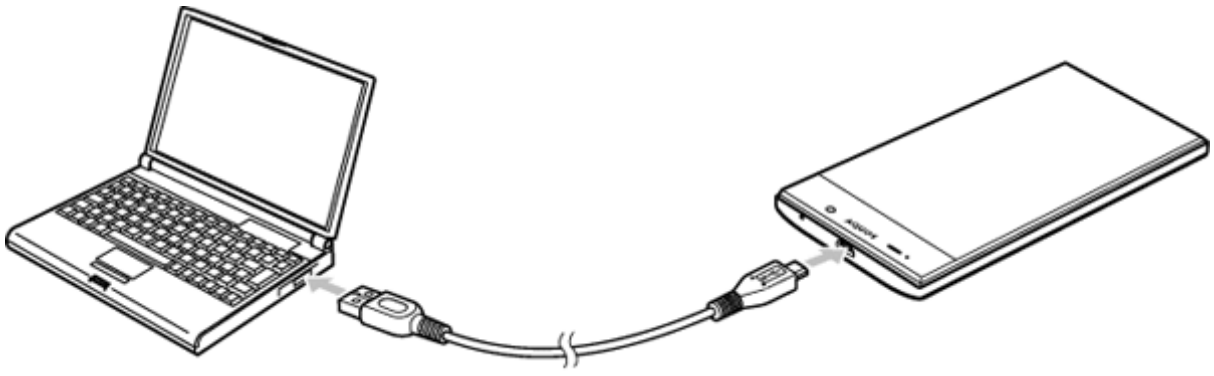
infostam

diagport toolkit

User Manual



V1.8

Table of Contents

1 Introduction

The **diagport toolkit** (dtk) Windows application is a tool communicating with Qualcomm-based smartphones and CPE modems, allowing to capture raw 2G/3G/4G/5G radio frames. The tool uses the Qualcomm diagnostic protocol, also called QCDM (Qualcomm Diagnostic Monitor) to communicate with the device. It allows us to generate packets captures in PCAP file format using either an Android smartphone or a modem. Additionally, it is capable of decoding proprietary 5G frames and create decoded PCAPNG files can be used and interpreted by any network protocol analyzer application which handles this type of file format.

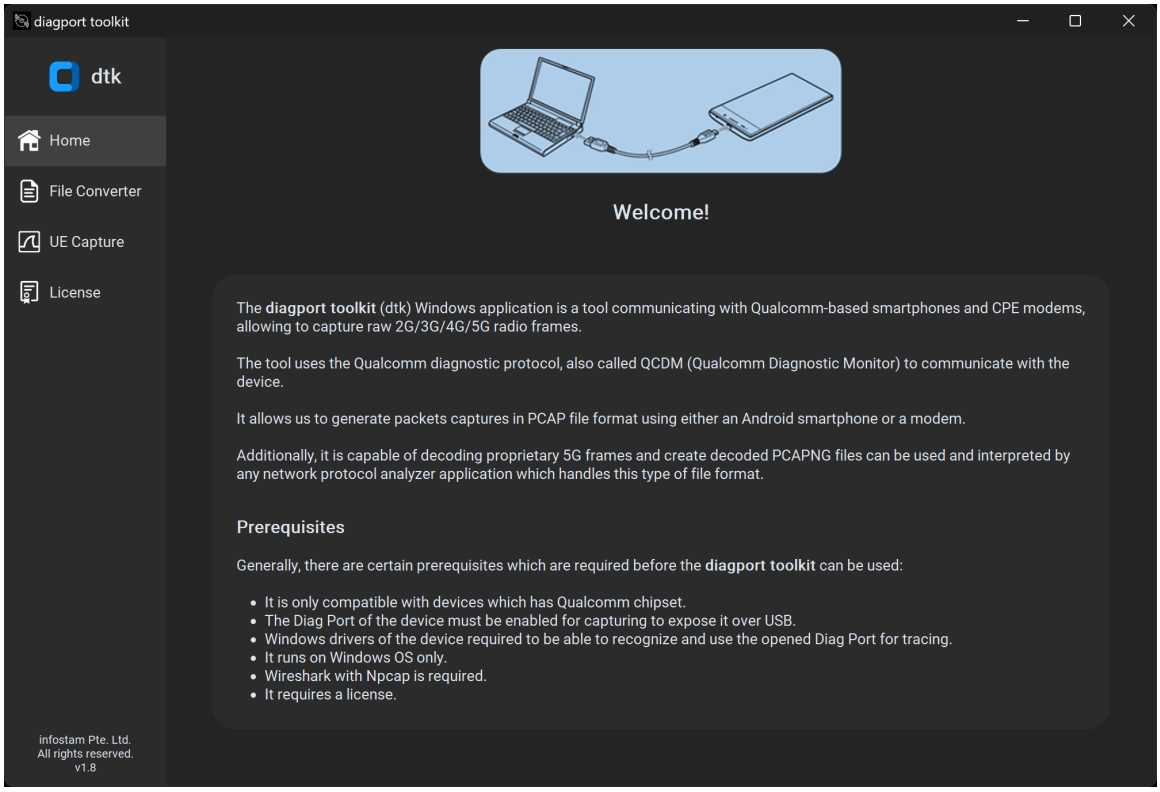


Figure 1: The **diagport toolkit** Windows application

1.1 The diagport toolkit fundamentals

- Supports capturing a handful of mobile radio protocols.
- Allows to capture on layer 3, as it is the most practical to analyze using a network protocol analyzer (e.g. Wireshark), and is what the Diag protocol provides natively.
- By default, the IP traffic sent by the device is not included, only the signaling frames can be seen. Additional parameter needs to be set to include IP traffic.
- Different mode and module options are available.
- Supports converting PCAP or PCAPNG files with proprietary 5G frame headers by removing those headers and decoding those 5G frames.
- Supports converting the following file types to PCAPNG with decoded 5G frames:
- Qtrun: NSG Android app log file and AirScreen PC app exported text file,
- Rohde & Schwarz: QualiPoc app SQZ and MF files.
- Handles the license.

