Оглавление

Часто задаваемые Вопросы и Ответы (ЧаВО)

- q. Как формируется рейтинг файла в папке с программерами?

  a. 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)?

  a. 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: - emmcdl 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»?

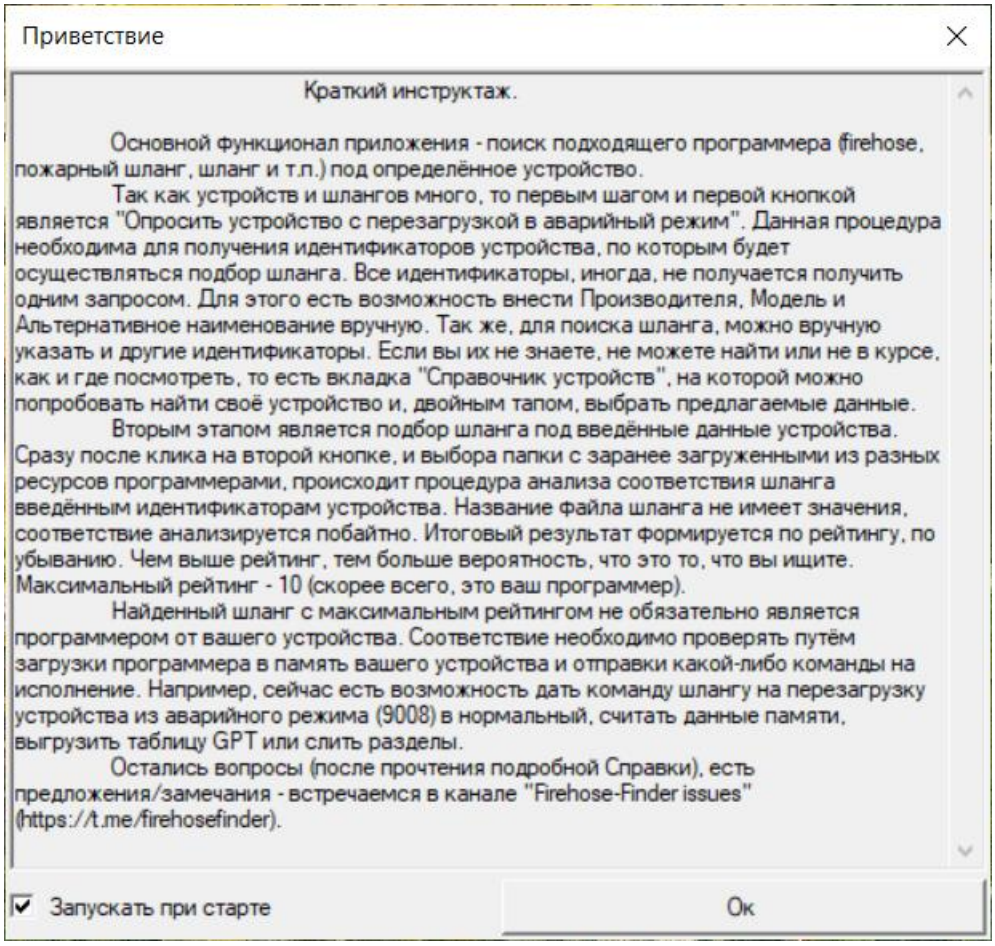
  a. Большинство программеров имеют в начале файла код, определяющий принадлежность файла (magic_number). При этом попадаются программеры, у которых, по разным причинам, в шапке применён другой набор байт (маска), и такие файлы системой не идентифицируются, как рабочий программер. Цветом и подсказкой такие 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?

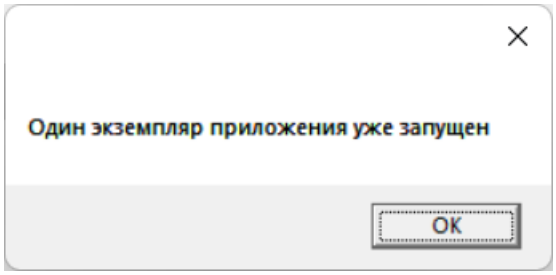
  a. Данные отправляются ботом (программный код) в публичный телеграмм-канал «Firehose - Finder issues». Информация из этого канала обрабатывается для изменения/добавления/исправления программы. Вся поступающая информация находится в открытом доступе, любой пользователь Телеграмм может подписаться на этот 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.**

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.

