

Table of contents

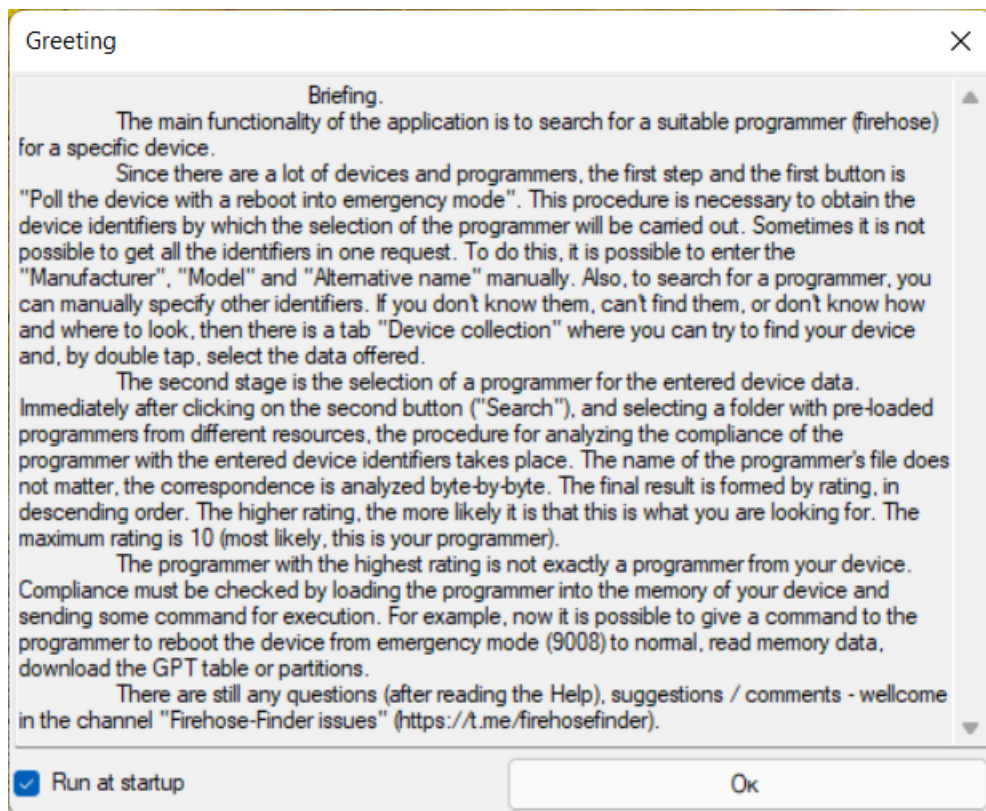
Frequently Asked Questions and answers (FAQ)	2
Welcome window	3
Menu item «Change language»	4
The "Work with files" tab (main)	4
The "Work with device" tab (hidden)	7
Chapter «ADB (Android Debug Bridge)»	7
Chapter «Fastboot (bootloader)»	8
Chapter «Sahara & Firehose loader»	9
Context menu commands	12
Device collection tab (hidden)	14
The window "Insert model"	16
The window "Share the programmer" (disabled)	16
Menu item "Instruments"	18
Section "Binary search"	18
Section "Decode and repack ROM (AGM)"	19
Menu item "Help"	21
Section "View help"	21
Section "About"	21

Frequently Asked Questions and answers (FAQ)

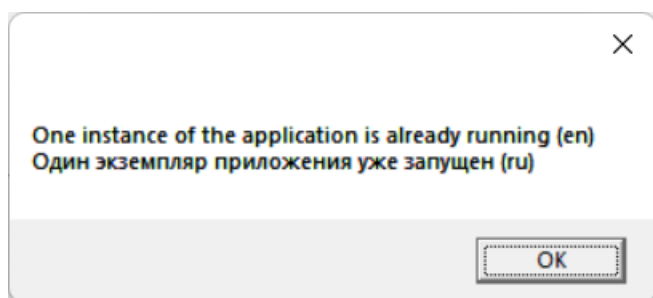
- q. How is the rating of a file in a folder with programmers formed?
 - a. Files with a rating of 0 are not executable files, and certificates are not searched in them. The ELF (ELF), BIN, MBN file has a rating of 1. These can be any firmware files (programmers, xbl, apps, etc.). 1 is added to the rating if the SWID (software identifier) starts with 3 (this is a sign of the loader for emergency mode – Firehose programmer), another +1 point to the rating if the identifiers of the phone model specified in the field match search, and in the programmer's certificate. Also, 1 is added to the rating if the manufacturer matches and another 1 if the processor. Matching the hash sum of the root certificate adds 5 points to the rating at once. The higher the rating of the file (programmer), the higher the probability that it will come to the phone, the parameters of which are entered for search. The maximum rating value is 10 points.
- q. Where can I get my device ID (HW_ID, OEM_ID, MODEL_ID, OEM_HASH)?
 - a. Automatically, from the "[Work with files](#)" tab, by clicking the "Poll the device with a reboot into emergency mode" button; manually, by selecting the appropriate device on the "[Reference book](#)" tab with a double click; using other programs to access memory to request identifiers: - emmcdl with the command -info: - QLMCPUInfo; - QSaharaServer with teams -c 02(03.07).
- q. Why are some files in the report highlighted in red and have a hint "The file is not ELF!", "The file is encoded"?
 - a. Most programmers have a code at the beginning of the file that determines the ownership of the file (magic_number). At the same time, programmers come across who, for various reasons, have a different set of bytes (mask) applied in the header, and such files are not identified by the system as a working programmer. Such files are highlighted with a color and a hint to inform the user about the impossibility of using them by this program (perhaps other software will be able to work with them).
- q. Where and to whom are the data from my device sent, and what exactly?
 - a. The data is sent by the bot (program code) to the public telegram channel "[Firehose - Finder issues](#)". Information from this channel is processed to change/add/correct the program. All incoming information is publicly available, any Telegram user can subscribe to this channel and control the transmission of information. Device identifiers are sent – processor type, serial number, model, manufacturer, vendor. **No personal information capable of unambiguously linking device data to the user is transmitted.**
- q. I have a working programmer for my device. How do I share it or add it to the program database?
 - a. Through the program interface, you can only send a programmer who has successfully worked with a really connected device. A detailed description can be found in the section "[Share the programmer](#)".
- q. Where can I view the source code? How can I change it or offer my own improvements?
 - a. The source code of the FhF program is posted in a public repository on the GitHub platform ([link for viewing](#)). You can freely download the entire code or any part of it. To suggest your changes, you can use either the "Issues" section, or make a fork of the repository. These actions will require registration on GitHub.

Welcome window

When the program starts, the "Greeting" window opens. It saves the state of the "Run at startup" switch in the program, and if there is no need to constantly launch this window at the start of the program, then the check mark can be removed. If necessary, you can go back to this window in the "View" and open it from there.

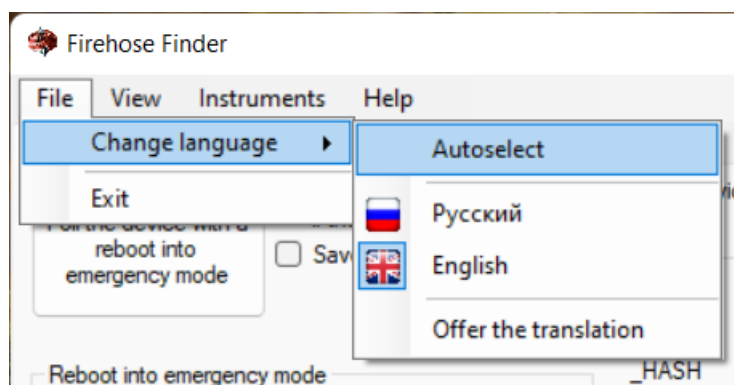


The program implements a mechanism for launching only one instance of the application. If you try to launch a second instance while the application is running, a warning will be displayed about the impossibility of performing such an operation.



Menu item «Change language»

For the convenience of working in the program, you can use the translation of text inscriptions into a familiar language.



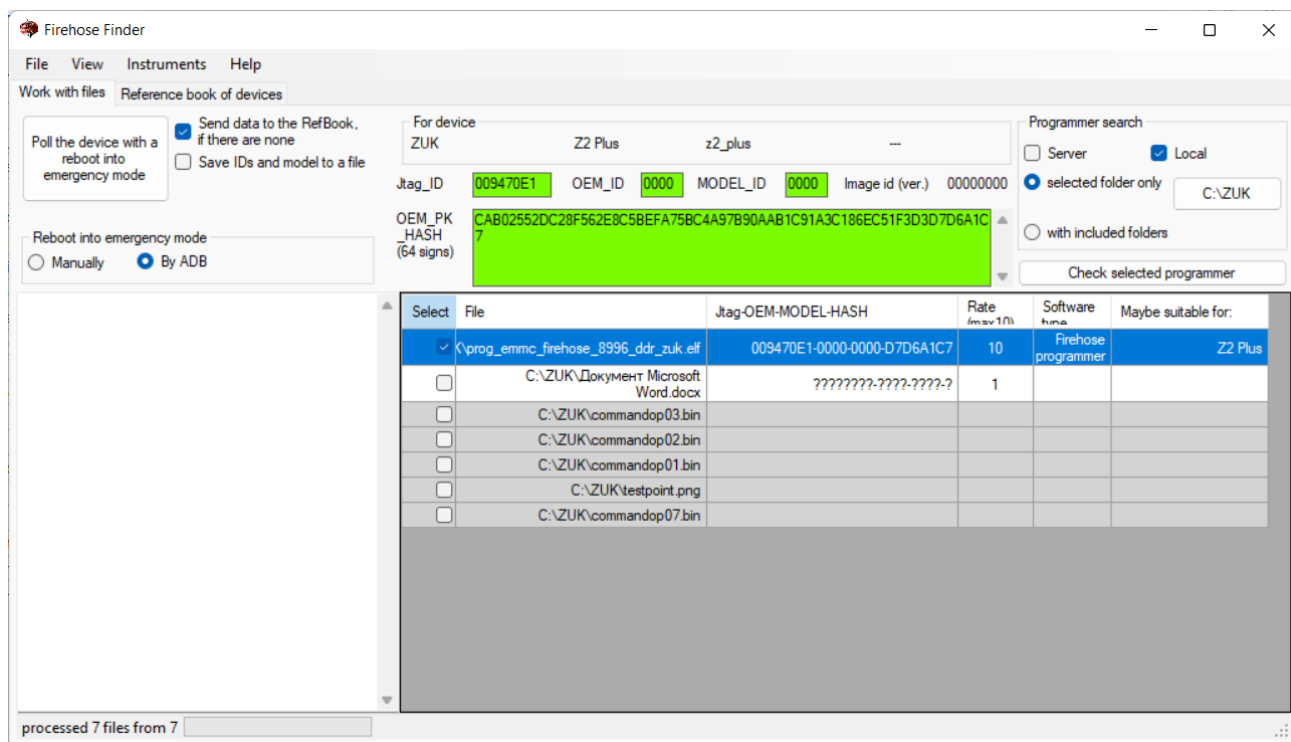
- «Autoselect» - it assumes automatic language selection in accordance with the regional settings of the operating system. By default, the application language is "Русский".
- «Русский» - regardless of the regional settings of the operating system, the application language is set as «Русский».
- «English» - regardless of the regional settings of the operating system, the application language is set as «English».
- «Offer the translation» - go to the telegram channel "[Chat for FhF](#)" to voice your readiness to translate the application into your language. Since the project is non-commercial, the translation work is not paid and is a symbol of the author's goodwill.