2 Quick Guide

2.1 Prerequisites

Generally, there are certain prerequisites which are required before the **diagport toolkit** application can be used:

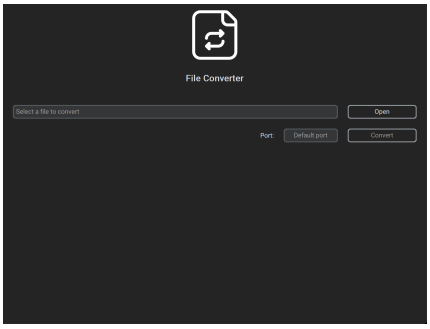
- It is only compatible with devices which has Qualcomm chipset.
- The Diag Port of the device must be enabled for capturing to expose it over USB.
- Windows drivers of the device required to be able to recognize and use the opened Diag Port for tracing.
- It runs on Windows OS only.
- Wireshark with Npcap is required.
- It requires a license.

Fulfilling these requirements is the responsibility of the end user. Further clarifications or discussing issues with any of those items above are possible, refer to section 5 Support.

2.2 File Converter

In order to use this tool:

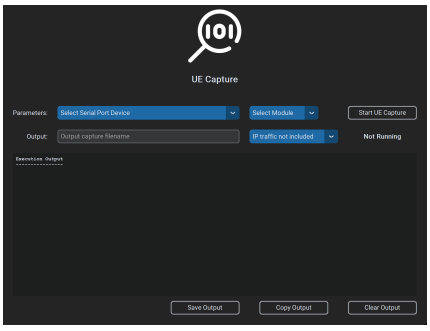
- Select a file to convert
- Optionally, define a port.



2.3 UE Capture

In order to use this tool:

- Select a Serial Port Device.
- Select a Module (`pcap`, `wireshak-live`, `info`).
- Provide an Output capture filename (in case of `pcap` Module is selected).
- Select if IP traffic is included or not.
- Start/Stop UE Capture

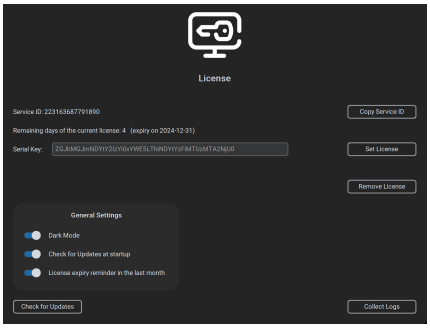


2.4 License

Options to handle license:

- Copy Service ID.
- Input Serial Key, if required.
- Set or Remove License.
- Additionally, Collect application logs.

General Settings, Checking for Updates, Collect Logs



3 Licensing and Upgrade

3.1 Fundamentals

The **diagport toolkit** is a commercialized application for telecom specific troubleshooting and engineering purpose. Only paid versions are available which require a time-based license subscription (e.g. annual subscription). As long as the subscription is active the application support and upgrade are automatically included.

3.2 License

The end user subscription is controlled via a license (Serial Key) which is generated with a code related to the computer hardware and therefore, the license is not transferrable automatically. In case of license transfer is required (e.g. the computer is replaced), the license must be regenerated.

The *License* frame shows the

- Unique Service ID.
- The remaining days of the current license.
- The Serial Key via the placeholder text of an entry field.
- General Settings.

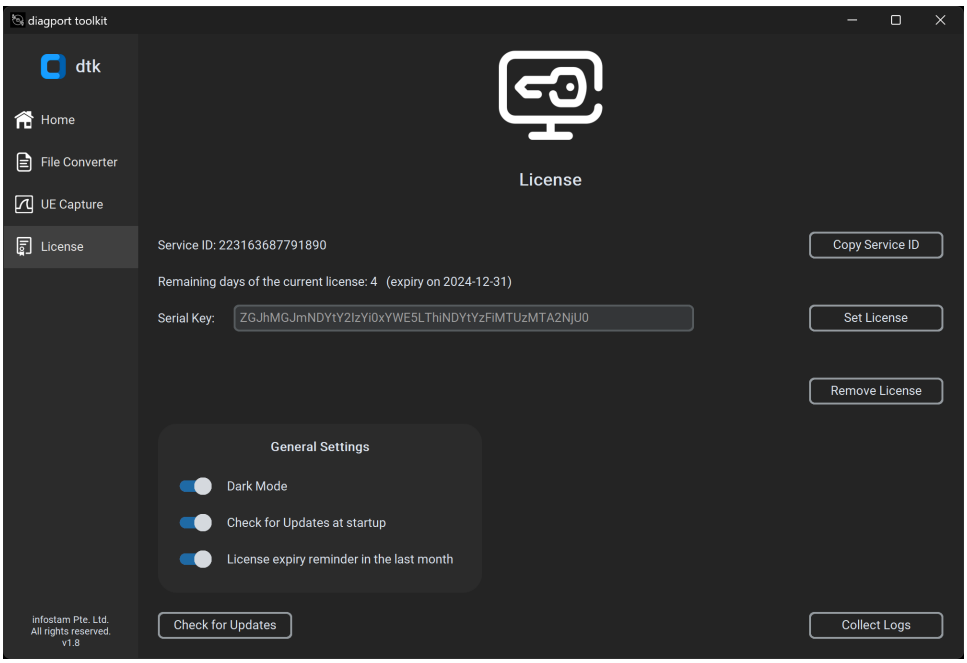


Figure 2: License Handling

The *Copy Service ID* button copies the service ID to the clipboard.

