

SharkFest'26 Europe

Does it Matter?

Tom Cordemans

Sponsored by:
PROFITAP DEEP NETWORK OBSERVABILITY
cPacket
TCP/IP training
endace Record. Respond.

Agenda

- Setting the scene
- Introduction to the Matter standard
- Exploring the packets
  - Using display filters and profiles
  - Claude joins the investigation
  - Enhancing Wireshark with Lua scripts
- Ready, Set, Solve!
- Additional resources
- Q&A



Setting the scene

Some info about the speaker

- Tom Cordemans
  - Senior lecturer @ Odisee
  - Researcher @ Distrinet Research Unit - KU Leuven
  - Sharing knowledge and expertise
  - My socials LinkedIn



Research on IoT devices





















Research on IoT devices

CONFERENCE PROCEEDING

Reverse Engineering the Eufy Ecosystem: A Deep Dive into Security Vulnerabilities and Proprietary Protocols

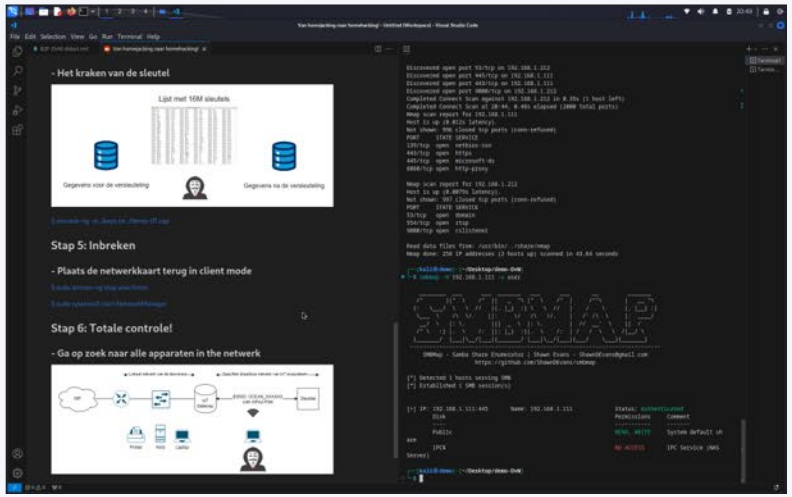
Goeman V, de Ruck D, Cordemans T, Lapon J, Naessens V see details (5)

18th USENIX WOOT Conference on Offensive Technologies (WOOT), PA, Philadelphia, 12 Aug 2024 - 13 Aug 2024. PROCEEDINGS OF THE 18TH USENIX WOOT CONFERENCE ON OFFENSIVE TECHNOLOGIES, WOOT 2024. USENIX ASSOC. 133-147. 2024



CVSS scores for CVE-2024-51346

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score
7.7	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	2.5	5.2



Introduction to the Matter standard

Background & goals

- An open, IP-based connectivity standard for IoT / smart-home devices.
- Runs locally over Wi-Fi, Thread and Ethernet. (no vendor cloud required)
- Guarantees interoperability across ecosystems. (Apple, Google, Samsung, open hubs,etc)
- Certificate-based authentication and encrypted communication by design.
- Governed by the Connectivity Standards Alliance (CSA)



Local-first

Works during internet outages



Interoperable

One device, every ecosystem



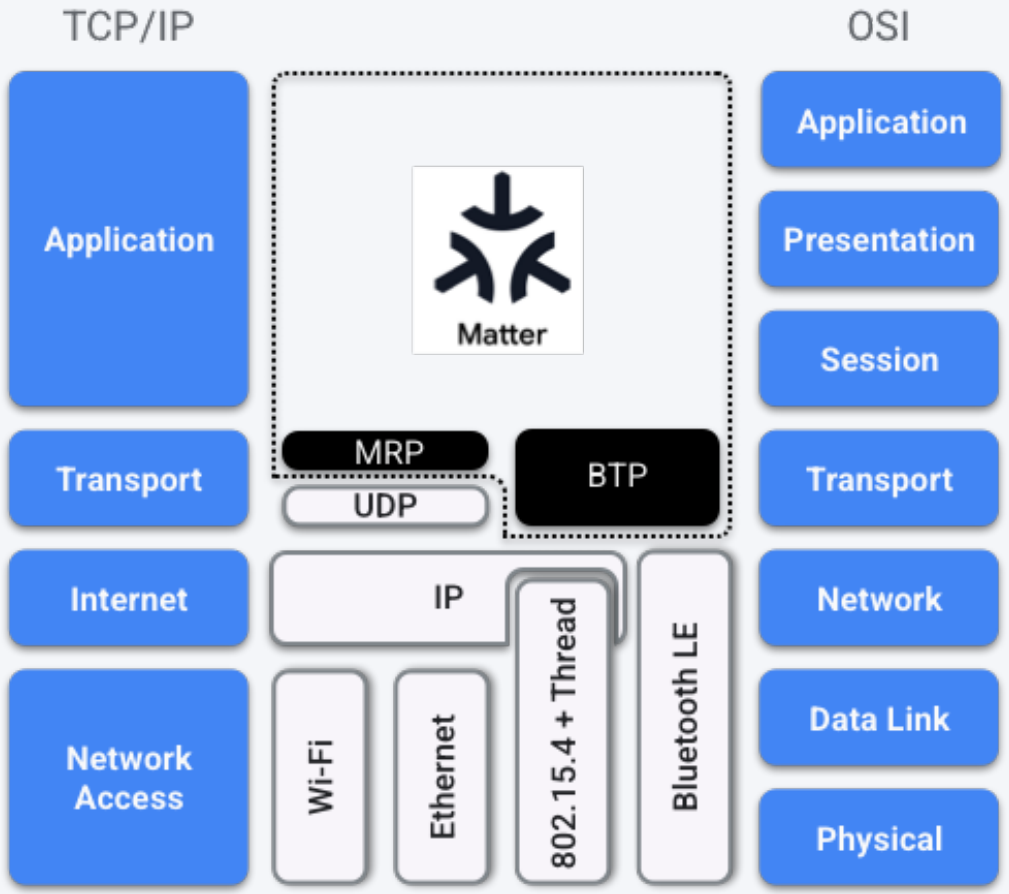
Secure

Certificates + encryption

Release history

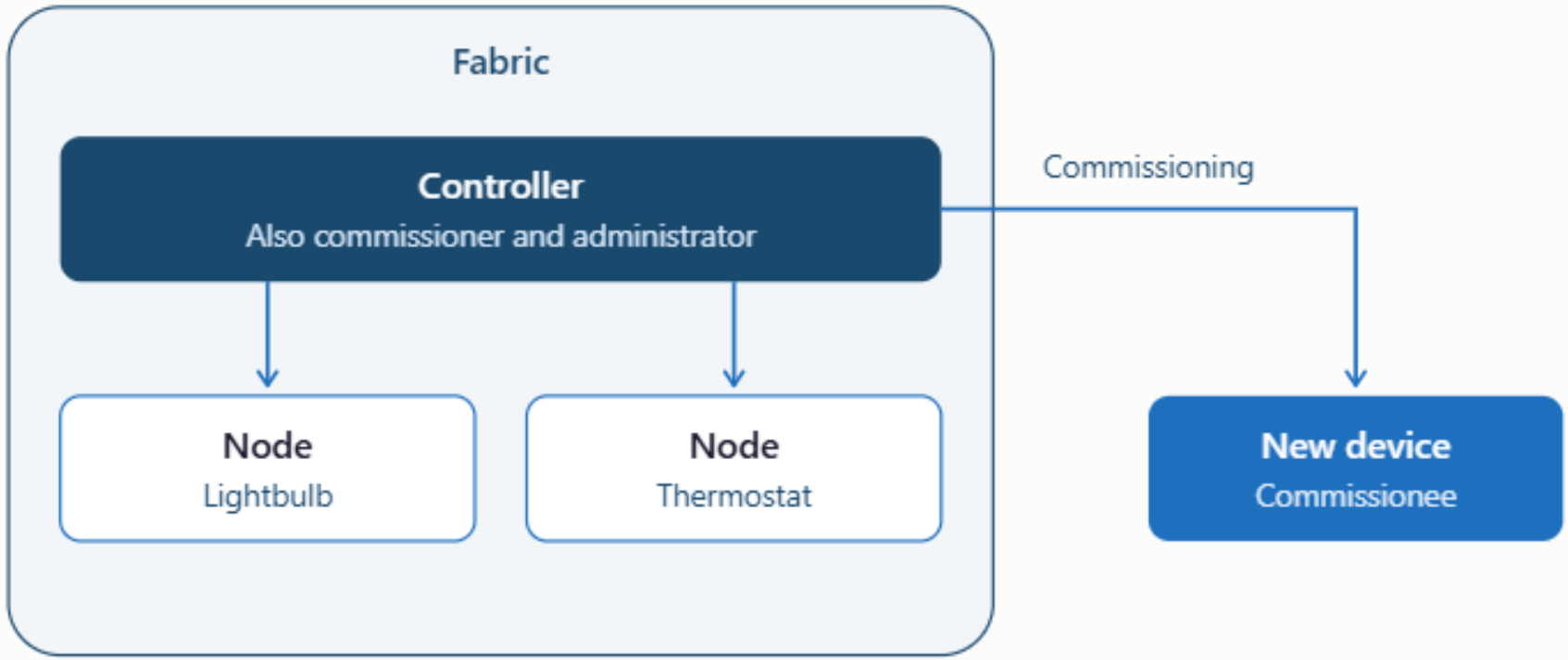
Version	Published	Some highlights
1.6.1	September 2026	Groupcast
1.6	June 2026	NFC-based commissioning, joint fabric, improved device status reporting, …
1.5.1	March 2026	Multi-stream video, additional format support for images and video, …
1.5	November 2025	Native camera support, smart garden, …
1.4.2	July 2025	Quality and reliability release
1.4.1	March 2025	Setup-focused release
1.4	November 2024	Network infrastructure and energy ecosystems
1.3	April 2024	Water and energy management
1.2	October 2023	First big device-type expansion
1.1	May 2023	Mainly minor improvements
1.0	September 2022	Launch specification