When the application is restarted, the language settings are saved. Changing the language requires restarting the application without restarting the operating system.

The "Work with files" tab (main)

The main tab for working with the program is "Work with files". She is always active. The basic functionality is to connect the device in normal mode (charging mode) and press the button "Poll the device with a reboot into emergency mode". With such work, ADB (Android Debug Bridge) requests device identifiers from the firmware (manufacturer, model, alternative name and serial number of the processor), the device is automatically overloaded into emergency mode, processor identifiers are requested (HW_ID, OEM_ID, MODEL_ID, OEM_PK_HASH), all received data is copied to the form.

By selecting the "Overload to emergency mode" items, you can set an automatic or manual reboot option (using ADB, it is not always possible to reboot into emergency mode, not all devices support this). You can also use the checkboxes to select saving data to a file and sending data to the [RefBook](#). When saving data to a file, you will need to specify the folder to which the data will be copied.



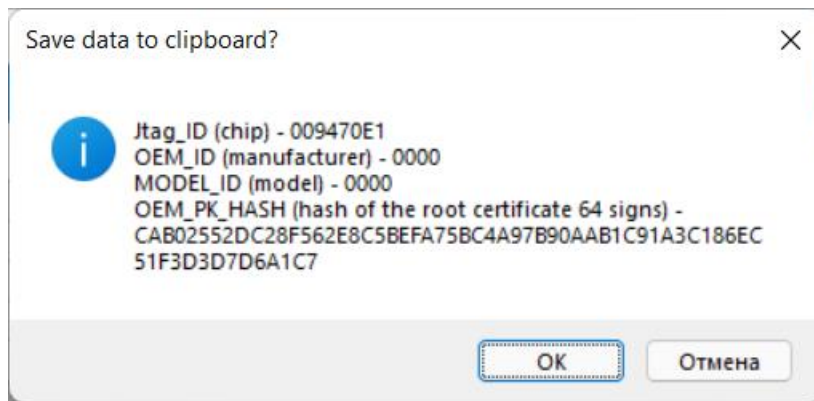
After receiving the IDs, the device can be disconnected and restarted. Usually, the exit from the emergency mode is carried out by pressing the "Power" button for a long time (more than 10 seconds).

When the device data on the form is filled in (in automatic or manual mode), you can click the "Search" button in the "Programmer Search" group and select the path to the folder with the collection of programmers. You can use the radio button to select the search area:

- «Server»;
- «Local».

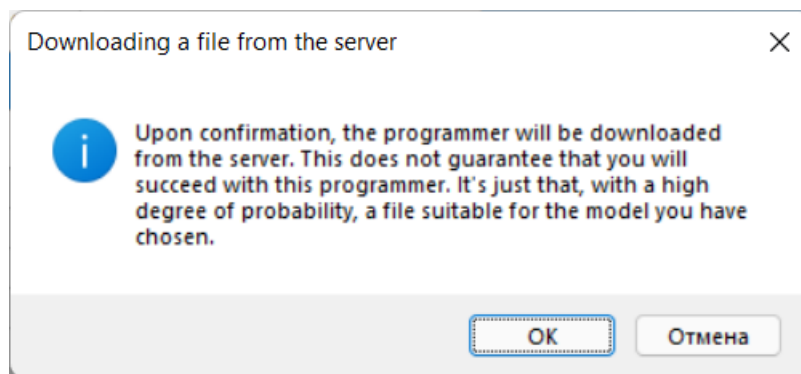
For the "Server" area, the completed form data is a kind of filter. Thus, leaving the identifier fields blank, you can get a complete list of programmers located on the server. Entering data into the identifier fields allows you to reduce the search results. Partial filling in of one or more fields is allowed.

For the "Local" area, either "selected folder only" or "including subfolders" is analyzed, depending on the selected switch position. All files located in folders are checked. The search for the programmer is carried out not by name, but by identifiers, respectively, the file name of the program for analysis is not important. Each verified file is assigned a rating. Sorting in the table is carried out [by rating](#) from higher to lower. The maximum is 10 (the probability that this is the right programmer is the highest). A double tap on the selected programmer allows you to copy to the clipboard information about the identifiers that this programmer will require when working.



The programmer can be checked whether it is suitable for the connected device. To do this, select the programmer from the analyzed list by putting a check mark at the beginning of the line. In this case, the "Check the selected programmer" button will become active.

If the programmer selected for testing is located on the server, it will be prompted to download it to a local folder.



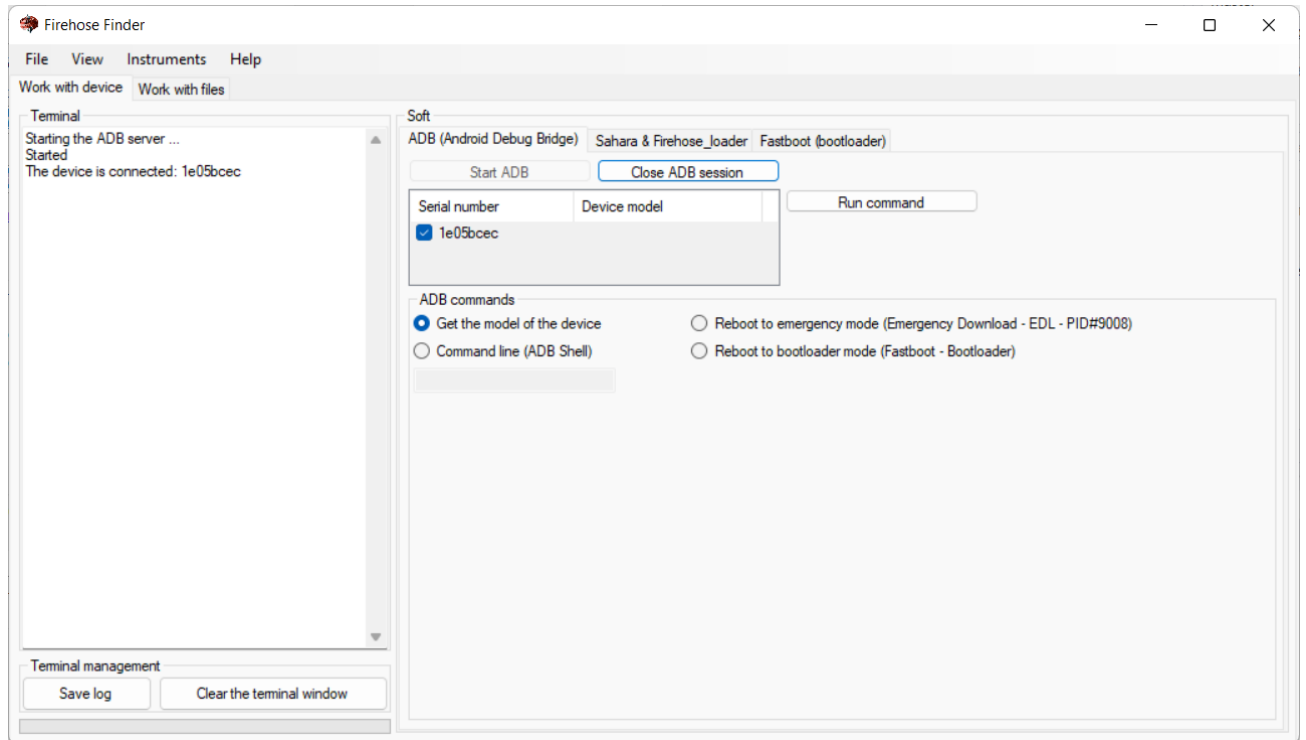
To check the programmers located locally, the device must be rebooted into emergency mode (9008) either manually or programmatically, from the "[Work with device](#)" tab. If the device was previously connected to receive identifiers, then it must be disconnected from the computer, rebooted and reconnected. This is due to the peculiarities of the "Sahara" protocol (the second time a greeting is not sent to work on the protocol).

The "Work with device" tab (hidden)

You can activate the tab from the "View" menu. Designed for deeper control of the connected device.

Chapter «ADB (Android Debug Bridge)»

The commands for ADB become active after launching ADB, you need to click the "Start ADB" button. Upon successful start, the serial numbers of the connected devices are marked in the log.