The *Set License* button stores a license provided in the entry field.

The *Remove License* button deletes the earlier stored license.

The *Check for Updates* button is used for checking for new software version.

Additionally, the *Collect Logs* button is used for collecting history logs of the application executions.

3.2.1 Copy Service ID

After clicking on the *Copy Service ID* button, a popup message is shown.

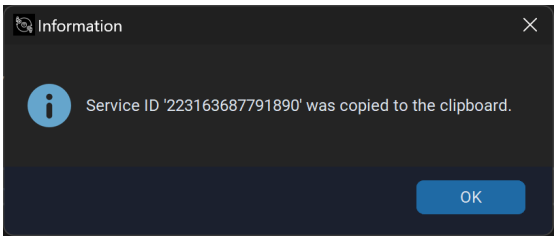


Figure 3: Copy Service ID popup message

3.2.2 Set License

If a valid license was entered into the entry field, then after clicking on the *Set License* button a popup message of successful license storing is shown.

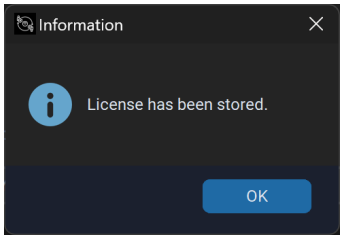


Figure 4: Set License successful popup message

If no license or invalid license was entered, after clicking on the *Set License* button an error popup message is shown.

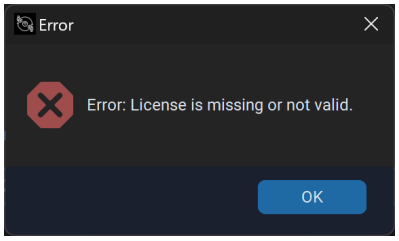


Figure 5: Set License error popup message

3.2.3 Remove License

After clicking on the *Remove License* button, first a confirmation warning is shown and after selecting *Yes* a popup message of successful license removal is shown.

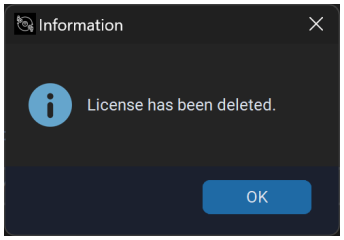


Figure 6: Remove License popup message

3.2.4 Collect Logs

After clicking on the *Collect Logs* button, a popup message is shown a the logs in a compressed file is stored under the `logs` subfolder.

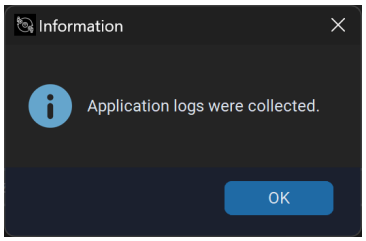


Figure 7: Collect Logs popup message

3.2.5 General Settings

The following setting options are available:

- **Dark Mode**: It is a switch to select between dark and light appearance mode.
- **Check for Upgrades at startup**: It is a switch to select an automatic check for new software version will be done at every application startup.
- **License expiry reminder in the last month**: It is a switch to select an automatic license expiry reminder within the last month of the license validity.

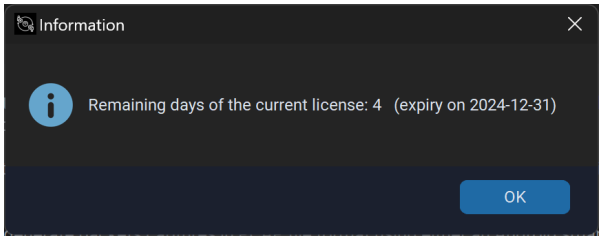


Figure 8: License expiry reminder popup message

3.3 Upgrade

The new version of the applications or the plugin is published either via e-mail or a cloud-based file sharing application (e.g. Google Drive, GitHub or similar). E-mail notification will be sent to end users with active subscription to download the software new version. Depending on the `changelog`, license regeneration might be required.

Additionally, the *License* frame has a *Check for Upgrades* button for manual check for new software version.

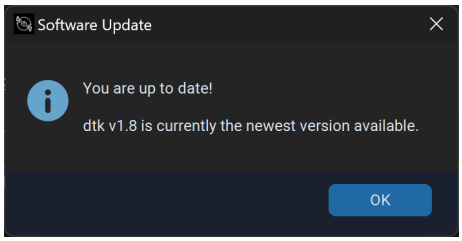


Figure 9: Checking for Upgrades popup message

Note, if the Internet is unreachable but the local network is working, the *Checking for Upgrades* popup message may take 10-15 seconds to show due to the “DNS client resolution timeouts” of the Windows OS.

If the *Check for Updates at startup* is selected on the *License* frame, an automatic check for new software version will be done at every application startup.

4 Features and Functionality

The popular Android smartphone devices in the global market come in two variants – one with **Qualcomm** and the other with **MediaTek chips**. Both variants offer excellent features and performance, but what sets Qualcomm devices apart from the rest is their ability to open a diagnostic port. With this port, users can access a range of diagnostic tools to troubleshoot their device effectively.

4.1 What is a Diag Port?

A *Diag Port* is a special diagnostic port used to test and troubleshoot electronic equipment. This port is typically found on computers and other electronic devices. It allows technicians to connect special diagnostic equipment to the device to test its functionality. It is used for various purposes, including system troubleshooting, debugging, and performance analysis.