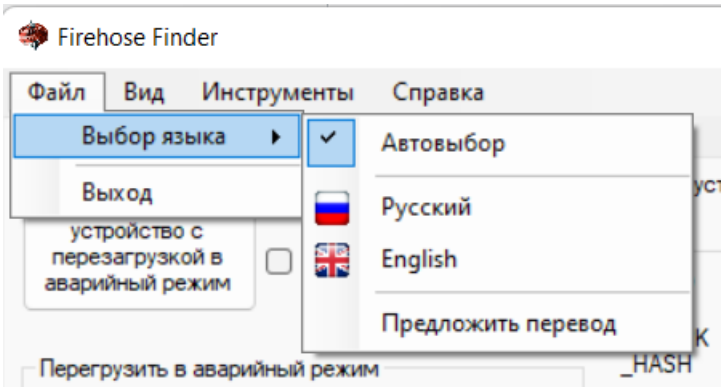


В программе реализован механизм запуска только одного экземпляра приложения. Если при запущенном приложении попытаться запустить второй экземпляр, то будет выведено предупреждение о невозможности осуществления такой операции.



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».

- «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.

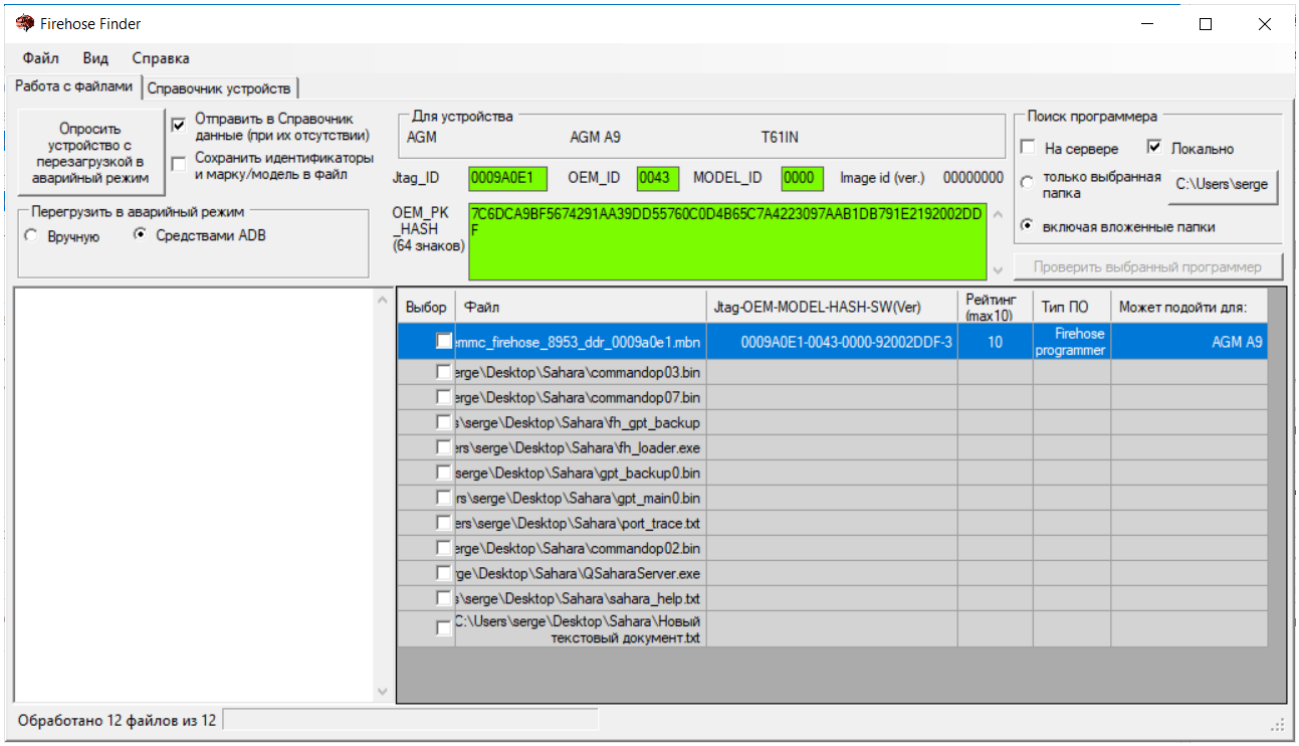
- «Предложить перевод» - переход в телеграм-канал «Чат для FhF» для озвучивания своей готовности в переводе приложения на свой язык. Так как проект не коммерческий, то работа по переводу не оплачивается и является символом доброй воли автора.