Currently there are four commands available for ADB in the list:

1. Get the model of the device. Device properties are requested from the firmware to fill out the form.
 - Manufacturer – analog of the command `$ adb shell getprop | grep ro.product.manufacturer`
 - Model – analog of the command `$ adb shell getprop | grep ro.product.model`
 - Alt name – analog of the command `$ adb shell getprop | grep ro.product.name`
 - Chip serial number – analog of the command `$ adb shell cat /sys/bus/soc/devices/soc0/serial_number`

The data is automatically copied to the "[Work with files](#)" tab.

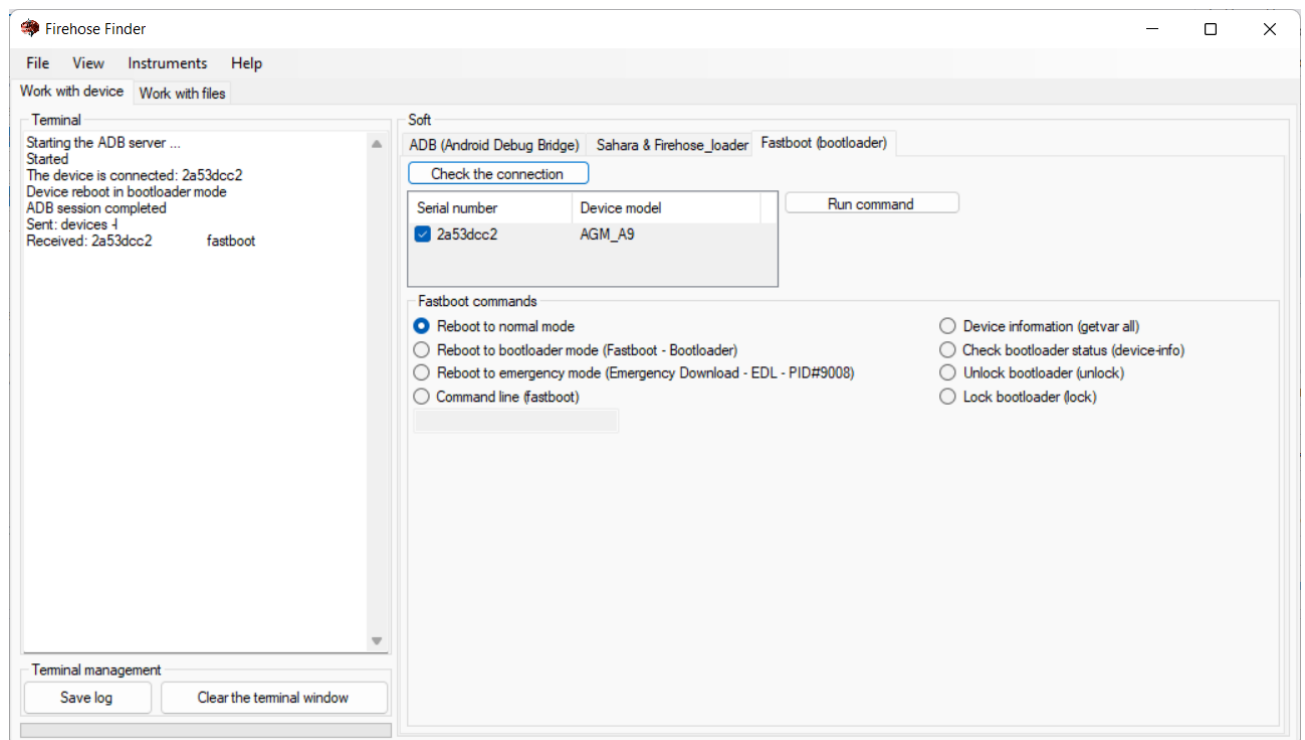
2. Reboot to emergency mode. The device will be rebooted at 9008 by means of ADB. This is an analog of the command `$ adb reboot edl` Not all devices support this command.
3. Command line (ADB Shell). When you select this item, a command entry window will become available. You can send a command by pressing the "Run command" button or by

pressing "Enter". Before the command **you do not need to enter adb shell**, only the command by itself. For example, to get a list of all commands supported by the device, it is enough to enter **ls -l /system/bin** or **ls -l /system/xbin**

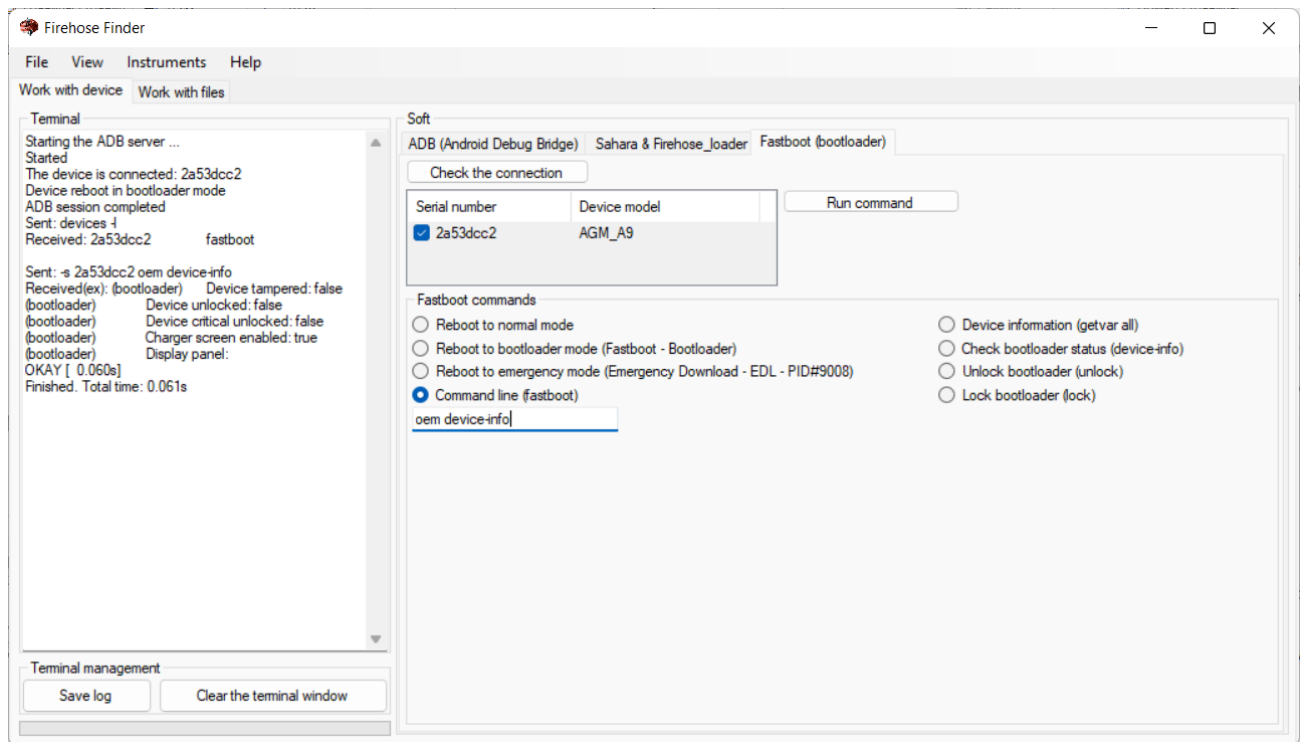
4. Reboot to bootloader mode. The ADB session ends, the tab opens «Fastboot (bootloader)», the device only accepts bootloader commands.

Chapter «Fastboot (bootloader)»

To determine the connected device, click the "Check the connection" button. If the device was previously connected via ADB, then its model will be pulled up along with the serial number of the device. It is allowed to connect several devices, the choice for the team is made by putting a check mark next to the required device.



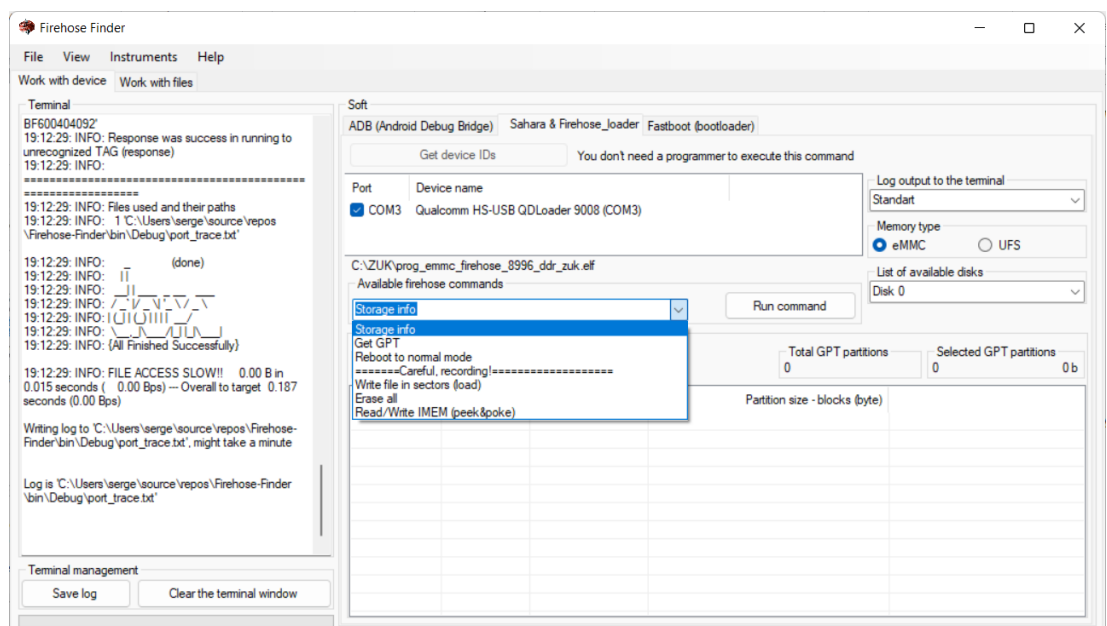
Currently, there are eight loader commands available. Some of them may not be supported by the device loader, in which case it is suggested to use the command line. When you select the command line (fastboot), a command entry window will be available. You can send a command by pressing the "Run command" button or by pressing "Enter". **You do not need to enter fastboot before the command**, only the command by itself. For example, to get information about the device, you need to enter **oem device-info**



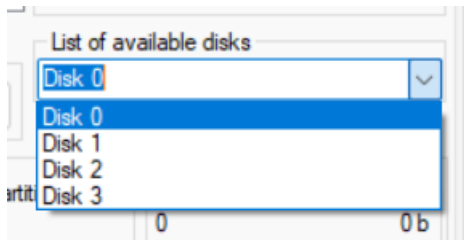
Chapter «Sahara & Firehose loader»

Commands for Sahara become active after the device is reset to emergency download mode (9008). The device port is determined automatically, but, if necessary, it can also be selected manually from the list of available com ports. The following commands are currently available:

- Get device IDs. The command is displayed on a separate button. The execution of the command is to fill in the identifiers on the "[Work with files](#)" tab. If it is necessary to execute several commands for the device, then the device must be restarted, because the program waits for the "greeting" data from the device via the protocol, and it is sent when the device is first connected in 9008 mode.
- To the left of the "Run command" button is a combo box with a selection of commands. The first command to execute is "Storage info".

