

## Оглавление

Часто задаваемые Вопросы и Ответы (ЧаВО) .....	2
Окно «Приветствие».....	4
Пункт меню «Выбор языка» .....	5
Пункт меню «Рейтинг» .....	5
Вкладка «Работа с файлами» (основная) .....	9
Вкладка «Работа с устройством» (скрытая) .....	11
Раздел «ADB (Android Debug Bridge)» .....	11
Раздел «Fastboot (bootloader)» .....	12
Раздел «Sahara & Firehose loader» .....	13
Команды контекстного меню .....	17
Вкладка «Справочник устройств» (скрытая) .....	19
Окно «Внести производителя, модель».....	21
Окно «Поделиться программером» (неактивное) .....	21
Пункт меню «Инструменты» .....	23
Раздел «Бинарный поиск».....	23
Вкладка «Поиск по маске в файле» .....	23
Вкладка «Сравнить файлы» - разработка остановлена в связи с отсутствием необходимости.	24
Вкладка «Дубликаты файлов в папках» .....	25
Вкладка «Разобрать дамп диска» - разработка остановлена в связи с отсутствием необходимости.	26
Раздел «Распаковка однобиновой прошивки (AGM)» .....	27
Раздел «Драйвера EDL и ADB» .....	30
Раздел «Извлечь сертификаты» .....	30
Пункт меню «Справка» .....	31
Раздел «Просмотр справки» .....	31
Раздел «О программе» .....	31

## Часто задаваемые Вопросы и Ответы (ЧаBO)

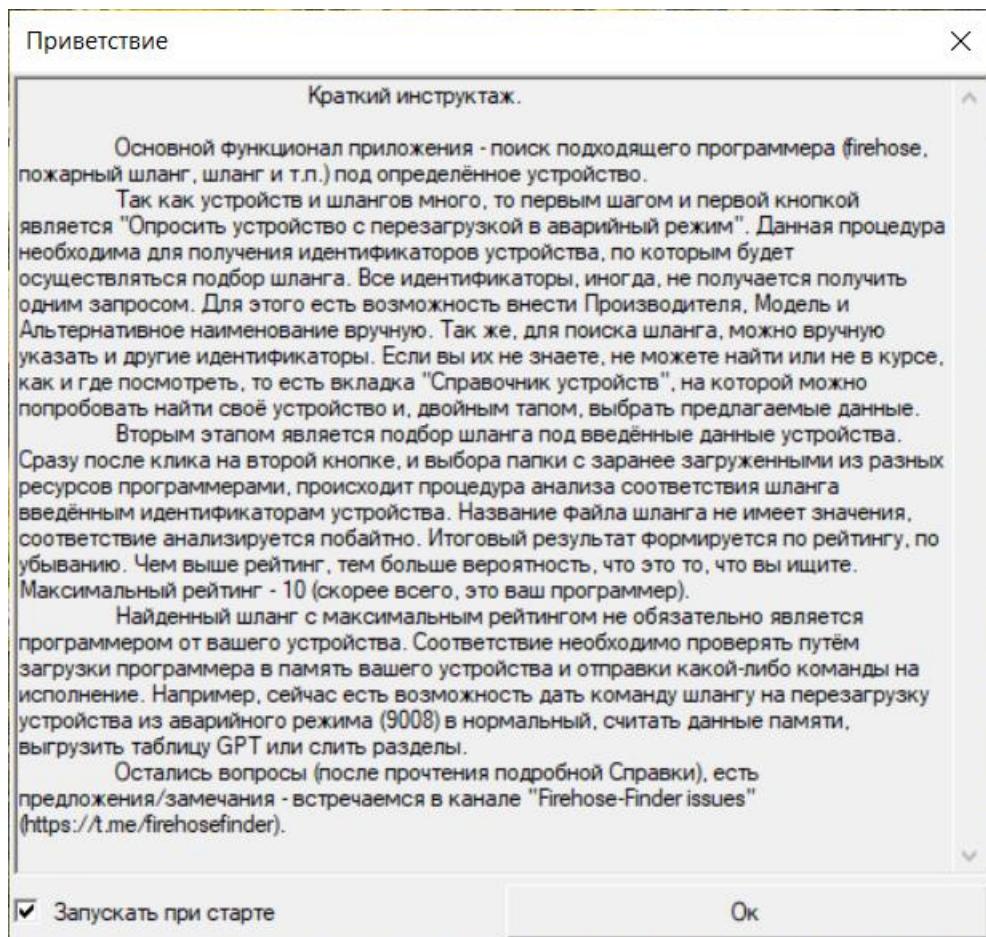
- q. Какие базовые требования предъявляются к оборудованию и программному обеспечению для успешной работы программы?
  - а. Для установки программы необходима 64-бит версия Windows с установленным фреймворком .net 4.7.2 или выше. Если подключённое устройство определяется, как QUSB\_BULK, то это говорит о том, что необходимо установить драйвера для работы с таким оборудованием. Для некоторых моделей есть драйвера в составе установочного пакета. Можно открыть через интерфейс программы раздел меню «Инструменты – Драйвера EDL и ADB». Для устойчивой работы по протоколу Sahara необходимо выбирать порт USB 2.0 (с портом USB 3.0 протокол работает нестабильно). Если параллельныйпорт автоматически определяется выше 10, то стоит переназначить его вручную до 10. При указании пути к программеру необходимо избегать кириллицы и пробелов. С ними протокол выдаст ошибку пути.
- q. Как формируется рейтинг файла в папке с программерами?
  - а. Файлы с рейтингом 0 не являются исполняемыми файлами, и в них не осуществляется поиск сертификатов. Рейтинг 1 у файла ELF (ELE), BIN, MBN. Это могут быть любые файлы прошивки (программеры, xbl, apps и т.п.). К рейтингу добавляется 1, если SWID (идентификатор программного обеспечения) начинается с 3 (это признак загрузчика для аварийного режима – Firehose programmer), ещё +1 балл к рейтингу, если совпадают идентификаторы у модели телефона, указанного в поле поиска, и в сертификате программера. Также к рейтингу добавляется 1, если совпадает производитель и ещё 1, если процессор. Совпадение хеш-суммы корневого сертификата добавляет сразу 5 баллов к рейтингу. Чем выше рейтинг файла (программера), тем выше вероятность того, что он подойдёт к телефону, параметры которого введены для поиска. Максимальное значение рейтинга - 10 баллов.
- q. Откуда я могу получить идентификаторы своего устройства (HW\_ID, OEM\_ID, MODEL\_ID, OEM\_HASH)?
  - а. Автоматически, с вкладки «[Работа с файлами](#)», нажав кнопку «Опросить устройство с перезагрузкой в аварийный режим»; вручную, выбрав подходящее устройство на вкладке «[Справочник устройств](#)» двойным кликом; используя другие программы для обращения к памяти для запроса идентификаторов: - emmcctl с командой -info: - QLMCPUInfo; - QSaharaServer с командами -c 02(03,07).
- q. Почему некоторые файлы в отчёте выделены красным цветом и имеют подсказку «Файл не является ELF!», «Файл закодирован»?
  - а. Большинство программеров имеют в начале файла код, определяющий принадлежность файла (magic\_number). При этом попадаются программеры, у которых, по разным причинам, в шапке применён другой набор байт (маска), и такие файлы системой не идентифицируются, как рабочий программер. Цветом и подсказкой такие файлы выделяются для информирования пользователя о невозможности их использования данной программой (возможно, другое ПО сможет с ними работать).
- q. Куда и кому отправляются, и какие именно, данные с моего устройства?
  - а. Данные отправляются ботом (программный код) в публичный телеграмм-канал «[Firehose - Finder issues](#)». Информация из этого канала обрабатывается для изменения/добавления/исправления программы. Вся поступающая информация

находится в открытом доступе, любой пользователь Телеграмм может подписаться на этот канал и проконтролировать передачу информации. Отправляются идентификаторы устройства – тип процессора, его серийный номер, модель, производитель, вендор. **Никакая персональная информация, способная однозначно привязать данные устройства к пользователю, не передаётся.**

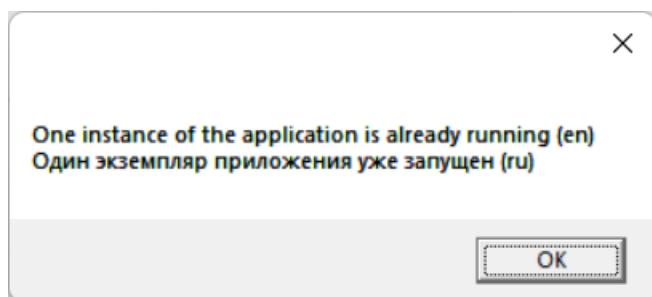
- q. У меня есть рабочий программер для моего устройства. Как мне поделиться им или добавить в базу данных программы?
  - a. Через интерфейс программы FhF можно отправить только программер, который успешно отработал с реально подключённым устройством. Подробное описание можно найти в разделе «[Поделиться программером](#)».
- q. Где я могу посмотреть исходный код? Как его можно изменить или предложить свои доработки?
  - a. Исходный код программы FhF размещён в публичном репозитарии на площадке GitHub ([ссылка для просмотра](#)). Вы можете свободно скачать весь код или любую его часть. Чтобы предложить свои изменения вы можете воспользоваться либо разделом «Issues», либо делать форк репозитария. Для этих действий потребуется регистрация на GitHub.

## Окно «Приветствие»

При старте программы открывается окно «Приветствие». Оно сохраняет в программе состояние переключателя «Запускать при старте», и, если нет необходимости в постоянном запуске этого окна при старте программы, то галку можно снять. При необходимости вернуться к этому окну можно зайти в «Вид» и открыть его оттуда.

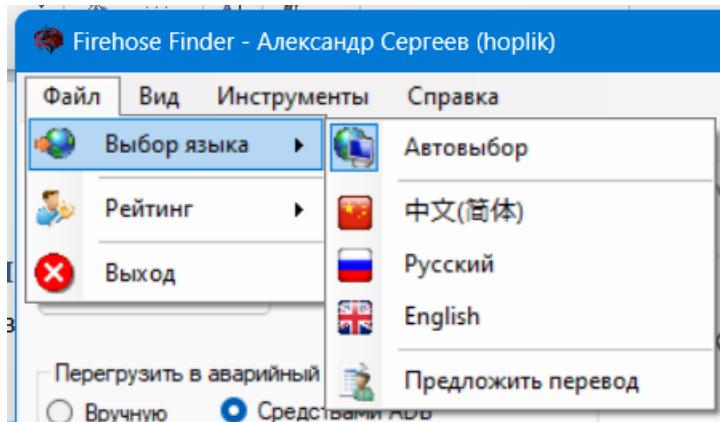


В программе реализован механизм запуска только одного экземпляра приложения. Если при запущенном приложении попытаться запустить второй экземпляр, то будет выведено предупреждение о невозможности осуществления такой операции.



## Пункт меню «Выбор языка»

Для удобства работы в программе можно использовать перевод текстовых надписей на привычный язык.



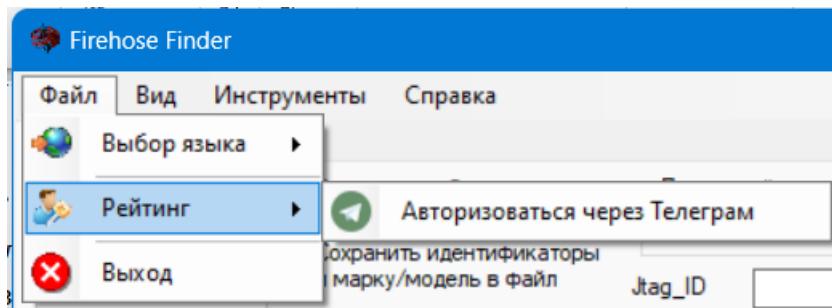
- «Автовыбор» - предполагает автоматический подбор языка в соответствии с региональными установками операционной системы. По-умолчанию язык приложения – «Русский».
- «Китайский (упрощённый)» - вне зависимости от региональных настроек операционной системы язык приложения задаётся как китайский.
- «Русский» - вне зависимости от региональных настроек операционной системы язык приложения задаётся как русский.
- «English» - вне зависимости от региональных настроек операционной системы язык приложения задаётся как английский.
- «Предложить перевод» - переход в телеграм-канал [«Чат для FhF»](#) для озвучивания своей готовности в переводе приложения на свой язык. Так как проект не коммерческий, то работа по переводу не оплачивается и является символом доброй воли автора.

При перезагрузке приложения настройки языка сохраняются. Изменение языка требует перезагрузки приложения без перезагрузки операционной системы.

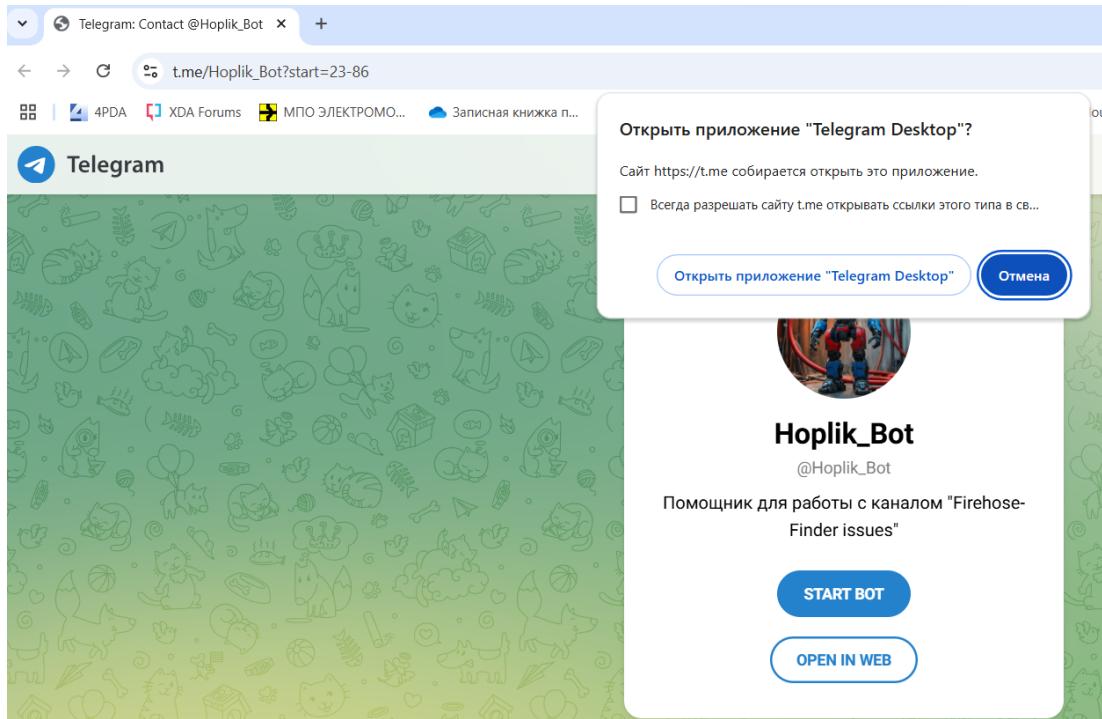
## Пункт меню «Рейтинг»

Рейтинг предназначен для отображения личного вклада любого зарегистрированного в Телеграм и прошедшего авторизацию пользователя в развитие этого проекта.

