SL1487A PC Software
CCS Charging Protocol Trace Viewer
SW Version 1.2.0

KEYSIGHT

USER GUIDE

Content

Notices

Copyright Notice

Edition

Edition 1.2.0, March 2024

Printed in

Germany

Published by

Keysight Technologies Deutschland GmbH

Suttner-Nobel-Allee 21

44803 Bochum, Germany

phone +49 234 41 75 78–0

mail info.sl@keysight.com

Technology Licenses

The hardware and / or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is “commercial computer software,” as defined by Federal Acquisition Regulation (“FAR”) 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement (“DFARS”) 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at www.keysight.com/find/sweula. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all

providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data.

Warranty

THE MATERIAL CONTAINED IN THIS DOCUMENT IS PROVIDED “AS IS,” AND IS SUBJECT TO BEING CHANGED, WITHOUT NOTICE, IN FUTURE EDITIONS. FURTHER, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, KEYSIGHT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, WITH REGARD TO THIS MANUAL AND ANY INFORMATION CONTAINED HEREIN, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. KEYSIGHT SHALL NOT BE LIABLE FOR ERRORS OR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, USE, OR PERFORMANCE OF THIS DOCUMENT OR OF ANY INFORMATION CONTAINED HEREIN. SHOULD KEYSIGHT AND THE USER HAVE A SEPARATE WRITTEN AGREEMENT WITH WARRANTY TERMS COVERING THE MATERIAL IN THIS DOCUMENT THAT CONFLICT WITH THESE TERMS, THE WARRANTY TERMS IN THE SEPARATE AGREEMENT SHALL CONTROL.

Safety Information

DANGER

A DANGER notice indicates a (extremely) hazardous situation which, if not avoided, will result in death or serious injury.

Do not proceed beyond a DANGER notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice indicates a hazardous situation which, if not avoided, could result in death or serious injury.

Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

CAUTION

A CAUTION notice indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

NOTICE

A NOTICE indicates to pay attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data.

Do not proceed beyond a NOTICE until the indicated conditions are fully understood and met.

NOTE

A NOTE refers exclusively to application notes without any security relevance.

---

1 Symbols

For this document, the following abbreviations apply:

API	Application Programming Interface
CCS	Combined Charging System
CPT	Charging Protocol Trace Viewer
EXI	Efficient XML Interchange
GPL	General Public License
HAL	Hardware Abstraction Layer
NSS	Network Security Services
SDP	Service Discovery Protocol
TLS	Transport Layer Security
V2G	Vehicle to Grid
XML	eXtensible Markup Language

2 License Management

The usage of the Keysight Charging Protocol Trace Viewer requires a valid license.

With order fulfillment, you should have received an email with instructions on how to register and redeem a license using the Keysight Software Manager (KSM).

For further assistance with the PathWave License Manager setup, please follow the proceeding defined in Keysight Licensing Quick Start Guide.

For a comprehensive understanding, please consult the Keysight Licensing Administrator's Guide.

3 Installation

This section describes how to install the CCS Charging Protocol Trace Viewer and the corresponding plugins for Wireshark.

Requirements

The following requirements are needed for using this software:

- Windows 10/11 (64Bit)
- Wireshark Version 4.2.X (64Bit)
  - https://www.wireshark.org/
- WinPcap 4.1.3 or Npcap (Implicitly enabled during Wireshark installation, install in WinPcap API-compatible Mode)
  - https://www.winpcap.org/
- PathWave License Manager
  - PathWave License Manager V2.7
    - Please use Version 2.7 under Previous Versions and not 7.2

NOTE

The Software was tested with the Wireshark Version 4.2.0 (v4.2.0-0-g54eedfc63953).

PathWave License Manager Version 2.7 was used.

Installing the Keysight Charging Protocol Trace Viewer - Decoder

NOTICE **If a previous version is already installed, make sure to deinstall it first to prevent update issues. Uninstallation can be done in Programs and Features in the Control Panel.**

To install the *Keysight Charging Protocol Trace Viewer - Decoder* software, please use the following procedure (see also Figure 1 - Figure 3):