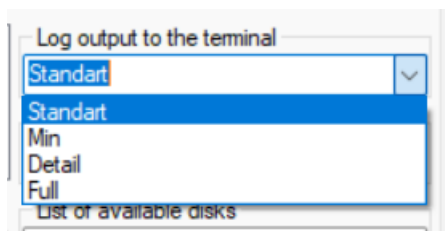


After its successful execution, other commands become available. The field with the selection "List of available disks" is filled with the numbers of physically available parts of the flash memory (in this example, there are four of them).

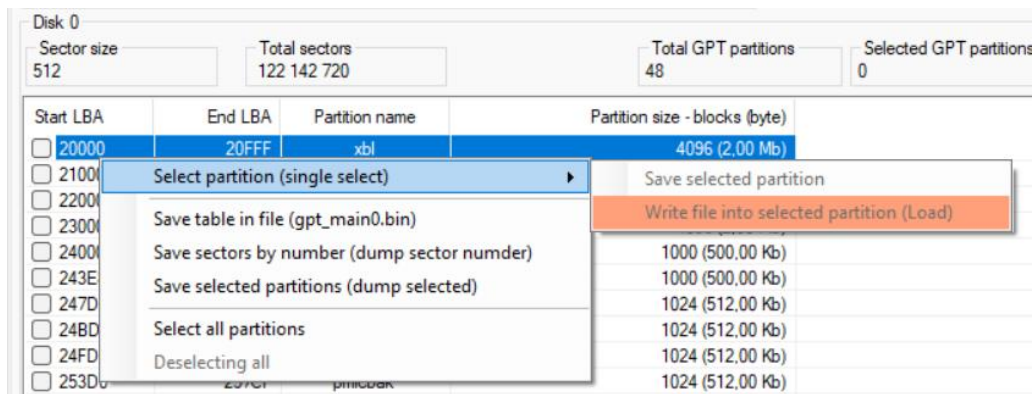


The memory type is automatically selected, but you can correct the selection manually if the memory was determined incorrectly.

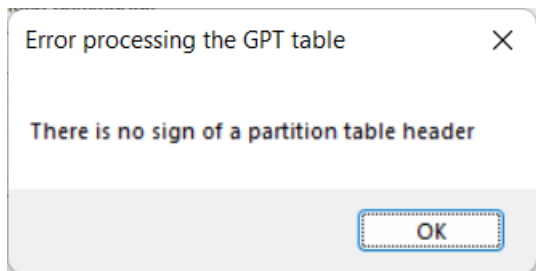
You can select four options for displaying the log. By default - "Standard"



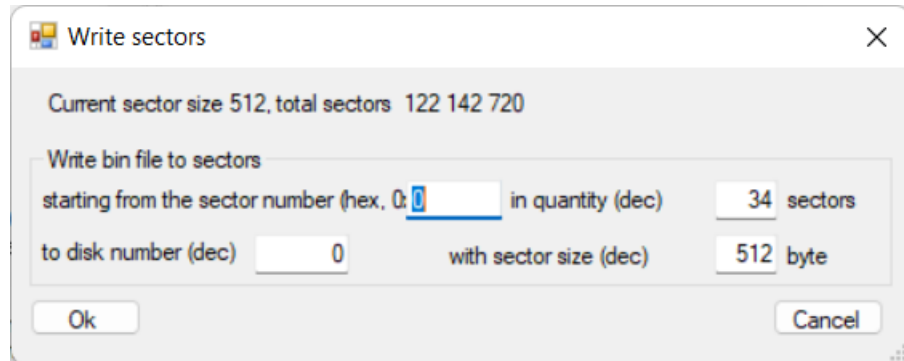
- "Get GPT". Successful execution of the command will give a list of partitions with the addresses of the initial and last sectors and the calculated number of sectors occupied by the partitions with the volume in bytes. In this case, the [context menu commands](#) will become available.



If there is no table on the disk, a warning will be displayed, while the ability to obtain sector-by-sector information remains, i.e., the presence of a partition table is not necessary to completely drain information from the disk.

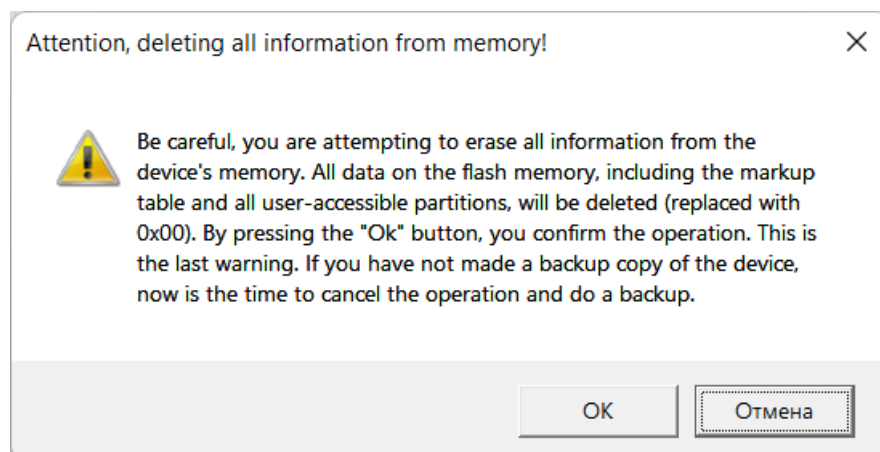


- "Reboot to normal mode". Selecting this command allows you to reboot the device from emergency to normal mode. The delay in executing the device reboot command to normal mode is 10 seconds.
- "Write file in sectors (load)". The command is necessary for writing, for example, markup tables. **Perform very carefully!**

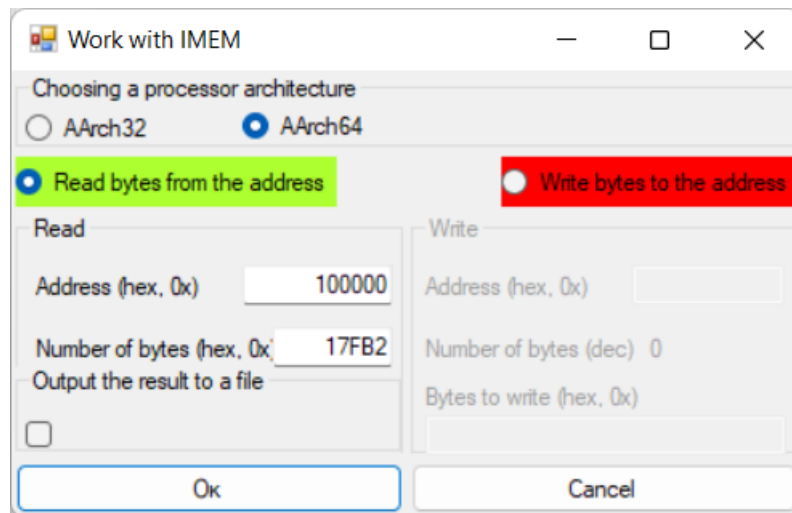


After confirming the entered information, you will be prompted to select a bin file to copy it to the device's memory at the specified address.

- "Erase all". **Perform very carefully and with full confidence of understanding what is happening.** All information from the flash memory will be deleted.

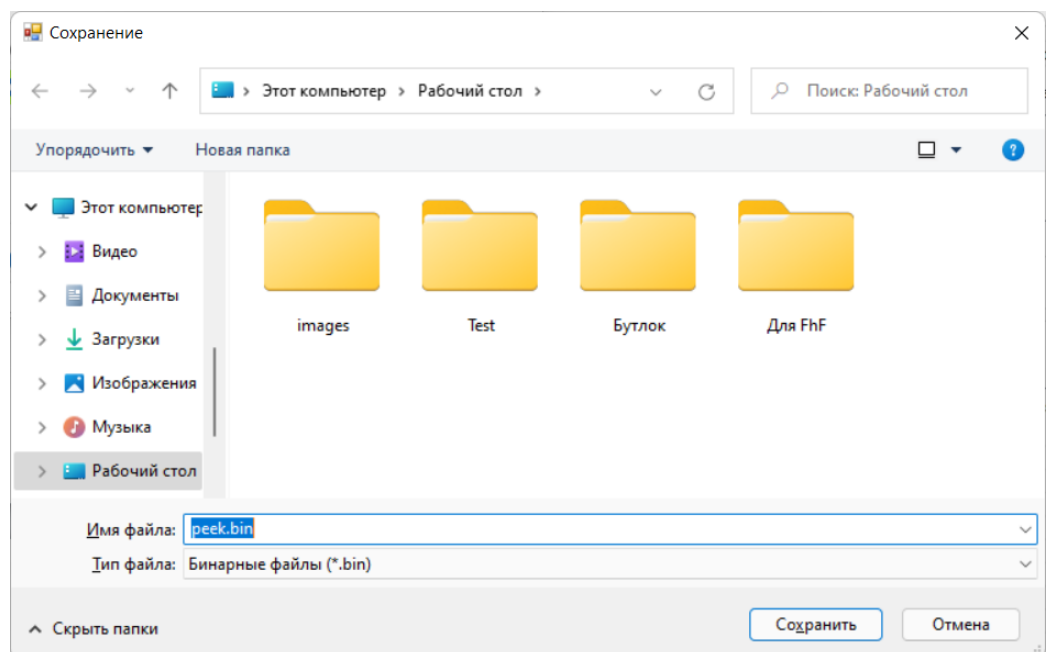


- "Read/Write IMEM (peek/poke)". The operation allows you to read the internal memory (IMEM) of the processor. Before reading or writing, you must first specify the address and the number of bytes to read/write for your processor. The addresses for the 32 and 64 byte architecture may differ. **Accessing some memory addresses may cause the processor to reboot or malfunction.**