Mapping Matter vs TCP/IP



Source: https://developers.home.google.com/matter/primer

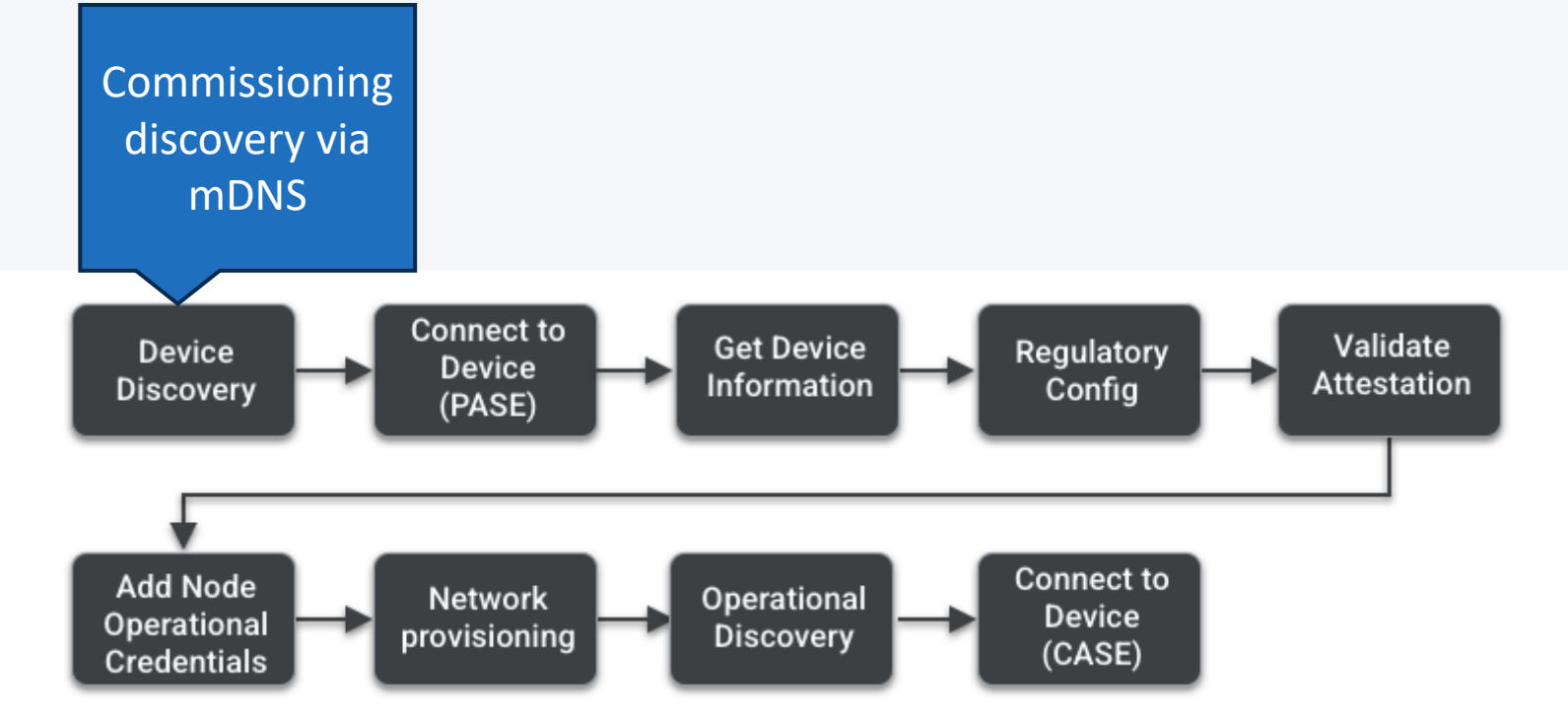
Terminology



Every node has an operational certificate linked to the fabric's root of trust

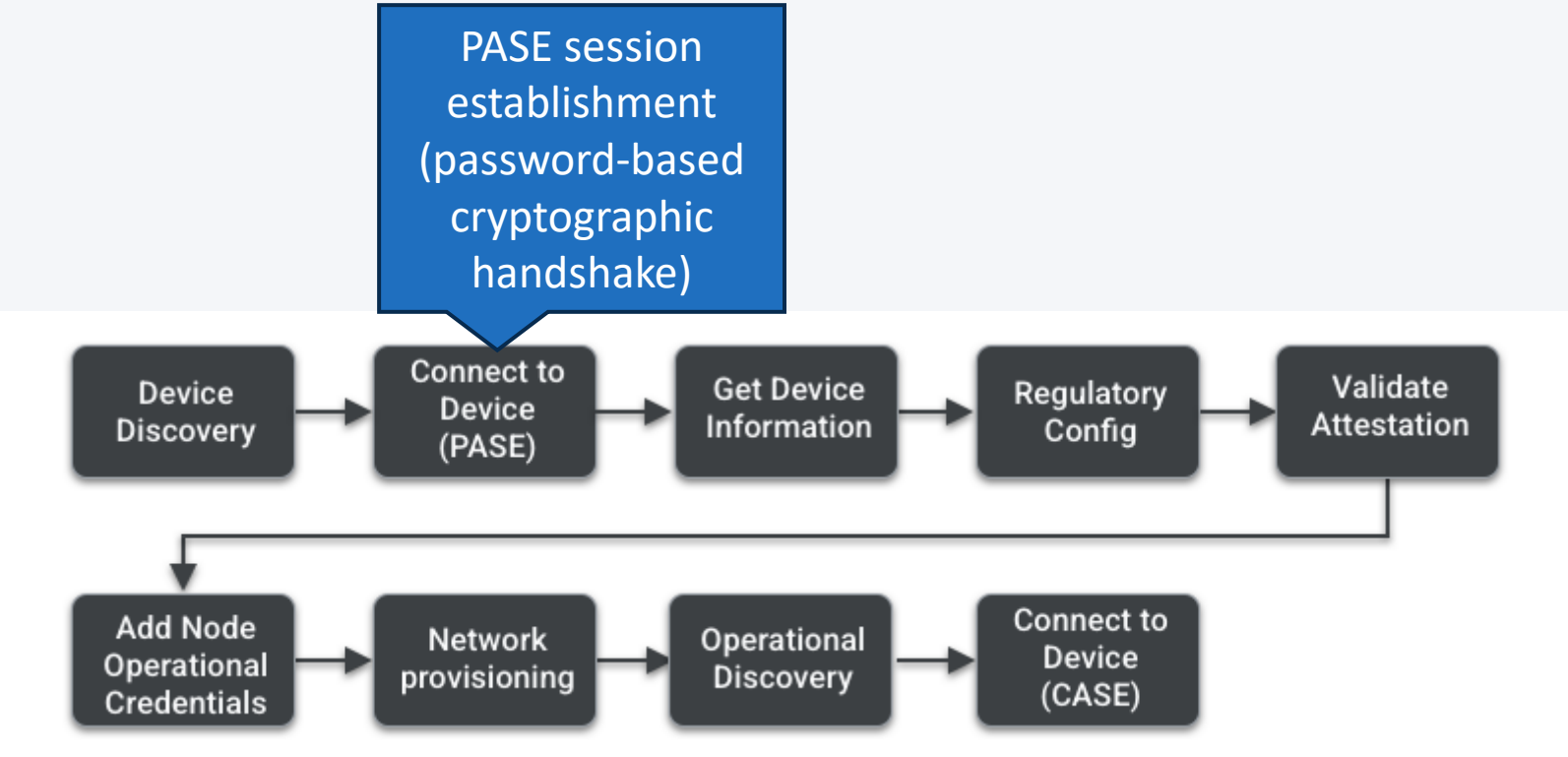
Multi-admin: one device can join several fabrics, with a separate node in each

Commissioning flow



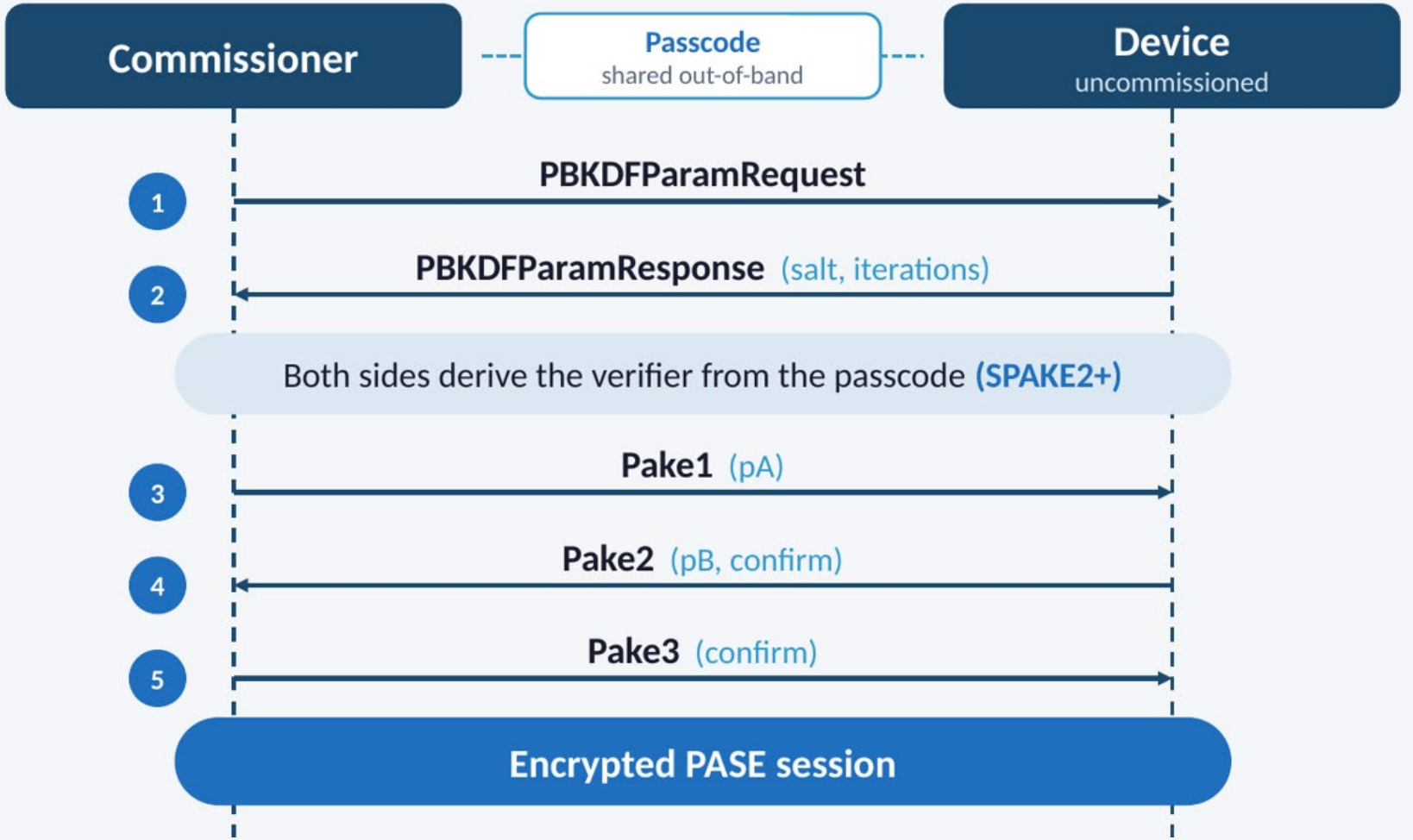
Source: https://developers.home.google.com/matter/primer/commissioning