1 Double-click on the installation file to start the setup wizard and confirm the process with "*Next*" button.

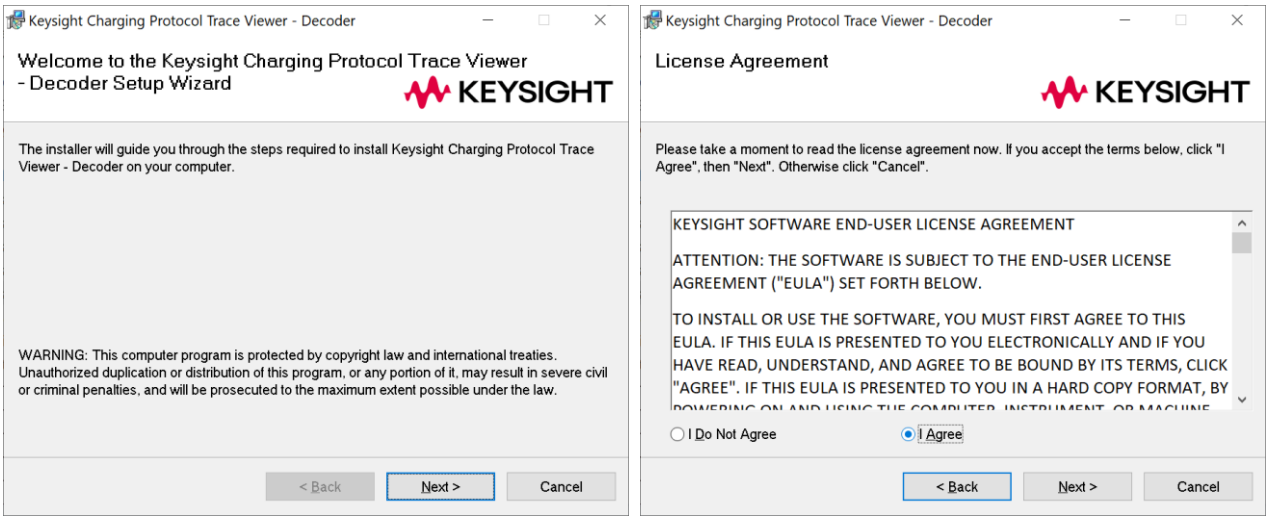

Figure 1: CPT - Decoder Installation - Welcome and EULA

2 Accept the license agreement with "*I Agree*" option and click on "*Next*" button.

3 Select the default installation path and click on "*Next*" button.

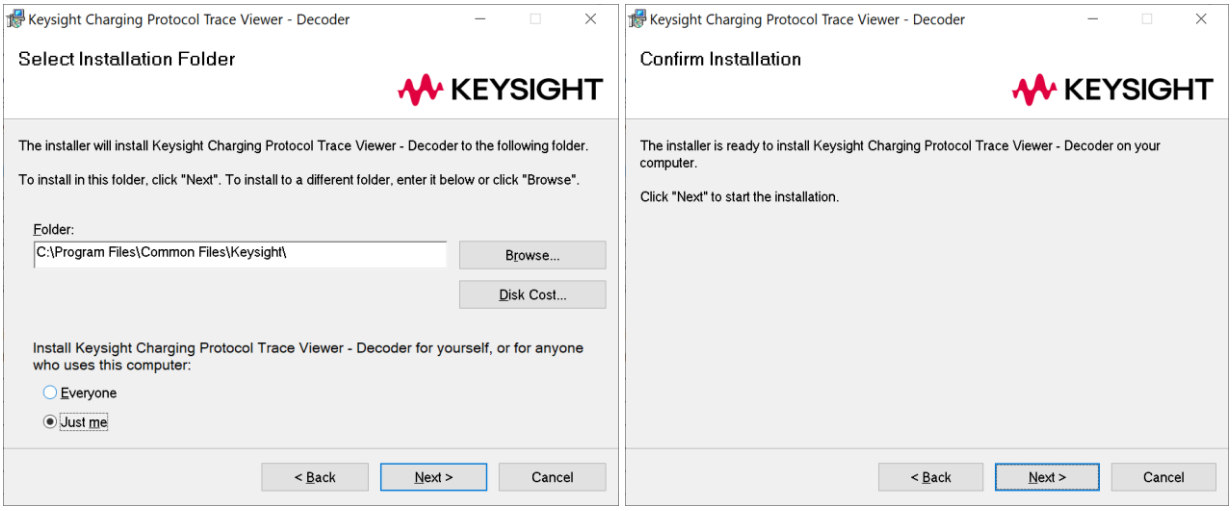

Figure 2: CPT- Decoder Installation - Installation folder selection

NOTICE **If the CPT Decoder is used with Wireshark, the default installation path must be used.**

4 Start the installation with the "*Next*" button, and the software will be installed on your machine. Once the installation is complete, you can close the window.

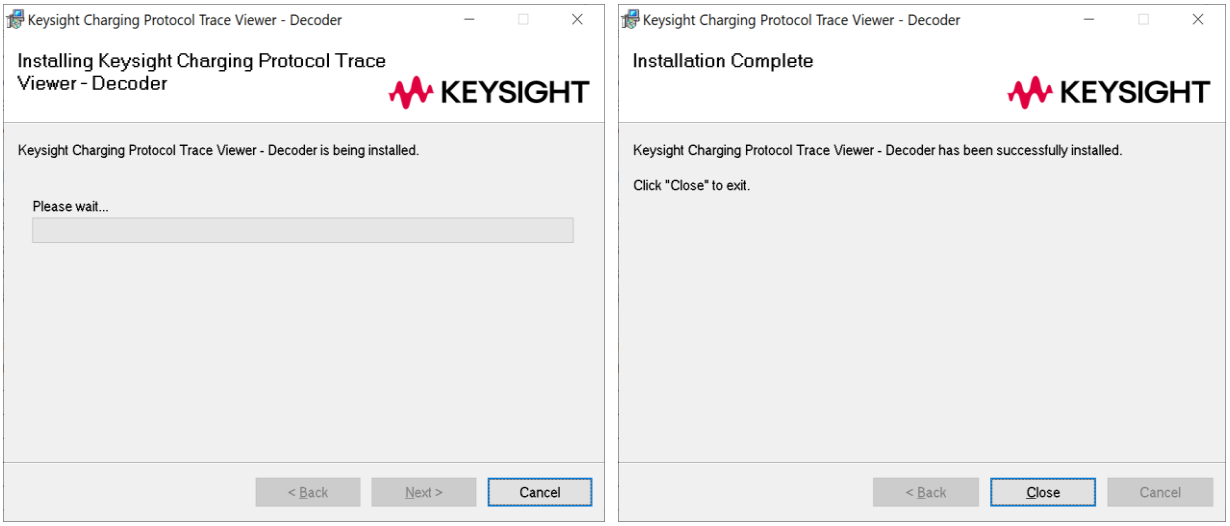

Figure 3: CPT - Decoder Installation - Installation progress and completion window

Installing the Keysight Charging Protocol Trace Viewer

NOTICE **If a previous version is already installed, make sure to deinstall it first to prevent update issues. Uninstallation can be done in Programs and Features in the Control Panel.**

To install the *Keysight Charging Protocol Trace Viewer*, please use the following procedure (see also Figure 4 - Figure 7):