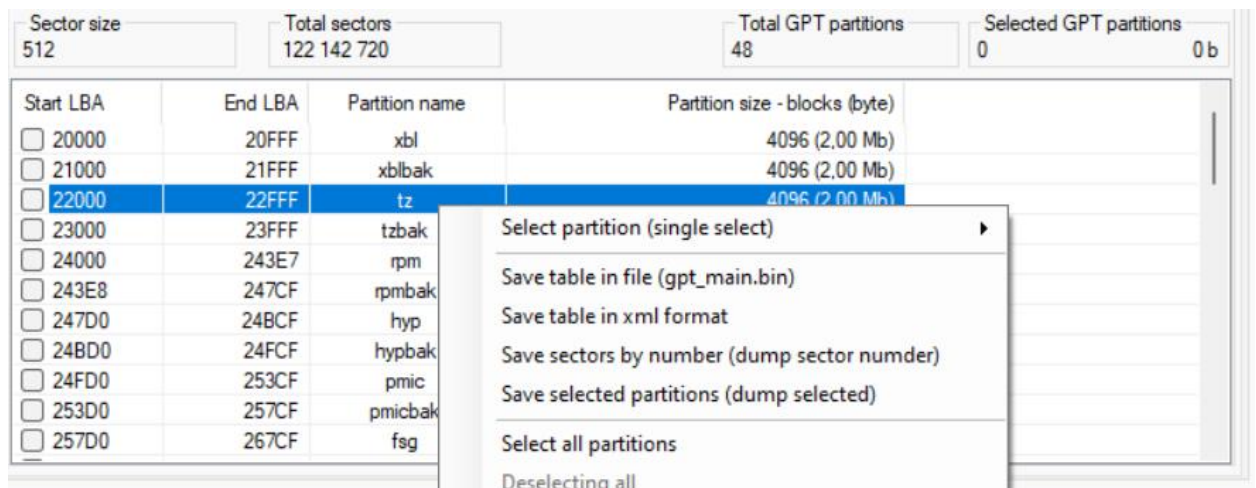
The processor architecture is selected automatically, depending on the programmer used. At the same time, if necessary, this parameter can be changed (for example, with the error "HANDLE_PEEK_FAILURE").

The result is output to the default log. If there is a need to save the result to a file, then it is necessary to mark the appropriate box. In this case, a window will open with the choice of the file saving path.



Context menu commands

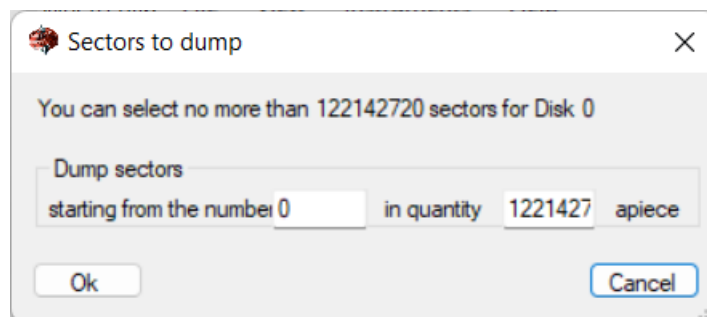
Become available by right-clicking.



- «Select partition». When selected, all the checkboxes on the sections are reset, and only one remains – the current one. At the same time, the menu items for single work with the section become active. Multiple selection is not allowed.

A single partition can be saved or a bin file can be written in its place. **The recording must be carried out with special care.** If it is necessary to simply erase a certain partition, it is allowed to form a bin file of the same size with the erasable partition and with a sequence of bytes 00 (or FF - depends on the specifics of memory). Then write this "null" file to the place of the partition intended for deletion. At the same time, the partition is not deleted from the partition table or from the location on the flash drive, just the information in such a section is overwritten with zeros.

- «Save table in file (gpt_main0.bin)». This command allows you to save a copy of the markup table to the specified folder.
- «Save the table in xml format». Allows you to save the table in a universal format for further processing, for example, in excel.
- «Save sectors by number (dump sector number)». This command allows you to save a byte-by-byte backup copy of the specified sectors to the specified folder. You must specify the first sector to save and their number. By default, the following are substituted: the first sector is 0, the number is all sectors of the disk selected above.




- «Save selected partitions (dump selected)». Multi-sector partition dump. You can select one, several, or all partitions to save. It is worth paying attention to the sufficiency of space on the local disk for the dump of the selected partitions. Usually, the **"userdata"** section carries the majority of user data, **is the largest and, when saving a backup, is not copied because of the size.**

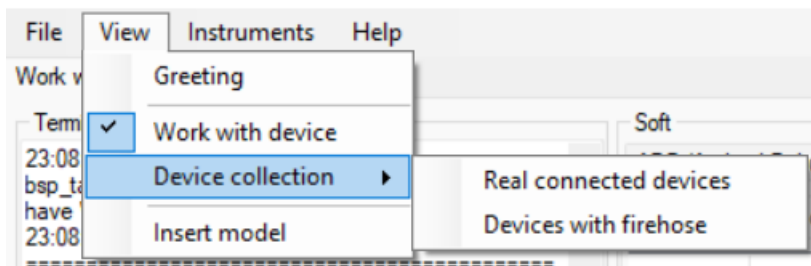
	FCF000	7403FD4	userdata	105 074 645 (50.10 Gb)
	7403FD5	747BFDE	grow	491 530 (240.00 Mb)

- You can select all sections with one command and cancel the entire selection with one command.

Device collection tab (hidden)

You can activate the tab from the "View" menu. The "Device collection" contains the filter "fully verified devices" - this is a list of devices from which all identifiers were received automatically (without manual input).

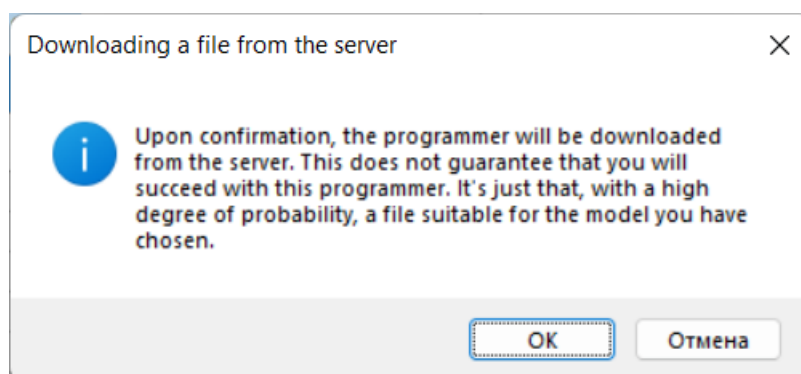
 Firehose Finder



You can reset the filter and display all "Real connected devices" by selecting the appropriate menu item. All devices that, when connected, gave ids automatically and those for which the make/model had to be filled in manually will be displayed.

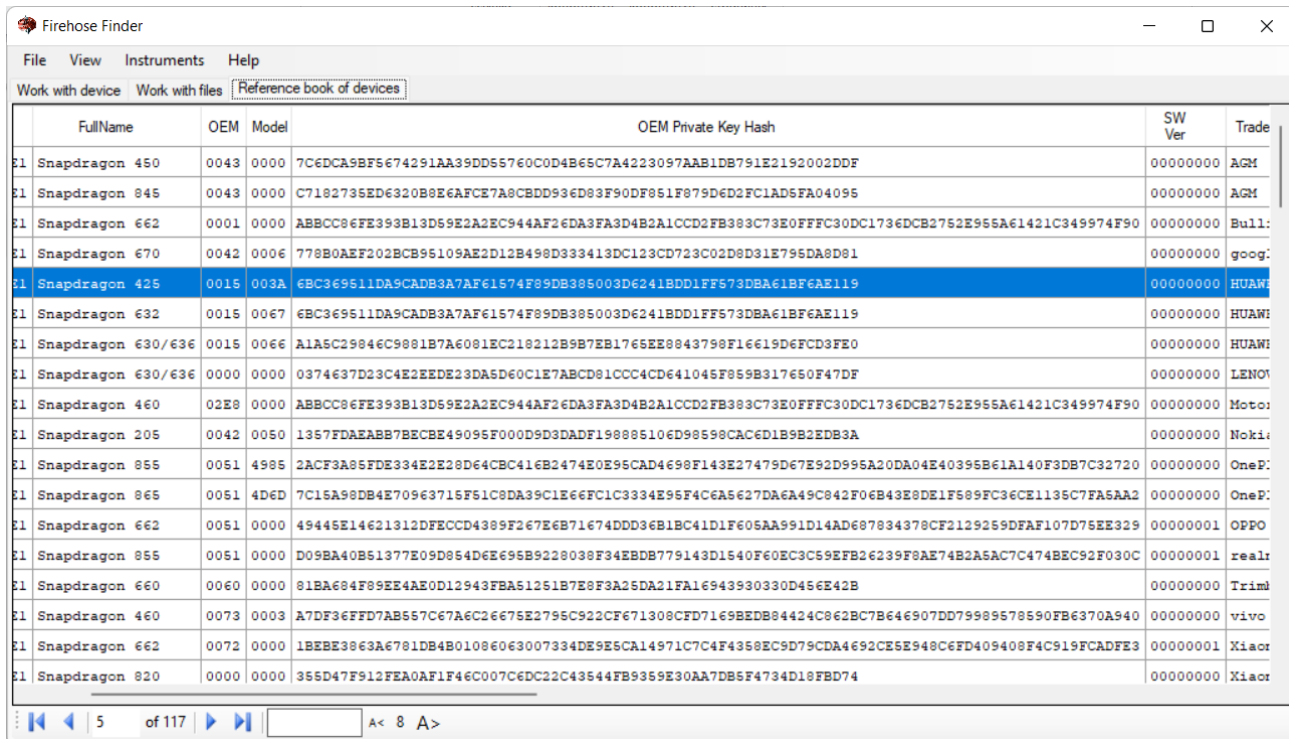
"Devices with firehose" will reduce this list by applying a filter to display devices for which programmers were found and stored on the server. The data was obtained from open sources from users who were able to successfully connect a certain programmer to their specific device. The device and the programmer became interconnected, the data about the device got into the Directory, and the programmer was saved on the server.

