → Sie haben wieder mehr als 1 TB an Artefakten, die Wireshark nicht interaktiv verarbeiten kann.

„Wie wäre es denn mit einer Aufteilung der Datei in viele kleine?"

Das Aufteilen hilft, einzelne Dateien zu vermeiden, und manchmal werden die Dateien überhaupt geladen, aber es ändert nichts an der Gesamtarbeit. Sie zahlen immer noch 20 s/GB pro Shard, multipliziert mit der Anzahl der Shards, die Sie öffnen, erneut öffnen und miteinander korrelieren müssen.

Nun kommt noch die Zeitausrichtung über Links und Fragmente hinzu – Ihre Stoppuhr läuft weiter.

„Warum nicht einfach tshark verwenden?"

tshark ist für automatisierte Arbeiten von unschätzbarem Wert, verwendet jedoch dieselbe Dekodierungs-Engine.

Headless hilft bei der Automatisierung, nicht beim grundlegenden Durchsatz und beim erneuten Indizieren, wenn sich Fragen ergeben.

Einige Zahlen, die man von nun an berücksichtigen sollten:

Link-Kapazitäten bei 100 % Auslastung (Plausibilitätsprüfung):

- A²B 50 Mbit → 6,25 MB/s
- Eth 10 Mbit → 1,25 MB/s
- Eth 100 Mbit → 25 MB/s
- Eth 1 Gbit → 250 MB/s
- Eth 10 Gbit → 2.500 MB/s

Summe: 2.782,5 MB/s = 2,72–2,78 GB/s → ~ 10 TB/h → ~ 240 TB/Tag

Ein realistischeres Beispiel für eine gemischte Auslastung mit mehreren Verbindungen (jedoch ohne Sättigung):

- A²B (10× bei 60 %)
- Eth 10 M (10× bei 30 %)
- Eth 100 M (10× bei 25 %)
- Eth 1 G (6× bei 25 %)
- Eth 10 G (4× bei 25 %)

Ergebnis: ~ 2.962,5 MB/s ≈ 3 GB/s, ~ 180 GB/min, ~ 10 TB/h, ~ 250 TB/Tag.

Das sind ≈ 24 Gbit/s dauerhaft (etwa 20–25 Gbit/s).

Die Vier-Minuten-Barriere

Bei ~ 3 GB/s entspricht eine 4-minütige Aufzeichnung ~ 720 GB.

- Nur-Öffnungszeit (20 s/GB): 720 × 20 s = 14.400 s → ~ 4 Stunden
- Mit einem einfachen Anzeige-/Erfassungsfilter (~ × 1,7): ~ 6 h 48 m

Wenn die die Datenraten höher ausfallen (Aggregate nahe 1 TB in 4 min), sind Sie mit einem einzigen Filter wieder im Öffnungsbereich von ~ 9–10 Stunden – bevor Sie auf Ihre erste Konversation, Ihren ersten Ablauf oder Ihr erstes Diagramm klicken.

Das Fazit in Zahlen:

- Öffnen von 500 GB: ~ 2 h 46 m (kein Filter) → ~ 4 h 43 m (ein einfacher Filter)
- Öffnen von 1 TB: ~ 5 h 33 m – 5 h 41 m (kein Filter) → ~ 9 h 26 m – 9 h 40 m (ein Filter)
- Realistische gemischter Auslastung: ~ 3 GB/s → ~ 10 TB/Stunde → ~ 250 TB/Tag
- Eine 4-minütige Aufnahme bei dieser Rate ~ 720 GB → ~ 4 Stunden nur zum Öffnen;

...und ~ 6 h 48 m mit einem einfachen Filter.

Schlussfolgerung:

Wireshark ist ein großartiges Tool! Aber in modernen Automobilarchitekturen ist Wireshark als primäres Analyse-Tool operativ nicht einsetzbar.

Das Tool eignet sich hervorragend für, forensische Untersuchungen im kleinen Maßstab, und genau so sollte es von den Experten eingesetzt werden, die damit umgehen können!

Alternativen:

Bei GB/s und TB/Tag führt der einzig gangbare Weg über verteilte, stream-first-Telemetrie mit einem integrierten, dedizierten Capture- und Analysewerkzeug, das gewaltige Datenmengen parallel, synchron und über alle gültigen Transportschichten hinweg nanosekundengenau und zuverlässig ingestieren kann – und die benötigten Daten in Echtzeit oder in sehr kurzer Zeit präsentiert.

Es muss automatisierbar, skalierbar und in der Lage sein, tiefgehende, sinnvolle Paketanalysen über den gesamten Datenbestand durchzuführen – blitzschnell, genau so, wie es die TSN CoreSolution 4 Toolchain macht.

Bei Interesse finden Sie uns hier:

www.tsn.systems

TSN Systems GmbH

Dalbergstraße 7

36037 Fulda, Deutschland

Telefon: +49 661 410 951 80