Commissioning flow

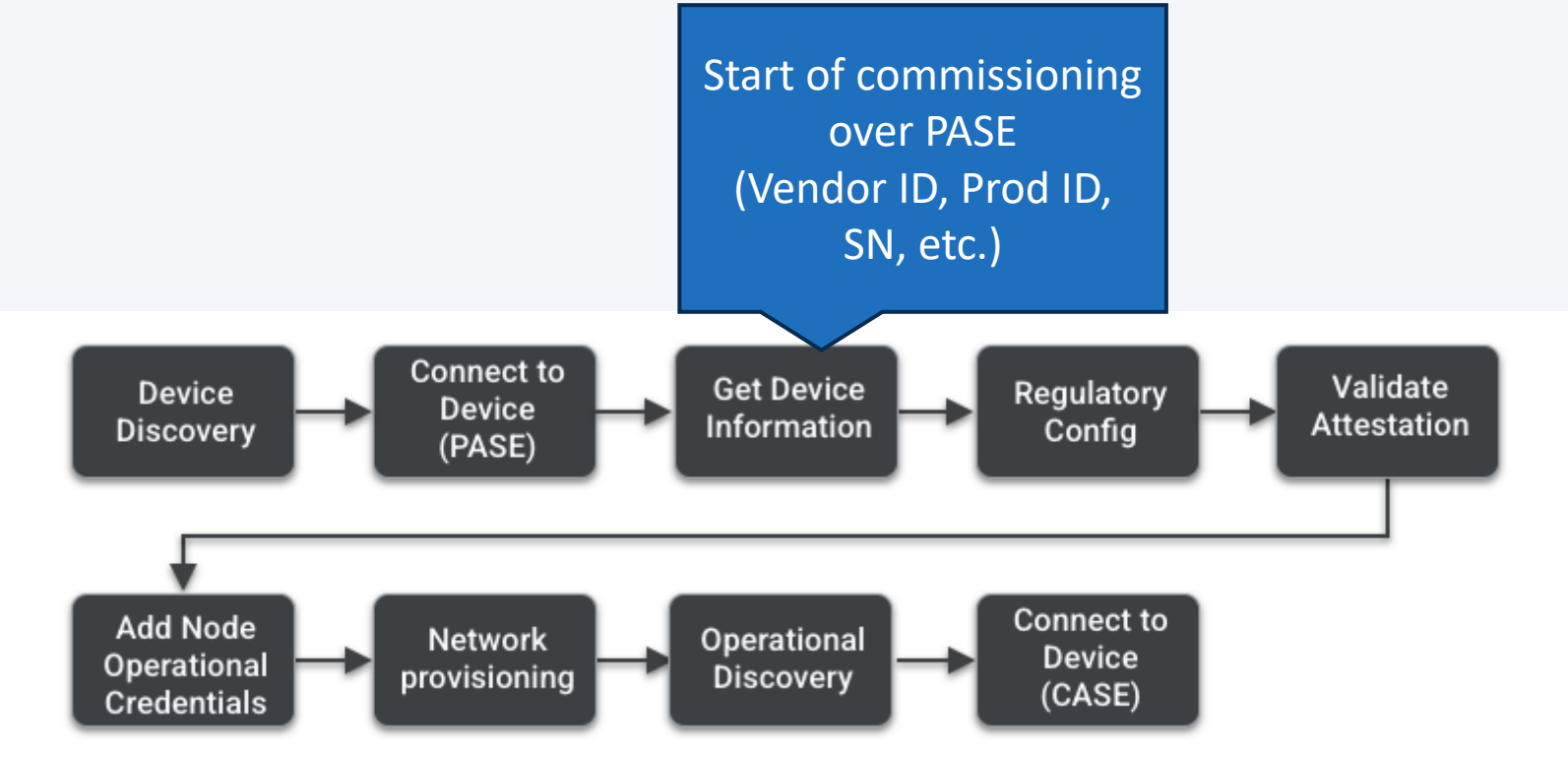


Source: https://developers.home.google.com/matter/primer/commissioning

PASE - Passcode Authenticated Session Establishment

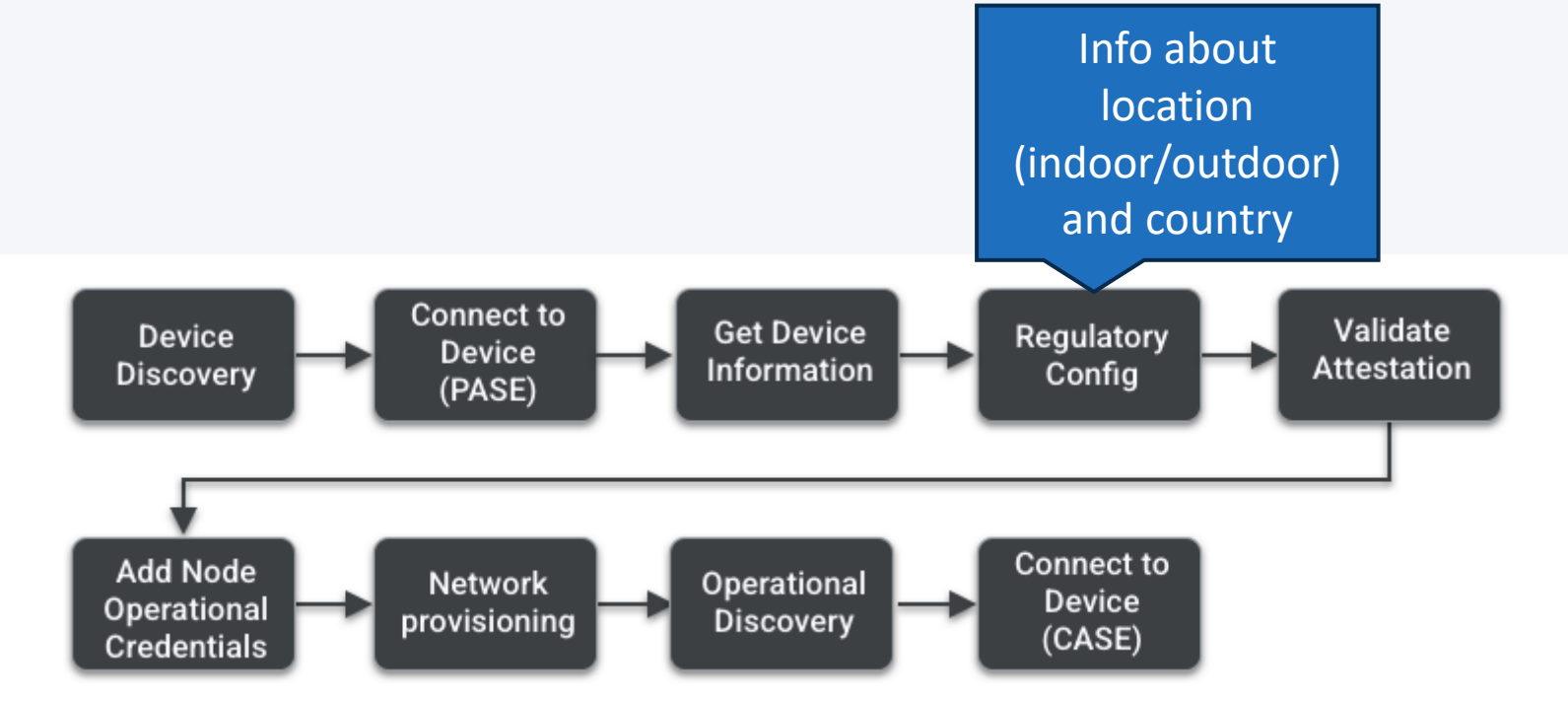


Commissioning flow



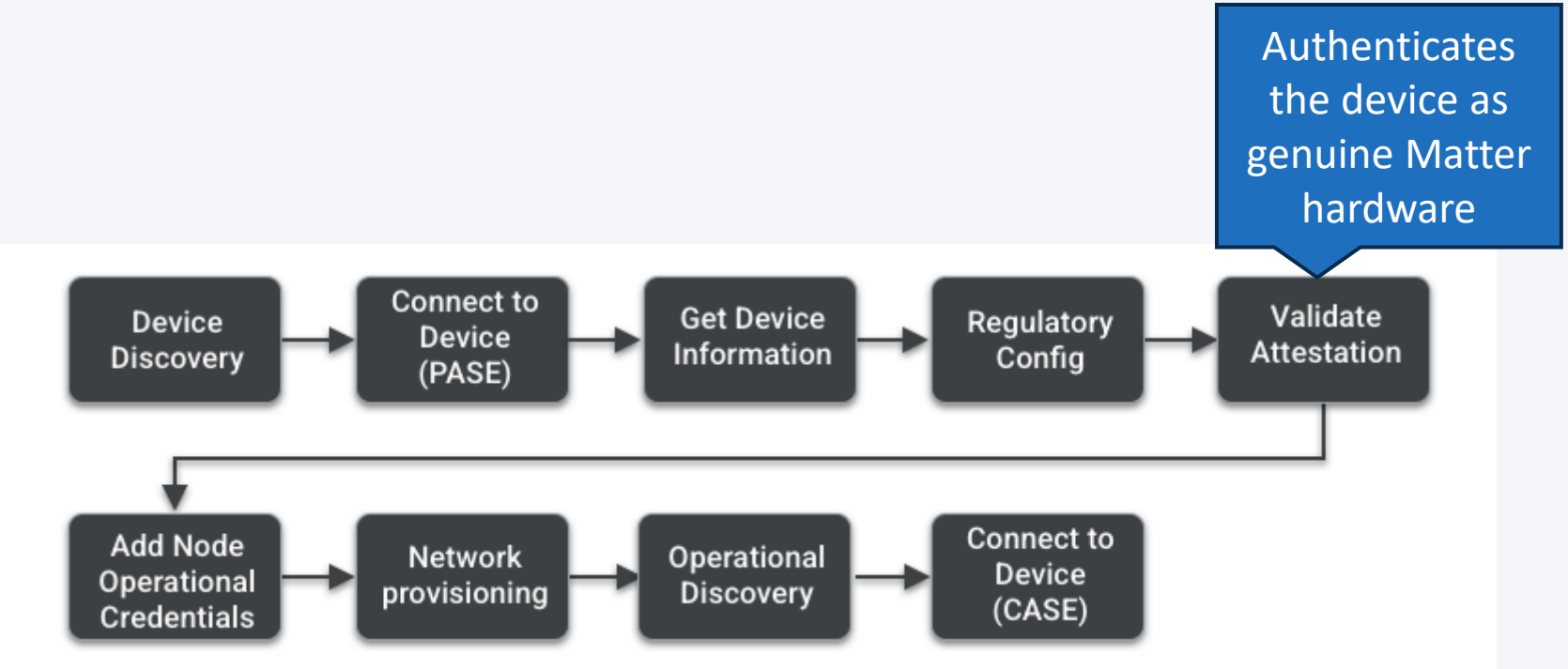
Source: https://developers.home.google.com/matter/primer/commissioning

Commissioning flow



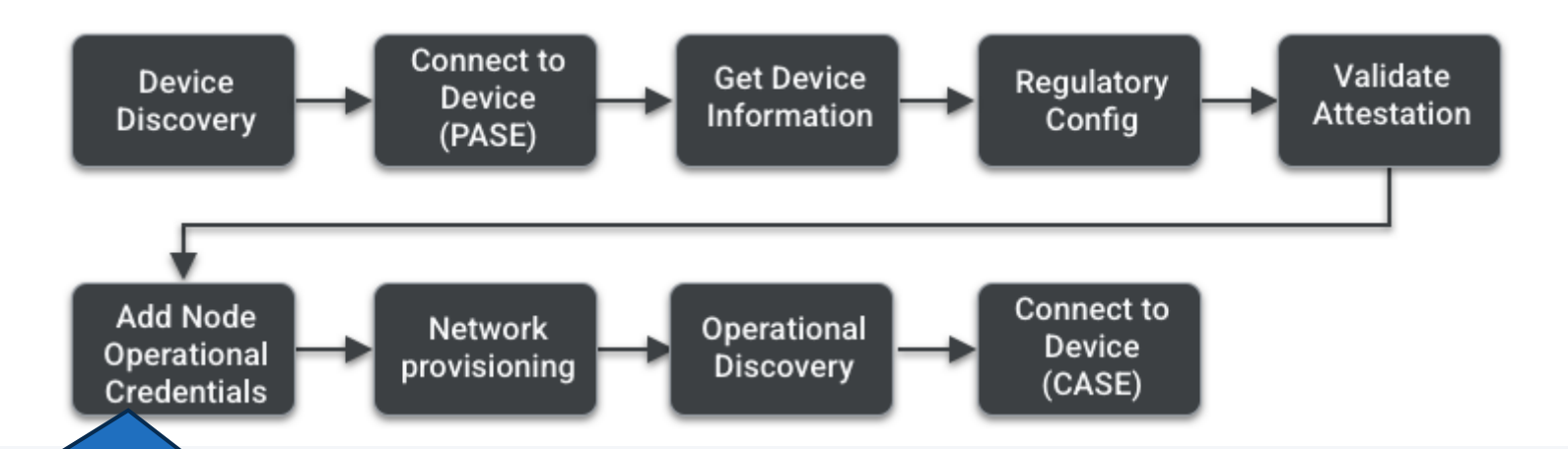
Source: https://developers.home.google.com/matter/primer/commissioning

Commissioning flow



Source: https://developers.home.google.com/matter/primer/commissioning

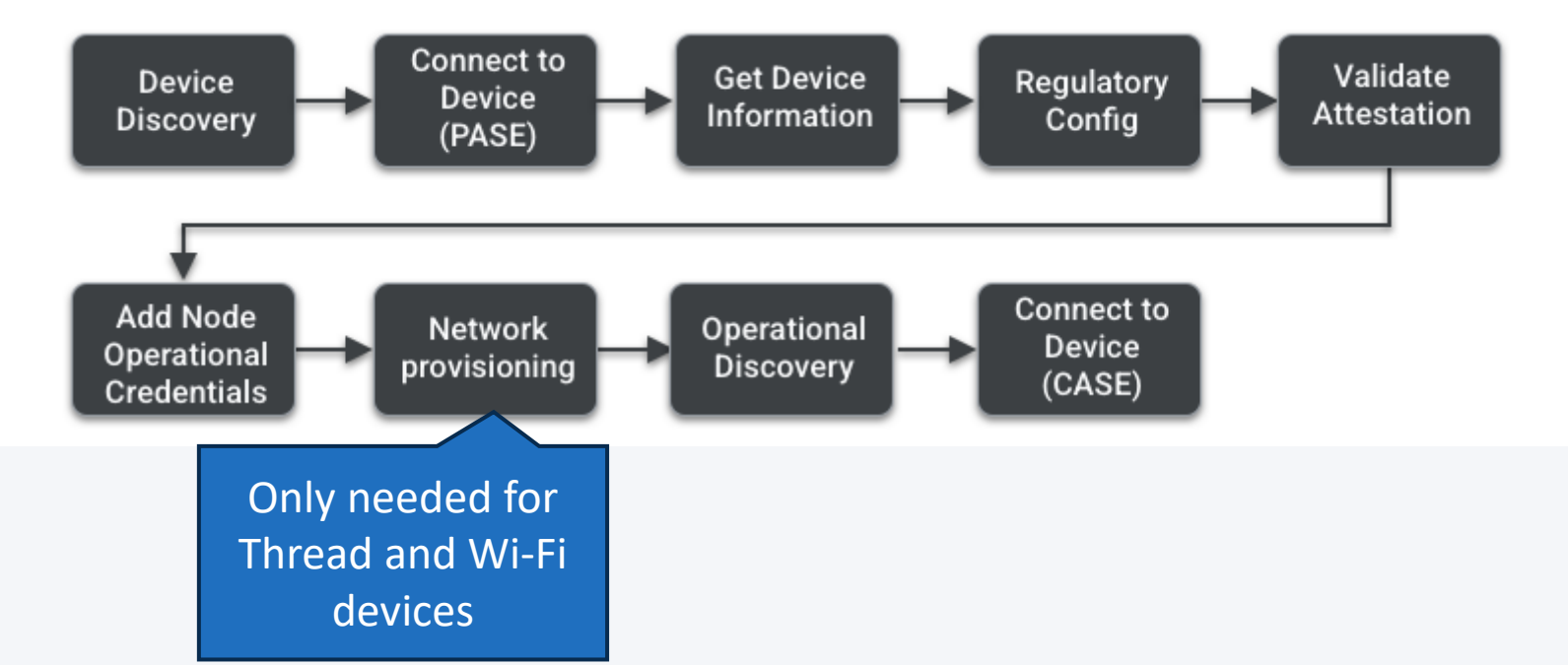
Commissioning flow



Generation and installation of node operational certificate and commissioning completed

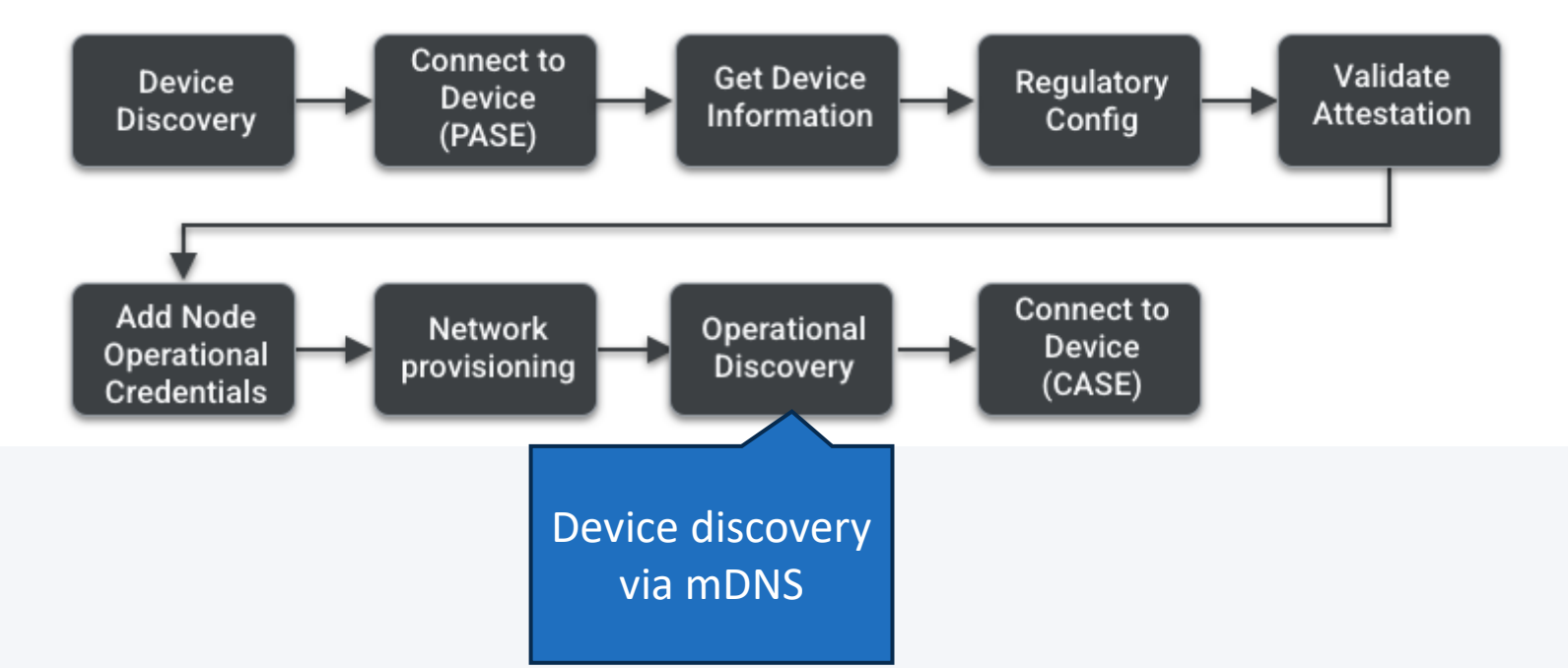
Source: https://developers.home.google.com/matter/primer/commissioning

Commissioning flow



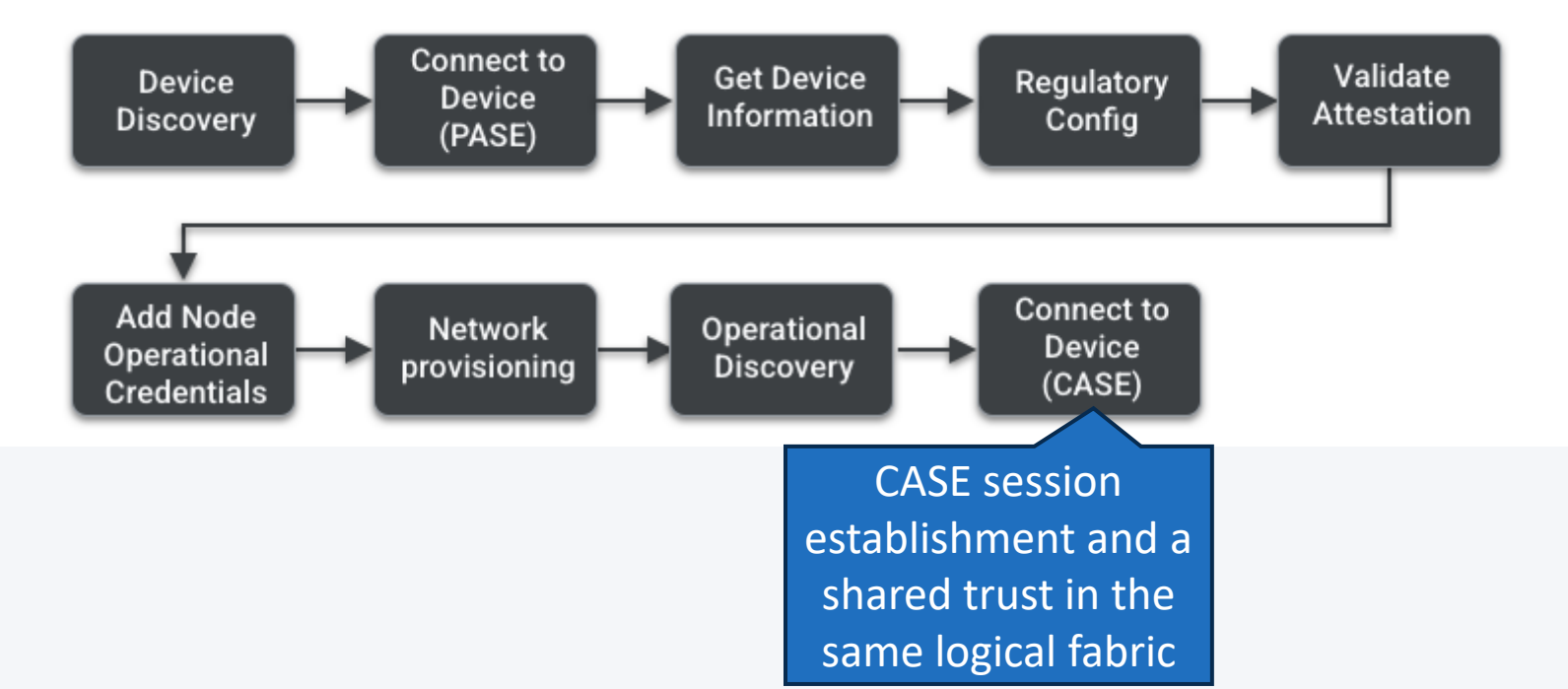
Source: https://developers.home.google.com/matter/primer/commissioning