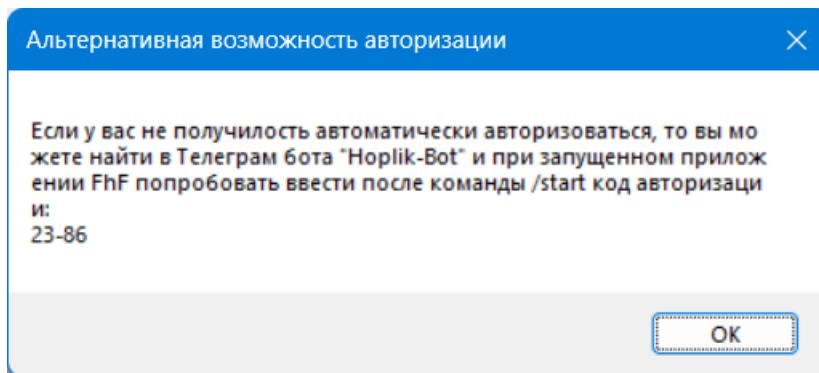
Для участия в рейтинге необходимо пройти авторизацию.



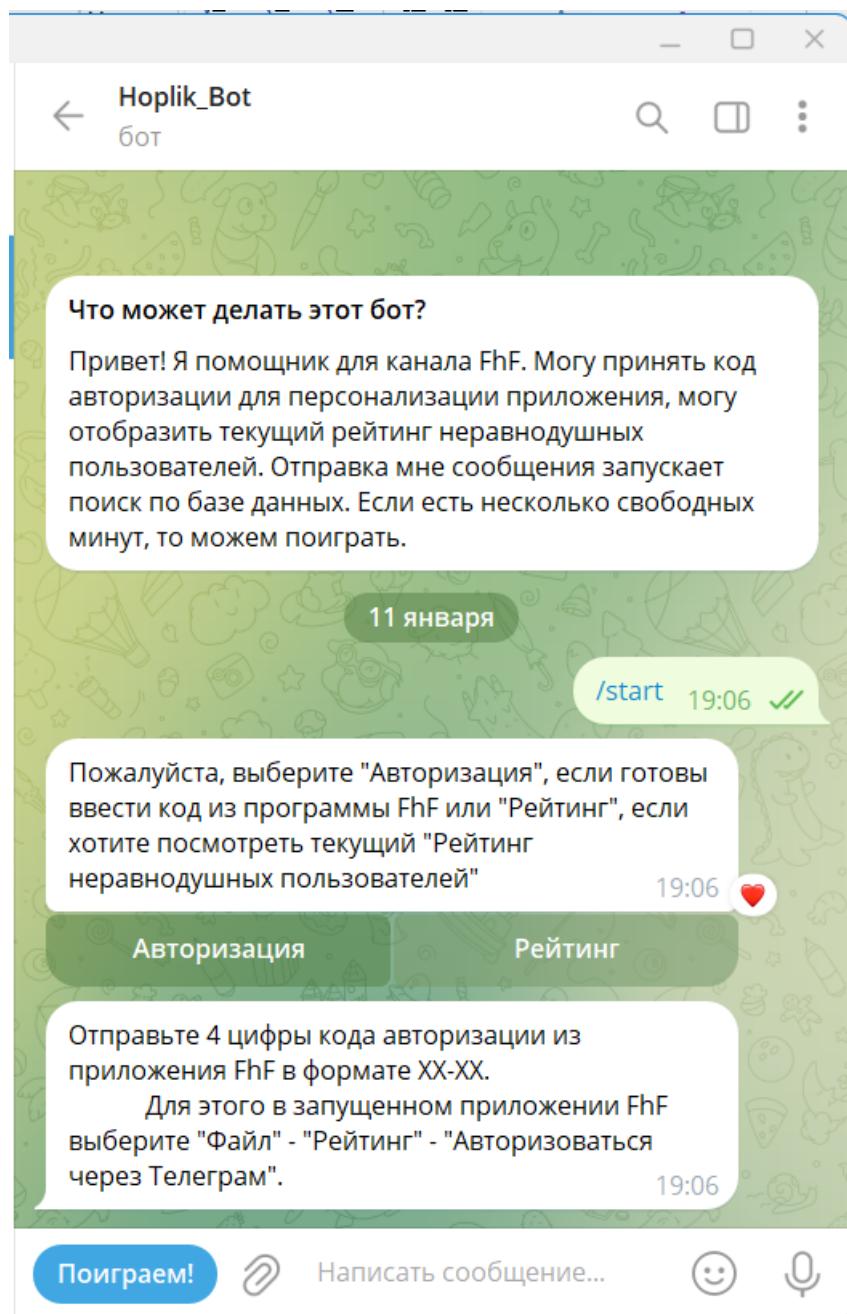
При запуске процедуры авторизации **никакого доступа к профилю пользователя в Телеграм не осуществляется**. Проверяется только персональная привязка программы и профиля в Телеграм путём ввода аналогичного случайного кода.



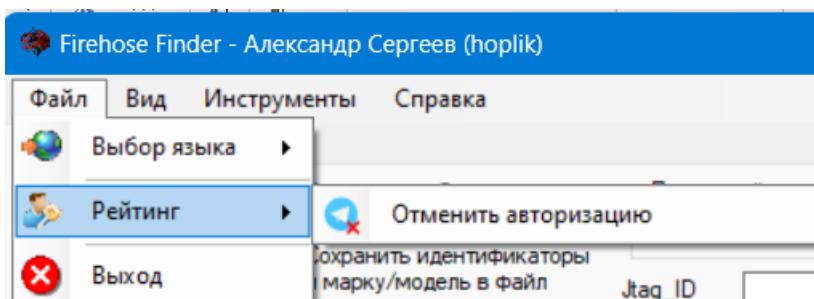
Боту автоматически отправляется команда /start с кодом авторизации. Приложение пытается этот код получить. Если процедура закончится неудачей, то авторизация не подтвердится и выскочит предупреждение о необходимости повторить процедуру.



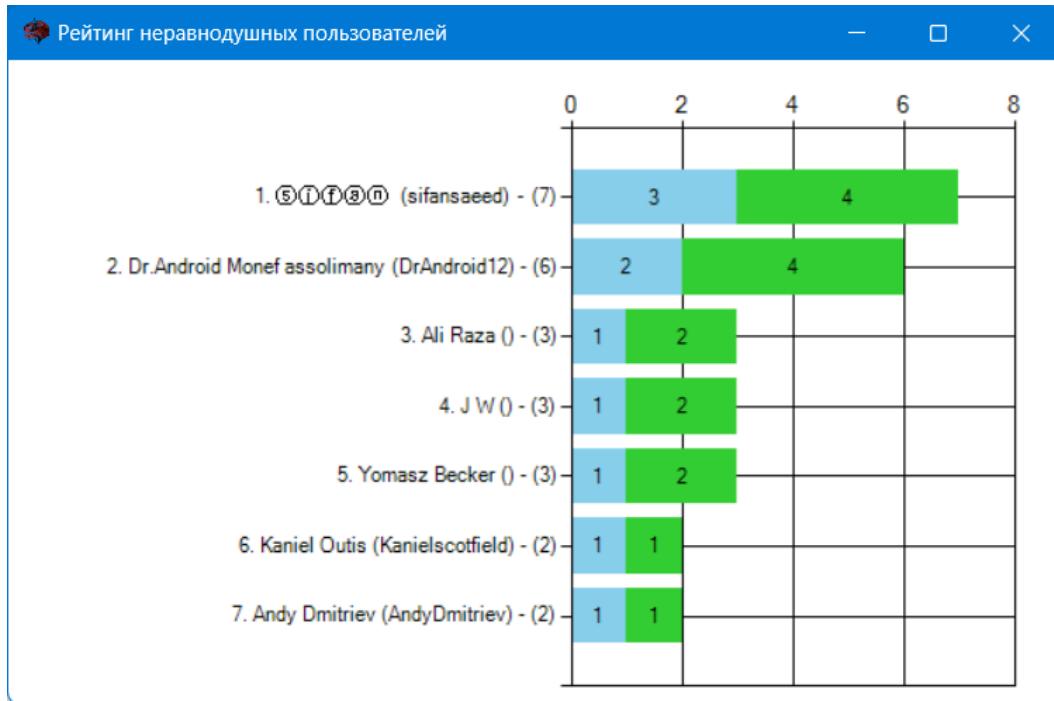
Если на компьютере не установлена desktop версия Телеграм, то код авторизации можно отправить боту в мобильного устройства. Необходимо найти бота @Hoplik\_Bot, отправить ему команду /start и выбрав пункт «Авторизация» передать код авторизации в формате xx-xx из приложения (на данном примере 23-86).



При успешной авторизации приложение автоматически перезагрузится и вы увидите свои данные профиля Телеграм в титуле приложения. С этого момента при отправке данных в канал в конце сообщения будет дописываться ссылка на ваш профиль. При отсутствии желания передавать в канал информацию с привязкой к профилю, пользователь может отменить авторизацию. Из рейтинга пользователь выбирает автоматически, через 6 месяцев от даты последнего сообщения, отправленного в канал с привязкой к профилю.



Выбирая пункт меню «Рейтинг», открывается новое окно, в котором представлен «Рейтинг неравнодушных пользователей». Авторизованный пользователь при попадании в рейтинг выделяется **красным цветом**.



Принципы формирования рейтинга и выплаты вознаграждений участникам:

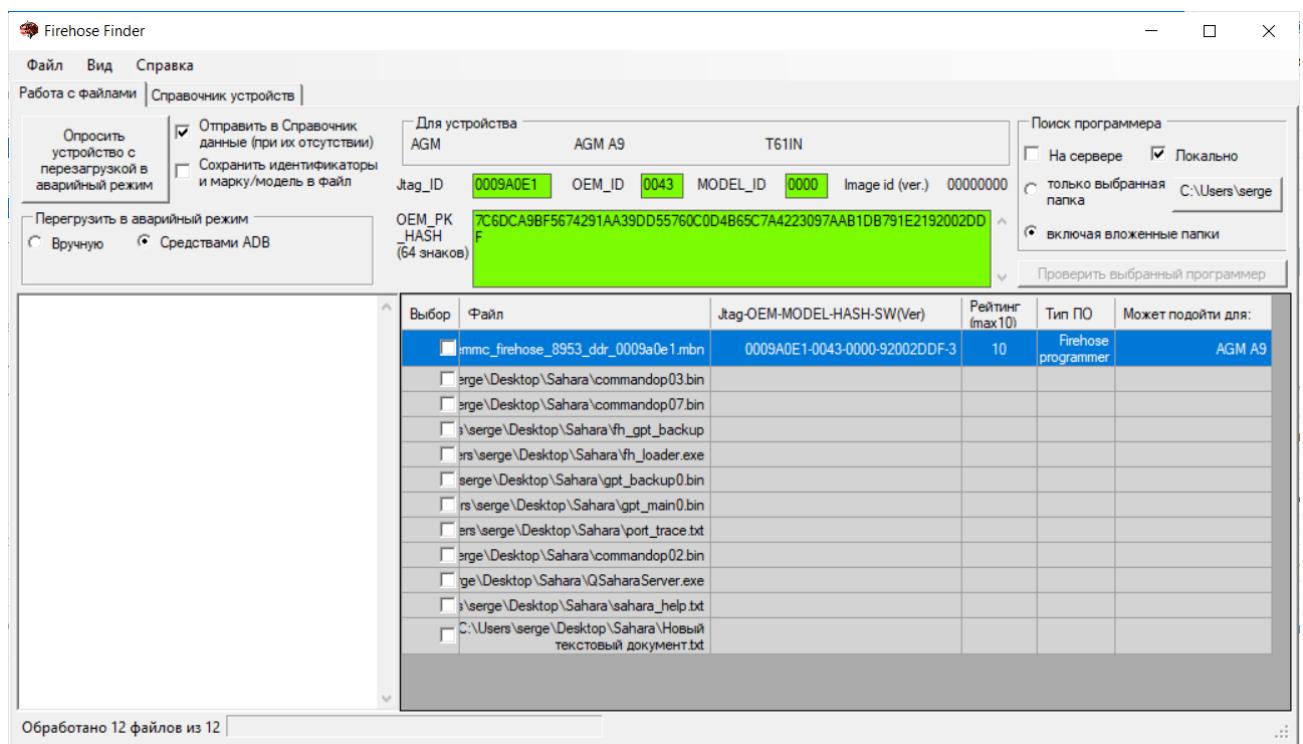
- Выплата вознаграждения - в пределах остатка счёта. Пополнение счёта вознаграждений - от донатов пользователей.
- Минимальная сумма для получения вознаграждения - 0.03 тон (по лимитам Телеграм на момент формирования Принципов). У кого получается меньше – вознаграждение не выплачивается. Американцам, корейцам и ещё ряду жителей "специализированных" стран воспользоваться средствами не удастся. Смотрите ограничения Телеграм по странам (<https://walletru.helpscoutdocs.com/article/60-znakomstvo-s-wallet#----urscr>).
- Для каждого месяца берётся для распределения 50% от остатка. Если после подготовки выплат остаток на счёте окажется меньше минимальной суммы для выплаты лидеру рейтинга, то за этот месяц распределяется не 50%, а 100% средств на счёте.
- Единицей рейтинга пользователя считается **сообщение со ссылкой на его профиль** в канале.
- Для увеличения рейтинга считаются **реакции (лайки) других пользователей** на это сообщение. Один лайк = один балл к рейтингу.
- Текущая сумма выплат делится на каждого участника рейтинга в его доле от общей активности (сообщения + лайки).
- Старые сообщения (сроком давности более полугода) не анализируются. Суммы для пользователя меньше минимума не выплачиваются и не накапливаются.

- По правилам Телеграм получатель платежа имеет свободу воли явно принять платёж или явно от него отказаться. При бездействии со стороны получателя, после 14 дней с момента платежа, платёж будет возвращён отправителю автоматически.

## Вкладка «Работа с файлами» (основная)

Основная вкладка для работы с программой – «Работа с файлами». Она всегда активна. Базовый функционал – подключить устройство в нормальном режиме (режиме зарядки) и нажать кнопку «Опросить устройство с перезагрузкой в аварийный режим». При такой работе средствами ADB (Android Debug Bridge) запрашиваются идентификаторы устройства из прошивки (производитель, модель, альтернативное имя и серийный номер процессора), устройство автоматически перегружается в аварийный режим, запрашиваются идентификаторы процессора (HW\_ID, OEM\_ID, MODEL\_ID, OEM\_PK\_HASH), все полученные данные копируются на форму.

Выбором пунктов «Перегрузить в аварийный режим» можно задать автоматический или ручной вариант перезагрузки (средствами ADB не всегда можно произвести перезагрузку в аварийный режим, не все аппараты это поддерживают). Также галками можно выбрать сохранение данных в файл и отправку данных в [Справочник](#). При сохранении данных в файл необходимо будет указать папку, в которую данные будут скопированы.