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

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).

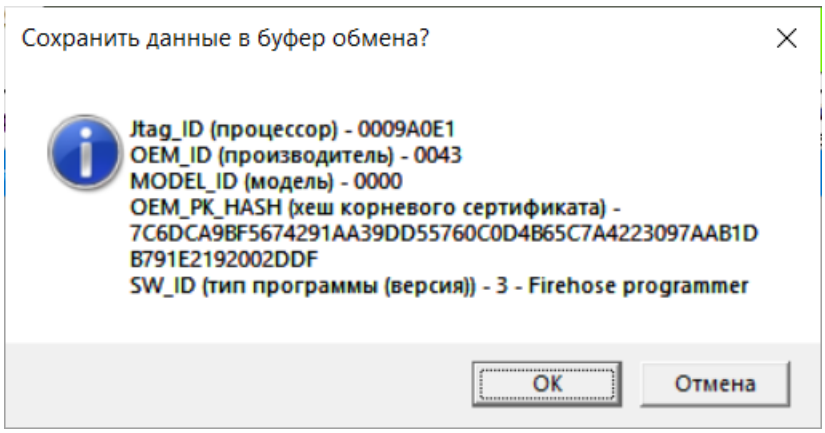
Когда данные устройства на форме заполнены (в автоматическом или ручном режиме), можно нажать кнопку «Поиск» в группе «Поиск программера» и выбрать путь к папке с коллекцией программеров. Переключателем можно выбрать область поиска:

- «На сервере»;

- «Локально».

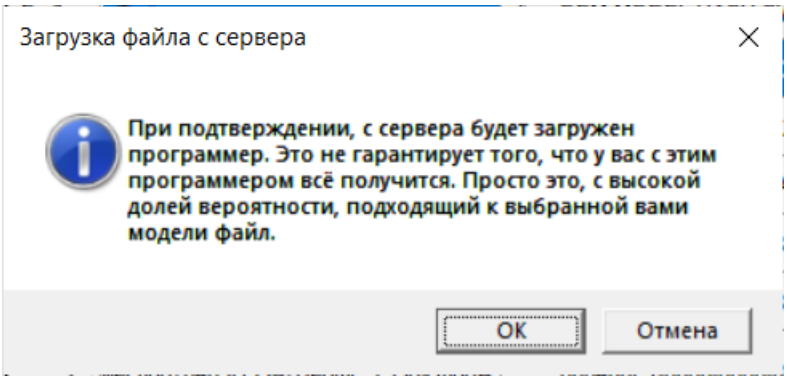
Для области «На сервере» заполненные данные формы являются своего рода фильтром. Таким образом, оставляя поля идентификаторов незаполненными, можно получить полный список программеров, расположенных на сервере. Внесение данных в поля идентификаторов позволяет сократить результаты поиска. Допускается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