Commissioning flow



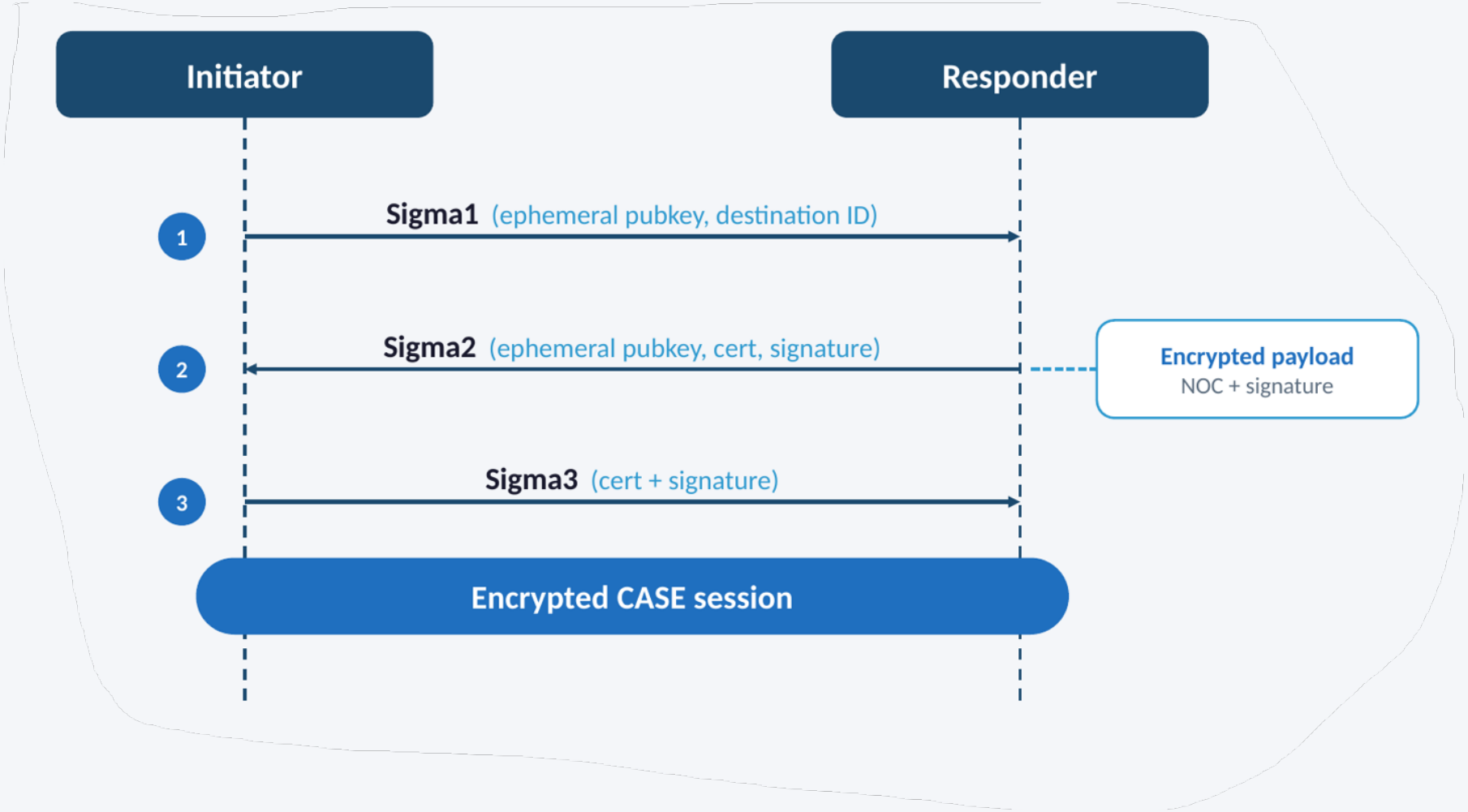
Source: https://developers.home.google.com/matter/primer/commissioning

Commissioning flow



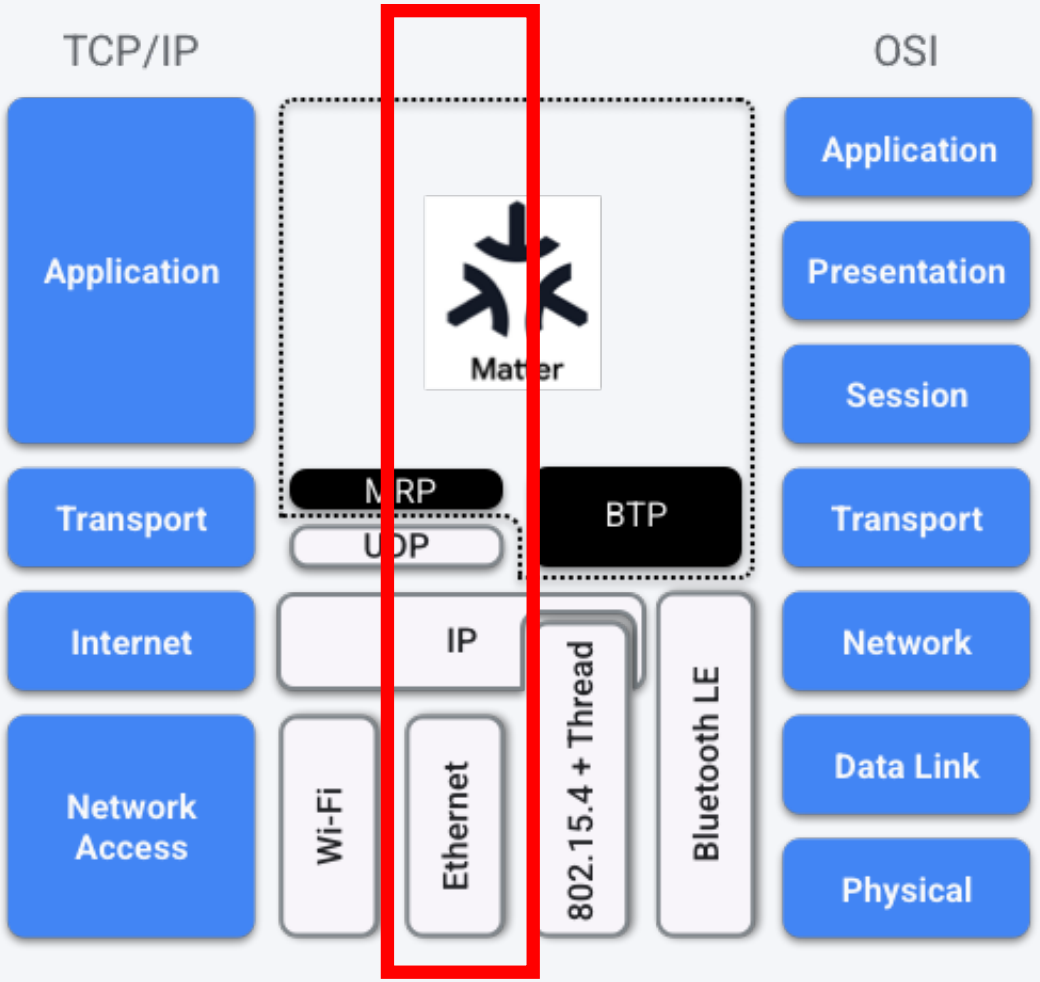
Source: https://developers.home.google.com/matter/primer/commissioning