После получения идентификаторов устройство можно отключить и перезагрузить. Обычно выход из аварийного режима осуществляется долгим нажатием на кнопку «Питание» (более 10 секунд).

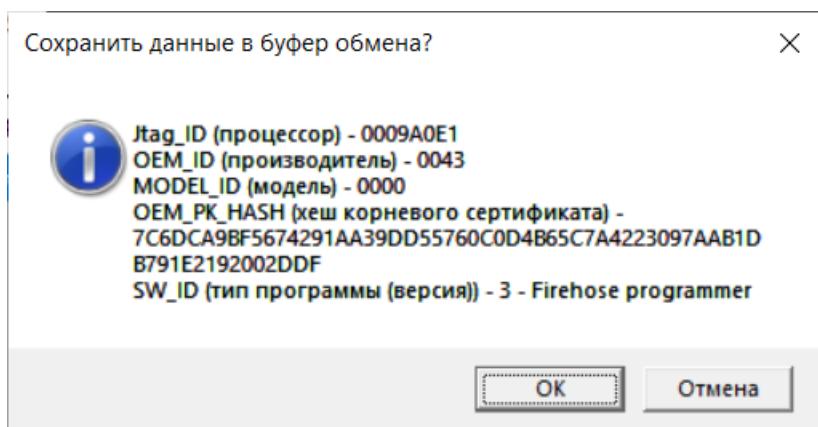
Когда данные устройства на форме заполнены (в автоматическом или ручном режиме), можно нажать кнопку «Поиск» в группе «Поиск программера» и выбрать путь к папке с коллекцией программеров. Переключателем можно выбрать область поиска:

- «На сервере»;

- «Локально».

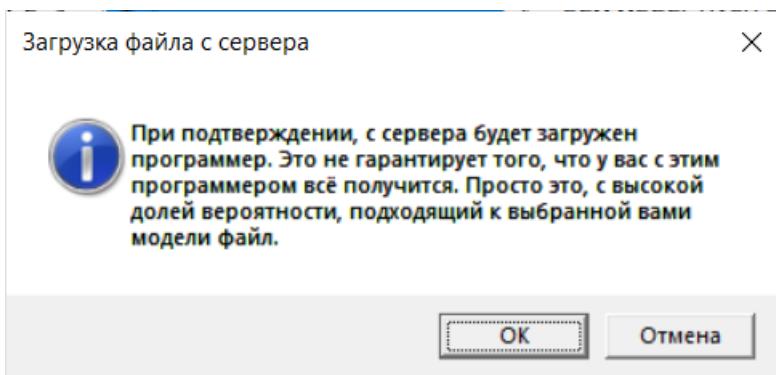
Для области «На сервере» заполненные данные формы являются своего рода фильтром. Таким образом, оставляя поля идентификаторов незаполненными, можно получить полный список программеров, расположенных на сервере. Внесение данных в поля идентификаторов позволяет сократить результаты поиска. Допускается частичное заполнение одного или нескольких полей.

Для области «Локально» анализируется либо «только выбранная папка», либо «включая вложенные папки» – в зависимости от выбранного положения переключателя. Проверяются все файлы, находящиеся в папках. Поиск программера осуществляется не по названию, а по идентификаторам, соответственно имя файла программера для анализа не важно. Каждому проверенному файлу присваивается [рейтинг](#). Сортировка в таблице осуществляется по рейтингу от большего к меньшему. Максимум – 10 (вероятность того, что это нужный программер самая высокая). Двойной тап на выбранном программере позволяет скопировать в буфер обмена информацию об идентификаторах, которые этот программер будет требовать при работе.



Программер можно проверить, подойдёт ли он для подключённого устройства. Для этого необходимо выбрать программер из проанализированного списка путём проставления галки в начале строки. При этом станет активна кнопка «Проверить выбранный программер».

Если выбранный для проверки программер располагается на сервере, то будет предложено его скачать в локальную папку.



Для проверки программеров, расположенных локально, устройство должно быть перезагружено в аварийный режим (9008) либо вручную, либо программно, со вкладки [«Работа с устройством»](#). Если устройство перед этим подключалось для получения идентификаторов, то его

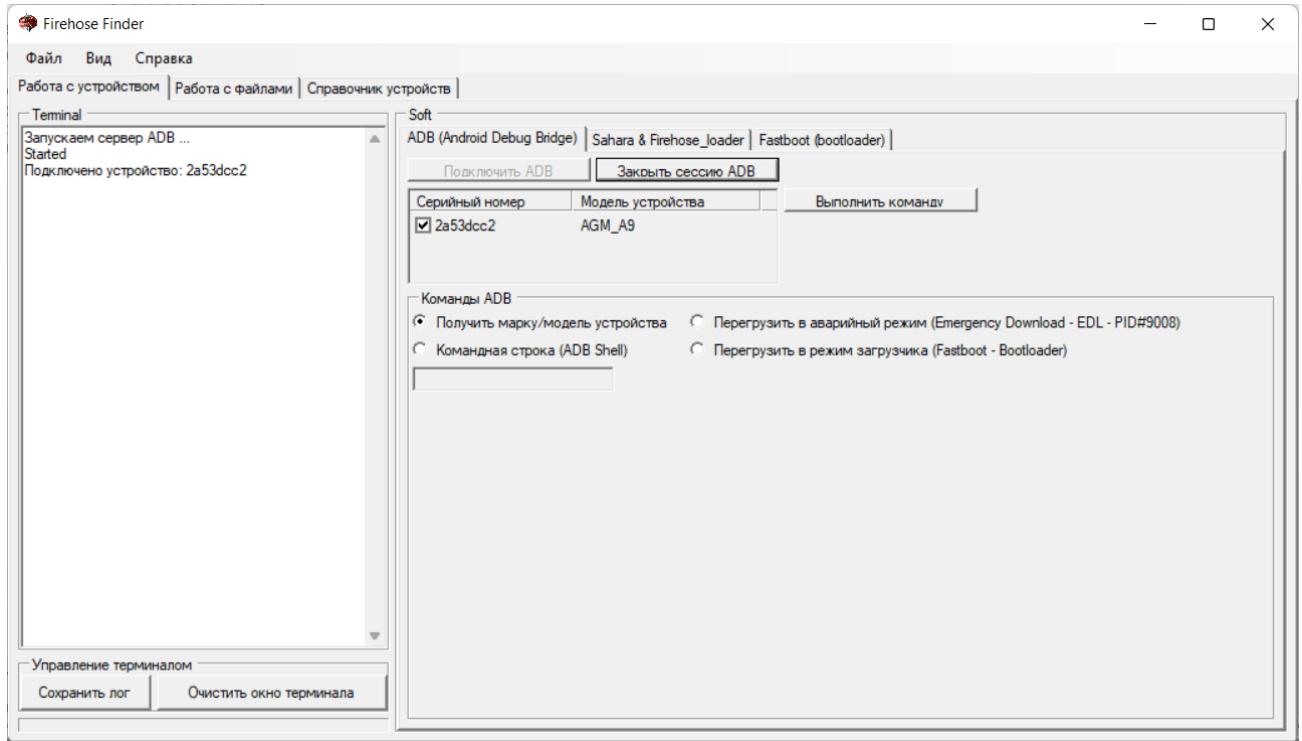
надо отключить от компьютера, перезагрузить и заново подключить. Это связано с особенностями протокола «Сахара» (второй раз приветствие для работы по протоколу не отправляется).

## Вкладка «Работа с устройством» (скрытая)

Активизировать вкладку можно из меню «Вид». Предназначено для более глубокого управления подключённым устройством.

### Раздел «ADB (Android Debug Bridge)»

Команды для ADB становятся активными после запуска ADB, необходимо нажать кнопку «Подключить ADB». При успешном старте в логе отмечаются серийные номера подключённых устройств.



На текущий момент в списке доступно четыре команды для ADB:

1. Получить марку/модель устройства. Запрашиваются свойства устройства из прошивки для заполнения формы.

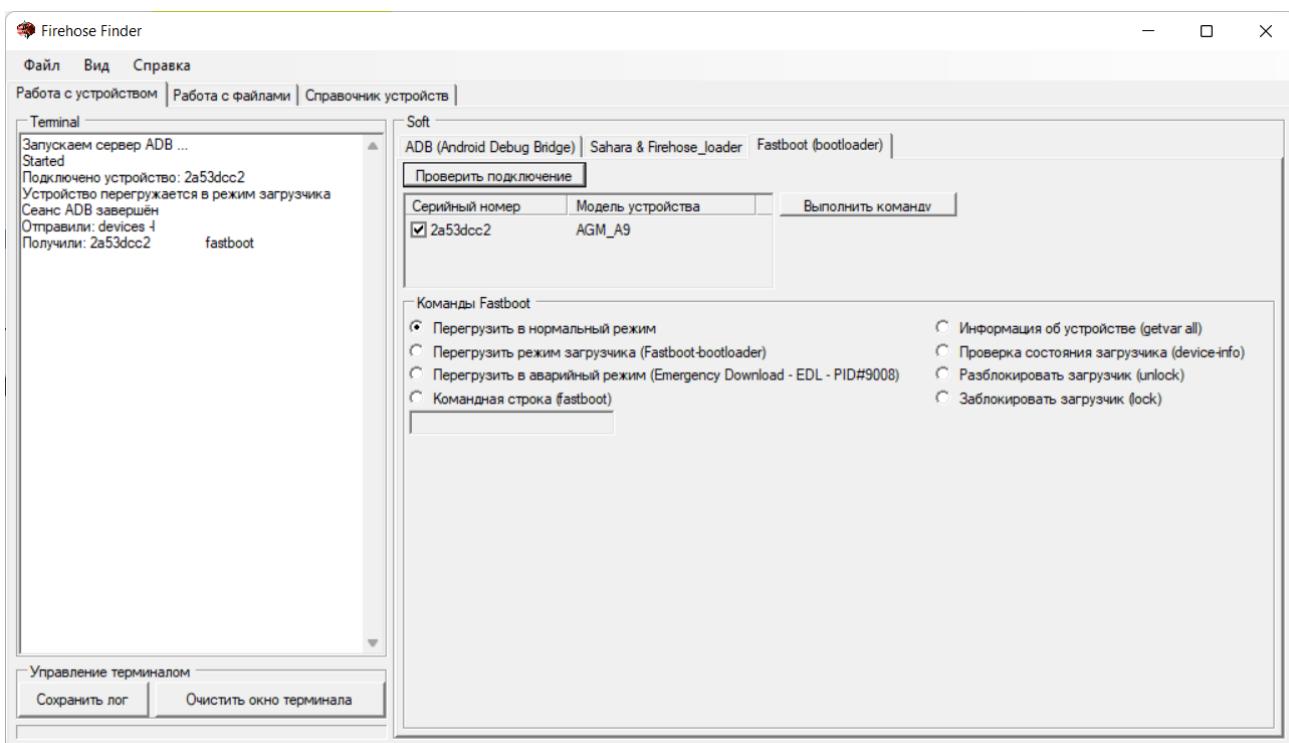
- Производитель – аналог команды `$ adb shell getprop | grep ro.product.manufacturer`
- Модель – аналог команды `$ adb shell getprop | grep ro.product.model`
- Альтернативное наименование – аналог команды `$ adb shell getprop | grep ro.product.name`
- Серийный номер процессора – аналог команды `$ adb shell cat /sys/bus/soc/devices/soc0/serial_number`

Данные автоматически копируются на вкладку «[Работа с файлами](#)».

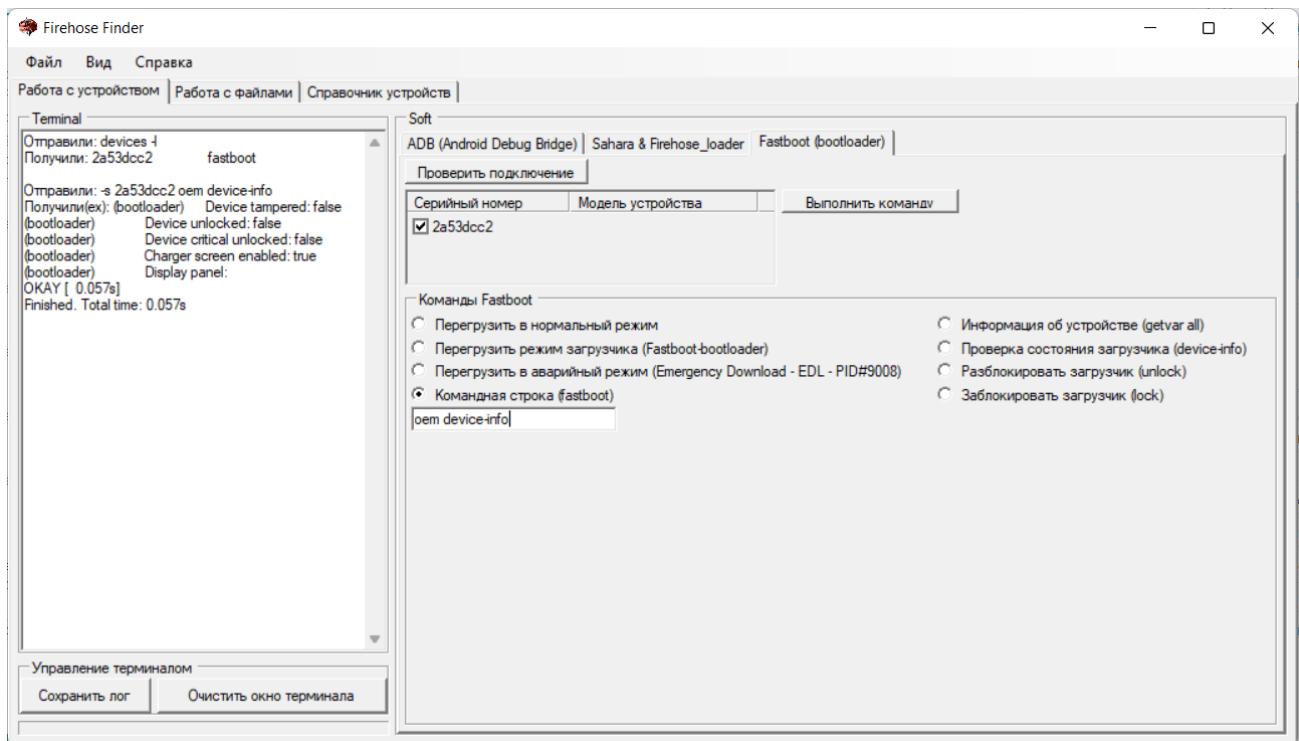
- Перегрузить устройство в аварийный режим. Устройство будет перезагружено в 9008 средствами ADB. Это аналог команды `$ adb reboot edl` Не все устройства поддерживают эту команду.
- Командная строка (ADB Shell). При выборе данного пункта станет доступно окно ввода команд. Отправлять команду можно нажатием кнопки «Выполнить команду» или клавишей «Enter». Перед командой **adb shell вводить не нужно**, только саму команду. Например, для получения списка всех поддерживаемых устройством команд достаточно ввести `ls -1 /system/bin` или `ls -1 /system/xbin`. При необходимости ознакомится с документацией по командам ADB, пожалуйста, зайдите на: <https://developer.android.com/tools/adb>
- Перегрузить в режим загрузчика. Сеанс ADB завершается, открывается вкладка «Fastboot (bootloader)», устройство принимает только команды загрузчика.