1 Double-click on the installation file to start the setup wizard and confirm the process with "*Next*" button.

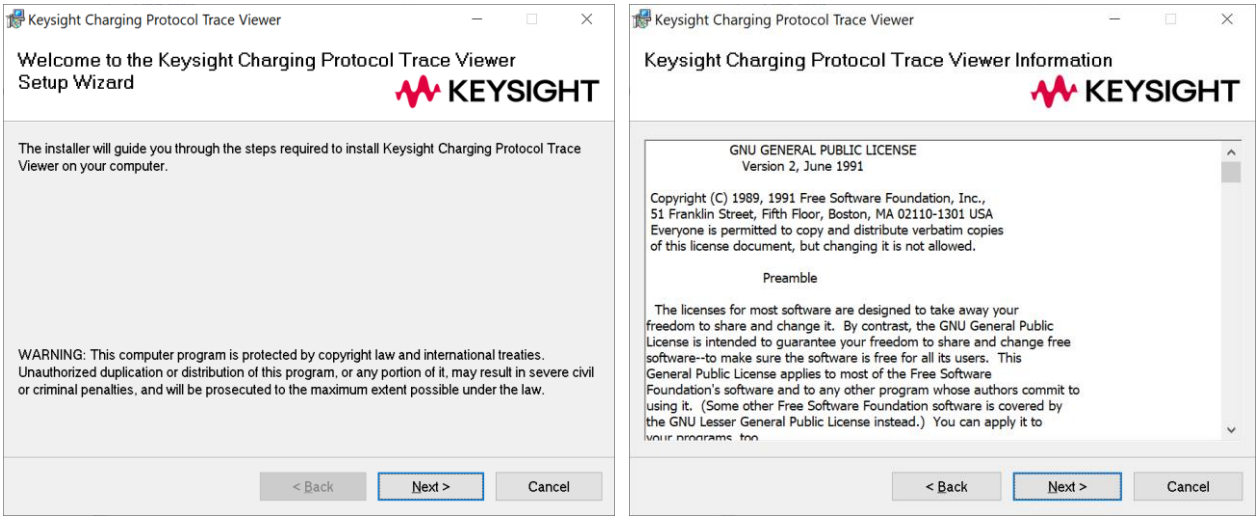

Figure 4: Keysight CPT Installation - Welcome and GNU GPL 2 license notice

2 Confirm the GNU GPL v2 license notice with *"Next"* button.

3 Select the default installation path and click on "*Next*" button.

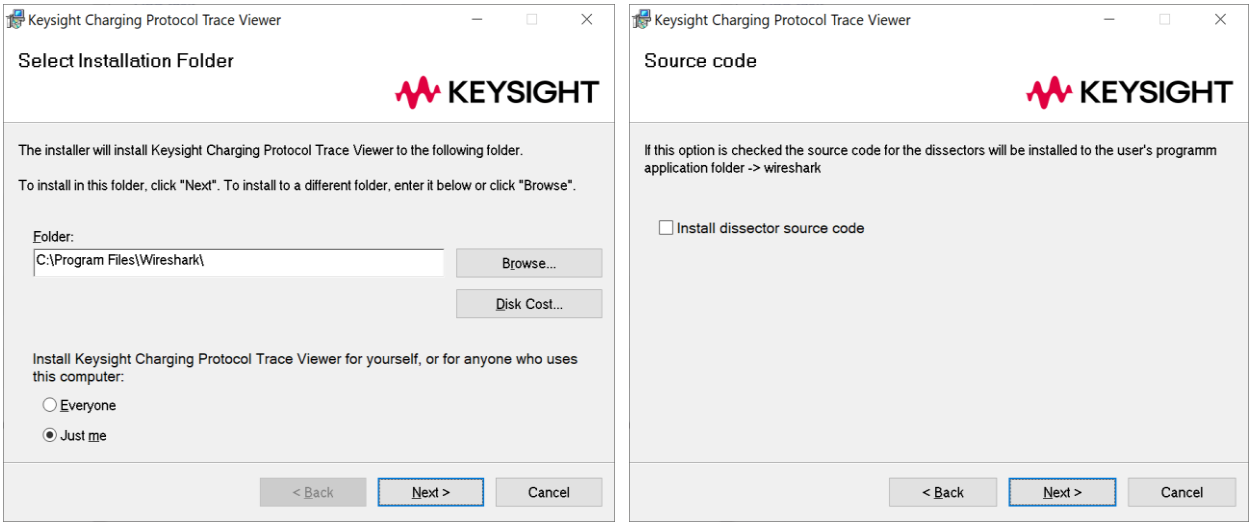

Figure 5: Keysight CPT Installation - Installation path and source code

NOTICE **When prompted, select the installation path of Wireshark on your machine. If the wrong path is used, the dissectors cannot be used correctly.**

4 As an option, the source code of the dissector can be installed under ***C:\Users\Username\AppData\Roaming\Wireshark\Source_Code_Wireshark_Dissector*** by enabling the checkbox "*Install dissector source code*".

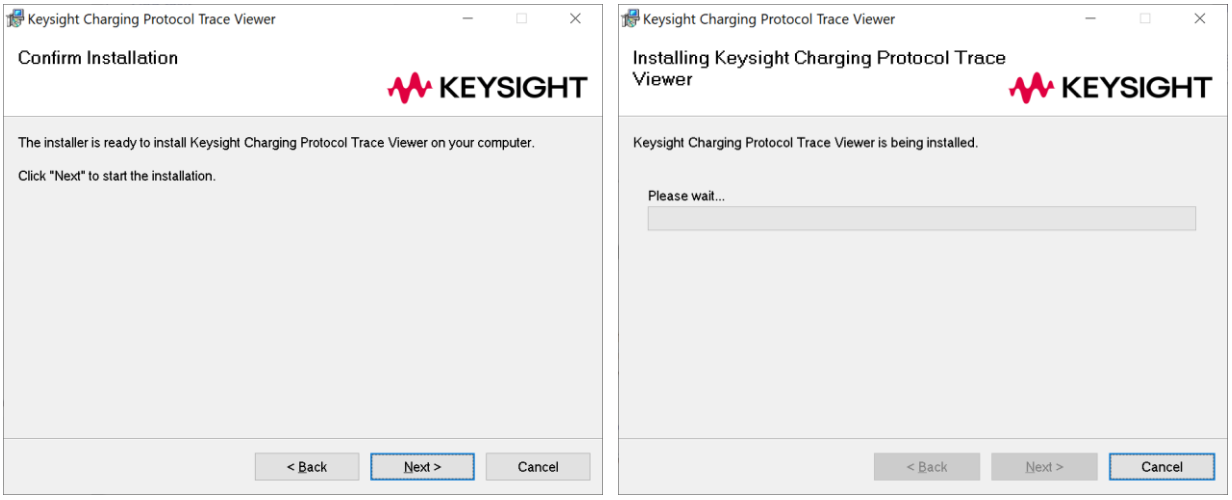

Figure 6: Keysight CPT Installation - Installation progress

5 Start the installation with "*Next*" button, and the software will be installed on your machine. Once the installation is complete, you can close the window.