CASE - Certificate Authenticated Session Establishment



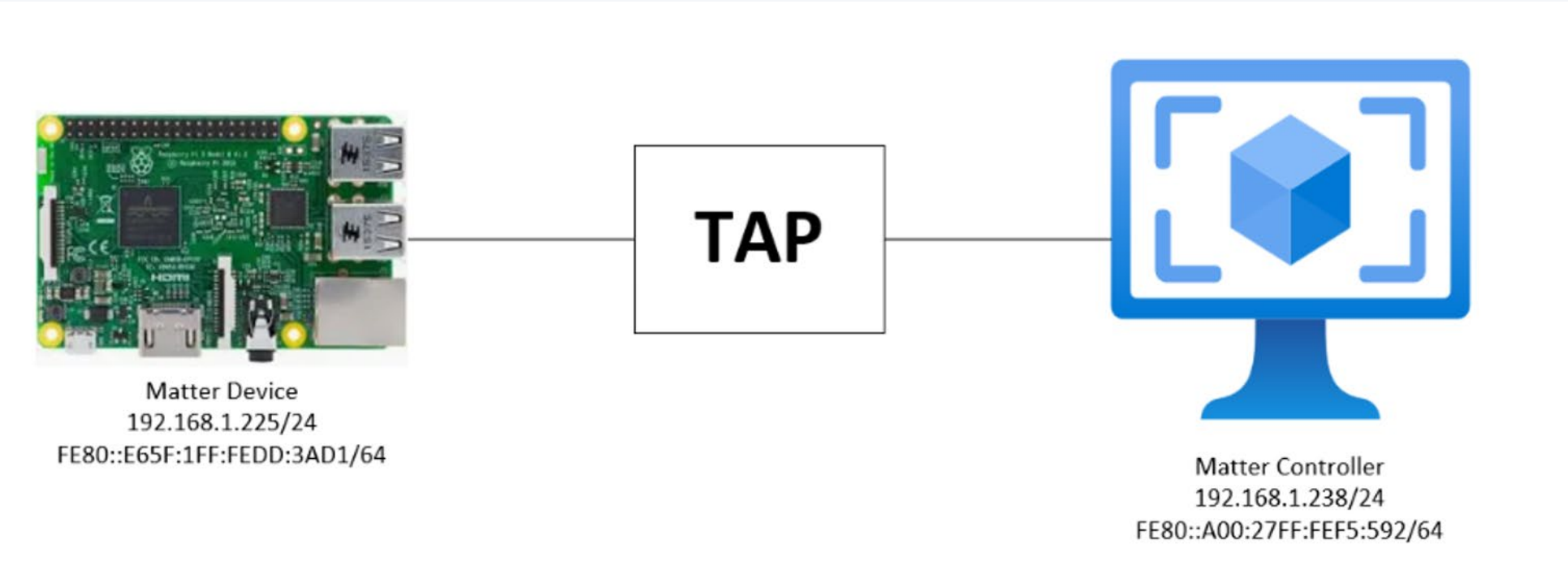
Exploring the packets

The primary focus

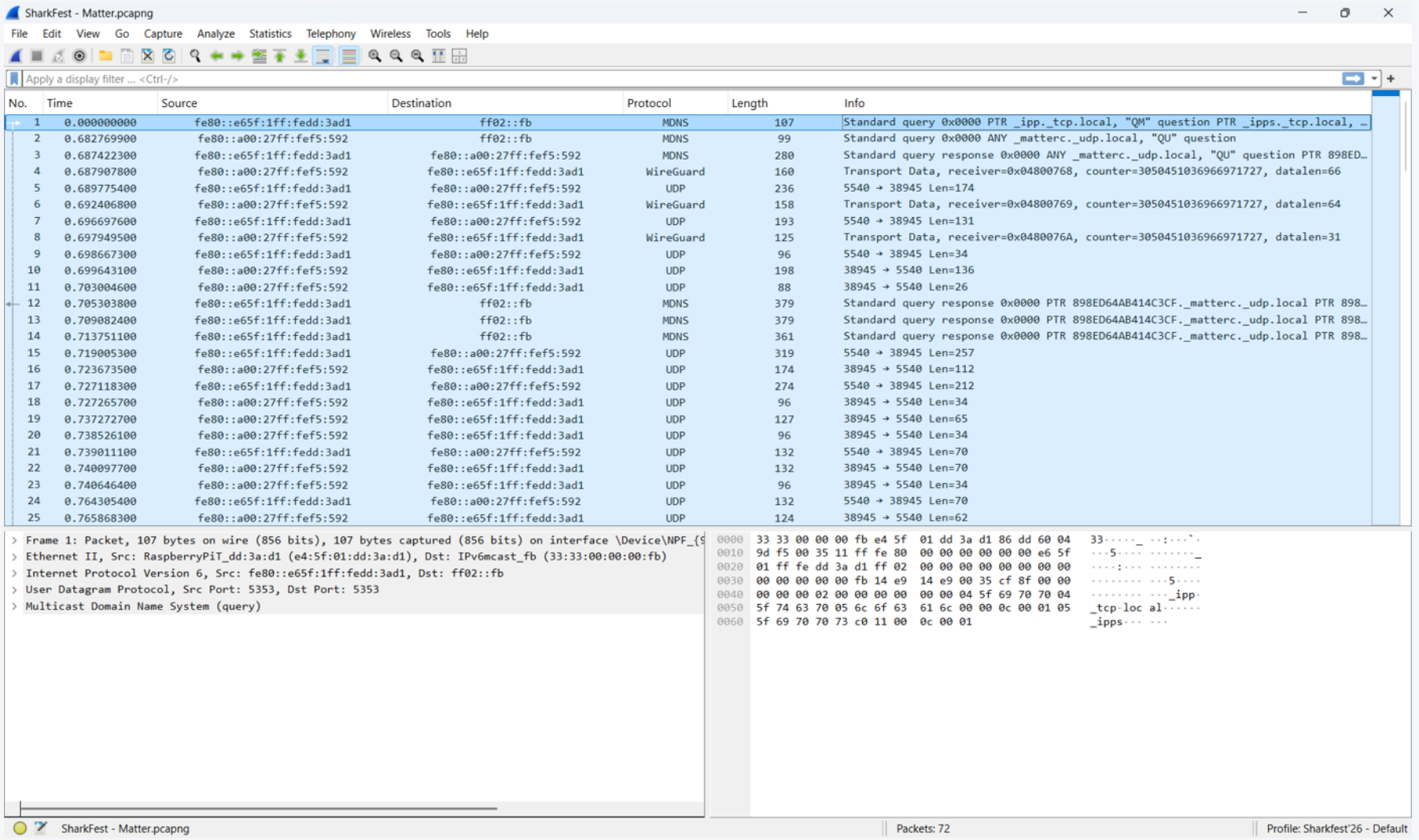


Source: https://developers.home.google.com/matter/primer

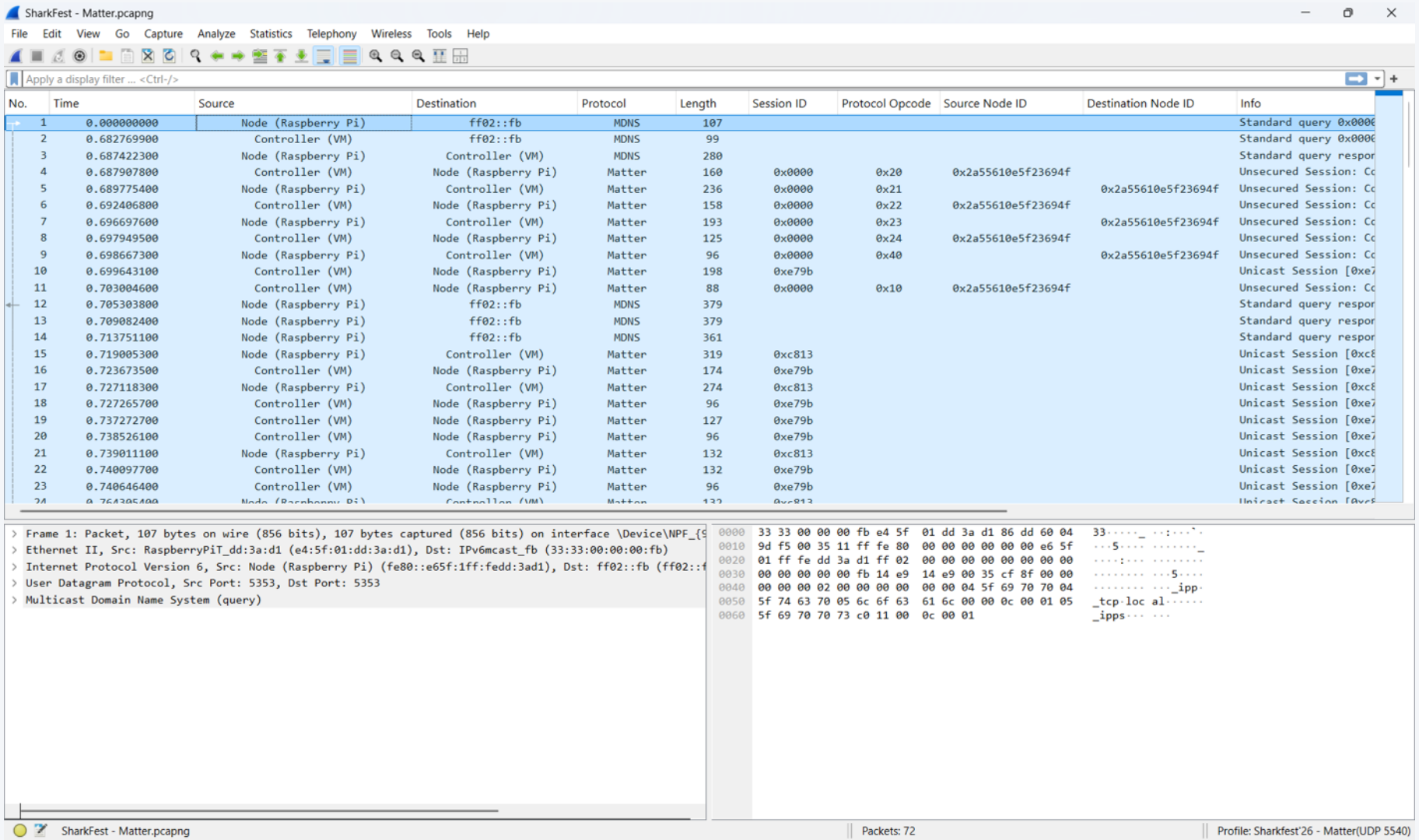
Used test setup based on the CHIP tool



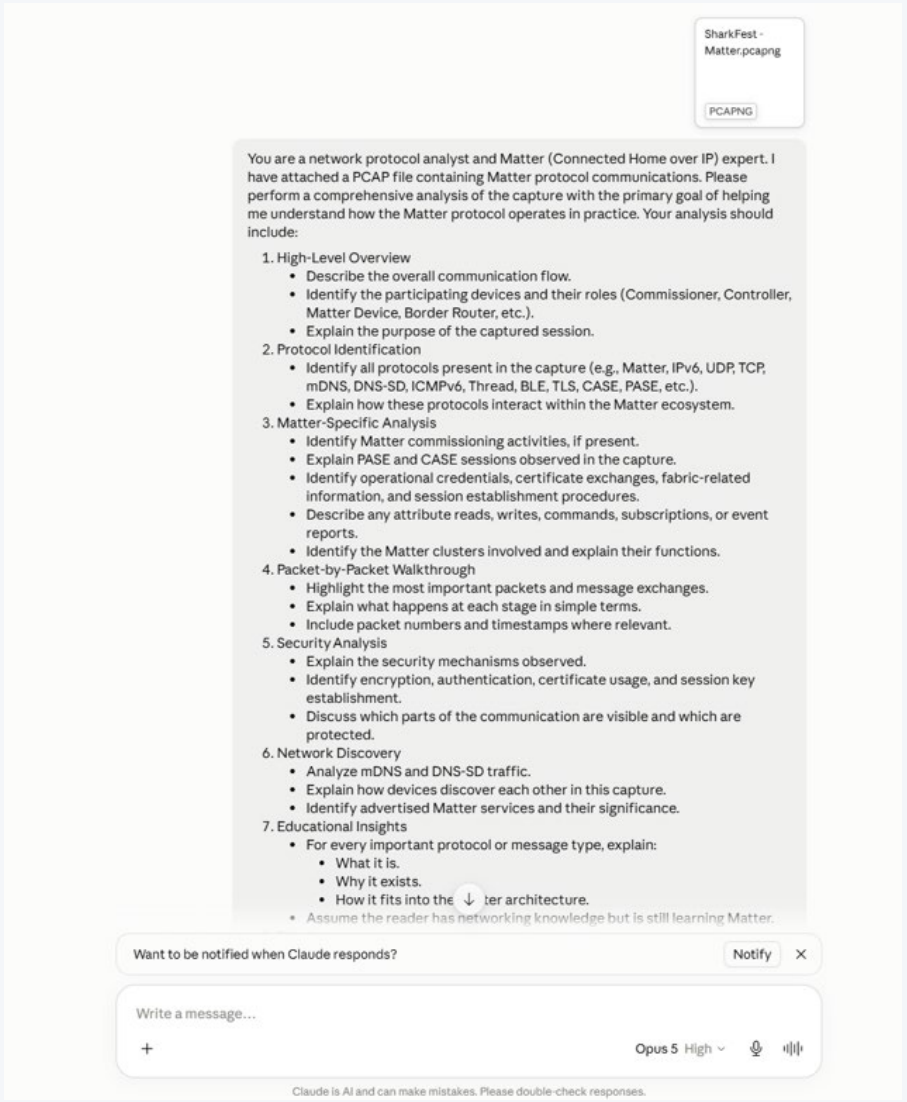
Wireshark (Default profile)

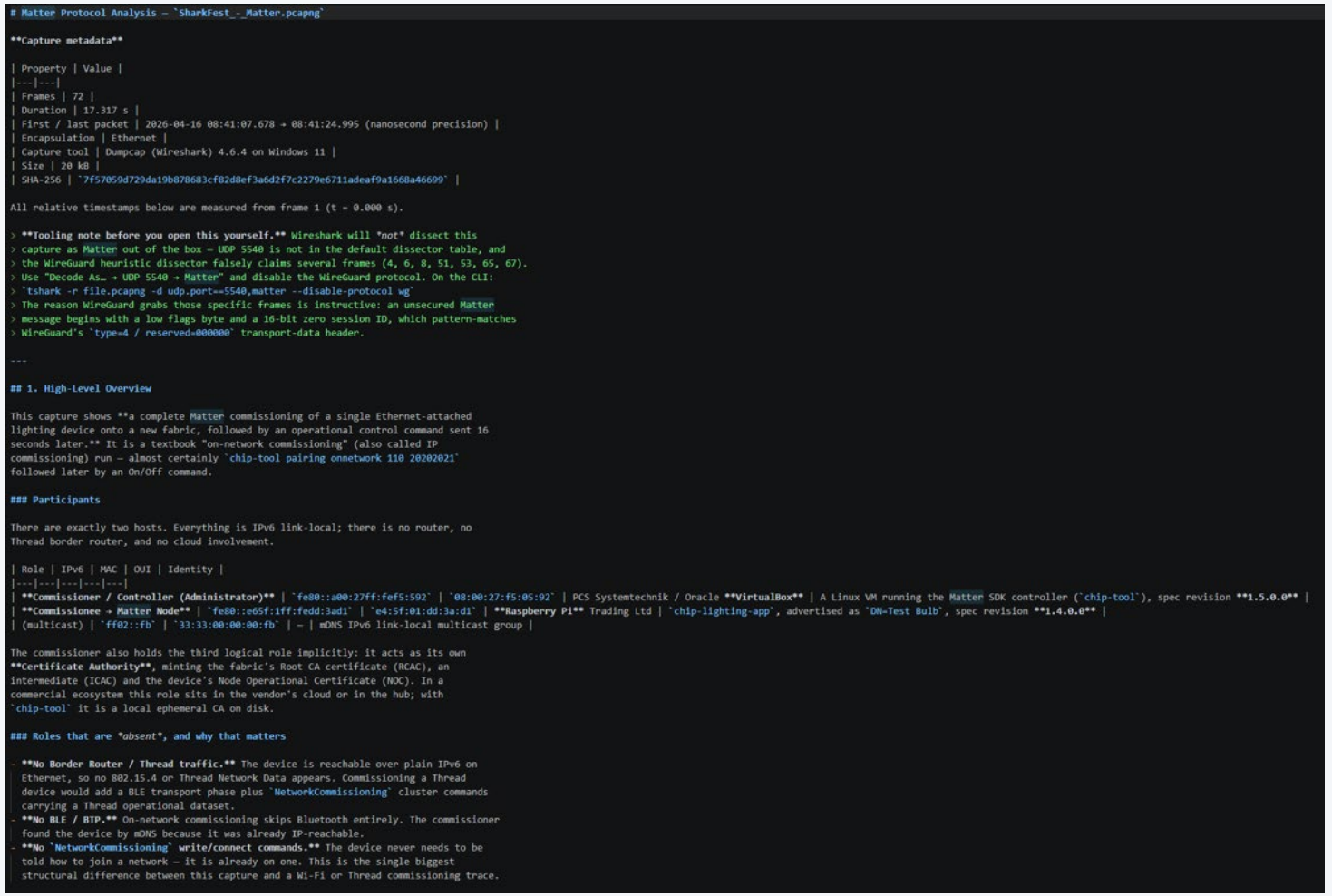


Wireshark (Custom Matter profile)