Diag Port on smartphones is used to repair the IMEI number of Qualcomm Snapdragon-powered smartphones. However, it's worth mentioning that the MediaTek processor-powered smartphones do not require opening the *Diag Port* for IMEI repair.

4.2 Open the Diag Port on smartphones

Samsung, OnePlus, Realme, OPPO and other Android based smartphones all have a feature called "*Diag Port*", if it is based on Qualcomm chipset. This feature lets you access diagnostic information about your phone's hardware and software. This information can be helpful if you're having problems with your phone or trying to diagnose a problem or restore something like IMEI.

There are three ways you can open the *Diag Port* on your smartphone:

- Using Secret Dialer Code; or
- Using ADB; or
- Using Terminal APK.

The *Diag Port* of the device must be **enabled** for capturing to expose it over USB.

4.3 Supported Protocols

The **diagport toolkit** application supports capturing a handful of mobile radio protocols. These protocols are put after a GSMTAP header, a standard header (encapsulated into UDP/IP) permitting to identify the protocol, and GSMTAP packets are put into a PCAP file that is fully analyzable using Wireshark.

The 2G/3G/4G/5G protocols can be broken into a few "layers": layer 1 is about the digital radio modulation and multiplexing, layer 2 handles stuff like fragmentation and acknowledgement, layer 3 is the proper signaling (RRC) or user data.

The 3GPP 5G gNB and UE Protocol Stack tightly coupled to the underlying radio protocol stack and utilize proprietary vendor specific communication mechanism (instead GSMTAP). This requires additional decoding the proprietary interface (e.g. the Qualcomm header part).

The **diagport toolkit** application allows us to capture on layer 3, as it is the most practical to analyze using Wireshark and is what the Diag protocol provides natively.

4.4 Installation

The **diagport toolkit** application runs on Windows, but beforehand ensure that the device is correctly recognized in *Device Manager* (Figure 10) since the application directly needs to connect to the *Diag Port* over pseudo-serial USB. This means the smartphone's USB driver or a generic Qualcomm USB driver installation is required.

The **diagport toolkit** application has been tested on Windows 11 only.

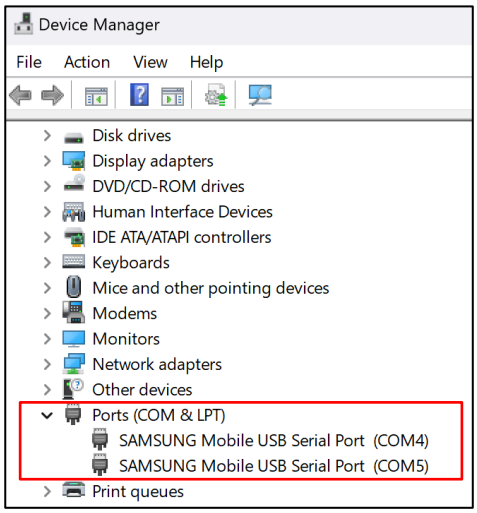


Figure 10: Device Manager in Windows OS

Download the toolkit from the provided location and store it in any folder on the computer. No specific installation is required. It shall contain the following file and folder(s):

- `libs` folder: this folder contains necessary libraries to run the executable files
- `CHANGELOG.md` file: this file contains a curated, chronologically ordered list of notable changes
- `dtk.exe` file: this is the main executable file
- `dtk.ini` file: this file contains basic settings such as appearance mode
- `LICENSE` file: this file contains the license terms and conditions
- `README.md` file: this file contains basic information in markdown (md) format

After the first execution, the application will automatically create `captures` and `logs` folders and the `dtk.ini` file.

Deleting any of the files under the `libs` folder will result abnormal behavior and the application won't work correctly.

4.5 File Converter Usage

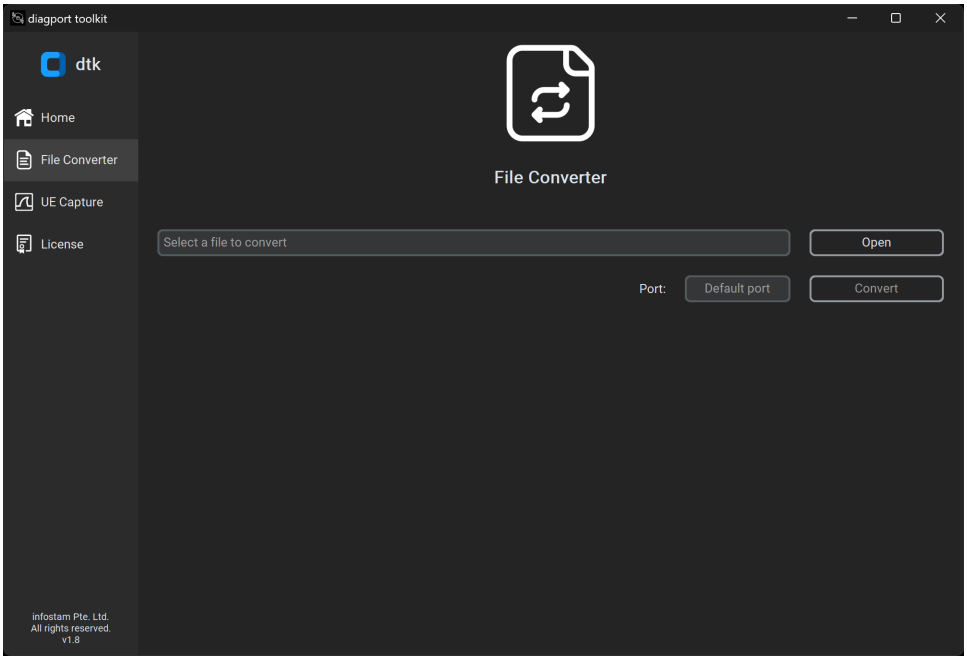


Figure 11: File Converter

In order to use the **File Converter** tool, click on the *Open* button, select a file with a supported file type to convert, and click on the *Convert* button.