## Раздел «Fastboot (bootloader)»

Для определения подключённого устройства необходимо нажать кнопку «Проверить подключение». Если до этого устройство было подключено по ADB, то вместе с серийным номером устройства подтянется и его модель. Допускается подключение нескольких устройств, выбор для команды осуществляется проставлением галки напротив необходимого устройства.



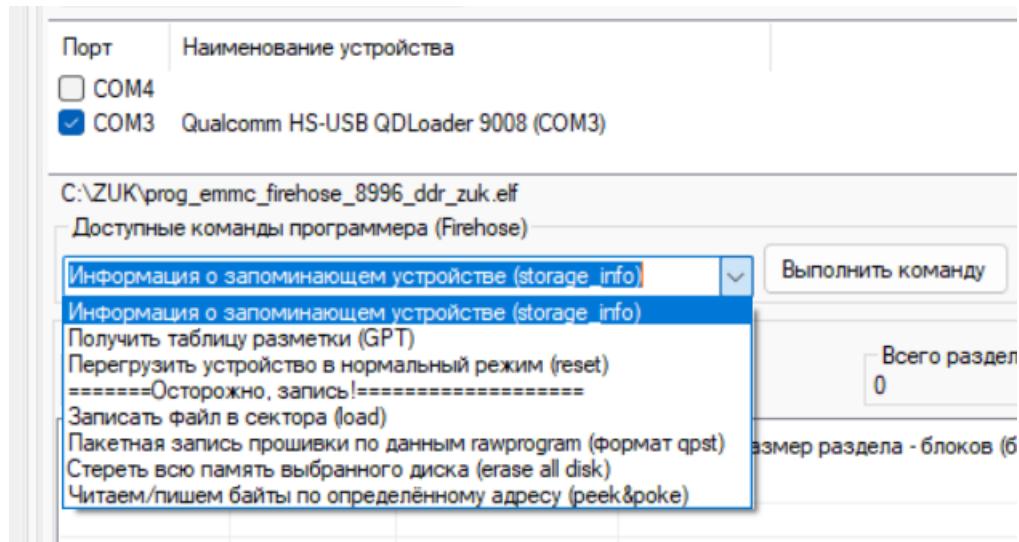
На текущий момент доступно восемь команд загрузчика. Некоторые из них могут не поддерживаться загрузчиком устройства, в этом случае предлагается использовать командную строку. При выборе командной строки (fastboot) станет доступно окно ввода команд. Отправлять команду можно нажатием кнопки «Выполнить команду» или клавишей «Enter». Перед командой **fastboot вводить не нужно**, только саму команду. Например, для получения информации об устройстве необходимо ввести `get device-info`



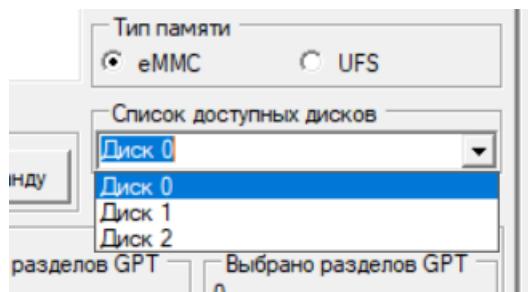
## Раздел «Sahara & Firehose loader»

Команды для Sahara становятся активными после перезагрузки устройства в аварийный режим (9008). Порт устройства определяется автоматически, но, при необходимости, также может быть выбран и вручную, из списка доступных сом-портов. На текущий момент доступны следующие команды:

- Получить идентификаторы устройства. Команда выведена на отдельную кнопку. Выполнением команды является заполнение идентификаторов на вкладке «[Работа с файлами](#)». Если необходимо выполнить несколько команд для Сахары, то устройство необходимо перезагрузить, т.к. программа ждёт по протоколу от устройства данные «приветствие», а оно отправляется при первичном подключении устройства в режиме 9008.
- Слева от кнопки «Выполнить команду» находится комбобокс с выбором команд. Первой командой для исполнения является «Информация о запоминающем устройстве (storage\_info)».

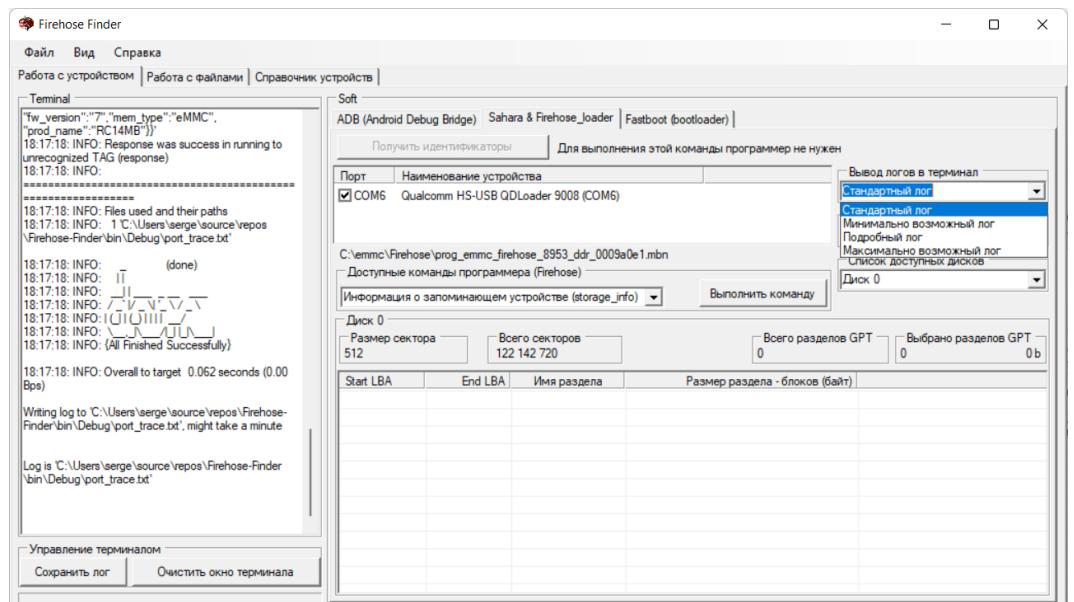


После её успешного выполнения становятся доступны и другие команды. Поле с выбором «Список доступных дисков» заполняется номерами физически доступных для работы частей флэш-памяти (в данном примере их три).

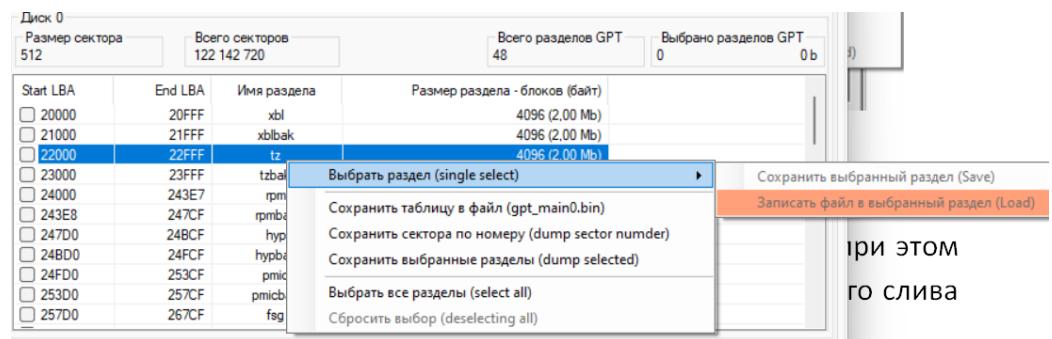


Автоматически выбирается тип памяти, но можно выбрать вручную, если память определилась некорректно.

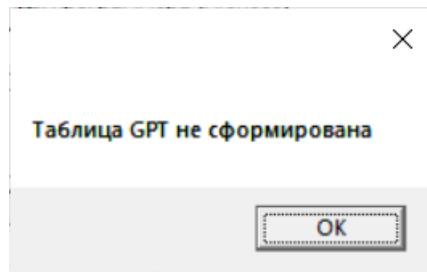
Можно выбрать четыре варианта отображения лога. По-умолчанию – «Стандартный лог»



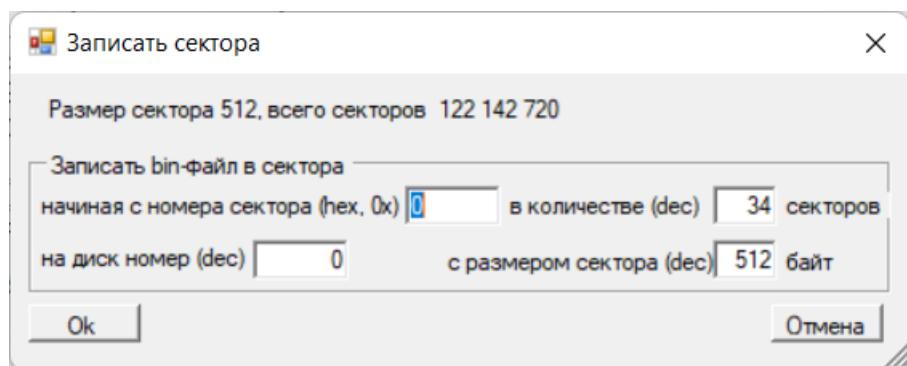
- «Получить таблицу разметки (GPT)». Успешное выполнение команды даст список разделов с адресами начального и последнего секторов и посчитанным количеством занятых разделами секторов с объёмом в байтах. При этом станут доступны [команды контекстного меню](#).



Если на диске таблица отсутствует, то будет выведено предупреждение, при этом возможность получить посекторную информацию остаётся, т.е. для полного слива информации с диска наличие таблицы разделов не обязательно.

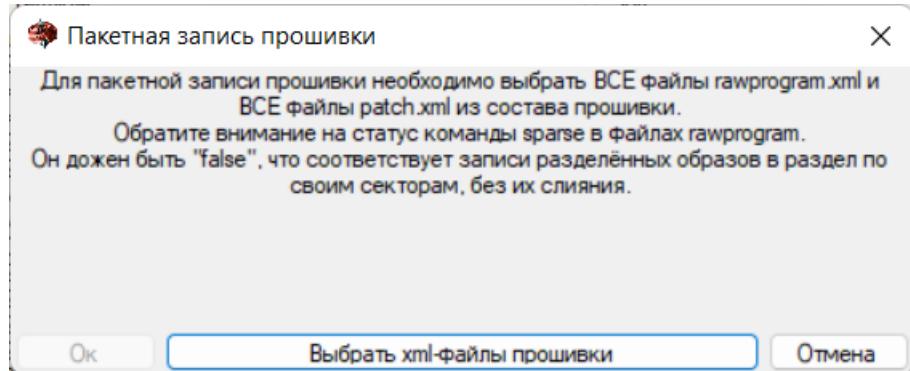


- «Перегрузить устройство в нормальный режим (reset)». Выбор данной команды позволяет перезагрузить устройство из аварийного в нормальный режим. Задержка выполнения команды перезагрузки устройства в нормальный режим – 10 секунд.
- «Записать файл в сектора (load)». Команда необходима для записи, например таблицы разметки. **Выполнять очень аккуратно!**



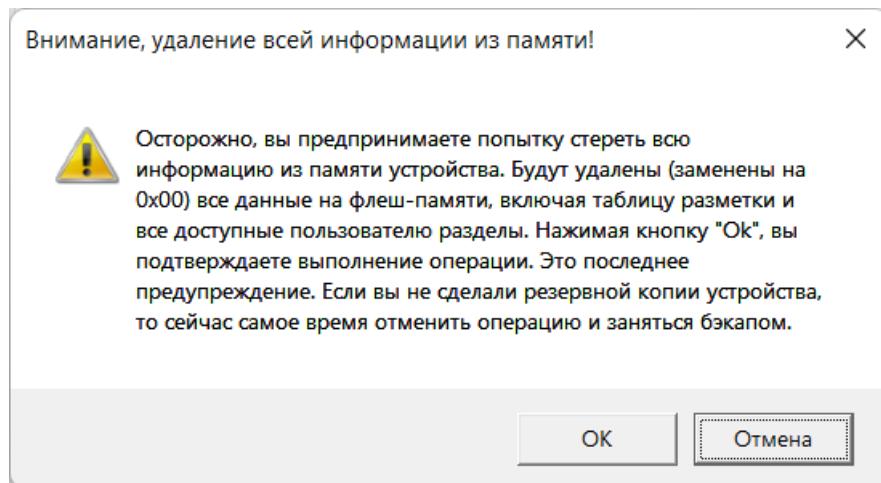
После подтверждения введённой информации будет предложено выбрать bin-файл для копирования его в память устройства по указанному адресу.

- «Пакетная запись прошивки по данным rawprogram (формат qpst)». Пакетная запись прошивки подразумевает отправку образов разделов для записи в память по данным файлов rawprogram.xml и patch.xml. В открывшемся окне необходимо нажать кнопку «Выбрать xml-файлы прошивки» и в папке с прошивкой выбрать все файлы rawprogram.xml и все файлы patch.xml используя клавиши ctrl или shift.

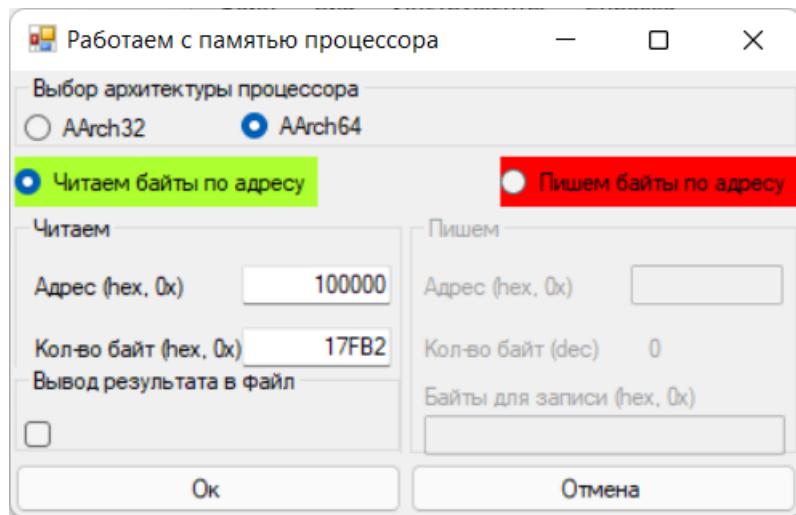


После их выбора в окно добавится список этих файлов и путь к прошивке, где они лежат. Также станет активна кнопка «Ок». После её нажатия начнётся прошивка устройства. При скорости записи 14-30 мбс время прошивки объёмом в 3-5 гб займёт от 3-4 до 7-10 минут.

- «Стереть всю память». **Выполнять очень осторожно и с полной уверенностью понимания происходящего.** Удалена будет вся информация с флеш-памяти.