Claude joins the investigation





```
# Matter Protocol Analysis — `SharkFest_-_Matter.pcapng`

**Capture metadata**

| Property | Value |
|---|---|
| Frames | 72 |
| Duration | 17.317 s |
| First / last packet | 2026-04-16 08:41:07.678 → 08:41:24.995 (nanosecond precision) |
| Encapsulation | Ethernet |
| Capture tool | Dumpcap (Wireshark) 4.6.4 on Windows 11 |
| Size | 20 kB |
| SHA-256 | `7f57059d729da19b878683cf82d8ef3a6d2f7c2279e6711adeaf9a1668a46699` |

All relative timestamps below are measured from frame 1 (t = 0.000 s).

> **Tooling note before you open this yourself.** Wireshark will *not* dissect this
> capture as Matter out of the box — UDP 5540 is not in the default dissector table, and
> the WireGuard heuristic dissector falsely claims several frames (4, 6, 8, 51, 53, 65, 67).
> Use "Decode As… → UDP 5540 → Matter" and disable the WireGuard protocol. On the CLI:
> `tshark -r file.pcapng -d udp.port==5540,matter --disable-protocol wg`
> The reason WireGuard grabs those specific frames is instructive: an unsecured Matter
> message begins with a low flags byte and a 16-bit zero session ID, which pattern-matches
> WireGuard's `type=4 / reserved=000000` transport-data header.

---

## 1. High-Level Overview

This capture shows **a complete Matter commissioning of a single Ethernet-attached
lighting device onto a new fabric, followed by an operational control command sent 16
seconds later.** It is a textbook "on-network commissioning" (also called IP
commissioning) run — almost certainly `chip-tool pairing onnetwork 110 20202021`
followed later by an On/Off command.

### Participants

There are exactly two hosts. Everything is IPv6 link-local; there is no router, no
Thread border router, and no cloud involvement.

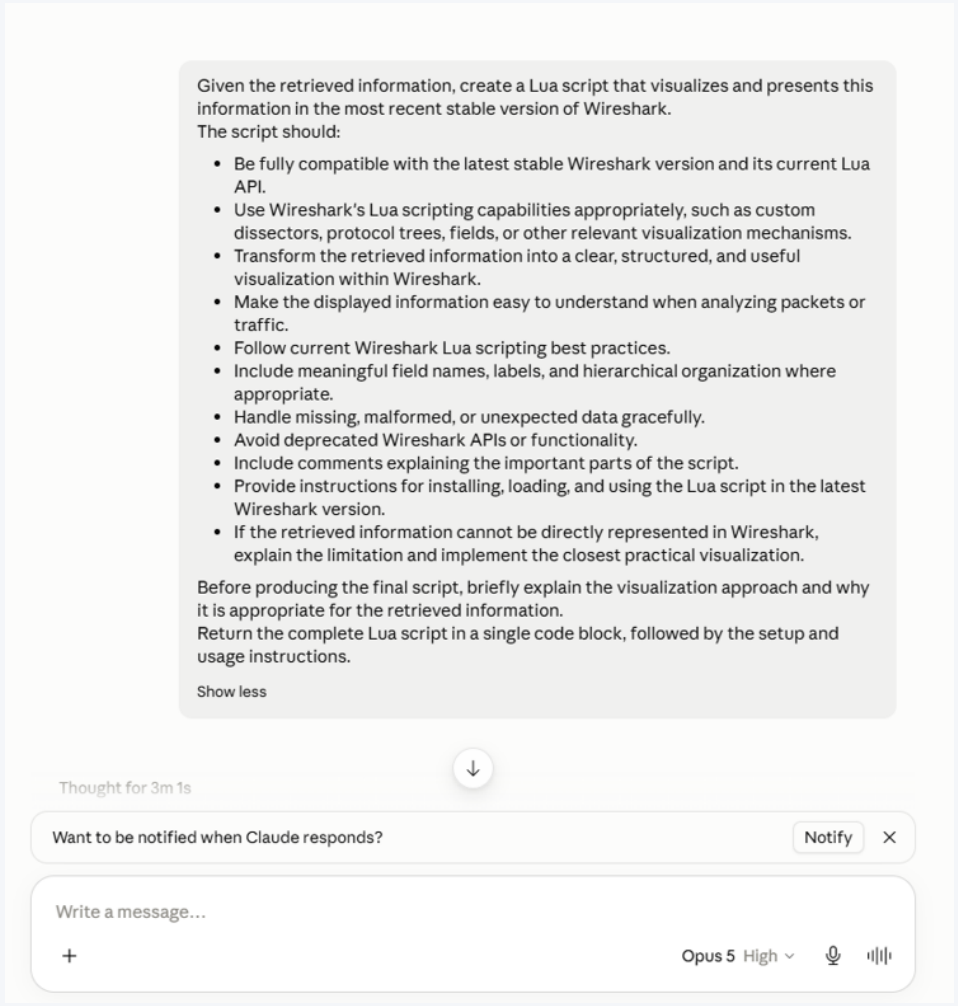
| Role | IPv6 | MAC | OUI | Identity |
|---|---|---|---|---|
| **Commissioner / Controller (Administrator)** | `fe80::a00:27ff:fef5:592` | `08:00:27:f5:05:92` | PCS Systemtechnik / Oracle **VirtualBox** | A Linux VM running the Matter SDK controller (`chip-tool`), spec revision **1.5.0.0** |
| **Commissionee → Matter Node** | `fe80::e65f:1ff:fedd:3ad1` | `e4:5f:01:dd:3a:d1` | **Raspberry Pi** Trading Ltd | `chip-lighting-app`, advertised as `DN=Test Bulb`, spec revision **1.4.0.0** |
| (multicast) | `ff02::fb` | `33:33:00:00:00:fb` | — | mDNS IPv6 link-local multicast group |

The commissioner also holds the third logical role implicitly: it acts as its own
**Certificate Authority**, minting the fabric's Root CA certificate (RCAC), an
intermediate (ICAC) and the device's Node Operational Certificate (NOC). In a
commercial ecosystem this role sits in the vendor's cloud or in the hub; with
`chip-tool` it is a local ephemeral CA on disk.

### Roles that are *absent*, and why that matters

- **No Border Router / Thread traffic.** The device is reachable over plain IPv6 on
  Ethernet, so no 802.15.4 or Thread Network Data appears. Commissioning a Thread
  device would add a BLE transport phase plus `NetworkCommissioning` cluster commands
  carrying a Thread operational dataset.
- **No BLE / BTP.** On-network commissioning skips Bluetooth entirely. The commissioner
  found the device by mDNS because it was already IP-reachable.
- **No `NetworkCommissioning` write/connect commands.** The device never needs to be
  told how to join a network — it is already on one. This is the single biggest
  structural difference between this capture and a Wi-Fi or Thread commissioning trace.
```

Enhancing Wireshark with Lua scripts

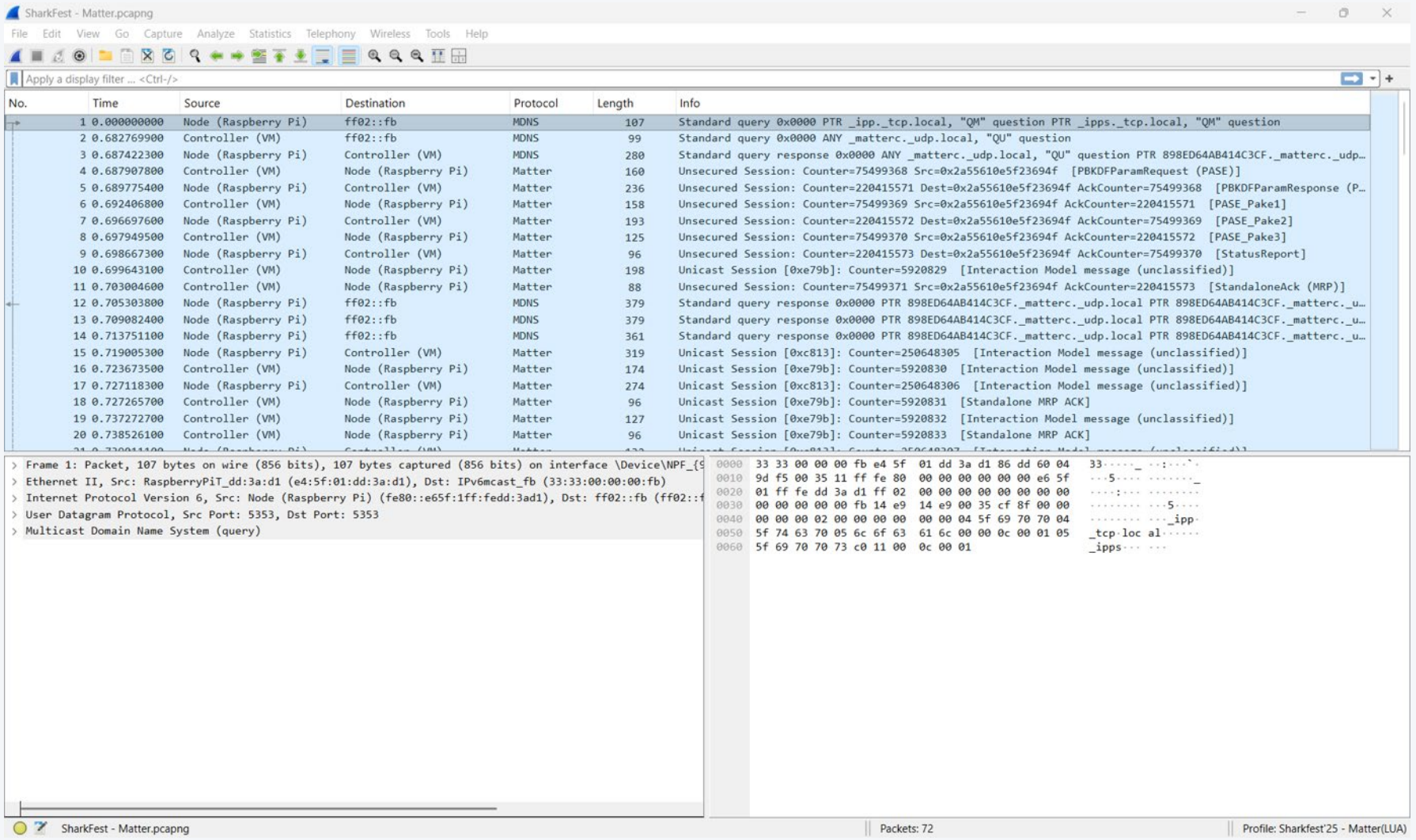



```
-- matter_analysis.lua  (v3 - self-contained)
--
-- Matter (CSA Connected Home over IP) analysis for Wireshark.
--
-- WHAT CHANGED IN v3
--   v1/v2 were postdissectors that read fields from Wireshark's built-in
--   "matter" dissector.  That dissector is registered for "Decode As" only, so
--   on most builds it never runs on UDP 5540 and the script produced nothing.
--   v3 parses the Matter message header itself and registers directly on
--   UDP 5540, so it has no external dependencies at all.
--
-- WHAT IT DOES
--   * Parses the Matter message header and exchange header from raw bytes.
--   * Full Matter TLV decoding of the plaintext Secure Channel handshakes
--     (PASE: PBKDFParamRequest/Response, Pake1/2/3; CASE: Sigma1/2/3, Resume;
--      plus the non-TLV StatusReport).
--   * Session tracking, role attribution, MRP acknowledgement analysis.
--   * Inference of ENCRYPTED Interaction Model messages from direction, size
--     and ordering -- always labelled as inference, never as observation.
--   * Matter DNS-SD decoding (_matterc._udp / _matter._tcp, subtypes, TXT).
--   * Expert info for state transitions and security findings.
--   * Tools > Matter > Capture Analysis Report   (timeline + summary)
--   * Tools > Matter > Diagnostics              (why am I seeing nothing?)
--
-- LUA COMPATIBILITY
--   Restricted to the Lua 5.1 subset so it loads on every Wireshark build:
--   no goto/labels, no bitwise operators, no // division, no bit library.
--
-- Nothing here decrypts traffic.
-------------------------------------------------------------------------------

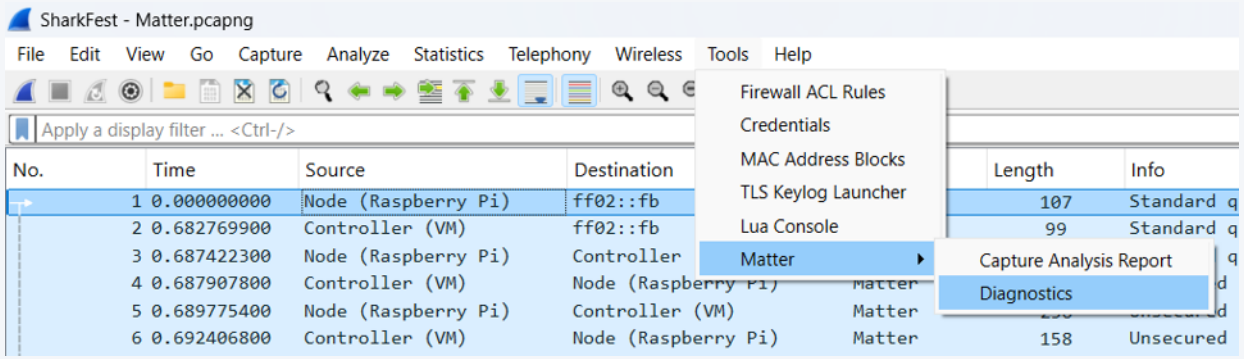

-------------------------------------------------------------------------------
-- 0.  Protocols and preferences
-------------------------------------------------------------------------------

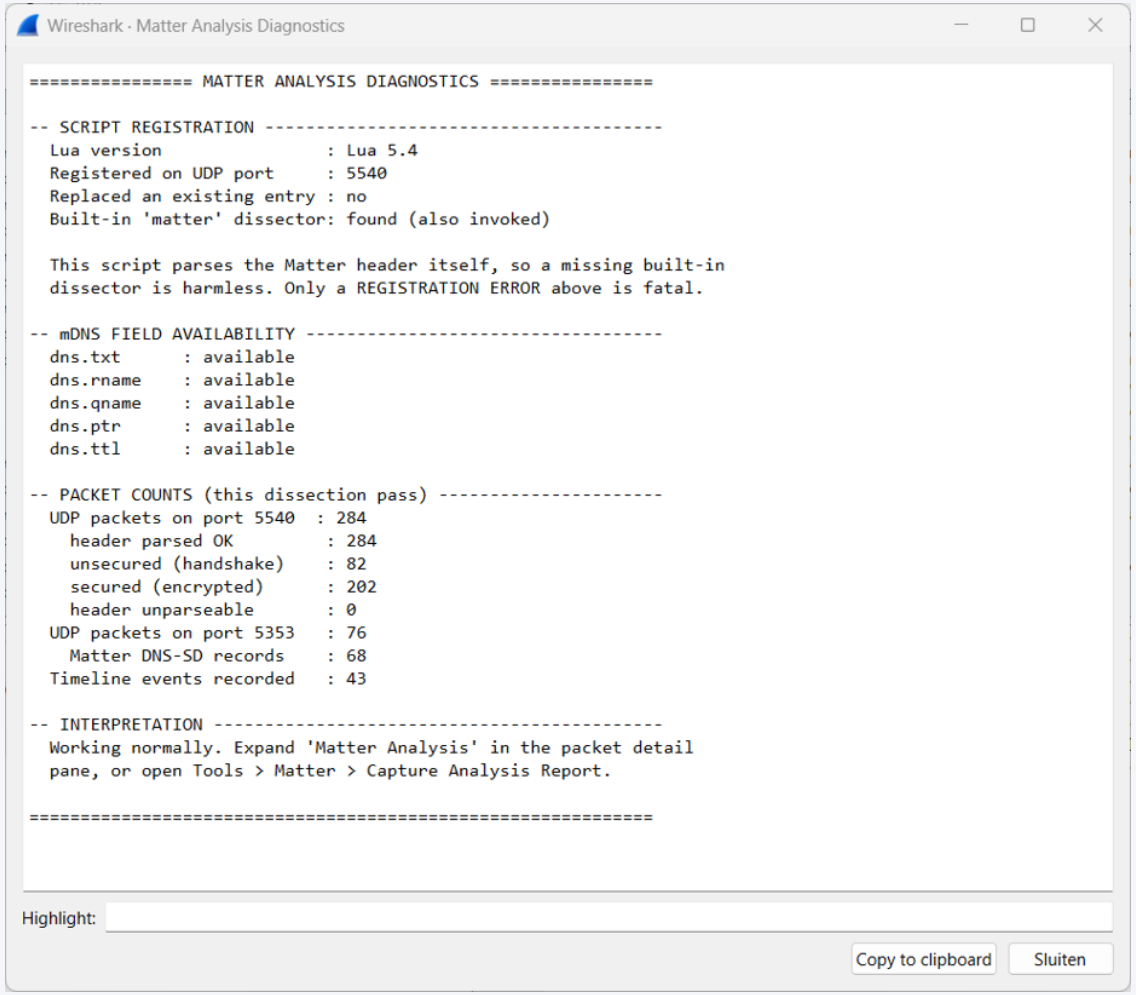
-- Main protocol: owns every field and expert, dissects UDP 5540.
local matterx = Proto("matterx", "Matter Analysis")
```