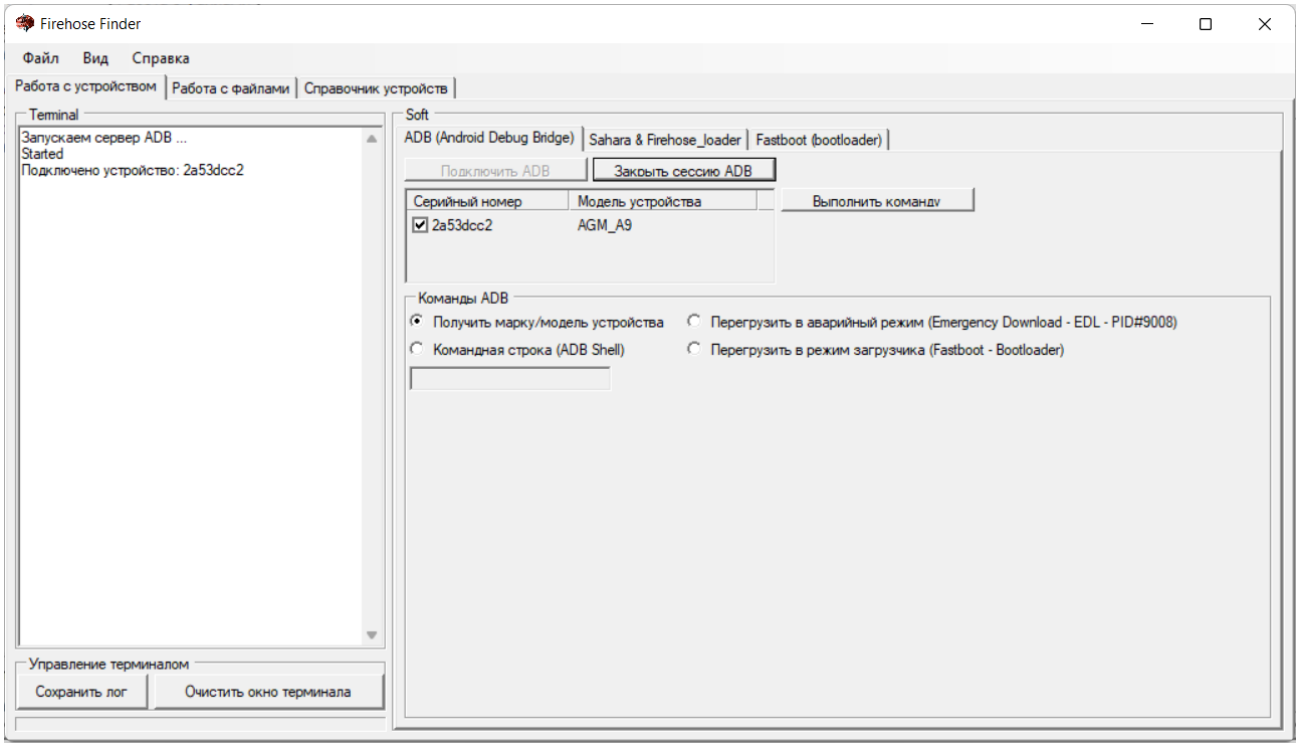
Для проверки программеров, расположенных локально, устройство должно быть перезагружено в аварийный режим (9008) либо вручную, либо программно, со вкладки «Работа с устройством». Если устройство перед этим подключалось для получения идентификаторов, то его надо отключить от компьютера, перезагрузить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