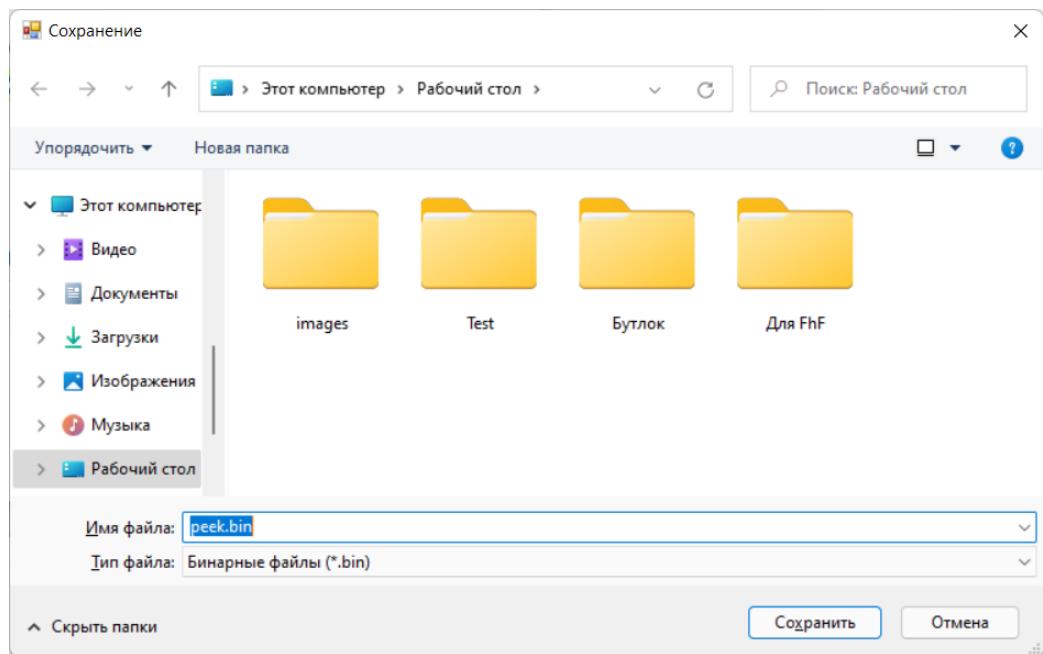


- «Читаем/пишем байты по определённому адресу (peek/poke)». Операция позволяет считать внутреннюю память (Internal memory - IMEM) процессора. Перед чтением или записью необходимо сначала уточнить адрес и количество байт для чтения/записи для вашего процессора. Адреса для архитектуры 32 и 64 байта могут различаться. **Обращение к некоторым адресам памяти может привести к перезагрузке или сбою в работе процессора.**



Выбор архитектуры процессора происходит автоматически, в зависимости от используемого программера. При этом, если есть необходимость, то этот параметр можно изменить (например, при ошибке [«HANDLE\\_PEEK\\_FAILURE»](#)).

Результат выводится в лог по-умолчанию. Если есть необходимость сохранить результат в файл, то необходимо отметить соответствующий бокс. При этом будет открыто окно с выбором пути сохранения файла.



## Команды контекстного меню

Становятся доступны по клику правой кнопкой мыши.

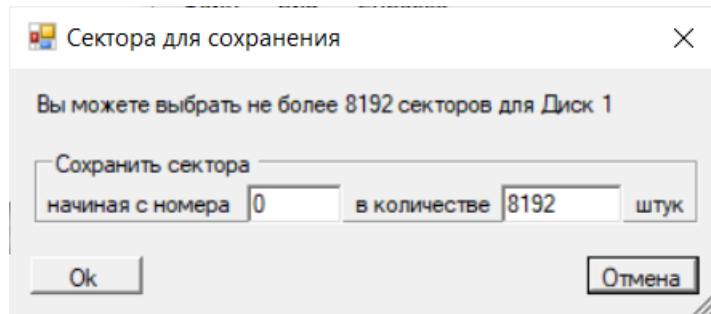
Диск 0				Выбрано разделов GPT
Размер сектора	Всего секторов	Всего разделов GPT	Выбрано разделов GPT	
512	122 142 720	48	0	0 b
Start LBA	End LBA	Имя раздела	Размер раздела - блоков (байт)	
<input type="checkbox"/> 20000	20FFF	xbl	4096 (2,00 Mb)	
<input checked="" type="checkbox"/> 21000	21FFF	xblbak	4096 (2,00 Mb)	
<input type="checkbox"/> 22000	22FFF	tz		
<input type="checkbox"/> 23000	23FFF	tzbak		
<input type="checkbox"/> 24000	243E7	rpm		
<input type="checkbox"/> 243E8	247CF	rpmbak		
<input type="checkbox"/> 247D0	24BCF	hyp		
<input type="checkbox"/> 24BD0	24FCF	hypbak		
<input type="checkbox"/> 24FD0	253CF	pmic		
<input type="checkbox"/> 253D0	257CF	pmicbak		
<input type="checkbox"/> 257D0	267CF	fsg		

- Выбрать раздел (single select) ▾
- Сохранить таблицу в файл (gpt\_main.bin)
- Сохранить таблицу в формате xml
- Сохранить сектора по номеру (dump sector number)
- Сохранить выбранные разделы (dump selected)
- Выбрать все разделы (select all)
- Сбросить выбор (deselecting all)

- «Выбрать раздел». При выборе сбрасываются все флагки на разделах, и остаётся только на одном – текущем. При этом становятся активны пункты меню для одиночной работы с разделом. Множественный выбор разделов не допускается.

Одиночный раздел можно сохранить или на его место записать bin-файл. **Запись необходимо осуществлять с особой внимательностью.** При необходимости просто стереть определённый раздел допускается сформировать bin-файл одинаковым размером со стираемым разделом и с последовательностью байт 00 (или FF – зависит от специфики памяти). Потом записать этот «нулевой» файл на место раздела, предназначенного для удаления. При этом ни из таблицы разделов, ни из места на флешке раздел не удаляется, просто информация в таком разделе перезаписывается нулями.

- «Сохранить таблицу в файл (gpt\_main0.bin)». Эта команда позволяет сохранить в указанную папку копию таблицы разметки.
- «Сохранить таблицу в формате xml». Позволяет сохранить таблицу в универсальном формате для дальнейшей обработки, например, в excel.
- «Сохранить сектора по номеру (dump sector number)». Данная команда позволяет сохранить побайтно считанную резервную копию указанных секторов в указанную папку. Необходимо указать первый для сохранения сектор и их количество. По умолчанию подставляются: первый сектор – 0, количество – все сектора выбранного выше диска.



- «Сохранить выбранные разделы (dump)». Мультисекторный дамп разделов. Можно выбрать один, несколько или все разделы для сохранения. Стоит обратить

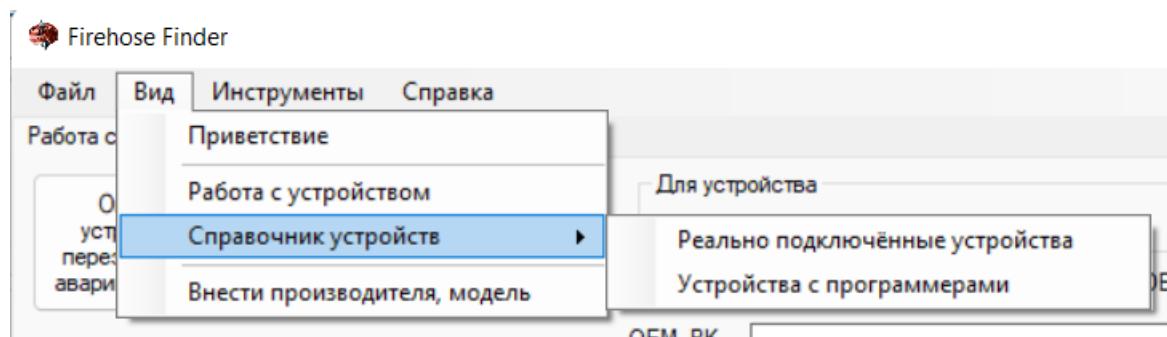
внимание на достаточность места на локальном диске для дампа выбранных разделов. Обычно, раздел «**userdata**» несёт в себе большинство пользовательских данных, **является самым большим** и, при сохранении резервной копии, **не копируется из-за размера.**

	FCF000	7403FD4	userdata
	7403FD5	747BFDE	grow

- Можно выбрать все разделы одной командой и одной командой отменить весь выбор.

## Вкладка «Справочник устройств» (скрытая)

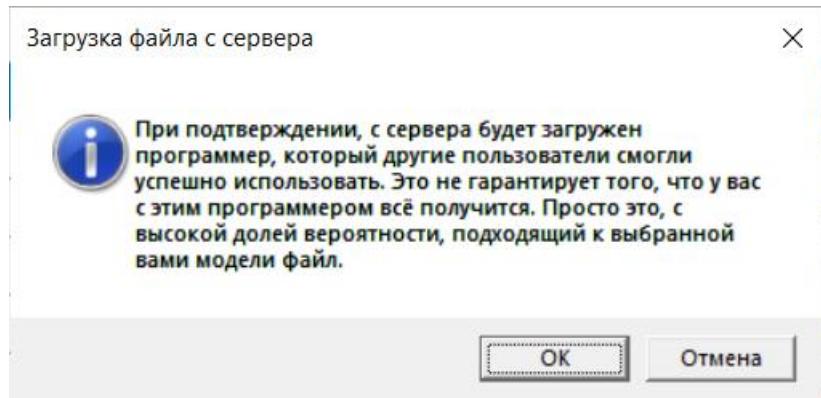
Активизировать вкладку можно из меню «Вид». «Справочник устройств» содержит фильтр «помощью подтверждённые устройства» - это список устройств, с которых все идентификаторы были получены в автоматическом режиме (без ручного ввода).



Сбросить фильтр и отобразить все «Реально подключённые устройства» можно выбрав соответствующий пункт меню. Будут выведены все устройства, которые при подключении отдавали идентификаторы в автоматическом режиме и те, для которых марку/модель приходилось заполнять вручную.

«Устройства с программерами» позволит сократить этот список, применив фильтр для отображения устройств для которых были найдены и сохранены на сервере программеры. Данные были получены из открытых источников от пользователей, которые смогли успешно подключить определённый программер к своему определённому устройству. Устройство и программер стали взаимосвязаны, данные об устройстве попали в Справочник, а программер сохранён на сервере.

При двойном клике на строке с выбранным устройством произойдёт автозаполнение данных на вкладке «[Работа с файлами](#)» и будет предложено загрузить программер с сервера.



В полном списке соответствие программера устройству может оказаться далеко не у всех. Некорректные или отсутствующие данные в «Справочнике устройств», с согласия пользователя (галка на вкладке [«Работа с файлами»](#)), отправляются в публичный телеграмм-канал [«Firehose-Finder issues»](#) для проверки и внесения корректировок. Добавление/изменение данных в «Справочник устройств» происходит обычно с автоматическим обновлением версии релиза (для версий старше 3.1.0.4).

Внизу формы Справочника присутствует поле поиска. Поиск работает по всем ячейкам Справочника, и в процессе набора применяет фильтр. При этом поиск идёт не только по «Реально подключённым устройствам», а вообще по всей базе устройств, которые когда-либо присутствовали в Справочнике.

Firehose Finder					
Файл		Вид		Инструменты	
Работа с файлами		Справочник устройств			
HWID	FullName	OEM	Model	OEM Private Key Hash	SW Ver
0009A0E1	Snapdragon 450	0043	0000	7C6DCA9BF5674291AA39DD55760C0D4B65C7A4223097AAB1DB791E2192002DDF	00000000
0008B0E1	Snapdragon 845	0043	0000	C7182735ED6320B8E6AFC7A8CBDD936D83F90DF851F879D6D2FC1AD5FA04095	00000000
0014D0E1	Snapdragon 662	0001	0000	A8BC086FE393B13D59E2A2EC944AF26DA3FA3D4B2A1CCD2FB883C73E0FFF30DC1736DCB2752E955A61421C349974F90	00000000
000910E1	Snapdragon 670	0042	0006	778B0AEF202BCB95109AE2D12B498D333413DC123CD723C02D8D31E795DA0D81	00000000
000560E1	Snapdragon 425	0015	003A	6BC369511DA9CABD9A7AF61574F89DB385003D6241BDD1FF573DBA61BF6AE119	00000000
000BA0E1	Snapdragon 632	0015	0067	6BC369511DA9CABD9A7AF61574F89DB385003D6241BDD1FF573DBA61BF6AE119	00000000
000CC0E1	Snapdragon 630//636	0015	0066	A1A5C29846C9881B7A6081EC218212B9B7EB1765EE884379F16619D6FCD3FE0	00000000
000CC0E1	Snapdragon 630//636	0000	0000	0374637D23C4E2EEDE23DA5D60C1E7ABC81CCC4CD641045F859B317650F47DF	00000000
000940E1	Snapdragon 205	0042	0050	1367FDAAEBB7BECBE49096F000D9D3DADF198885106D98598CAC6D1B9B2EDB3A	00000000
000A50E1	Snapdragon 855	0051	4985	2ACF3A85FDE6334E2E28D64CBC416B2474E0E95CAD4698F143E27479D67E92D995A20DA04E40395B61A140F3DB7C32720	00000000
000C30E1	Snapdragon 865	0051	4D6D	7C15A98DB4E70963715F51C8DA39C1E66FC1C3334E95F4C6A5627DA6A49C042F06B43E8DE1F689FC36CE1135C7FA5AA2	00000000
0014D0E1	Snapdragon 662	0051	0000	49446E14621312DFECCD4389F267E6B71674DDD36B1BC41D1F605AA991D14AD687834378CF2129259DFAF107D75EE329	00000000
000A50E1	Snapdragon 855	0051	0000	D09BA40B51377E09D854D6E695B9228038F34EBDB779143D1540F60E6C3C59EFB26239F8AET74B2A5AC7C474BEC92F030C	00000000
0009C0E1	Snapdragon 660	0060	0000	81BA684F99EE4AE0D12943FBA51251B7E8F3A25DA21FA16943930330D456E42B	00000000
001360E1	Snapdragon 460	0073	0003	A7DF36FFD7AB557C67A6C26675E2795C922CF671308CFD7169BEDB94424C862BC7B646907DD79989578590F86370A940	00000000
0014D0E1	Snapdragon 662	0072	0000	1BEBE3863A6781DB4B0108603007334DE9E5CA14971C7C4F4358EC9D79CDA4692CE5E948C6FD409408F4C919FCADFE3	00000000
009470E1	Snapdragon 820	0000	0000	355D47F912FEAOAFLF46C007C6DC22C43544FB9359E30AA7DB5F4734D18FBD74	00000000
0005F0E1	Snapdragon 821	0000	0000	355D47F912FEAOAFLF46C007C6DC22C43544FB9359E30AA7DB5F4734D18FBD74	00000000

В результате поиска будут отображены все модели устройств, которые содержат введённые символы в любом поле (наименование, хеш, процессор и т.п.). При этом список будет содержать реально подключённые устройства без окраски, а неподтверждённые данные будут окрашены в оттенки **красного**.