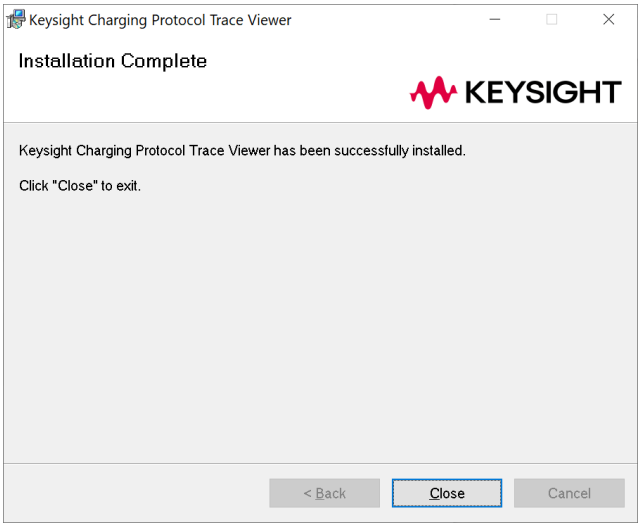

Figure 7: Keysight CPT Installation - Completion window

4 Keysight Charging Protocol Trace Viewer

Charging Protocol Trace Viewer

After the installation of the *Keysight Charging Protocol Trace Viewer* the plugin can be used in Wireshark. The CPT Decoder will always be executed with Wireshark on the startup. The decoder is started on port 1111 by default but can be changed to any number between 1023 and 65535 in the corresponding settings under **Tools → Keysight CPT Plugin → Keysight CPT Settings**. Besides that, the current decoder status is illustrated in the dissector settings as can be seen in Figure 8.

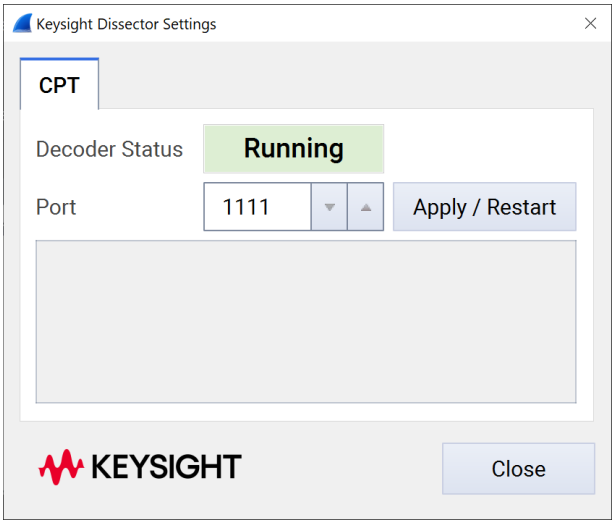

Figure 8: Dissector settings for the CPT Decoder

NOTE **A port change terminates all previous decoder processes and restarts them on the new port. This process may take a few seconds.**

HAL Protocol

The CPT Decoder supports proprietary messages defined for the hardware abstraction layer (HAL). HAL messages consist of two parts: A header and a payload field. The protocol is used in the following scenarios:

- Internal VERISCO configuration messages for the CCS Hardware Test Adapter
- IEC 61851-1:2017 Control Pilot configuration and event messages related to PWM signal characteristics
- IEC 61851-1:2017 Proximity configuration and event messages

NOTICE **.pcap files with HAL messages that belong to previous Software versions released before 2021 are not displayed correctly due to major changes in the HAL library.**

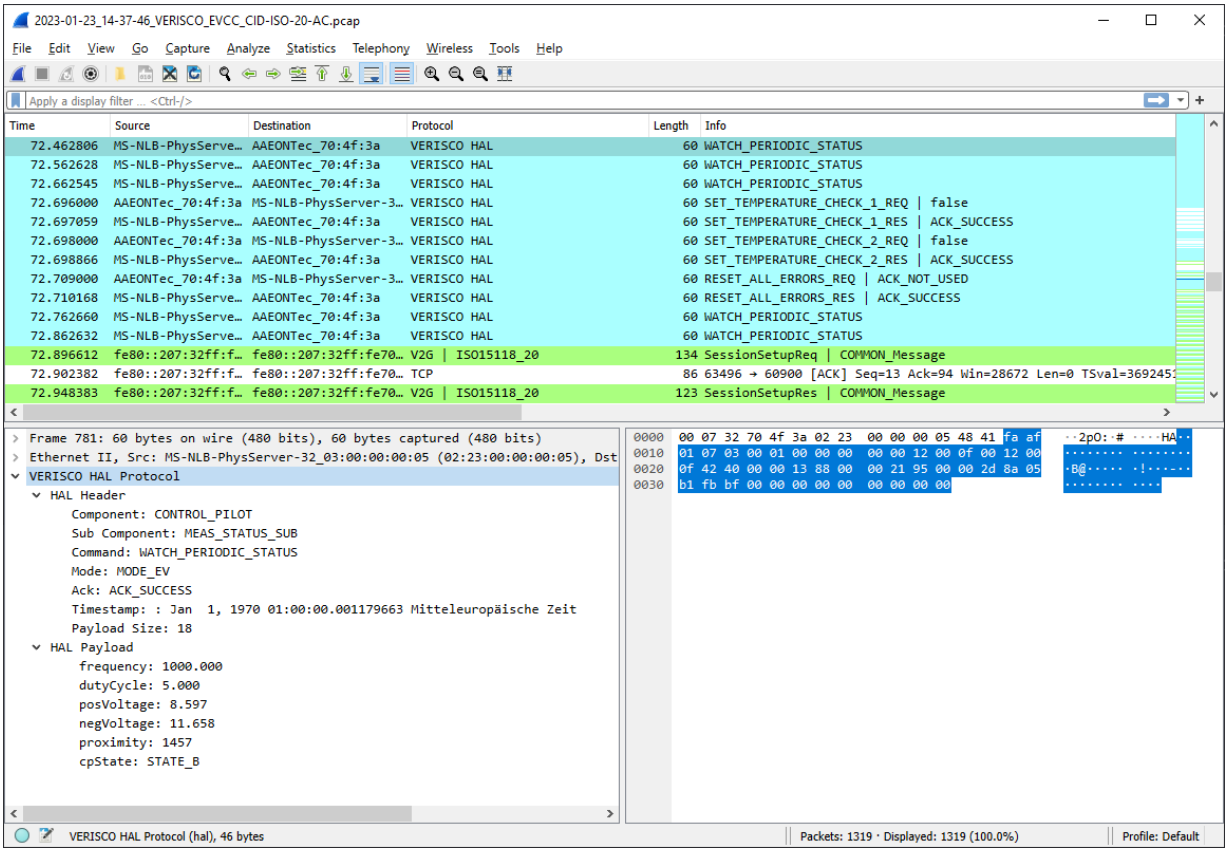

Figure 9: Example for HAL message decoding

V2G Protocol

The CPT Decoder supports message decoding of Combined Charging System (CCS) charging protocols according to DIN 70121, ISO 15118-2/-20. All relevant messages are listed in the following:

- DIN 70121:2014
  - SDP Messages
  - EXI-encoded SupportedAppProtocol messages
  - EXI-encoded V2G Protocol messages
- ISO 15118-2:2014
  - SDP messages
  - EXI-encoded SupportedAppProtocol messages
  - EXI-encoded V2G Protocol messages
- ISO 15118-20

- SDP messages
- EXI-encoded V2G messages

NOTE **All EXI-encoded V2G messages are dissected to human-readable plain XML data format**

NOTE **In case of TLS, V2G messages can only be dissected, when the randomly generated shared TLS session key is available (see section**

Homeplug AV Extended Protocol

This dissector extends the regular Homeplug AV dissector which is part of Wireshark already. In this build there are the following messages that are being able to be decoded further, or to hold some extra information.

Message type	Description
VS_ATTEN_CHAR (Qualcomm)	Displays the gr filed.
VS_GET_PWM_STATS.IND (Vertexcom)	Displays inform
VS_HOST_ACTION.REQ (Qualcomm)	Displays additic

Table 1: Supported messages by the Homeplug AV Extended dissector

NOTICE **If the Ethernet Frame containing the Home using the optional VLAN tag inside the hea the header for 2 more bytes.**

To still be able to decode the messages go "Edit → Preferences… → Protocols → Hon and check the box "VLAN Tag is used by E

TLS Session Master Key).

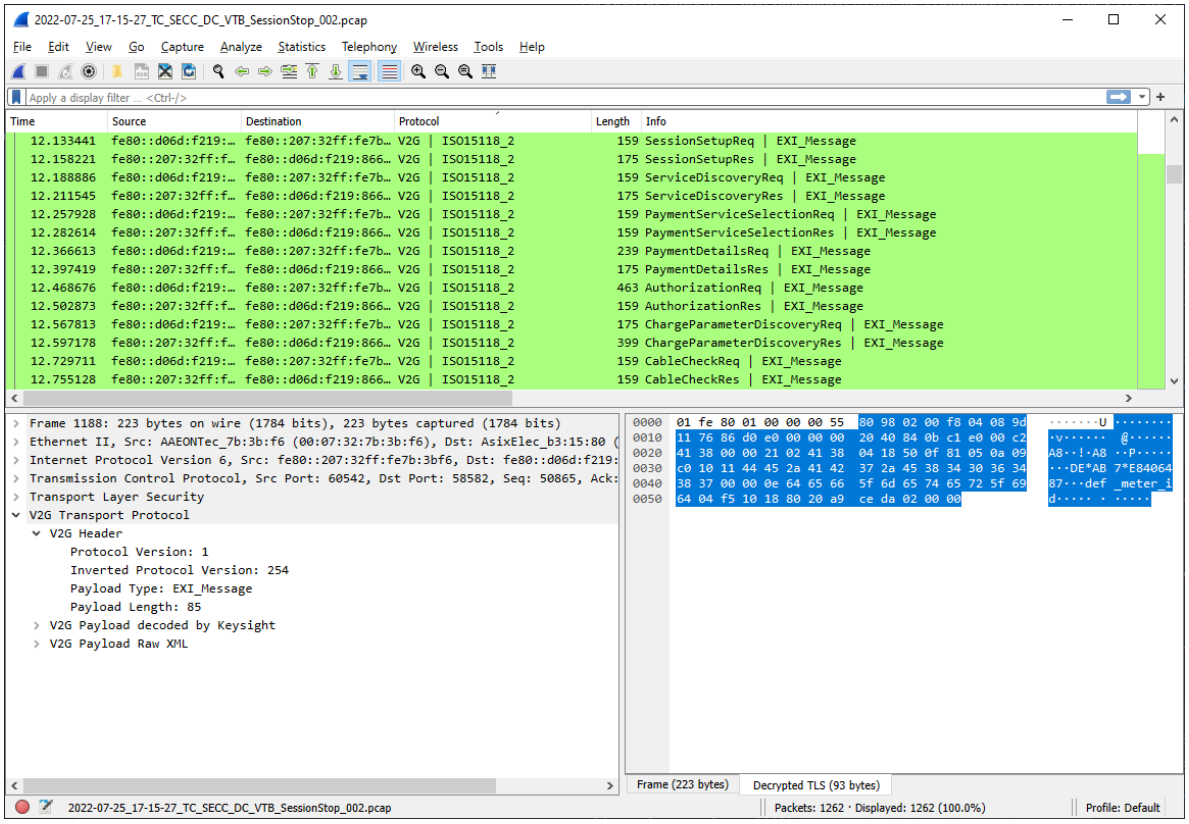

Figure 10: Example for V2G message decoding

There are two different views for decoded V2G messages:

1 V2G payload as a Key Value Pair representation (see Figure 11). This view can be used to get a quick overview of the data that is exchanged via the V2G protocol.

1.