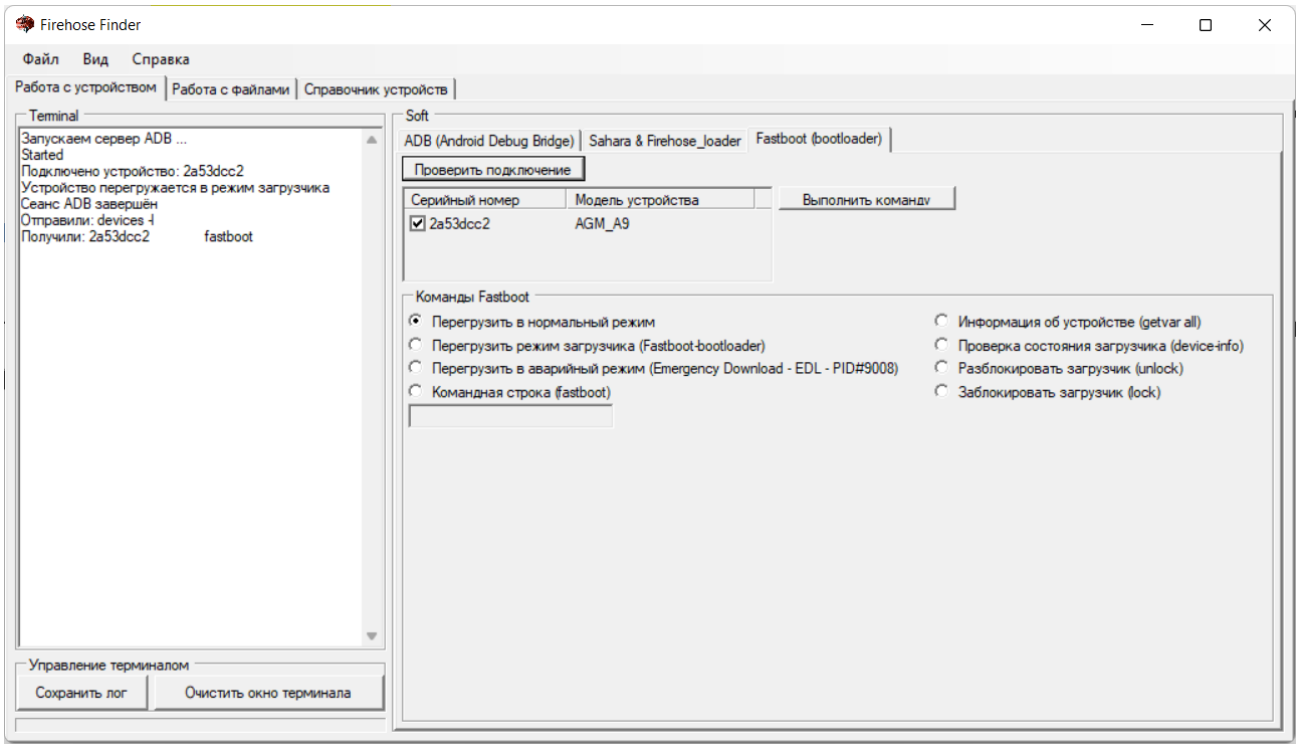
2. Перегрузить устройство в аварийный режим. Устройство будет перезагружено в 9008 средствами ADB. Это аналог команды *$ adb reboot edl* Не все устройства поддерживают эту команду.

3. 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*

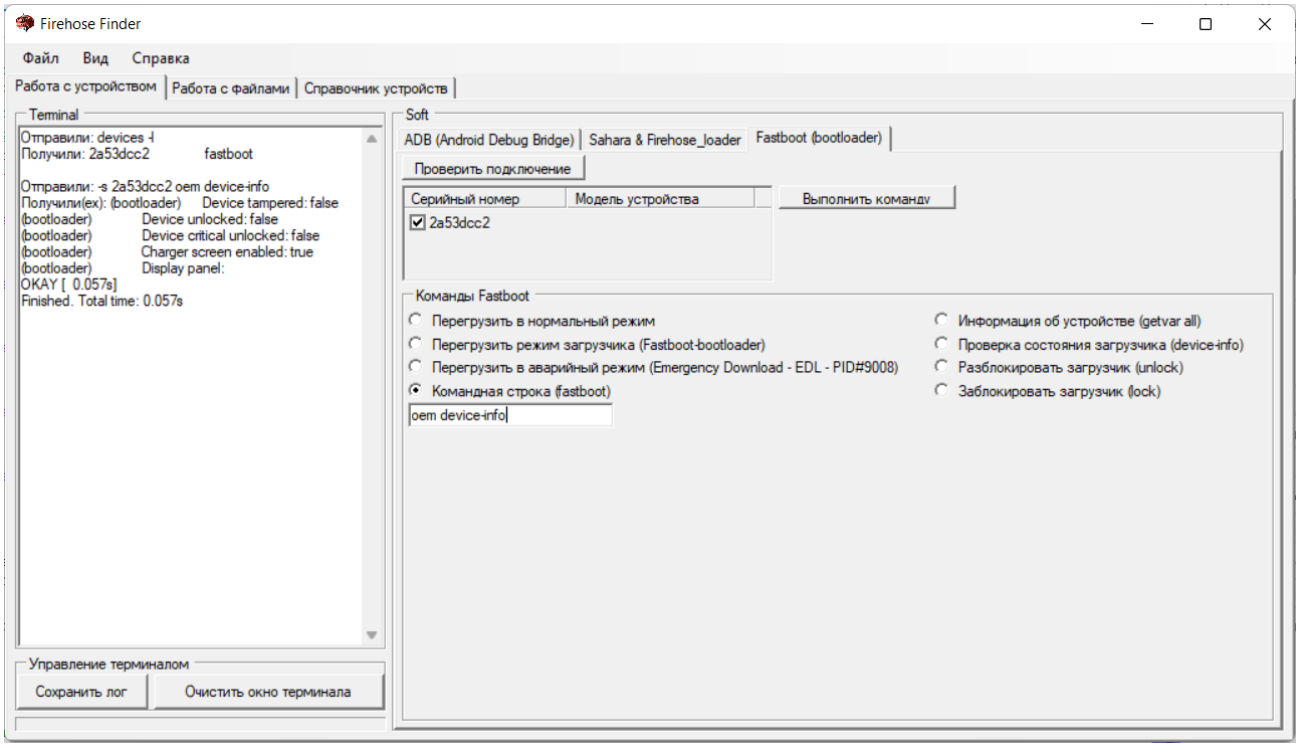
4. Перегрузить в режим загрузчика. Сеанс ADB завершается, открывается вкладка «Fastboot (bootloader)», устройство принимает только команды загрузчика.