Enhancing Wireshark with Lua scripts

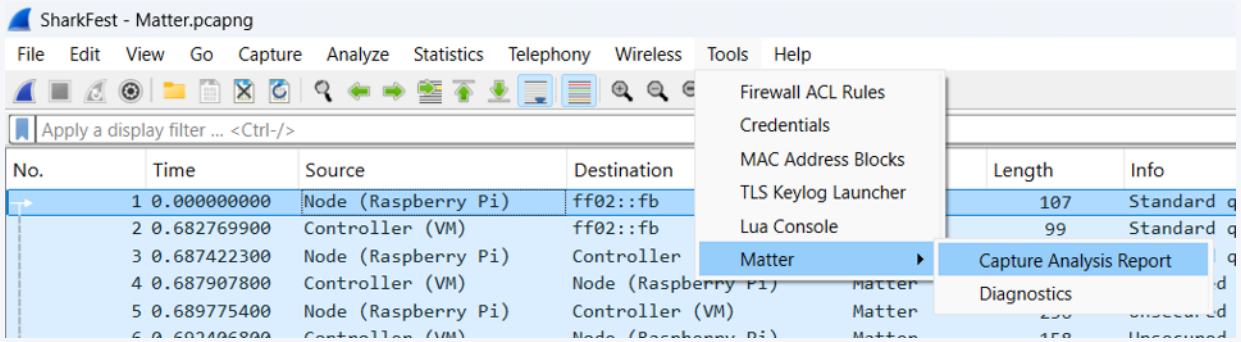


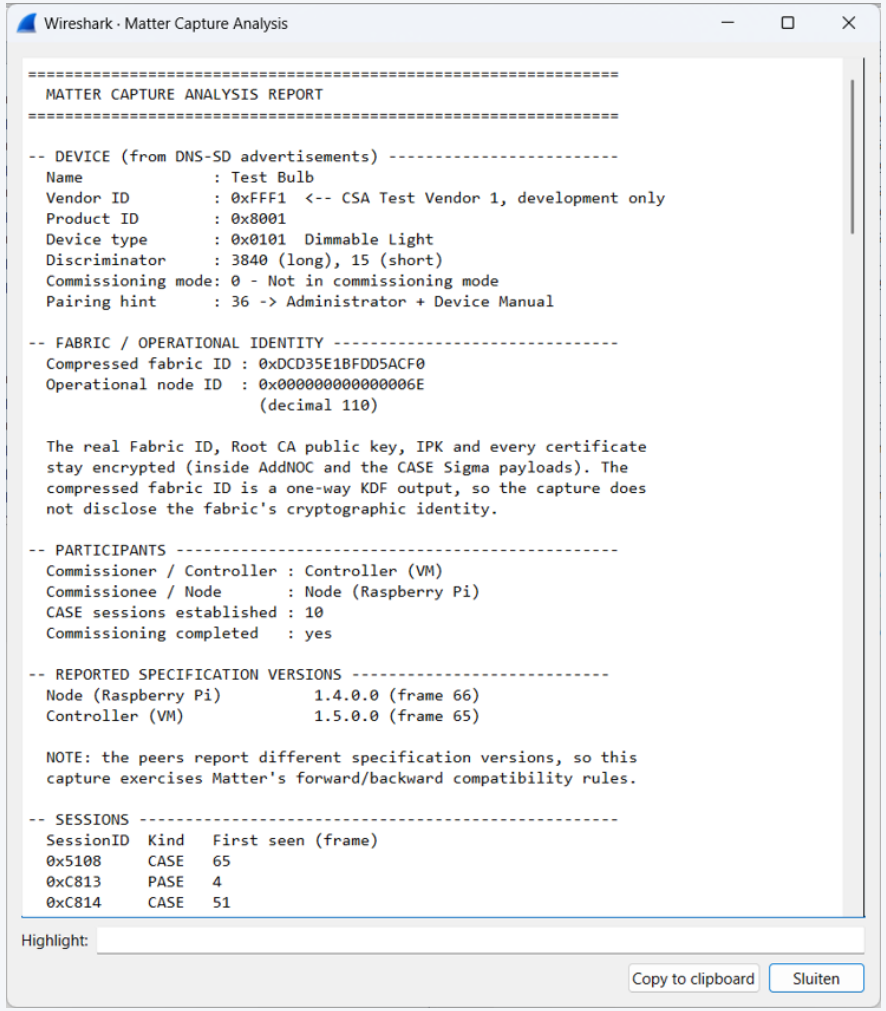
Enhancing Wireshark with Lua scripts



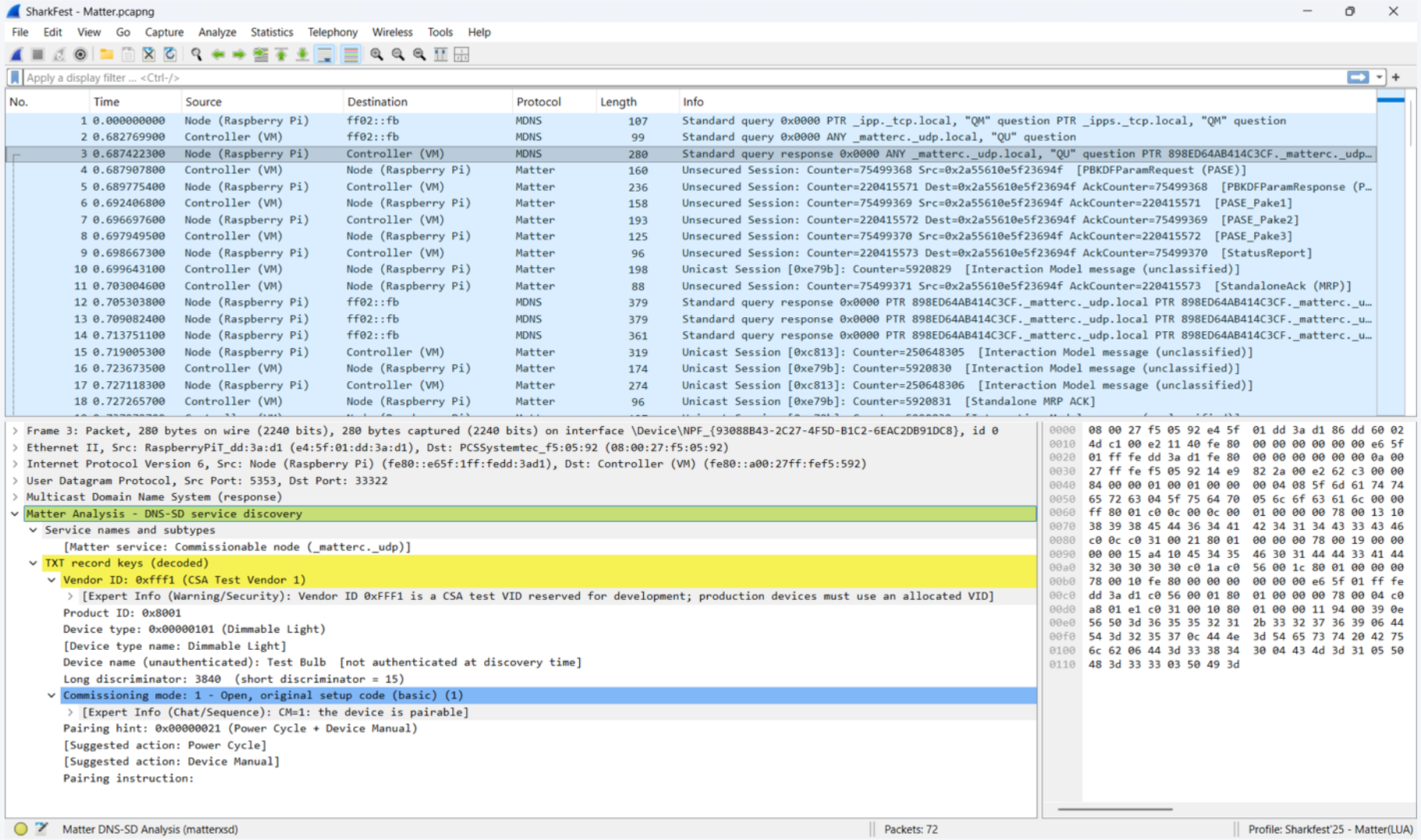


Enhancing Wireshark with Lua scripts

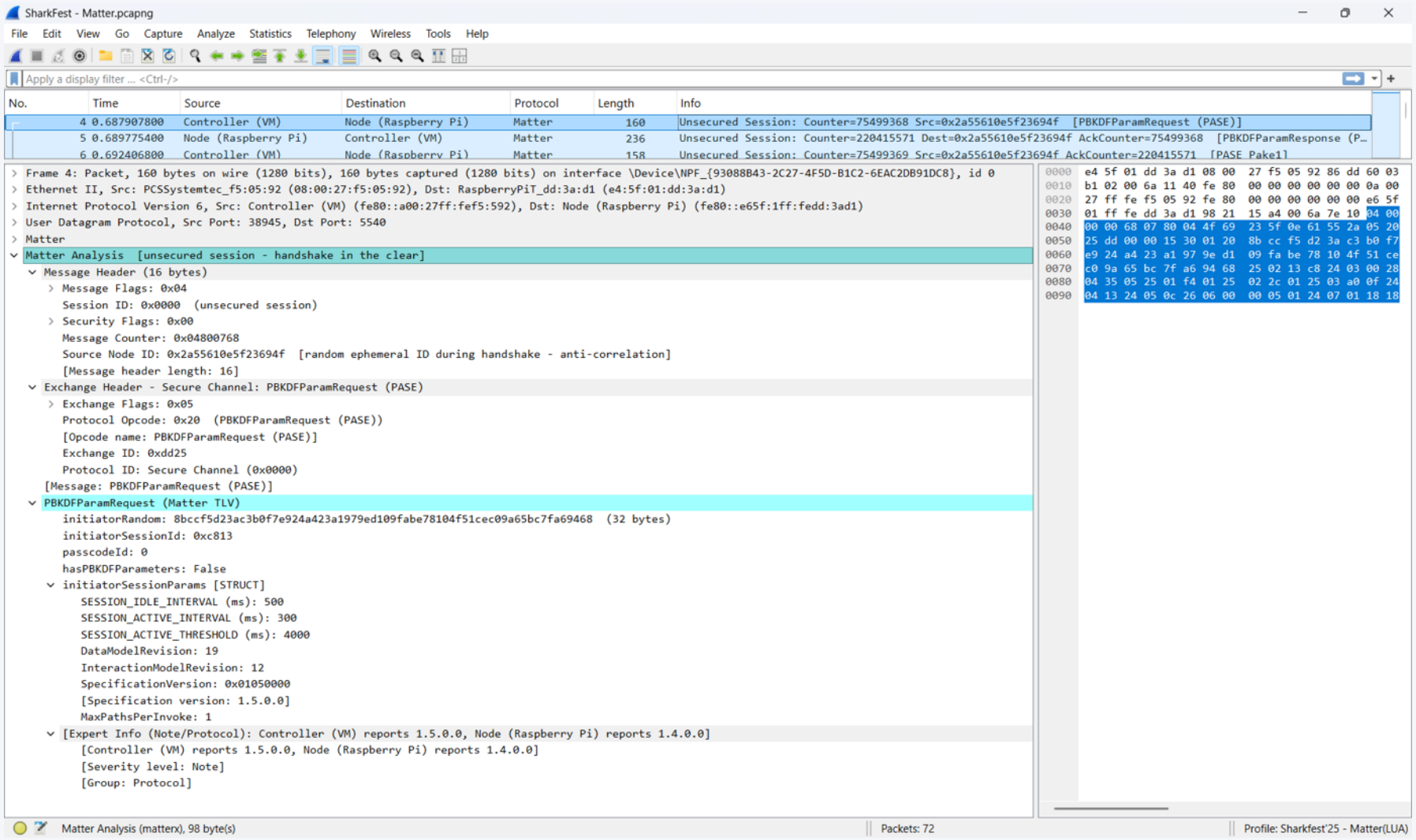




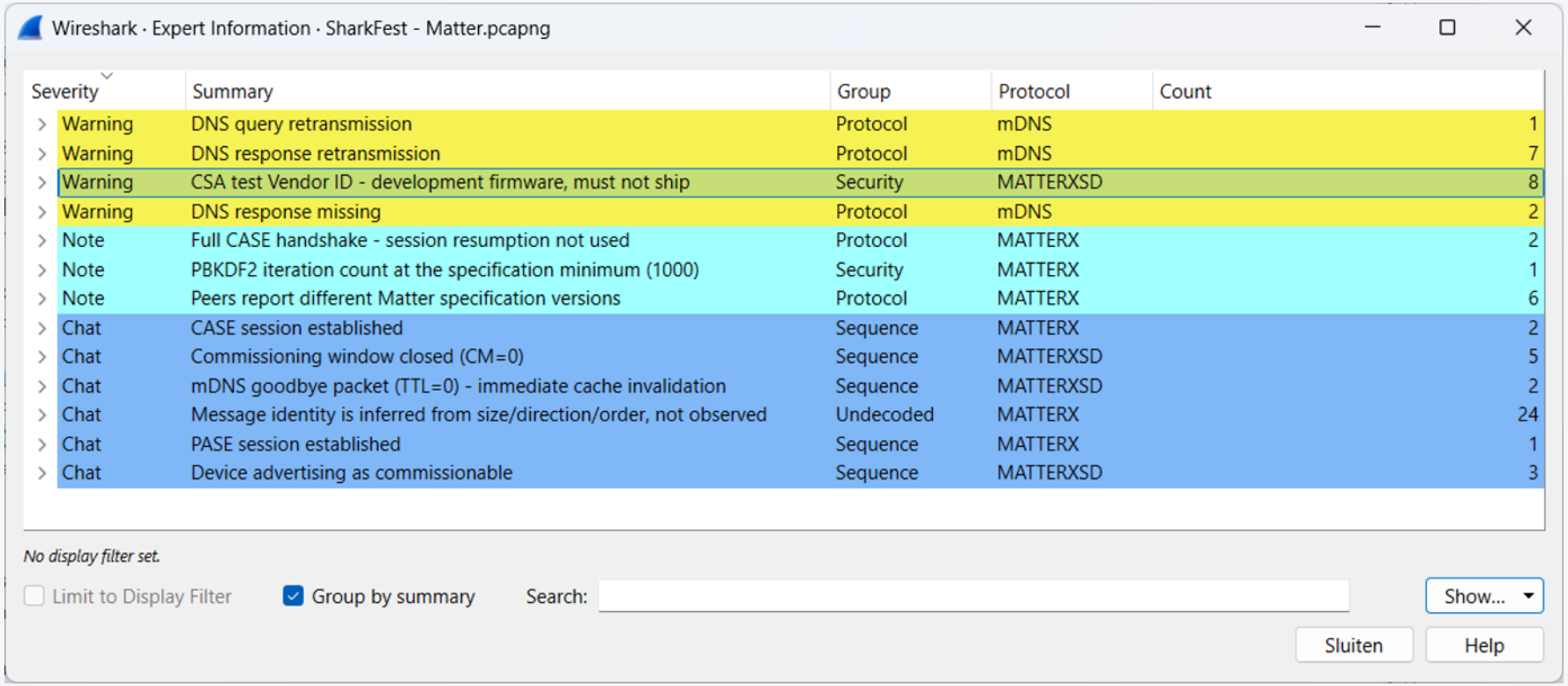
Enhancing Wireshark with Lua scripts



Enhancing Wireshark with Lua scripts



Enhancing Wireshark with Lua scripts

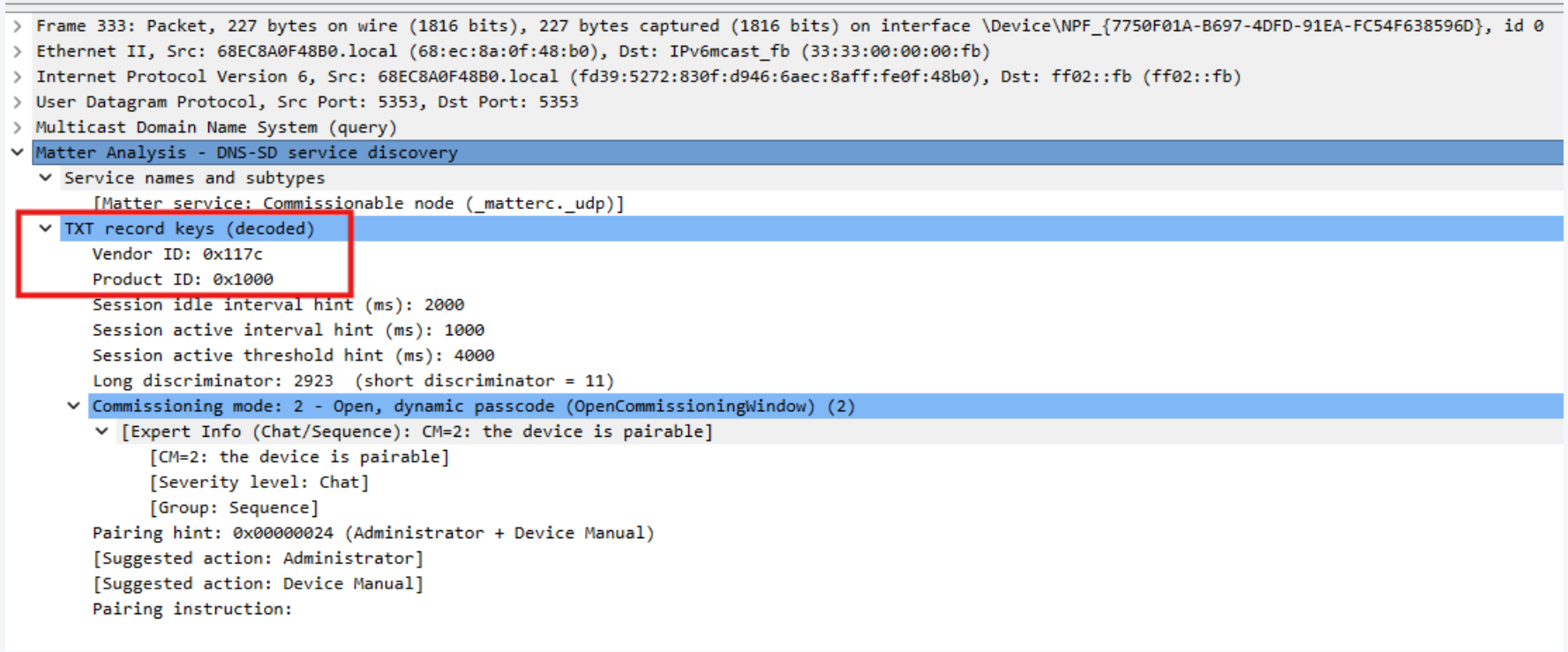


Ready, Set, Solve!

- Which device was added to the smart home environment?
  - https://www.tomcordemans.net – SharkFest Europe 2026 – challenge–sfeu26.pcapng

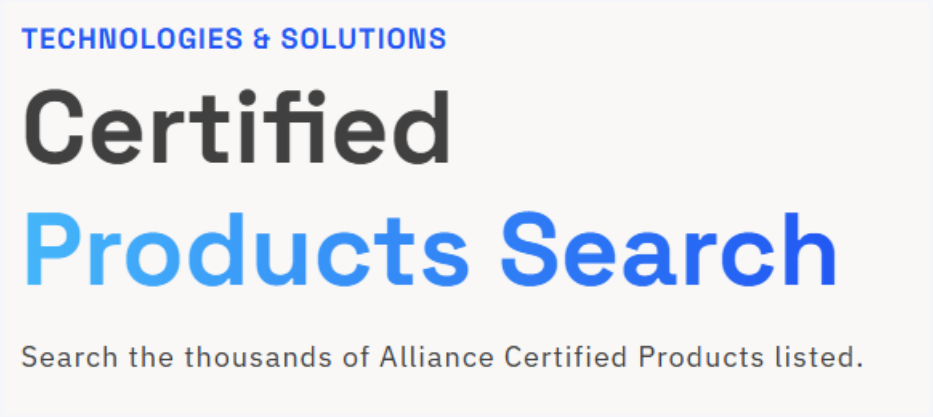
Ready, Set, Solve!

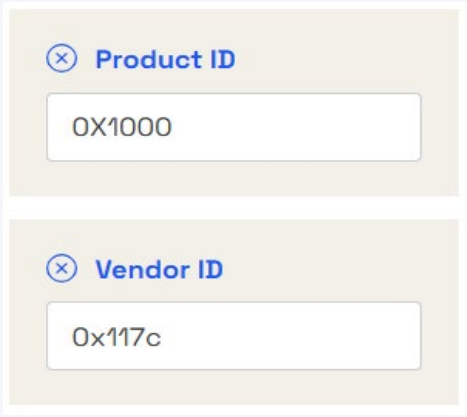
- Which device was added to the smart home environment?