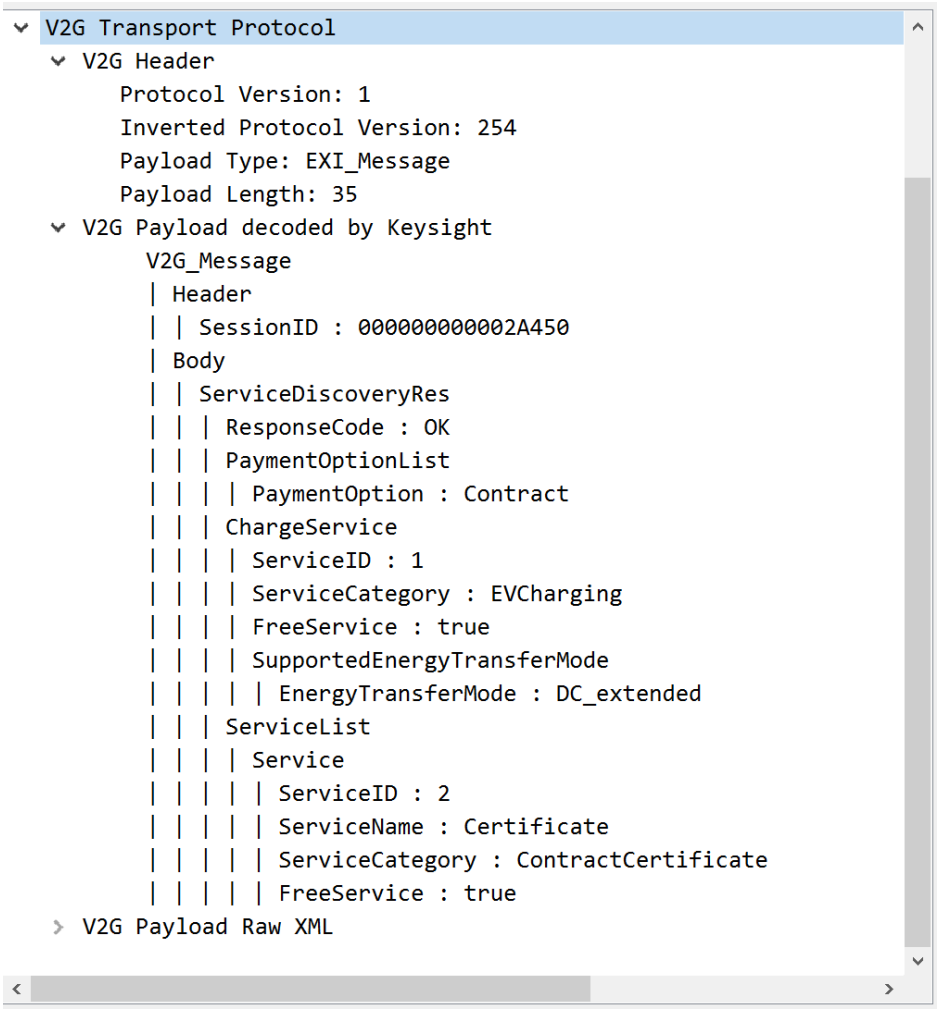

Figure 11: Decoded V2G payload with the Key Value Pair representation

2 V2G payload in the RAW XML format (see Figure 12). This view shows the unfiltered XML messages that are used for the V2G communication.

Figure 12: Decoded V2G payload with the Raw XML representation

Homeplug AV Extended Protocol

This dissector extends the regular Homeplug AV dissector which is part of Wireshark already. In this build there are the following messages that are being able to be decoded further, or to hold some extra information.

Message type	Description
VS_ATTEN_CHAR (Qualcomm)	Displays the groups + average attenuation in the info filed.
VS_GET_PWM_STATS.IND (Vertexcom)	Displays information that the Sniffer took
VS_HOST_ACTION.REQ (Qualcomm)	Displays additional info about the payload

Table 1: Supported messages by the Homeplug AV Extended dissector

NOTICE

If the Ethernet Frame containing the Homeplug AV Protocol is using the optional VLAN tag inside the header, this will extend the header for 2 more bytes.

To still be able to decode the messages go to:
“Edit → Preferences… → Protocols → Homeplug AV Extended”
and check the box “VLAN Tag is used by Ethernet Frame”.

TLS Session Master Key

This section outlines the usage of a TLS Session Master Key and automated decryption of V2G messages encrypted with TLS. An example of a TLS Session Master Key message is shown in Figure 13.

If the dissector identifies an UDP package matching the standards from the NSS Key Log Format the transmitted key will be saved in a log file located in “*C:\Users\username\AppData\Roaming\Wireshark\TLS_Keys*”.