When you double-click on the line with the selected device, the data will be autofilled on the "[Work with files](#)" tab and you will be prompted to download the programmer from the server.



In the full list, the programmer's compliance with the device may not be at all. Incorrect or missing data in the "Device collection", with the consent of the user (check mark on the "[Work with files](#)" tab), are sent to the public telegram channel "[Firehose-Finder issues](#)" for verification and adjustments. Adding/changing data to the "Device collection" usually occurs with an automatic update of the release version (for versions older than 3.1.0.4).

There is a search field at the bottom of the Directory form. The search works in all the cells of the Directory, and applies a filter during the recruitment process. At the same time, the search goes not only on "Real connected devices", but in general on the entire database of devices that have ever been present in the Directory.



The screenshot shows the 'Firehose Finder' application window. It has a menu bar with 'File', 'View', 'Instruments', and 'Help'. Below the menu bar are three tabs: 'Work with device', 'Work with files', and 'Reference book of devices'. The 'Reference book of devices' tab is active, displaying a table with the following columns: 'FullName', 'OEM', 'Model', 'OEM Private Key Hash', 'SW Ver', and 'Trade'. The table contains 20 rows of device data. The 10th row is highlighted in blue. At the bottom of the window, there is a search bar with the text 'A < 8 A >' and navigation buttons.

FullName	OEM	Model	OEM Private Key Hash	SW Ver	Trade
Snapdragon 450	0043	0000	7C6DCA9BF5674291AA39DD55760C0D4B65C7A4223097AAB1DB791E2192002DDF	00000000	AGM
Snapdragon 845	0043	0000	C7182735ED6320B8E6AFCE7A8CBDD936D83F90DF851F879D6D2FC1AD5FA04095	00000000	AGM
Snapdragon 662	0001	0000	ABBCC86FE393B13D59E2A2EC944AF26DA3FA3D4B2A1CCD2FB383C73E0FFFC30DC1736DCB2752E955A61421C349974F90	00000000	Bull:
Snapdragon 670	0042	0006	778B0AEF202BCB95109AE2D12B498D333413DC123CD723C02D8D31E795DA8D81	00000000	goog:
Snapdragon 425	0015	003A	6BC369511DA9CADB3A7AF61574F89DB385003D6241BDD1FF573DBA61BF6AE119	00000000	HUAW
Snapdragon 632	0015	0067	6BC369511DA9CADB3A7AF61574F89DB385003D6241BDD1FF573DBA61BF6AE119	00000000	HUAW
Snapdragon 630/636	0015	0066	A1A5C29846C9881B7A6081EC218212B9B7EB1765EE8843798F16619D6FCD3FE0	00000000	HUAW
Snapdragon 630/636	0000	0000	0374637D23C4E2EEDE23DA5D60C1E7ABCD81CCC4CD641045F859B317650F47DF	00000000	LENO
Snapdragon 460	02E8	0000	ABBCC86FE393B13D59E2A2EC944AF26DA3FA3D4B2A1CCD2FB383C73E0FFFC30DC1736DCB2752E955A61421C349974F90	00000000	Moto:
Snapdragon 205	0042	0050	1357FDAEABB7BECBE49095F000D9D3DADF198885106D98598CAC6D1B9B2EDB3A	00000000	Noki:
Snapdragon 855	0051	4985	2ACF3A85FDE334E2E28D64CBC416B2474E0E95CAD4698F143E27475D67E92D995A20DA04E40395B61A140F3DB7C32720	00000000	OneP:
Snapdragon 865	0051	4D6D	7C15A98DB4E70963715F51C8DA39C1E66FC1C3334E95F4C6A5627DA6A49C842F06B43E8DE1F589FC36CE1135C7FA5AA2	00000000	OneP:
Snapdragon 662	0051	0000	49445E14621312DFECCD4389F267E6B71674DD36B1BC41D1F605AA991D14AD687834378CF2129259DFAF107D75EE329	00000001	OPPO
Snapdragon 855	0051	0000	D09BA40B51377E09D854D6E695B9228038F34EBDB779143D1540F60EC3C59EFB26239F8AE74B2A5AC7C474BEC92F030C	00000001	realr
Snapdragon 660	0060	0000	81BA684F89EE4AE0D12943FBA51251B7E8F3A25DA21FA16943930330D456E42B	00000000	Trim
Snapdragon 460	0073	0003	A7DF36FFD7AB557C67A6C26675E2795C922CF671308CFD7169BEDB84424C862BC7B646907DD79989578590FB6370A940	00000000	vivo
Snapdragon 662	0072	0000	1BEBE3863A6781DB01086063007334DE95E5CA14971C7C4F4358EC9D79CDA4692CE5E948C6FD409408F4C919FCADFE3	00000001	Xiaor
Snapdragon 820	0000	0000	355D47F912FEE0AF1F46C007C6DC22C43544FB9359E30AA7DB5F4734D18FBD74	00000000	Xiaor

As a result of the search, all device models that contain the entered characters in any field (name, hash, processor, etc.) will be displayed. In this case, the list will contain actually connected devices without coloring, and unconfirmed data will be colored in shades of red.

There are two buttons behind the search field – decrease and increase the font size of the Directory. Changing the font size only affects the internal structure of the table.


Firehose Finder						
File View Instruments Help						
Work with device Work with files Reference book of devices						
u	HWID	FullName	OEM	Model	OEM Private Key Hash	Wrac
	0005F0E1	Snapdragon 821	0000	0000	355D47F912FEA0AF1F46C007C6DC22C43544FB9359E30AA7DB5F4734D18FBD74	Xi
	0008C0E1	Snapdragon 660	0000	0000	A7B8B82545A98ECA23D6E9105FB464568D1B5828264903441BDEF0CD57E3C370	Xi
	009B00E1	Snapdragon 650	0000	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A	Xi
	009B00E1	Snapdragon 650	0000	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A	Xi
	000560E1	Snapdragon 425	0020	0000	5C08AA84F75507D14F7E6C18D46106E8A0DAA2B580FE0EEA64D249DAD681D004	Xi
	000950E1	Snapdragon 675	0072	0000	1BE8E3863A6781DB4B01086063007334DE9E5CA14971C7C4F4358EC9D79CDA4692CE5E948C6FD409408F4C919FCADFE3	Xi
	001630E1	Snapdragon 750G	0072	0000	1BE8E3863A6781DB4B01086063007334DE9E5CA14971C7C4F4358EC9D79CDA4692CE5E948C6FD409408F4C919FCADFE3	Xi
	007050E1	Snapdragon 400/410	0000	0000	CC3153A80293939B90D02D3BF8B23E0292E452FEF662C74998421ADAD42A380F	Xi
	000BA0E1	Snapdragon 632	0072	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A	Xi
f	0014D0E1	Snapdragon 662	0072	0000	1BE8E3863A6781DB4B01086063007334DE9E5CA14971C7C4F4358EC9D79CDA4692CE5E948C6FD409408F4C919FCADFE3	0. Xi
f	0004F0E1	Snapdragon 430	0000	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A	0. Xi
f	0006B0E1	Snapdragon 435	0000	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A	0. Xi
f	000560E1	Snapdragon 425	0000	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A	0. Xi
f	000BF0E1	Snapdragon 439	0072	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A	0. Xi
f	000BF0E1	Snapdragon 439	0072	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A	0. Xi
f	0011E0E1	Snapdragon 765G	0072	0000	1BE8E3863A6781DB4B01086063007334DE9E5CA14971C7C4F4358EC9D79CDA4692CE5E948C6FD409408F4C919FCADFE3	0. Xi
f	000460E1	Snapdragon 625/636	0000	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A	0. Xi
f	000CC0E1	Snapdragon 630/636	0000	0000	A7B8B82545A98ECA23D6E9105FB464568D1B5828264903441BDEF0CD57E3C370	0. Xi

When erasing the characters in the search box, the results will be reset and the output will display the data according to the selection in the menu.

The window "Insert model"

This window is intended for manual entry of information about the manufacturer of the device, its model and alternative name. According to this data, a "[Device collection](#)" will be formed. Since it is not always possible to get this data in automatic mode, you have to use manual input.

The "Manufacturer" field is required to be filled in, "Model" and "Alternative name" are not required to be filled in. You can select the device manufacturer from the drop-down list or enter your own if there is no such manufacturer in the list.