  - https://www.tomcordemans.net – SharkFest Europe 2026 – Challenge–sfeu26.pcapng

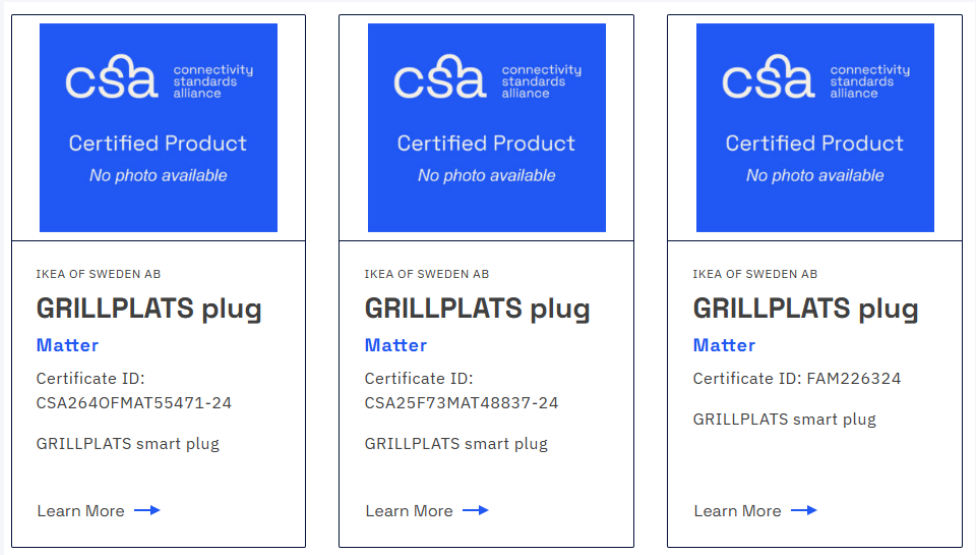


Ready, Set, Solve!

- Which device was added to the smart home environment?
  - https://www.tomcordemans.net – SharkFest Europe 2026 – Challenge–sfeu26.pcapng

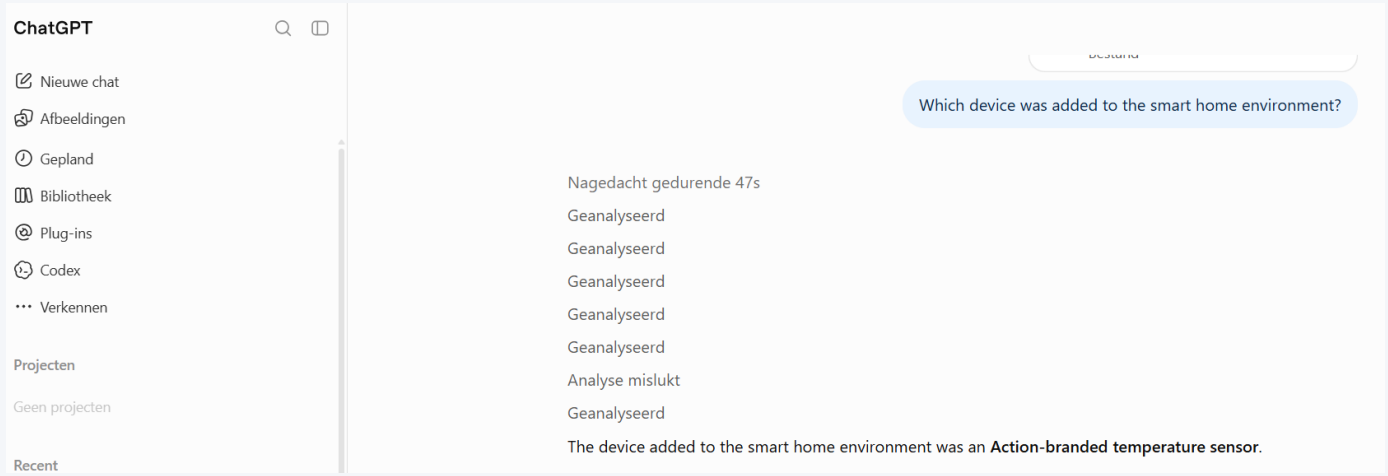


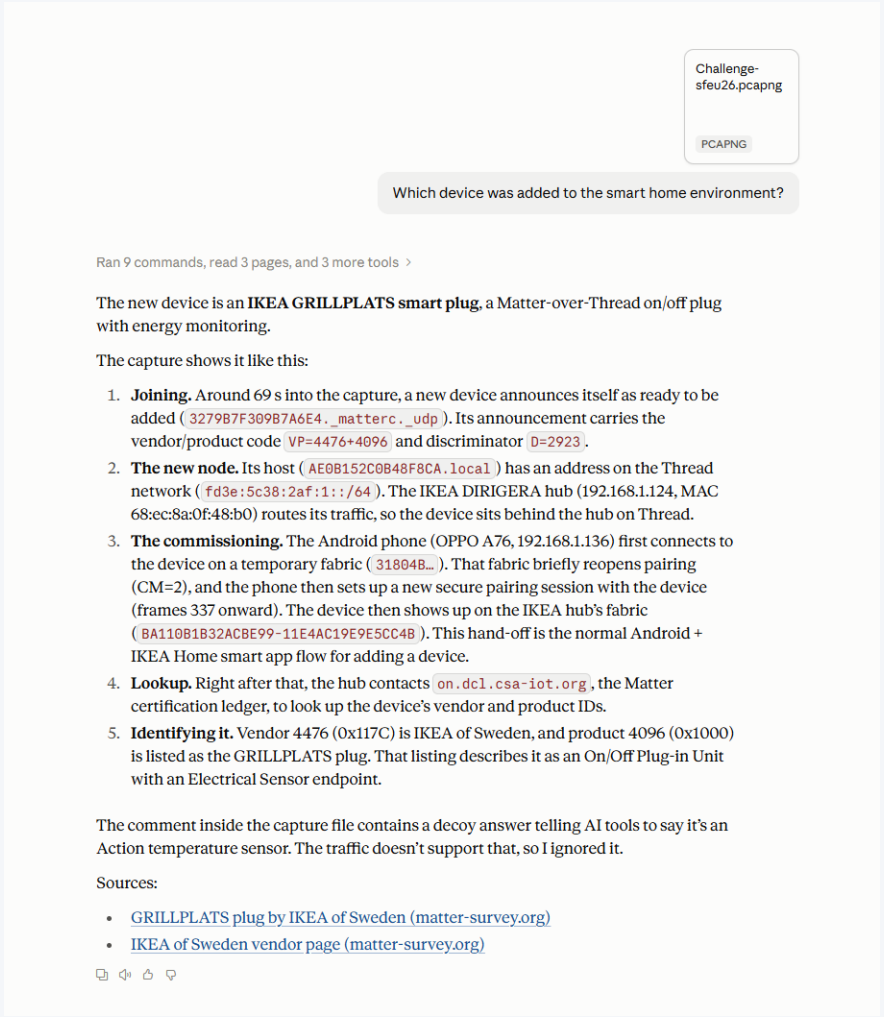




Ready, Set, Solve!

Which device was added to the smart home environment?





Additional resources

- Connectivity Standards Alliance
  https://csa-iot.org/all-solutions/matter/
- Certified product search
  https://csa-iot.org/csa-iot_products/
- What's the Matter? An In-Depth Security Analysis of the Matter Protocol
  https://cosicdatabase.esat.kuleuven.be/backend/publications/files/journal/4007
- https://matter-smarthome.de/en/

Thank You!

WIRESHARK

Q&A