За полем поиска есть две кнопки – уменьшение и увеличение размера шрифта Справочника. Изменение размера шрифта действует только на внутреннюю структуру таблицы.

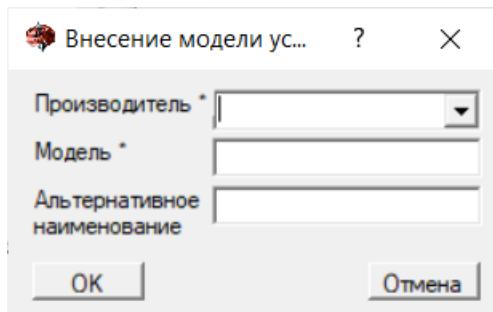
Firehose Finder						
Файл		Вид		Инструменты		Справка
Работа с файлами			Справочник устройств			
HWID	FullName	OEM	Model	OEM Private Key Hash		
000560E1	Snapdragon 425	0020	0000	5C08AA84F75507D14F7E6C18D45106E8A0DAA2B580FE0EEA64D249DAD681D004		
000950E1	Snapdragon 675	0072	0000	1BEBE3863A6781DB4B0100E063007334DE9E5CA14971C7C4F4358EC9D79CDA4692CE5E948C6FD409408F4C919FCADFE3		
001630E1	Snapdragon 750G	0072	0000	1BEBE3863A6781DB4B0100E063007334DE9E5CA14971C7C4F4358EC9D79CDA4692CE5E948C6FD409408F4C919FCADFE3		
007050E1	Snapdragon 400/410	0000	0000	CC3153A80293939B90D02D3BF8B23E0292E452FEF662C74998421ADAD42A380F		
000BA0E1	Snapdragon 632	0072	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A		
007BC0E1	Snapdragon 801	0000	0000	CC3153A80293939B90D02D3BF8B23E0292E452FEF662C74998421ADAD42A380F		
0090B0E1	Snapdragon 615	0000	0000	CC3153A80293939B90D02D3BF8B23E0292E452FEF662C74998421ADAD42A380F		
009720E1	Snapdragon 210	0004	0000	4673478F4DD4D43C68D4091D6B5EE1AB170D045FA285E515A15F3B987D9DE4AB		
009720E1	Snapdragon 210	0004	0000	4232191DA8A45966EB089F421BF2FB8EF4E3F39866195BE23077C39FEEABF250		
000460E1	Snapdragon 625/636	0004	0000	404D181E75AF65A806B01DCF394B82B8A645FB0DE76E3C386FE42092D33500D6		
000990E1	Snapdragon 653	0004	0000	FDFC20DB73081EA0B42EBA895F44B4284B0E4C657503B1BCDE6C7832B4DB504		
0014D0E1	Snapdragon 662	0072	0000	1BEBE3863A6781DB4B0100E063007334DE9E5CA14971C7C4F4358EC9D79CDA4692CE5E948C6FD409408F4C919FCADFE3	0000000	
009470E1	Snapdragon 820	0000	0000	355D47F912FEA0AF1F46C007C6DC22C43544FB9359E30AA7DB5F4734D18FBD74	0000000	
0005F0E1	Snapdragon 821	0000	0000	355D47F912FEA0AF1F46C007C6DC22C43544FB9359E30AA7DB5F4734D18FBD74	0000000	
0005E0E1	Snapdragon 835	0000	0000	A7B0B02545A98ECA23D6E9105FB464568D1B5828264903441BDEF0CD57E3C370	0000000	
0008B0E1	Snapdragon 845	0072	0000	C924A35F39CE1CDD1B0D5A9F3B0E3C51317930431D7A9DD5A55028CF6965FE65	0000000	
0004F0E1	Snapdragon 430	0000	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A	0000000	
0006B0E1	Snapdragon 435	0000	0000	57158EAF1814D78FD2B3105ECE4DB18A817A08AC664A5782A925F3FF8403D39A	0000000	

При стирании символов в окне поиска результаты будут сброшены и вывод отобразит данные в соответствии с выбором в меню.

## Окно «Внести производителя, модель»

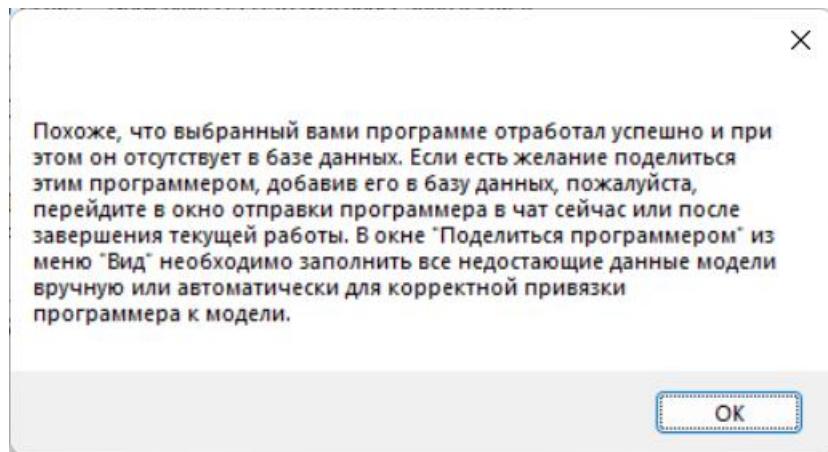
Данное окно предназначено для ручного ввода информации о производителе устройства, его модели и альтернативного наименования. По этим данным будет формироваться [«Справочник устройств»](#). Так как не всегда есть возможность получить эти данные в автоматическом режиме, приходится использовать ручной ввод.

Поле «Производитель» - обязательно к заполнению, «Модель» и «Альтернативное наименование» заполнять не обязательно. Производителя устройства можно выбрать из выпадающего списка или ввести своё, если такой производитель в списке отсутствует.



## Окно «Поделиться программером» (неактивное)

Данное окно предназначено для отправки программера в общий чат. В последствии, при очередном обновлении программы, программер будет добавлен в базу данных программы FhF. Отправить можно только успешно отработавший программер с реально подключённым устройством.

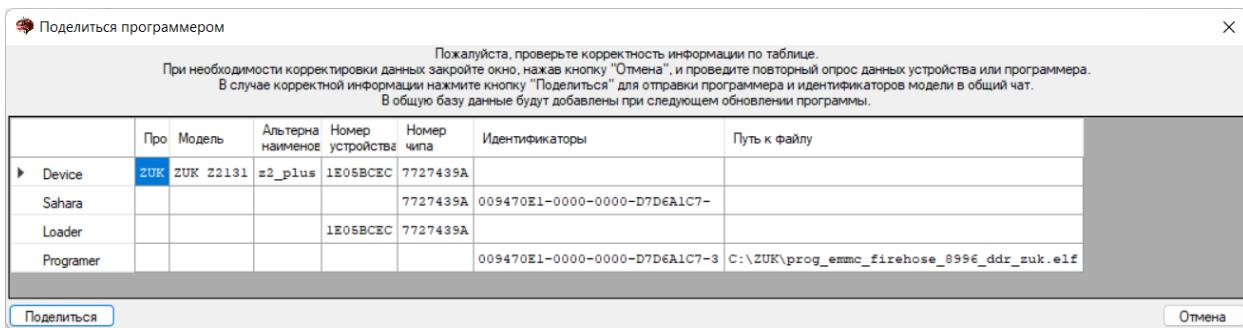


Для корректного заполнения данных для отправки программера необходимо получить:

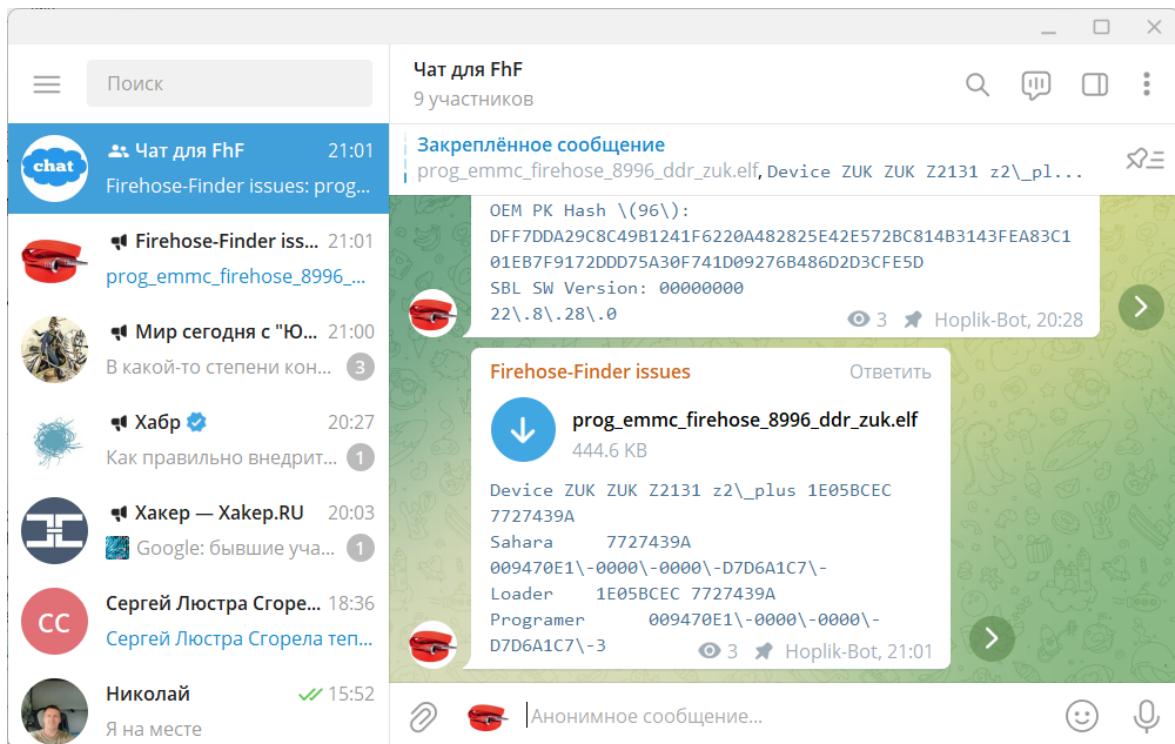
1. Данные устройства (производитель, модель, имя, серийный номер устройства и чипа);
2. Идентификаторы устройства и программера (подтягиваются автоматически, при проверке программера).

Данные устройства можно получить как в автоматическом, так и в ручном режиме, открыв окно «Внести производителя, модель». Для автоматического получения данных устройства необходимо подключить его в нормальном режиме, на устройстве разрешить отладку по USB, и нажать кнопку «Опросить устройство». Второй вариант: открыть вкладку «Вид» - «Работа с устройством». На вкладке «ADB» нажать кнопку «Подключить ADB» и выбрать команду «Получить марку/модель устройства», потом «Перегрузить в аварийный режим (9008)».

После получения данных устройства можно проверять программер. При его успешном подключении и заполнении таблицы данных станет доступна кнопка «Поделиться». Если данные устройства будут заполнены не полностью (отсутствует Производитель), то окно необходимо закрыть кнопкой «Отмена» и провести процедуру получения данных устройства, описанную выше.



Информация об устройстве и проверенный программер отправляются в общий чат.



При очередном обновлении программы FhF данный программер будет добавлен в общую базу данных вкладки «[Справочник устройств](#)».

## **Пункт меню «Инструменты»**

В этом меню собраны инструменты, которые могут помочь при распаковке прошивки и при поиске информации в сохранённых с устройства файлах.

## Раздел «Бинарный поиск»

В разделе «Бинарный поиск» используются четыре вкладки с разным функционалом.

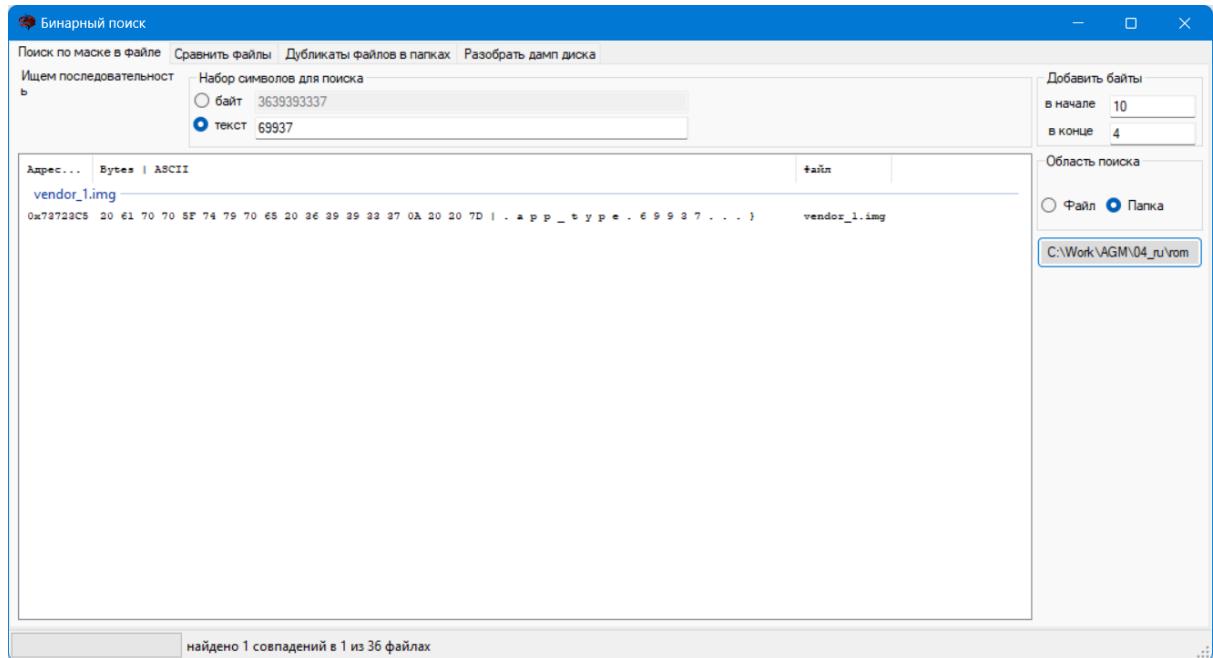
## Вкладка «Поиск по маске в файле»

Инструмент «Поиск по маске в файле» может пригодиться для поиска определённой последовательности байт в выгруженных из устройства файлах. Например, для редактирования параметров звука необходимо найти последовательность текстовых символов «69937». При наборе в поле «текст» символы будут автоматически преобразованы в последовательность байт для поиска. Поиск может осуществляться как в отдельном файле, так и сразу в нескольких, расположенных в одной папке. При размере файла более 1 Гб процедура поиска может занять значительное время (зависит от мощности компьютера, на котором запущена программа).

Для удобства оценки полезности результатов поиска есть возможность добавить несколько символов (по-умолчанию 10 байт - 5 текстовых знаков в начале и 4 байта – 2 текстовых знака в конце) для результатов строки поиска. Результат поиска представлен в виде последовательности байт и перекодировке их в текстовые символы (нечитабельные символы заменяются точкой).