Once the conversion completed, a new PCAPNG file is generated with the same name as the source file with an additional *_decoded* string, stored in the same folder as the source file, contains the decoded 5G frames along with other packets, and a popup message is shown. The number of successfully decoded packets is also mentioned.

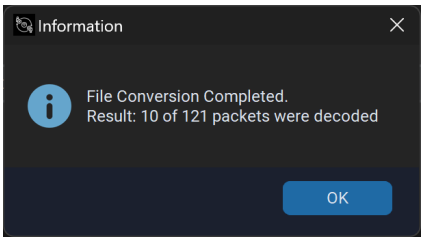


Figure 12: File Converter popup message

In case the source file is a PCAP file and it has the 5G frames on a different UDP port (not the default 49999 used by the application), add that port to the input field before conversion to identify the proprietary packets.

The result file includes decoded 5G frames and all other packets which can be 2G/3G/4G packets and UE payload, as shown below.

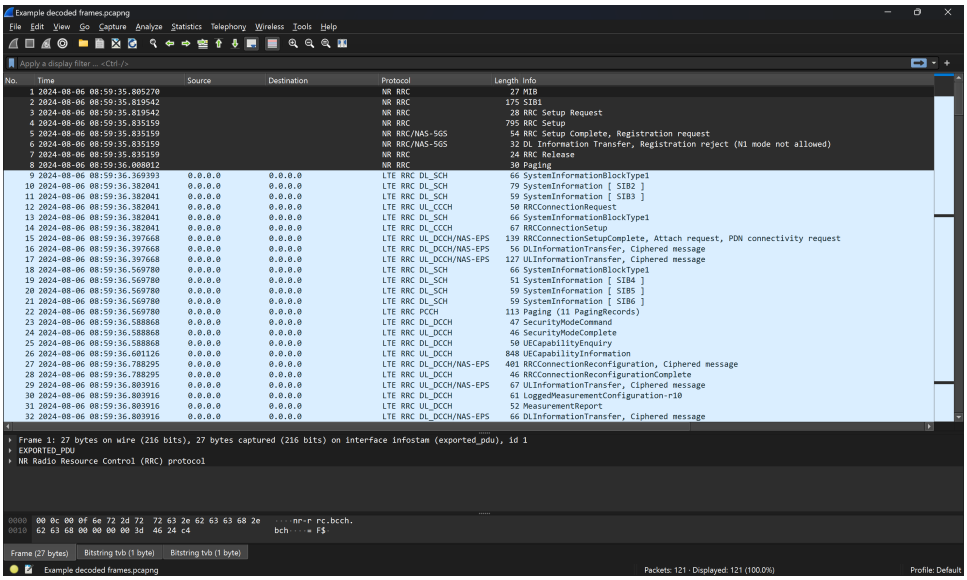


Figure 13: Decoded Frames Example

The following source file types are supported:

- Packet capture: `.pcap`, `.pcapng`
- Qtrun NSG Android application log file: `.log`, `.log.gz`
- Qtrun AirScreen PC application exported text file: `.txt`
- Rohde & Schwarz QualiPoc Android application file: `.sqz`, `.mf`

4.6 UE Capture Usage

In order to use the **UE Capture** tool, select a device and a module from the drop-down lists, add an output capture filename if `pcap` module was selected and include IP traffic if required.

Note, the filename should include file extension too such as `output.pcap`, and it will be saved under the `captures` folder.

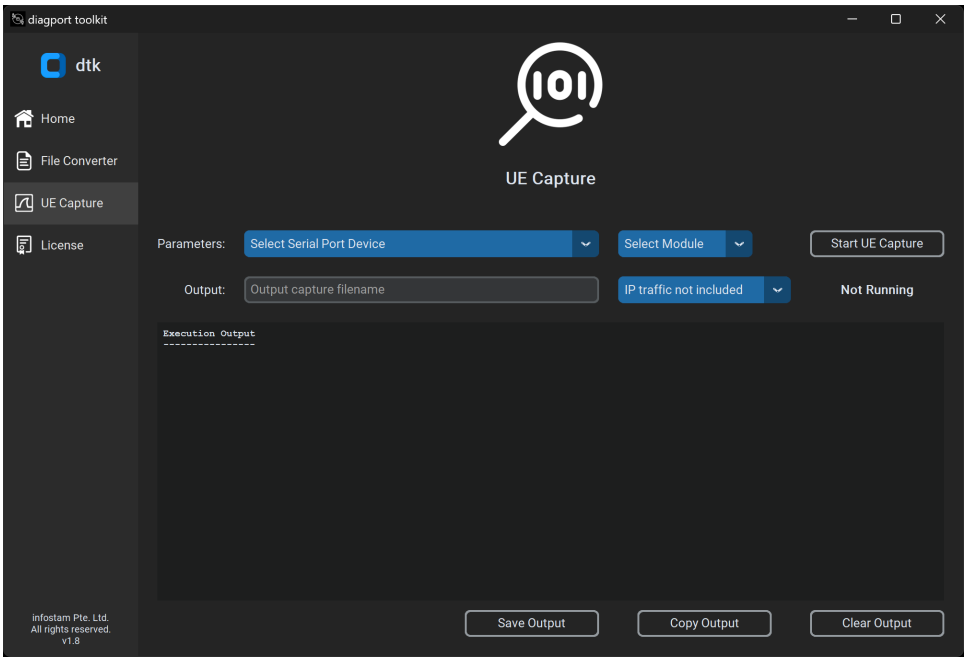


Figure 14: UE Capture

The device dropdown list contains all the COM ports related to the device which are also visible in *Device Manager* (Figure 10). This list has all the name of the pseudo-serial device as the COM port on Windows (such as COM2, COM3), allows the tool to connect to the Qualcomm diagnostics port over a pseudo-serial port over USB, independently from ADB, which is the most common way to connect to the Qualcomm Diag protocol of an Android-based phone using an external device. The Qualcomm diagnostic port must be enabled on the device.