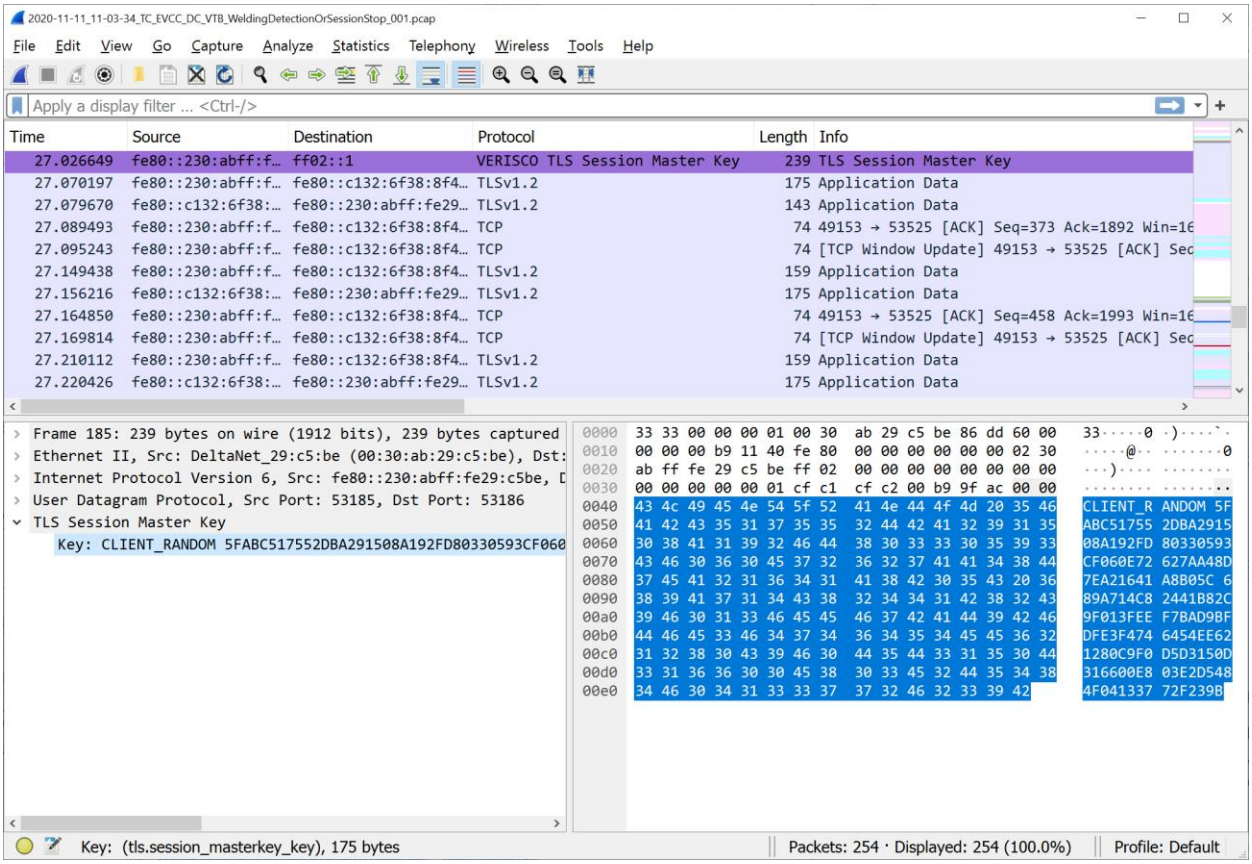

Figure 13: Example for a TLS Session Master Key message

Additionally, an empty Debug.txt file will be created to log potential issues. If a TLS Master Key message is detected in the pcap trace, the TLS decryption can be enabled by selecting

the corresponding protocol as defined in the following proceeding (see also Figure 14):

1 Right-click on one of the encrypted TLS packages and select "*Decode as*".

2 Select "*V2G*" from the dropdown menu and confirm the selection with “*OK*”.

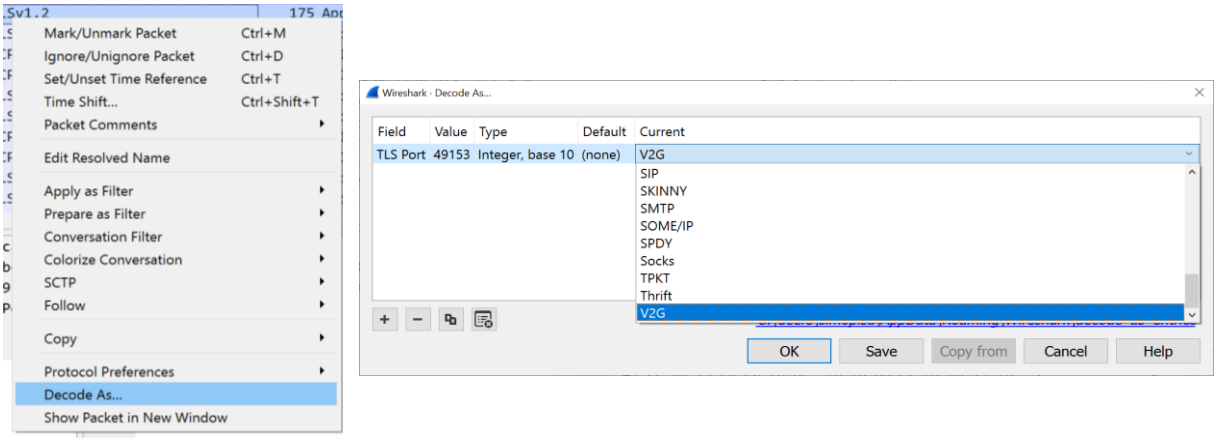

Figure 14: Context menu to specify a decoding protocol

Afterwards, the pcap trace will be reloaded with the decrypted V2G data content (see Figure 15).

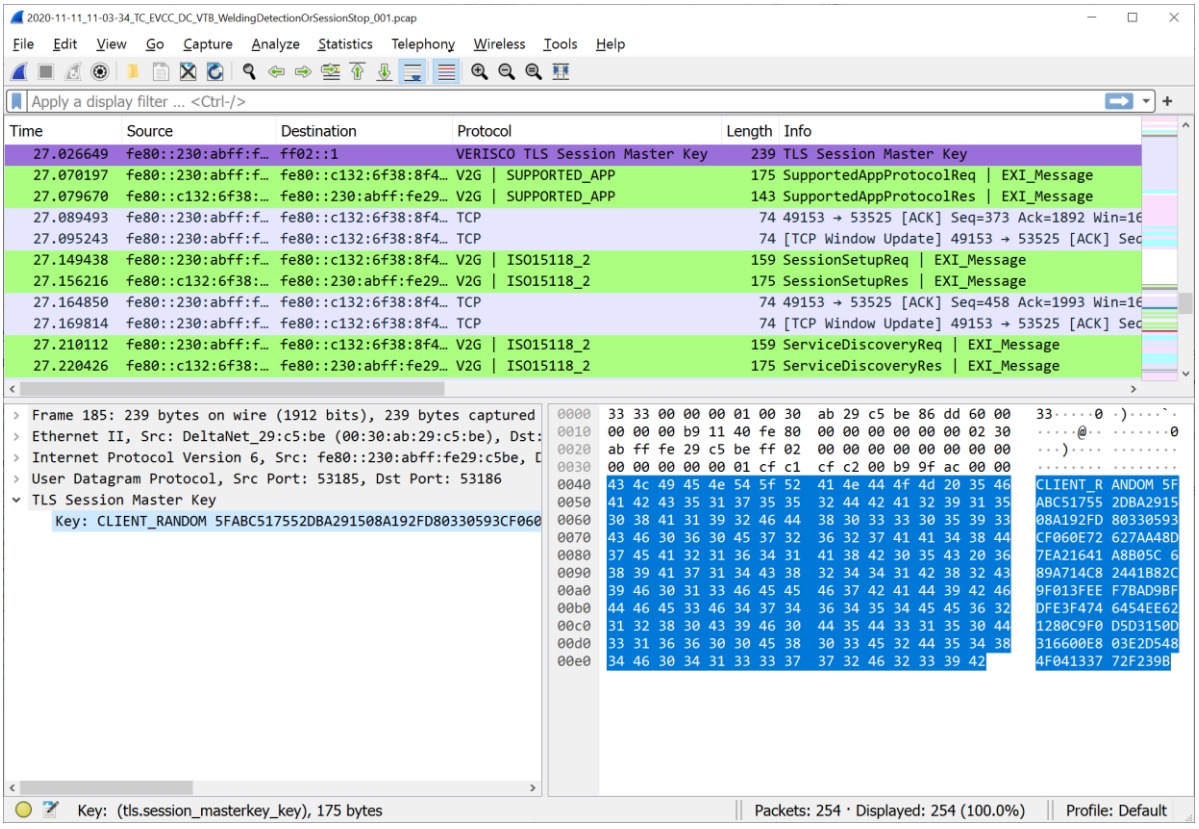

Figure 15: Decrypted V2G messages using the TLS Session Master Key

NOTICE

If multiple charging sessions with different TLS keys are located in a single .pcap file, this could lead to a decryption failure for the TLS messages that are not similar to the first key/charging session. In that case the charging sessions should be split to their own .pcap files.