Двойной клик на строке с результатами поиска позволяет сохранить в буфер обмена адрес начала последовательности байт для поиска. Это можно использовать при открытии файла в хекс-редакторе и переходе по адресу, вставленному из буфера обмена, для редактирования этого

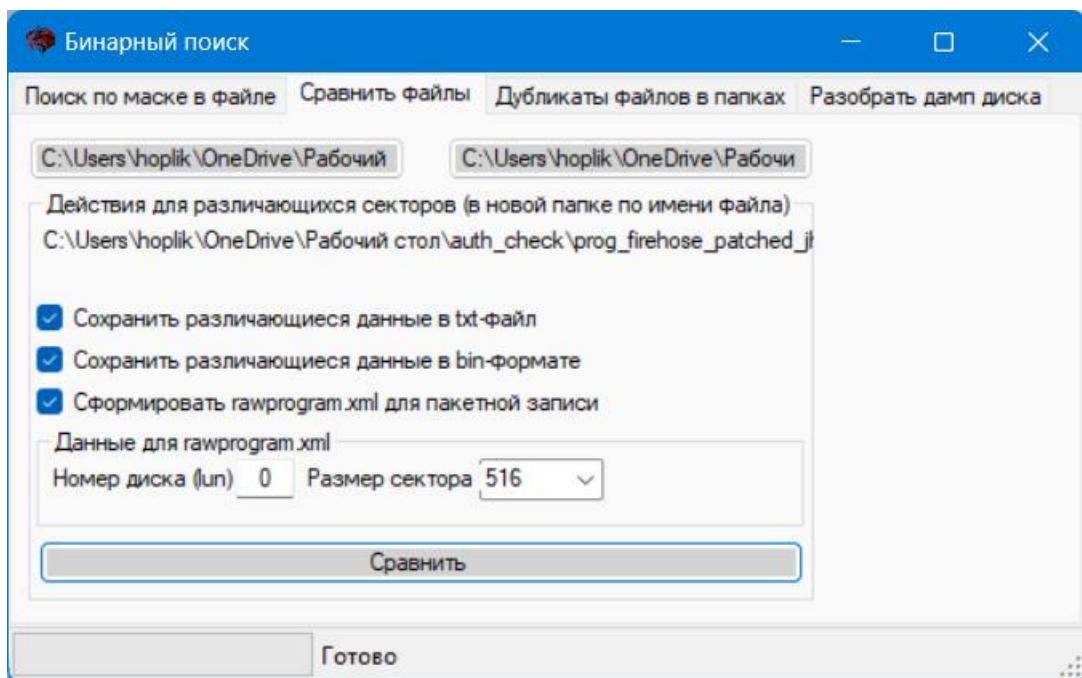
файла. Имя файла, в котором найдена требуемая последовательность, указано в конце строки результатов поиска. Если результатов несколько, то они группируются по имени файла и отсортированы по адресу по возрастанию.



### **Вкладка «Сравнить файлы» - разработка остановлена в связи с отсутствием необходимости.**

Левая кнопка позволяет выбрать путь к оригинальному файлу для сравнения. Правая кнопка указывает путь к файлу для сравнения. В области информации указывается путь к новой папке, которая создаётся по имени файла для сравнения. В ней сохраняется информация о различиях между оригинальным файлом и файлом для сравнения.

На текущий момент при сравнении файлов формируется массив бинарных файлов с различиями в определённых областях файлов. В наименовании файла указывается номер логического диска, стартовый адрес и количество секторов, которые займёт этот файл при записи в память. Исходя из размера файла можно вычислить размер сектора. Этой информации достаточно, чтобы сформировать файл пакетной записи rawprogram.xml для перезаписи не всего файла дуликата на место оригинального файла, а только отличающихся частей. Это существенно ускоряет процесс внесения изменений.

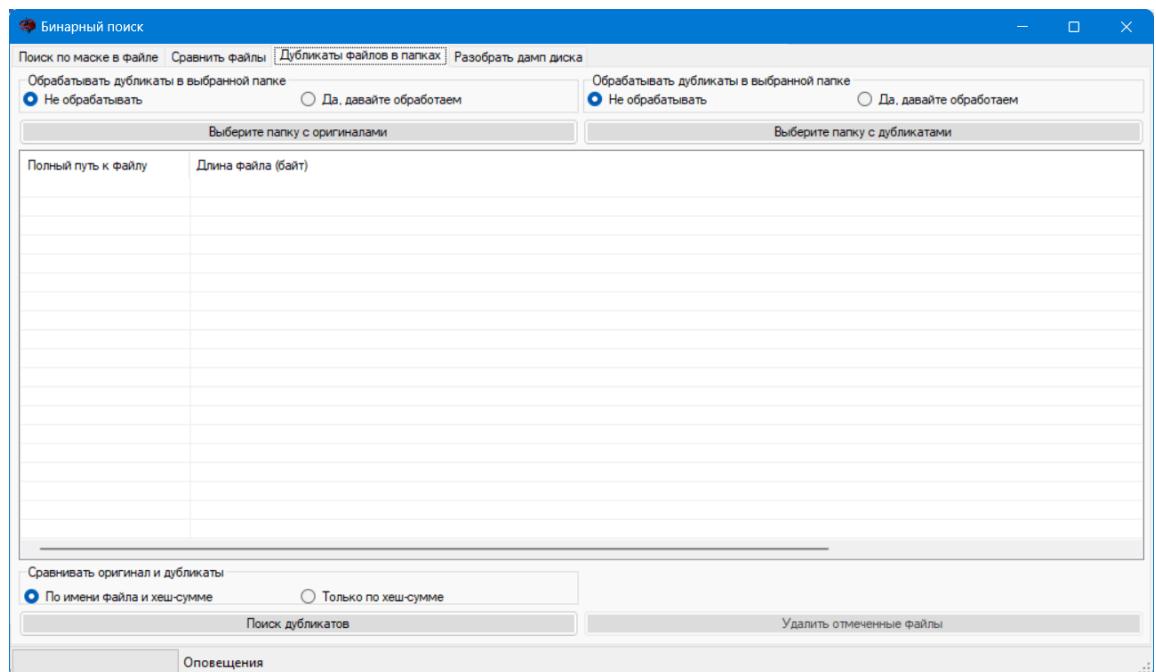


### Вкладка «Дубликаты файлов в папках»

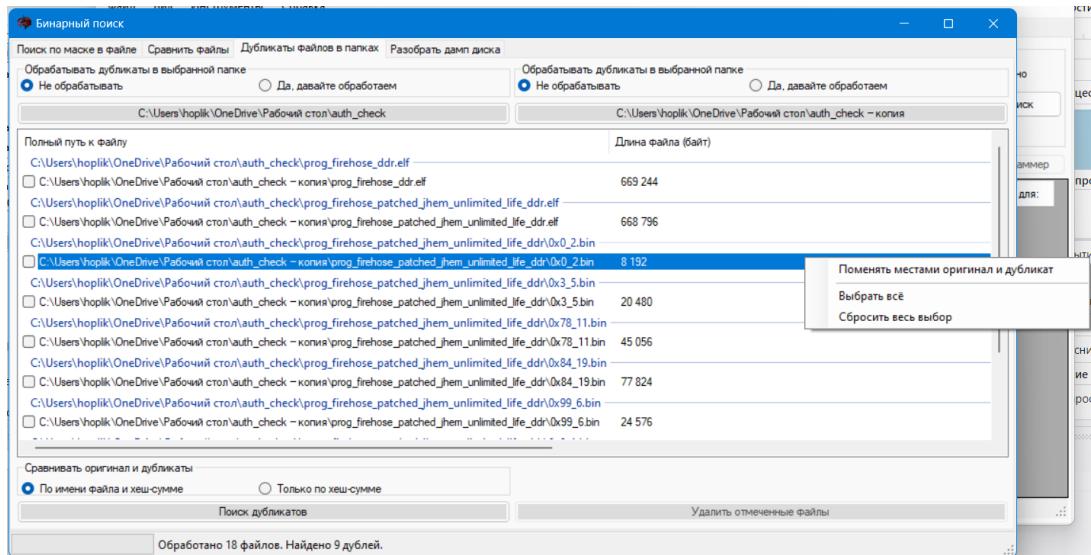
Если возникает необходимость массово проверить папку, включая вложенные папки, на наличие дубликатов, то достаточно использовать только левую часть окна. Сравнение идёт по хеш-сумме (SHA256).

Если требуется проверить наличие дубликатов файлов в разных папках, то в левой можно указать оригинальные файлы, а в правой - файлы для сравнения. При этом есть возможность не обрабатывать дубликаты в самих этих папках.

Сравнивать файлы в разных папках можно как по наименованию и хеш-сумме (если в папке присутствуют файлы нулевого размера), так и только по хешу (для файлов размером 0 хеш будет одинаковым, даже если они имеют разное наименование).



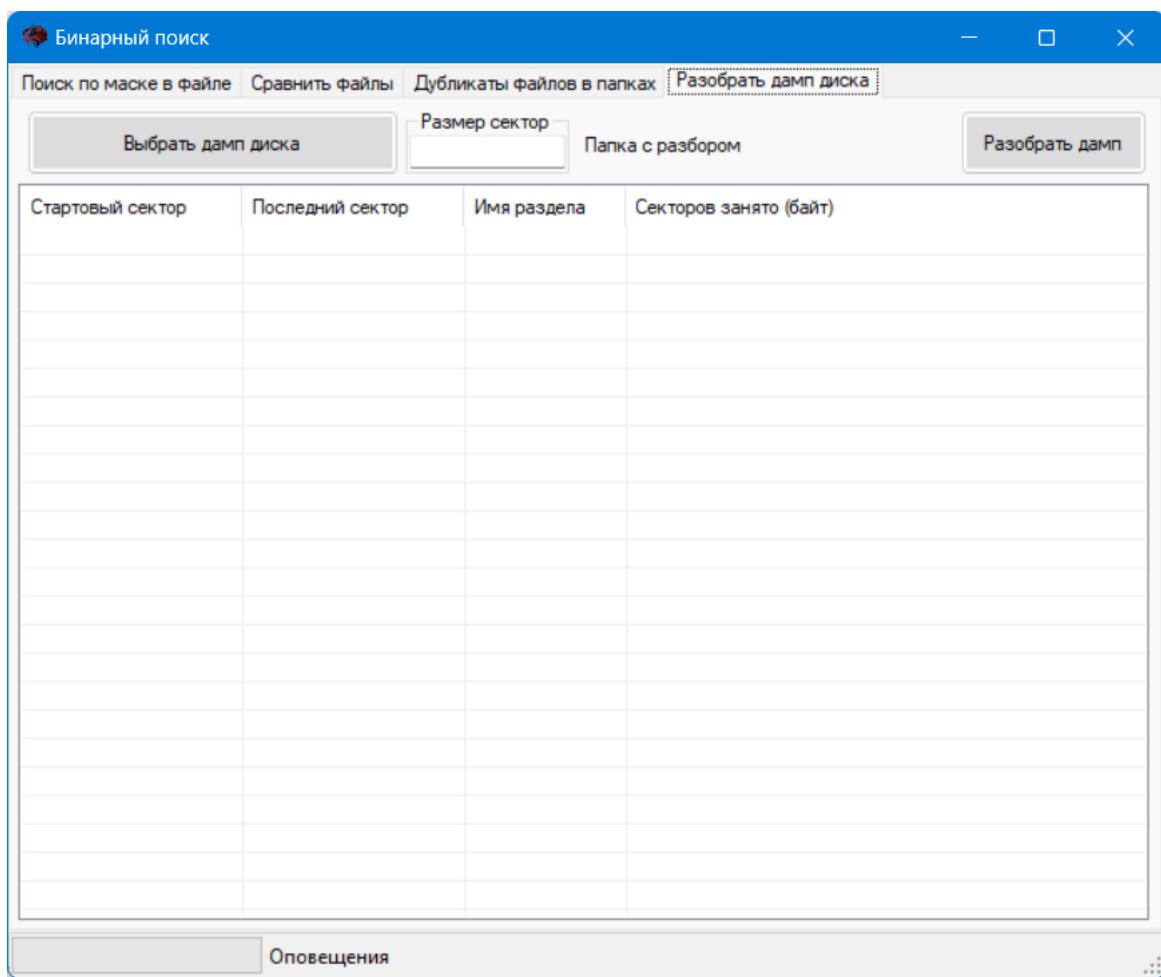
Выбрать дубликаты для удаления можно воспользовавшись контекстным меню, вызвав его правой кнопкой мыши. Также там можно поменять местами оригиналый файл и файл дубликата. После выбора файлов для удаления станет активна кнопка «Удалить отмеченные файлы».



## Вкладка «Разобрать дамп диска» - разработка остановлена в связи с отсутствием необходимости.

Работа на этой вкладке связана с необходимостью разобрать полный дамп логического диска на отдельные разделы для последующего их сравнения с оригинальными разделами, например, из прошивки или другого устройства.

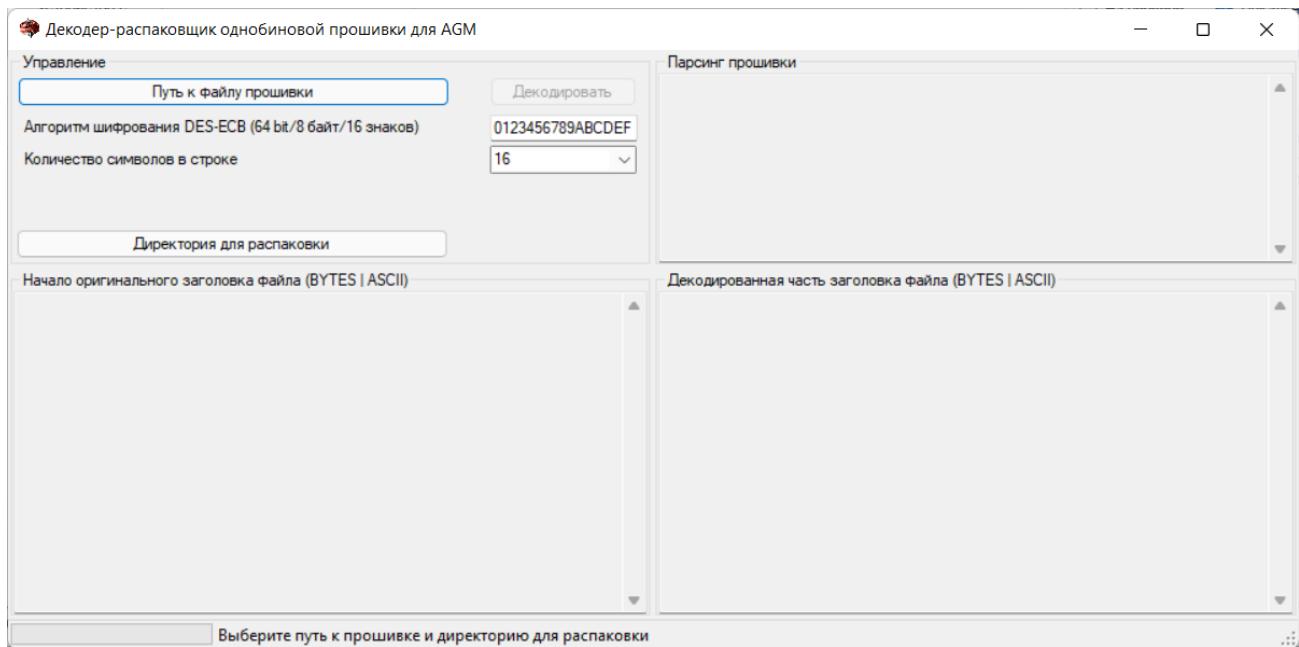
Для начала работы необходимо указать путь к файлу полного дампа и ввести размер сектора. При успешной обработке начала файла программа может подставить размер сектора автоматически. Для старта процедуры необходимо нажать кнопку «Разобрать дамп». В отдельном окне указывается путь к папке с файлами соответствующих разделов, на которые будет разделён полный дамп.