The module dropdown list contains 3 options:

- `pcap` is for writing packets to a PCAP file automatically.
- `wireshark-live` is for opening Wireshark and see frames in real-time.
- `info` is for generic information about the device which is printed under *Execution Output*.

By default, the IP traffic sent by the device is not included, only the signaling frames captured. The IP traffic generated by the device can be captured with selecting *IP traffic included* from the drop-down list. Note, IP being barely the layer 3 for the data traffic in 2G/3G/4G/5G, at the detail that its headers may be compressed (ROHC) and a tiny PPP header may be included.

The data traffic the device sends uses a channel different from the signaling traffic, this channel is setup through the signaling traffic; the tool should thus show all details relevant to how this channel is initiated.

Note, only one application can communicate with the device's Diag port at the same time.

The following example shows the generic information about a *Samsung Galaxy S22 Ultra* mobile. To enable the *Diag Port* on a Samsung device dial **`*#0808#`** USSD code and select "**`DM+MODEM+ADB`**".

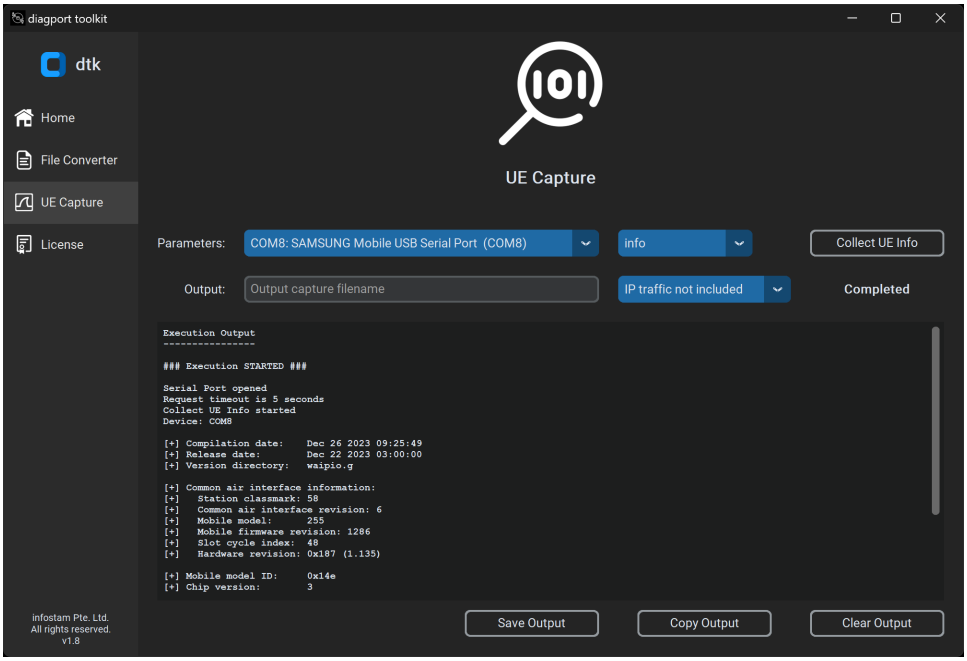


Figure 15: An example of generic information about a device

```
Execution Output
----------------

### Execution STARTED ###

Serial Port opened
Request timeout is 5 seconds
Collect UE Info started
Device: COM8

[+] Compilation date:    Dec 26 2023 09:25:49
[+] Release date:        Dec 22 2023 03:00:00
[+] Version directory:   waipio.g

[+] Common air interface information:
[+]   Station classmark: 58
[+]   Common air interface revision: 6
[+]   Mobile model:      255
[+]   Mobile firmware revision: 1286
[+]   Slot cycle index:  48
[+]   Hardware revision: 0x187 (1.135)

[+] Mobile model ID:     0x14e
[+] Chip version:        3
[+] Firmware build ID:   MPSS.DE.2.0-00822.3-WAIPIO_GEN_PACK-1.43425.52.55482.2

[+] Diag version:        8

[+] Serial number:       2160466985

Serial Port closed

### Execution COMPLETED ###
```