Select all packets needed in Wireshark then click on: "File -> Export Specified Packets…" Enter a new file name and select the option "Selected packets only", hit "Save" and open the new .pcap file and decode a above.

NOTICE

In case of a packet loss (TCP segment not captured, TCP retransmission, etc.) this could lead to a bahavior where some TLS messages are not decrypted.
A possible solution for this is to active the option "Message Authentication Code (MAC), ignore "mac failed"
Found in: "Edit -> Preferences… -> Protocols -> TLS"

NOTE

Example PCAP-Traces can be found in the following path: "C:\Users\USERNAME\AppData\Roaming\Wireshark\Example PCAPs".

Coloring rules

For better readability, each protocol is assigned to a different color. To apply the coloring rules used in this document, the user can import them as defined in the following:

1 Go to the menu and open "*View*" → "*Coloring Rule*".

2 Click on "*Import*" to select pre-defined filters.

3 Navigate to the file that contains the color rules. For the CPT protocols, this file can be found at: "*C:\Users\username\AppData\Roaming\Wireshark\Colorfilter_CPT*".

After importing, the new rules will appear at the bottom. To display packets in the correct color, select the imported rules and drag them to the top. The order defines the priority of the color rule. Your coloring rules should now look like Figure 16 below for the first four entries. To change the displaying colors simply click on "Foreground" / "Background" and choose a color you would like.

4 Click "OK" to apply changes.

Figure 16 - Coloring Rules

5 Charging Protocol Trace Viewer – Decoder

To start the CPT Decoder, please use the following procedure:

1 Open a console window (cmd.exe).

2 Navigate to the charging_protocol_decoder.exe and press enter. The executable file can be found in the following path:
C:\Program Files\Common Files\Keysight\Charging Protocol Trace Viewer

NOTICE **The path can be different if the default installation path has been changed during installation. In this case, the CPT Decoder cannot be used within Wireshark.**

2.

In general, the CPT Decoder can be used in two modes.

Standalone decoding via console

To use the decoder in simple application mode, the user must specify a protocol and the encoded hex data as can be seen in the following examples
(see also Figure 17 - Figure 18):

Command: C:\Path\to\my\File\charging_protocol_decoder.exe HAL faaf010300f0e000000185df105125000101fbbf

```
C:\Program Files\Common Files\Keysight\Charging Protocol Trace Viewer>charging_protocol_decoder.exe HAL faaf010300f0e000
000185df105125000101fbbf
{
  "timestamp" : 1674484666661,
  "opMode" : "MODE_PC",
  "ack" : "ACK_NOT_USED",
  "command" : "SET_STATE",
  "payloadSize" : 1,
  "payload" : "STATE_A",
  "commandType" : "REQUEST",
  "commandParameter" : "PARAM_CP_STATE",
  "component" : "CONTROL_PILOT",
  "subComponent" : "STATE_SUB"
}
```

Figure 17: Example for HAL message decoding

Command: C:\Path\to\my\File\charging_protocol_decoder.exe V2G 01fe8002000000138094043 3f88205a4d3eed3898dac6f8dd30228

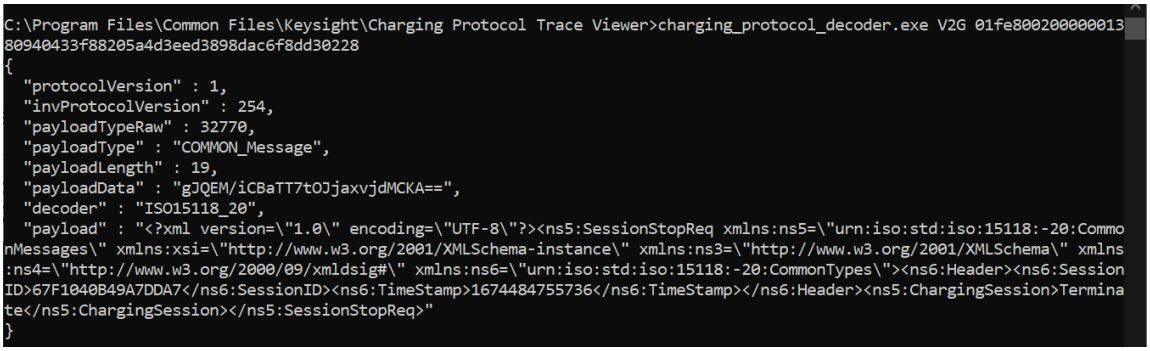

Figure 18: Example for V2G message decoding

Any invalid data input will result in an exception or error message containing further information.

Decoding as a WebSocket service

To use the decoder as a WebSocket service, the user must add a port number to the command line as can be seen in the following example:

Command: C:\Path\to\my\File\charging_protocol_decoder.exe 1234

Afterwards a WebSocket application is started on the local host and the defined port address. This approach is used by the *Keysight Charging Protocol Trace Viewer* as defined in the next section.

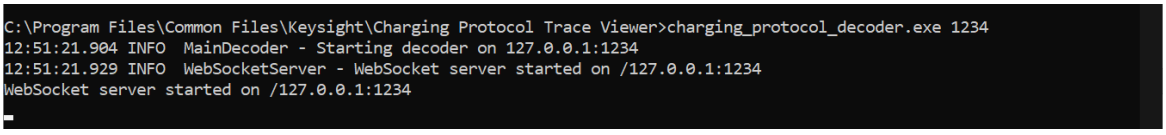

Figure 19: Example for a WebSocket based decoder

Edition 1.2.0, March 2024
www.keysight.com