Insert device model
✕

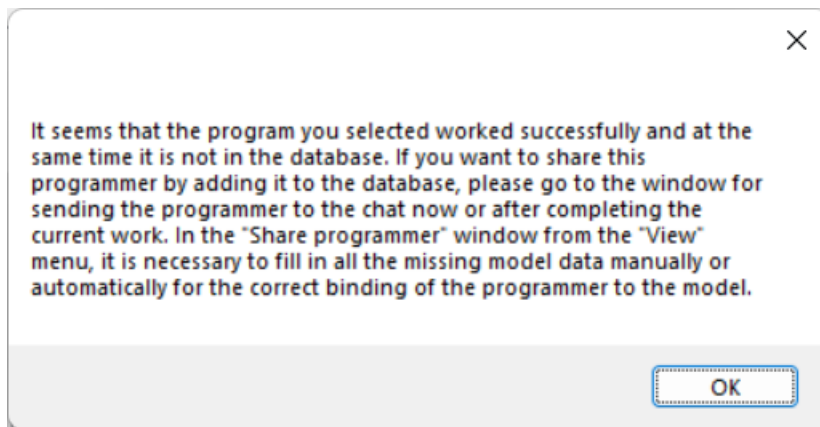
Manufacturer *

Model

Alternative name

The window "Share the programmer" (disabled)

This window is designed to send the programmer to the general chat. Later, at the next update of the program, the programmer will be added to the database of the FhF program. You can only send a successful programmer with a really connected device.



To correctly fill in the data for sending the programmer, you need to get:

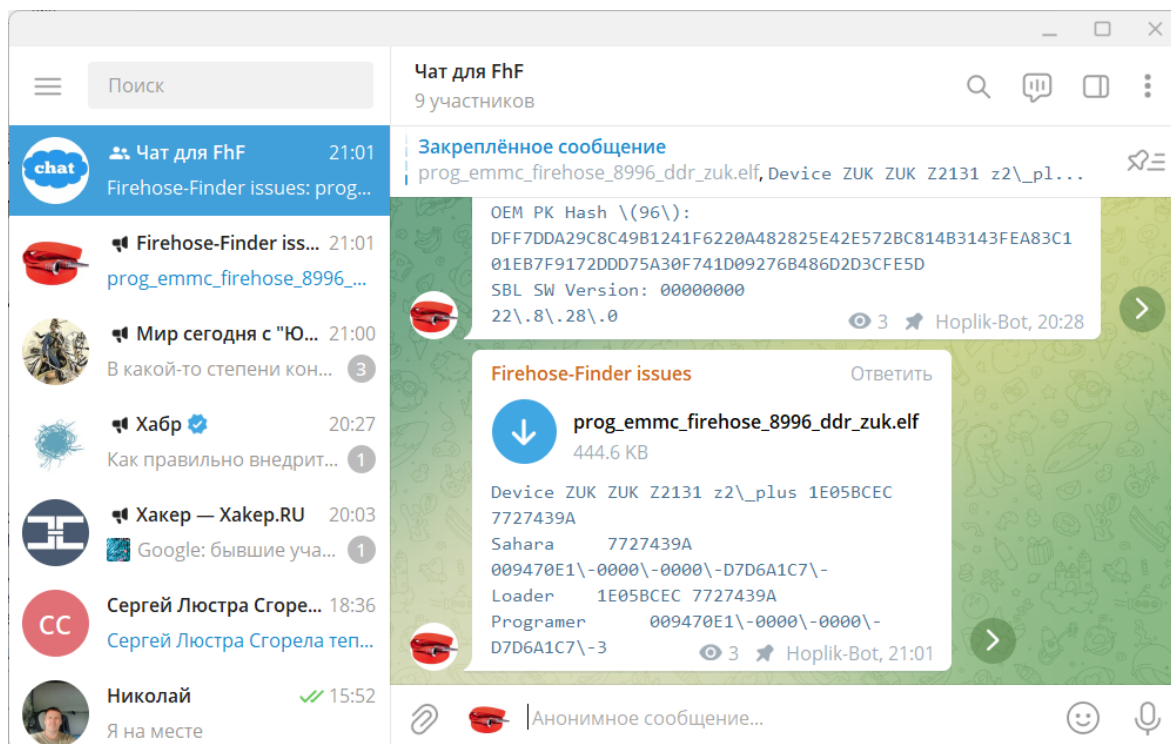
1. Device data (manufacturer, model, name, serial number of the device and chip);
2. Device and programmer IDs (are pulled up automatically when checking the programmer).

The device data can be obtained both automatically and manually by opening the "Insert model" window. To automatically receive device data, you need to connect it in normal mode, enable USB debugging on the device, and click the "Poll the device" button. Another option: open the "View" tab - "Work with device". On the "ADB" tab, click the "Start ADB" button and select the command "Get the model of the device", then "Reboot to edl mode (9008)".

After receiving the device data, you can check the programmer. When it is successfully connected and the data table is filled in, the "Share" button will become available. If the device data is not fully filled in (there is no Manufacturer), then the window must be closed with the "Cancel" button and the procedure for obtaining device data described above must be carried out.

	Man	Model	Alt name	Device number	Chip number	IDs	Path
Device	ZUK	ZUK Z2131	z2_plus	1E05BCEC	7727439A		
Sahara					7727439A	009470E1-0000-0000-D7D6A1C7-	
Loader				1E05BCEC	7727439A		
Programmer						009470E1-0000-0000-D7D6A1C7-3	C:\ZUK\prog_emmc_firehose_8996_ddr_zuk.elf

Information about the device and the verified programmer are sent to the general chat.



With the next update of the FhF program, this programmer will be added to the general database of the "[Device collection](#)" tab.

Menu item "Instruments"

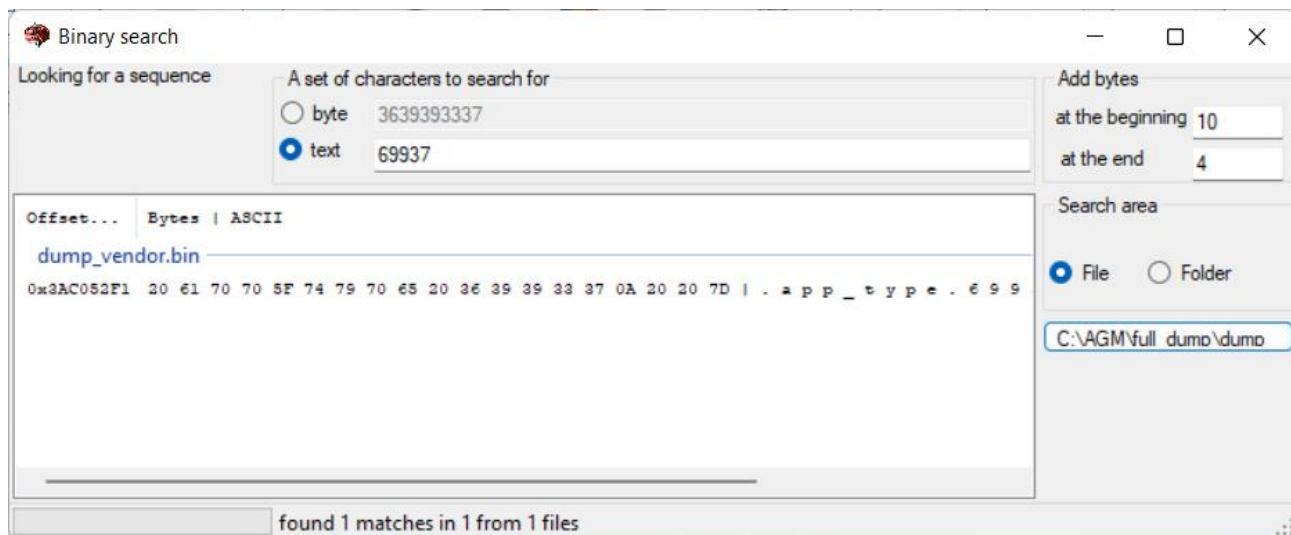
This menu contains tools that can help when unpacking the firmware and when searching for information in files saved from the device.

Section "Binary search"

The "Binary search" tool can be useful for searching for a certain sequence of bytes in files downloaded from the device. For example, to edit sound parameters, you need to find a sequence of text characters "69937". When typing in the "text" field, the characters will be automatically converted into a sequence of bytes for search. The search can be carried out either in a separate file or in several located in the same folder at once. If the file size is more than 1 GB, the search procedure may take a considerable time (depending on the power of the computer on which the program is running).

For the convenience of evaluating the usefulness of search results, it is possible to add several characters (by default, 10 bytes - 5 text characters at the beginning and 4 bytes - 2 text characters at the end) to the search string results. The search result is presented as a sequence of bytes and their transcoding into text characters (unreadable characters are replaced by a dot).