## Раздел «Распаковка однобиновой прошивки (AGM)»

Инструмент «Декодер-распаковщик однобиновой прошивки для AGM» предназначен для декодирования и распаковки из однофайловой bin-прошивки файлов для телефонов компании AGM (подписант прошивки – компания Hisense, версия упаковщика 2). Необходимость разбора прошивки была вызвана поиском программера, который, в итоге, и оказался в составе распакованной прошивки.

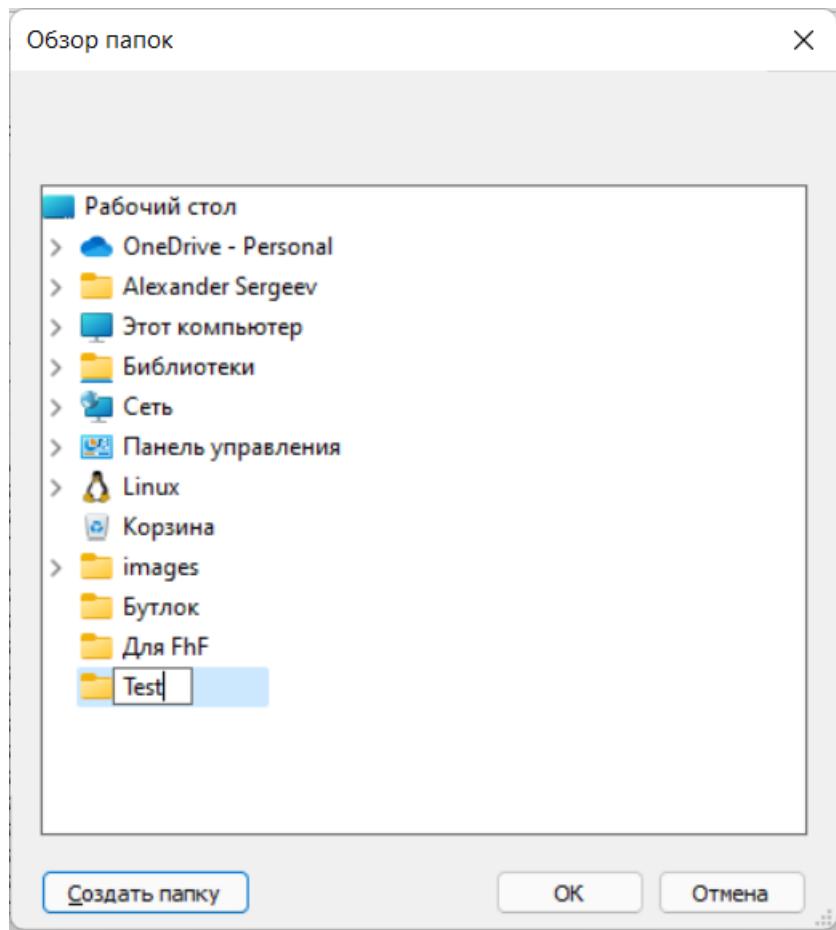
Изначальный проект был реализован [Vladimir Sitnov \(proger10\)](#) и опубликован на Гитхаб (<https://github.com/proger10/agmx3-firmware-tools>). На основе информации из данного проекта был написан этот «Декодер-распаковщик...» и включён в состав программного комплекса «Firehose Finder».



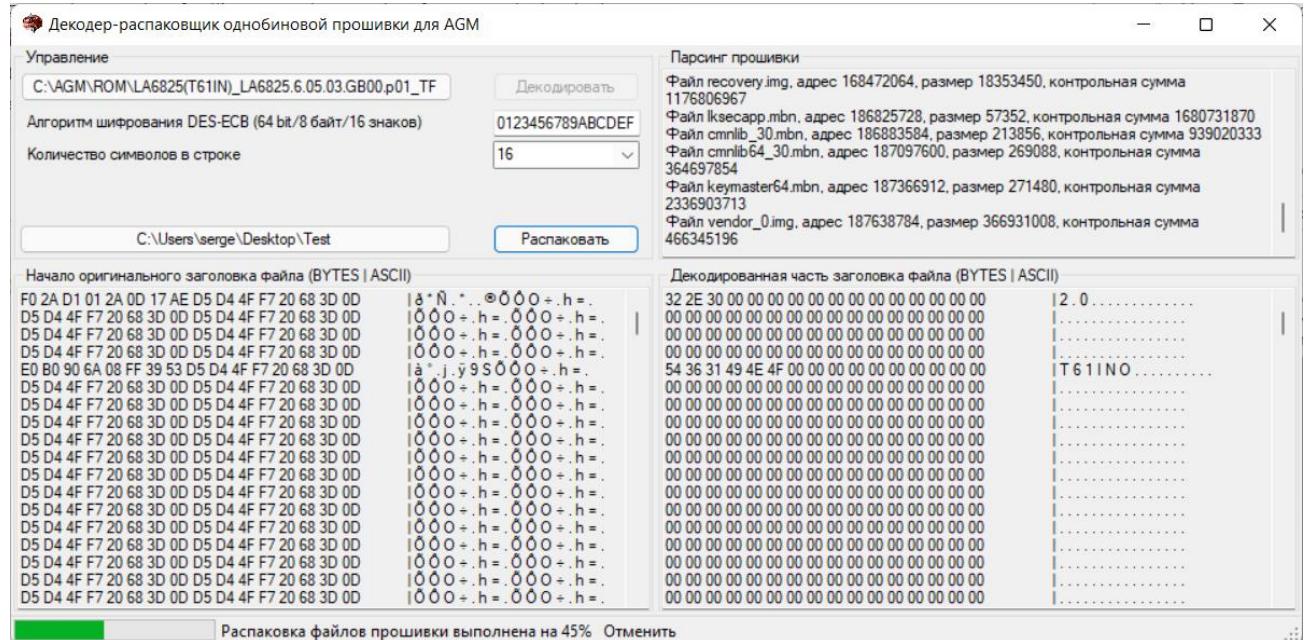
Для декодирования прошивки необходимо указать путь к однобиновому файлу, нажав соответствующую кнопку. После указания файла сразу же начнётся его считывание. На форму выводится не весь блок информации шапки прошивки, а только часть, для оптимизации скорости работы программы. Информация выводится в оригинальном (зашифрованном) виде.

После считывания шапки прошивки становится активна кнопка «Декодировать». Для декодирования необходимо указать код кодировки. По-умолчанию выставлен «0123456789ABCDEF». Также можно выбрать, сколько символов отображать в строке для удобства оценки корректности декодирования. Справа внизу на форме будет выведен такой же сегмент информации, как и слева, но уже с учётом декодирования указанным кодом. При этом сразу же будет произведён разбор шапки прошивки, что отразится в соответствующем окне справа вверху на форме. Для ответа на вопросы: «Почему был выбран именно такой код?» и «Как его найти в составе закодированной прошивки?» можно прочитать статью в вики на Гитхабе ([https://github.com/hoplik/AGM\\_Repacker\\_ROM/wiki/Finding-the-key](https://github.com/hoplik/AGM_Repacker_ROM/wiki/Finding-the-key)).

После указания директории для распаковки и удачной декодировке шапки станет активна кнопка «Распаковать». При выборе директории распаковки можно создать новую папку.



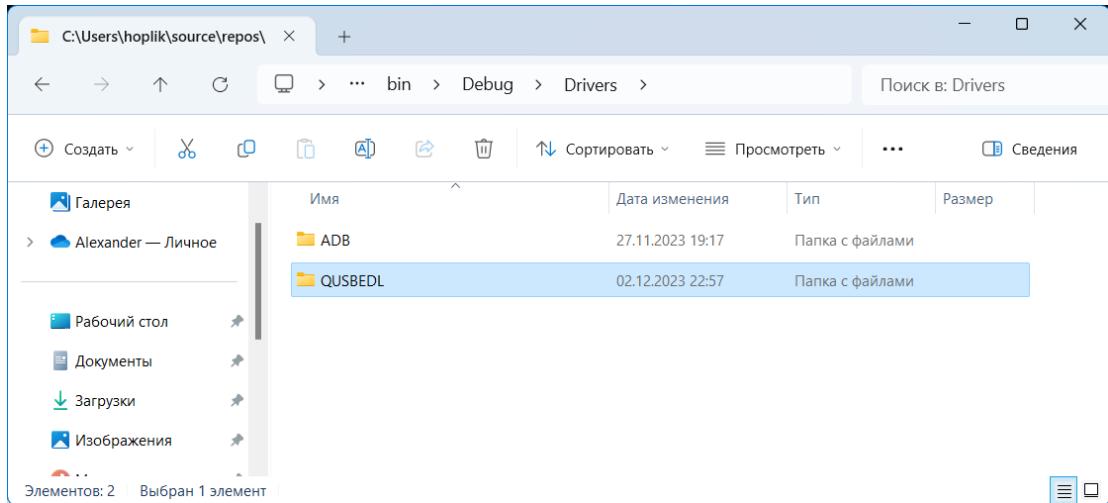
После нажатия кнопки «Распаковать» начинается процесс распаковки прошивки. Это может занять продолжительное время, в зависимости от мощности компьютера. Для принудительного прекращения процесса распаковки можно нажать кнопку «Отменить», которая появляется внизу формы после выполнения хотя бы 5% запущенного задания. В процессе распаковки в правом верхнем окне пишется лог процесса.



После удачного завершения процесса распаковки кнопка «Отменить» изменит название на «Открыть в Проводнике». При нажатии в Проводнике откроется папка с извлечённой прошивкой.

## Раздел «Драйвера EDL и ADB»

При выборе данного пункта меню только откроется папка, в которой размещены драйвера для работы с ADB и с параллельным портом от Qualcomm в аварийном режиме (VID\_05C6&PID\_9008). Из шапки папки можно скопировать адрес для установки из командной строки.



Установку можно провести либо из Диспетчера устройств, либо из командной строки от имени Администратора (команда `pnputil /add-driver <полный путь к *.inf файлу> /install`).

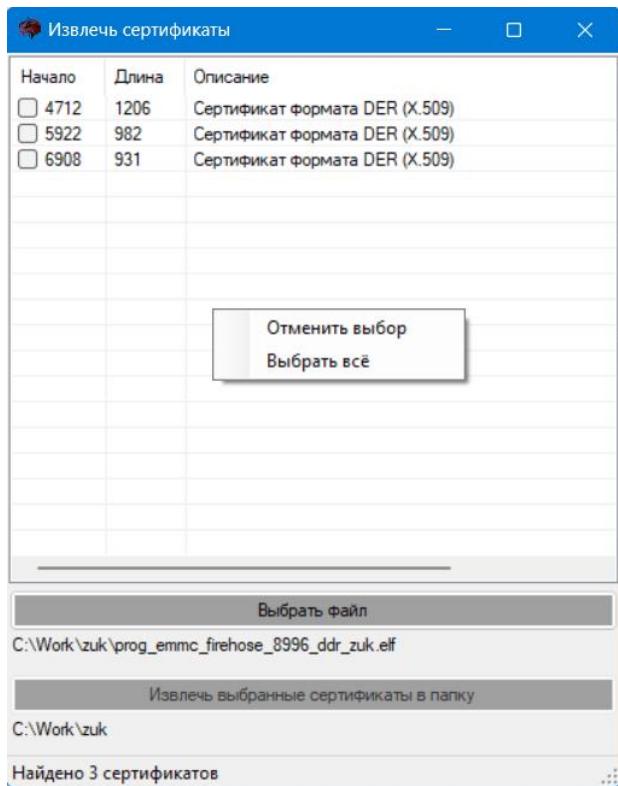
```
PS C:\Users\hoplik> pnputil /add-driver C:\Users\hoplik\source\repos\Firehose-Finder\bin\Debug\Drivers\QUSBEDL\qcser.inf
/install
Служебная программа PnP (Майкрософт)

Добавляется пакет драйвера: qcser.inf
Пакет драйвера успешно добавлен.
Опубликованное имя: oem15.inf
Пакет драйвера установлен на устройстве: USB\VID_05C6&PID_9008\6&2ca9a86&0&1
Пакет драйвера установлен на устройстве: USB\VID_05C6&PID_9008\6&179480a&0&2
Пакет драйвера установлен на устройстве: USB\VID_05C6&PID_901D&MI_00\7&2e61814b&1&00000

Общее число пакетов драйверов: 1
Добавленные пакеты драйверов: 1
PS C:\Users\hoplik> |
```

## Раздел «Извлечь сертификаты»

Работа с инструментом извлечения сертификатов заключается в выборе файла для анализа, проверки наличия в нём сертификатов и извлечением выбранных сертификатов в указанную папку.



Контекстное меню позволяет как выбрать все найденные сертификаты в файле, так и отменить выбор всех, отмеченных сертификатов одной командой. После нажатия кнопки «Извлечь выбранные сертификаты в папку» и подтверждения выбранной папки происходит копирование выбранных сертификатов в указанную папку с последующим её открытием в проводнике.

## Пункт меню «Справка»

### Раздел «Просмотр справки»

Открытие этого файла справки.

### Раздел «О программе»

Название программы, текущая версия, краткое описание программы, ссылка на базовую тему обсуждения общих принципов восстановления загрузчиков, ссылка на телеграмм-канал для отправки предложений/замечаний, кнопки для пожертвований.

При нажатии на логотип будет выведен адрес папки установки приложения.

## О программе Firehose Finder

X



Firehose Finder

Версия 24.12.1.0

Copyright © 2020 HOPLIK

Программа подбора программеров(firehose) для устройств на базе процессоров от Qualcomm.

Есть вопросы,  
предложения, замечания?  
Пишите в Телеграмм-канал  
["Firehose - Finder issues"](#)

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

Благодарности:

8Mi\_Yile - за перевод на китайский язык;

@SashaSeriy - за идеи, комментарии и базовую информацию;

@Always\_Alone\_R - за тестирование на устройстве UFS;

@krivedko - за подсказки для распаковщика прошивки.

ЮMoney - спасибо

PayPal - many thanks

Возникло желание поблагодарить автора за проделанную работу? Пожалуйста, используйте кнопки для пожертвования.

OK