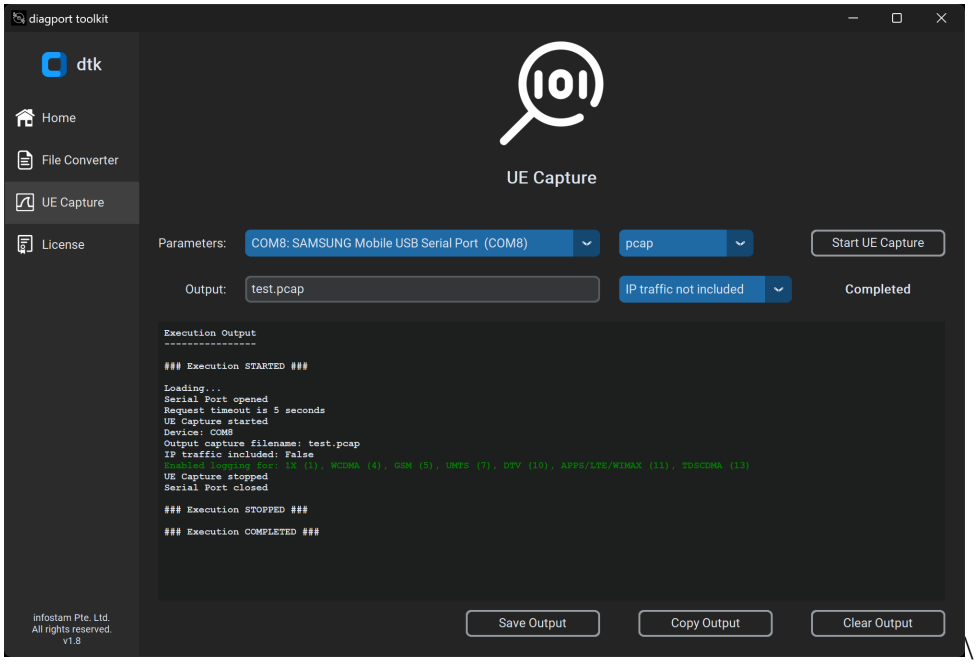


Figure 16: An example of capturing to a pcap file

When capturing to pcap file is selected, provide an output filename and click on *Start UE Capture* button to start the capture. Then, click on *Stop UE Capture* button when the trace should be stopped. In case of **`wireshark-live`**, the Wireshark application will automatically open.

The *Save Output* button saves the *Execution Output* content into a text file under the **`logs`** folder.

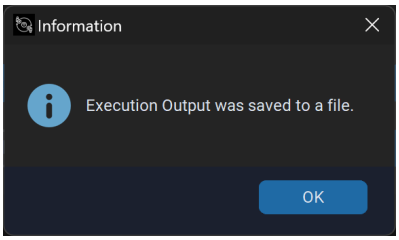


Figure 17: Save Output popup message

The *Copy Output* button copies the *Execution Output* content to the clipboard.

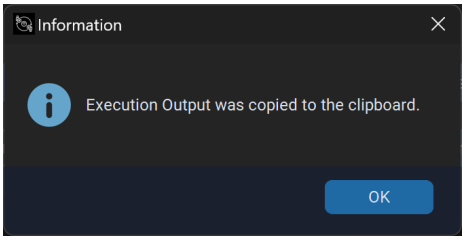


Figure 18: Copy Output popup message

The *Clear Output* button clears and resets the *Execution Output* after a confirmation warning.

If the device does not respond on the selected COM port, the application will have a 5 seconds request timeout.

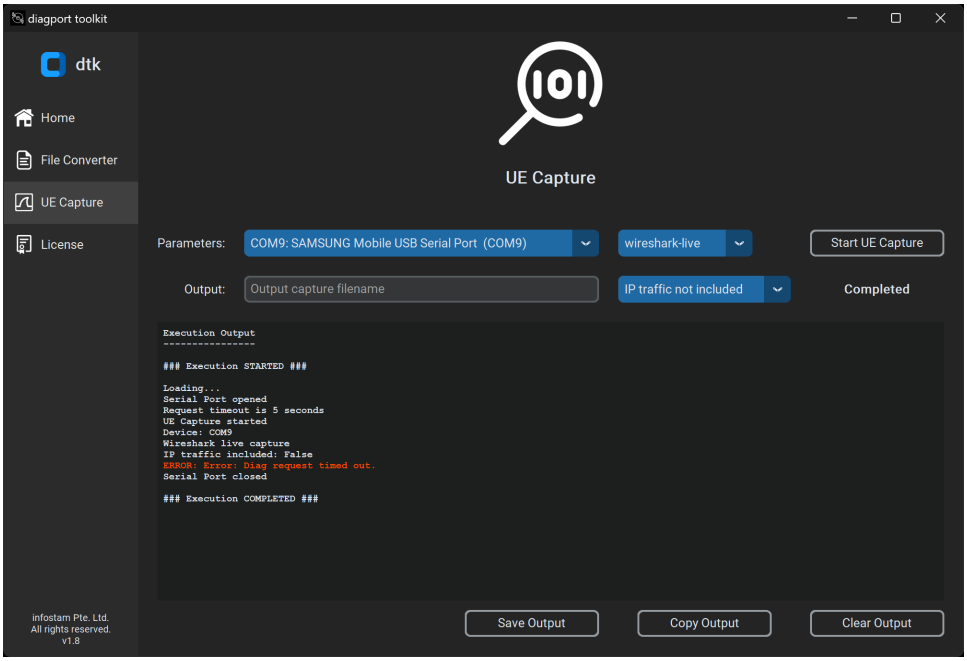


Figure 19: Request Timeout

4.7 Keyboard Shortcuts

The Dialog popup windows have keyboard shortcut control as well:

- **Esc**: Close the window.
- **Enter**: Close the window.
- **First letter of a button**: Activate the button.

The main window has keyboard shortcut control as well:

- **Alt-Shift-H**: Select *Home*.
- **Alt-Shift-F**: Select *File Converter*.
- **Alt-Shift-U**: Select *UE Capture*.
- **Alt-Shift-L**: Select *License*.

5 Support

5.1 Communicate with the team

If an end user with active subscription encounters any question while using the tool or the plugin, feel free to contact us via e-mail: info@infostam.com.