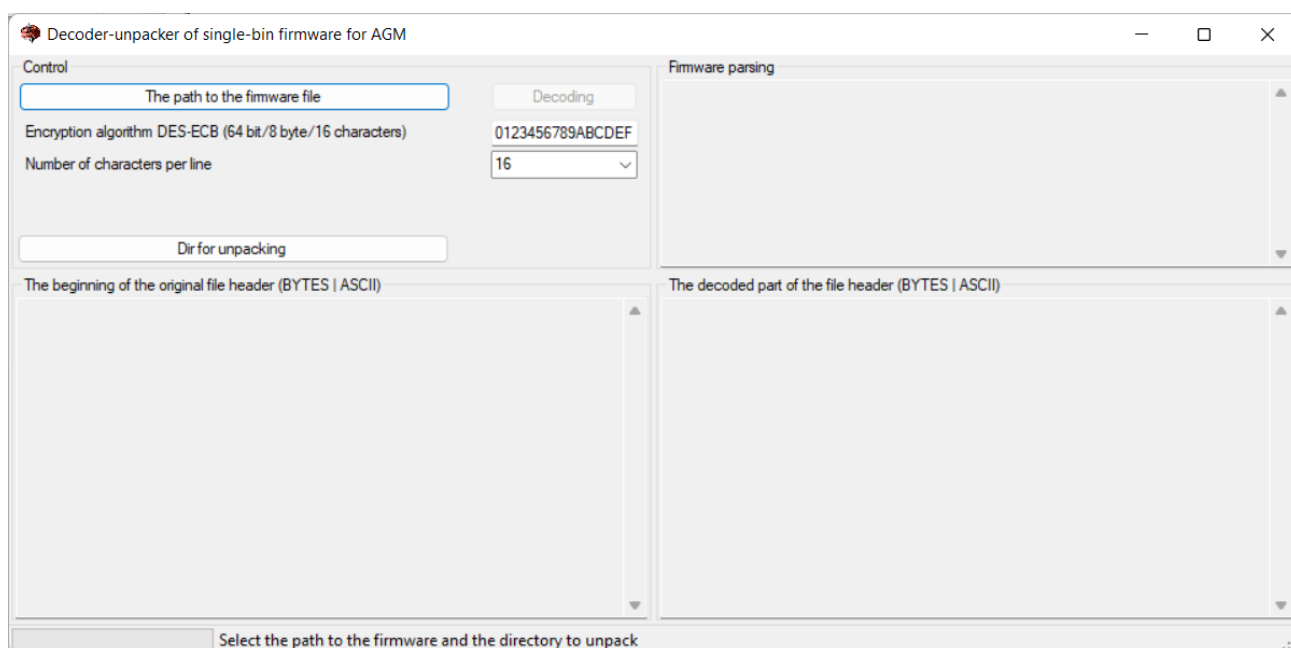
Double-clicking on the search results line allows you to save the address of the beginning of the byte sequence for the search to the clipboard. This can be used when opening a file in a hex editor and going to the address inserted from the clipboard to edit this file. The name of the file in which the required sequence is found is indicated at the end of the search results line. If there are several results, they are grouped by file name and sorted by address in ascending order.



Section "Decode and repack ROM (AGM)"

The tool "Decoder-decompressor of single-bin firmware for AGM" is designed for decoding and unpacking files for AGM phones from single-file bin firmware (the signatory of the firmware is Hisense, packer version 2). The need to parse the firmware was caused by the search for a programmer, who, as a result, turned out to be part of the unpacked firmware.

The initial project was implemented by [Vladimir Sitnov \(proger10\)](https://github.com/proger10/agmx3-firmware-tools) and published on github (<https://github.com/proger10/agmx3-firmware-tools>). Based on the information from this project, this "Decoder-Unpacker ..." was written and included in the Firehose Finder software package.

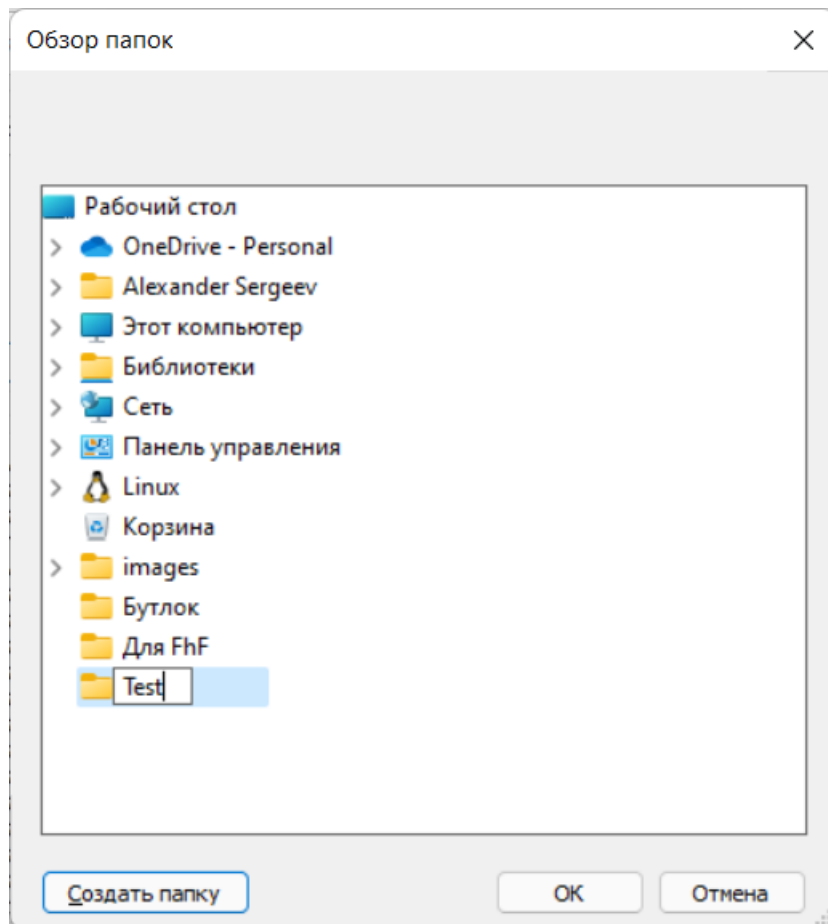


To decode the firmware, you must specify the path to the single-bit file by clicking the appropriate button. After specifying the file, its reading will begin immediately. Not the entire block of information of the firmware header is displayed on the form, but only a part, to optimize the speed of the program. The information is displayed in the original (encrypted) form.

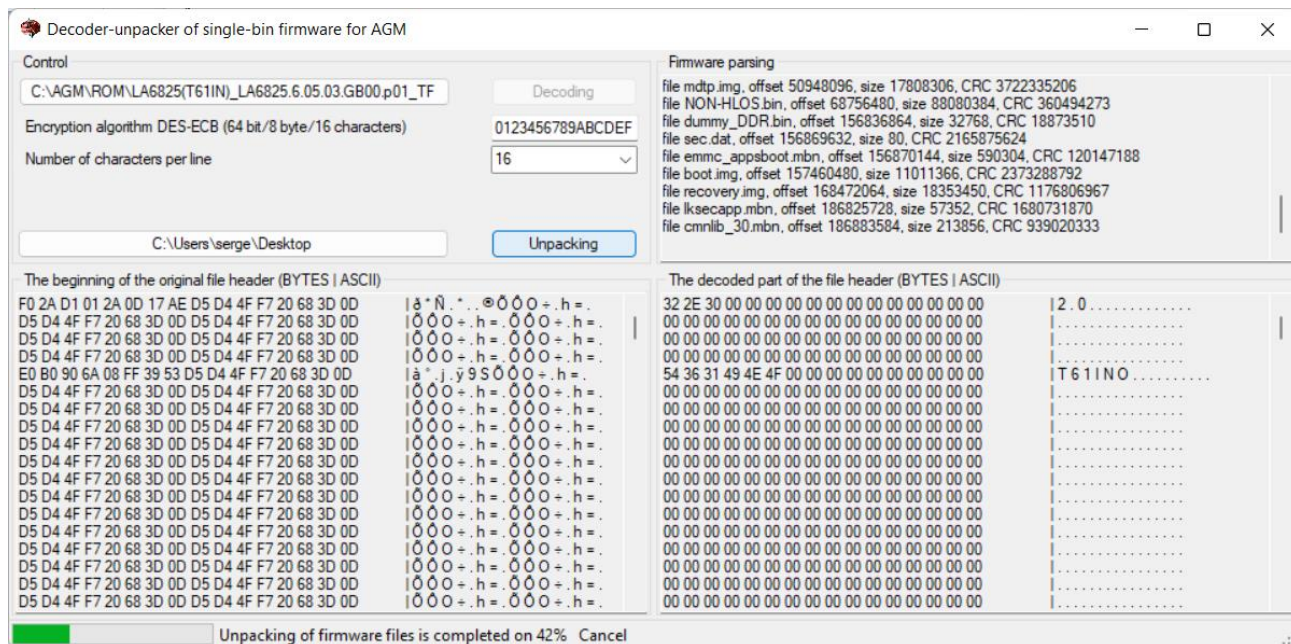
After reading the firmware header, the "Decoding" button becomes active. To decode, you must specify the encoding code. By default, "0123456789ABCDEF" is set. You can also choose how many characters to display in a string for the convenience of evaluating the correctness of decoding. The same

segment of information will be displayed on the bottom right of the form as on the left, but taking into account the decoding of the specified code. At the same time, the firmware header will be immediately disassembled, which will be reflected in the corresponding window at the top right on the form. To answer the questions: "Why was such a code chosen?" and "How to find it as part of the encoded firmware?" you can read the article in the wiki on Github (https://github.com/hoplik/AGM_Repacker_ROM/wiki/Finding-the-key).

After specifying the directory for unpacking and successfully decoding the header, the "Unpacking" button will become active. When you select the unpacking directory, you can create a new folder.



After clicking the "Unpacking" button, the process of unpacking the firmware begins. This may take a long time, depending on the power of the computer. To forcibly stop the unpacking process, you can click the "Cancel" button, which appears at the bottom of the form after completing at least 5% of the running task. In the process of unpacking, the process log is written in the upper right window.



After the unpacking process is successfully completed, the "Cancel" button will change the name to "Open in Explorer". When you click in Explorer, a folder with the extracted firmware will open.

Menu item "Help"

Section "View help"

Opening this help file.

Section "About"

The name of the program, the current version, a brief description of the program, a link to the basic topic of discussion of the general principles of bootloader recovery, a link to a telegram channel for sending suggestions / comments, buttons for donations.

When you click on the logo, the address of the application installation folder will be displayed.

About Firehose Finder



Firehose Finder

Version 22.9.8.0

Copyright © 2020 HOPLIK

The program of selection of programmers (firehose) for devices based on processors from Qualcomm.

Do you have any questions, suggestions, comments? Write to the Telegram channel "[Firehose - Finder issues](#)"

Topic 4PDA "[Общие принципы восстановления загрузчиков на Qualcomm | HS - USB QDLoader 9008, HS - USB Diagnostics 9006, QHUSB DLOAD и т.д.](#)"

Thanks:

@SashaSeri - for ideas, comments and basic information;
@Always_Alone_R - for testing on a UFS device;
@krvedko - for tips for the firmware unpacker.

ЮMoney - thank's

QiWi - many thank's

Did you have a desire to thank the author for the work done? Please use the buttons to donate.

OK