5.2 Report a bug

If an end user with active subscription encounters any problem or possible bug, please assist us to fix it. Attach all screenshots and any other valuable details, files, etc. that is related the bug and contact us via e-mail: info@infostam.com.

5.3 Links

Npcap: https://npcap.com

Wireshark: https://www.wireshark.org

Samsung Android USB Driver: https://developer.samsung.com/android-usb-driver

OnePlus (Qualcomm) USB Driver:
https://qcomdriver.com/wp-content/uploads/Qualcomm_USB_Driver_v1.0.10061.1.zip

6 Disclaimer

DISCLAIMERS OF WARRANTIES

YOU ACKNOWLEDGE AND AGREE THAT THE PROGRAM IS PROVIDED TO YOU ON AN "AS IS" BASIS. THE LICENSOR DISCLAIMS ANY AND ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY, OR HARDWARE OR SOFTWARE COMPATIBILITY, OR FITNESS FOR A PARTICULAR PURPOSE OR USE, INCLUDING YOUR PARTICULAR BUSINESS OR INTENDED USE, OR OF THE PROGRAM'S RELIABILITY, PERFORMANCE OR CONTINUED AVAILABILITY. THE LICENSOR DOES NOT REPRESENT OR WARRANT THAT THE PROGRAM OR CALCULATIONS OR PRINTS OR EXPORT DATA MADE THEREOF WILL BE FREE FROM VIRUSES, MALWARE, TROJAN HORSES OR ANY OTHER DEFECTS OR ERRORS AND THAT ANY SUCH EFFECTS OR ERRORS WILL BE CORRECTED, OR THAT IT WILL OPERATE WITHOUT INTERRUPTION. YOU AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR ALL COSTS AND EXPENSES ASSOCIATED WITH RECTIFICATION, REPAIR OR DAMAGE CAUSED BY SUCH DEFECTS, ERRORS OR INTERRUPTIONS. FURTHER, THE LICENSOR DOES NOT REPRESENT AND WARRANT THAT THE PROGRAM DOES NOT INFRINGE THE INTELLECTUAL PROPERTY RIGHT OF ANY OTHER PERSON. YOU ACCEPT RESPONSIBILITY TO VERIFY THAT THE PROGRAM MEETS YOUR SPECIFIC REQUIREMENTS.

LIMITATIONS OF LIABILITY

IN NO EVENT SHALL THE LICENSOR BE LIABLE TO YOU OR ANY THIRD PARTY UNDER THIS AGREEMENT OR OTHERWISE, WHETHER BY WAY OF INDEMNIFICATION OR OTHERWISE, UNDER ANY THEORY OF LIABILITY WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, NEGLIGENCE AND STRICT LIABILITY) FOR ANY DIRECT OR INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES OR REVENUE, LOST PROFITS OR EXPECTED BENEFIT NOT ACHIEVED, WHETHER FORESEEABLE OR NOT, WHETHER IN AN ACTION IN CONTRACT, TORT, PRODUCT LIABILITY OR STATUTE OR OTHERWISE, EVEN IF THE LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, RELATING TO THE PROGRAM OR YOUR USE THEREOF, OR INABILITY TO USE THE PROGRAM WHETHER OR EVEN IF THE LICENSOR HAS BEEN ADVISED, KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES AND WITHOUT REGARD AS TO WHETHER SUCH LOSS OR DAMAGE WAS FORESEEABLE OR NOT. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, THE LICENSOR HAS NO OBLIGATION TO PROVIDE AND YOU SHALL HAVE NO RIGHT TO SEEK ANY REMEDY FOR ANY DEFECT, ERROR OR FAILURE OF THE PROGRAM.

THE LICENSOR SHALL NOT HAVE ANY LIABILITY TO YOU OR THIRD PARTIES FOR THE LOSS OF INFORMATION OR OTHER LOSS RELATING TO THE PROGRAM OR THE USE.

THE LIMITATIONS OF LIABILITY UNDER THIS LICENSE ARE VALID TO THE EXTENT AS PERMITTED BY THE APPLICABLE MANDATORY LAW.

ACKNOWLEDGEMET

YOU ACKNOWLEDGE THAT YOU UNDERSTAND AND AGREE TO THE DISCLAIMERS OF WARRANTIES AND THE LIMITATIONS ON LIABILITY AND REMEDIES CONTAINED IN THIS LICENSE. YOU FURTHER ACKNOWLEDGE THAT THE PROGRAM IS BEING PROVIDED TO YOU FOR A SUBSCRIPTION FEE, THAT THE DISCLAIMERS AND LIMITATIONS ARE MATERIAL PROVISIONS OF THIS LICENSE AND THAT THE LICENSOR WOULD NOT MAKE THE PROGRAM AVAILABLE TO YOU IF SUCH DISCLAIMERS AND LIMITATIONS WERE DELETED OR MODIFIED TO BE MORE FAVORABLE TO YOU.

YOUR USE OF THE PROGRAM

YOU AGREE THAT THE PROGRAM IS PROVIDED TO YOU ENTIRELY FOR USE AT YOUR OWN RISK, ALTHOUGH THE LICENSOR HAS USED COMMERCIALLY REASONABLE EFFORTS TO CONTROL AND UPDATE THE PROGRAM AND TO VERIFY THAT THE PROGRAM WORKS ACCORDING TO THE DOCUMENTATION. AT ALL TIMES YOU SHALL USE THE LATEST UPDATED VERSION OF THE PROGRAM. YOU SHALL NOT SHARE OR TRY OUT THE PROGRAM ON ANY OTHER COMPUTER RATHER THAN THE ONE HAS THE LICENSE KEY RELATED TO THE COMPUTER SERVICE ID.