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 *oem device-info*

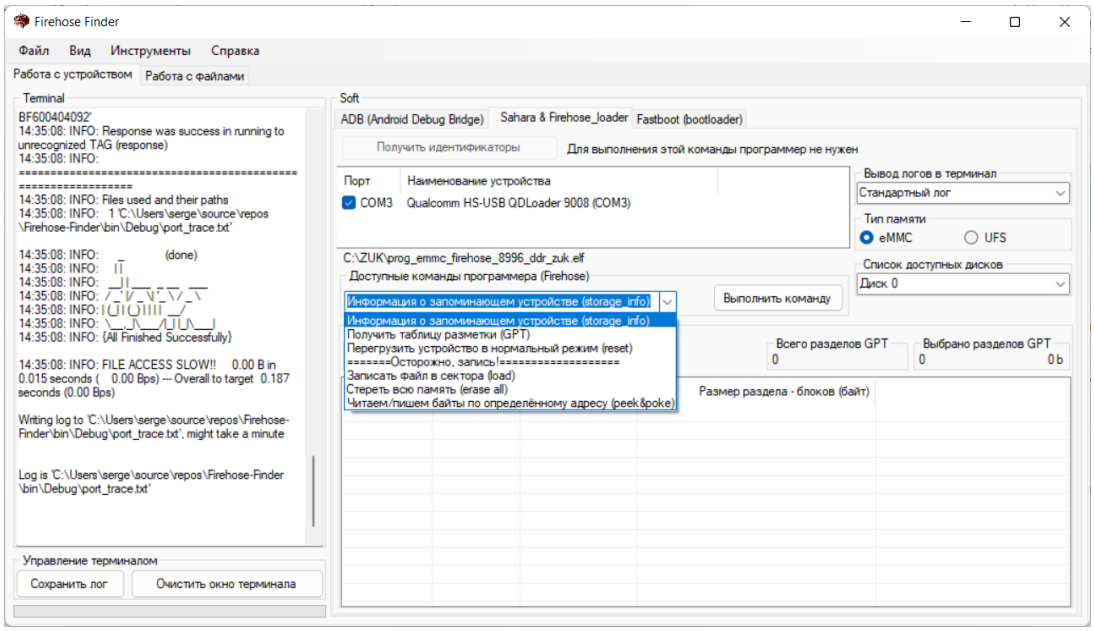


Раздел «Sahara & Firehose loader»

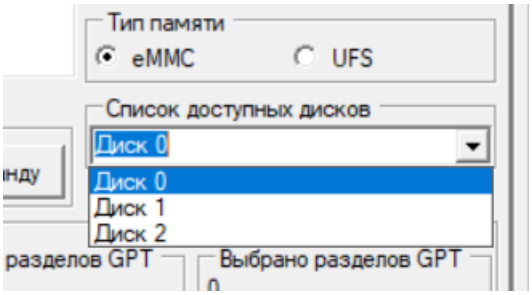
Команды для Sahara становятся активными после перезагрузки устройства в аварийный режим (9008). Порт устройства определяется автоматически, но, при необходимости, также может быть выбран и вручную, из списка доступных ком-портов. На текущий момент доступны следующие команды:

- 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. Программно сброс протокола пока не реализован.

- Слева от кнопки «Выполнить команду» находится комбобокс с выбором команд. Первой командой для исполнения является «Информация о запоминающем устройстве (storage_info)».

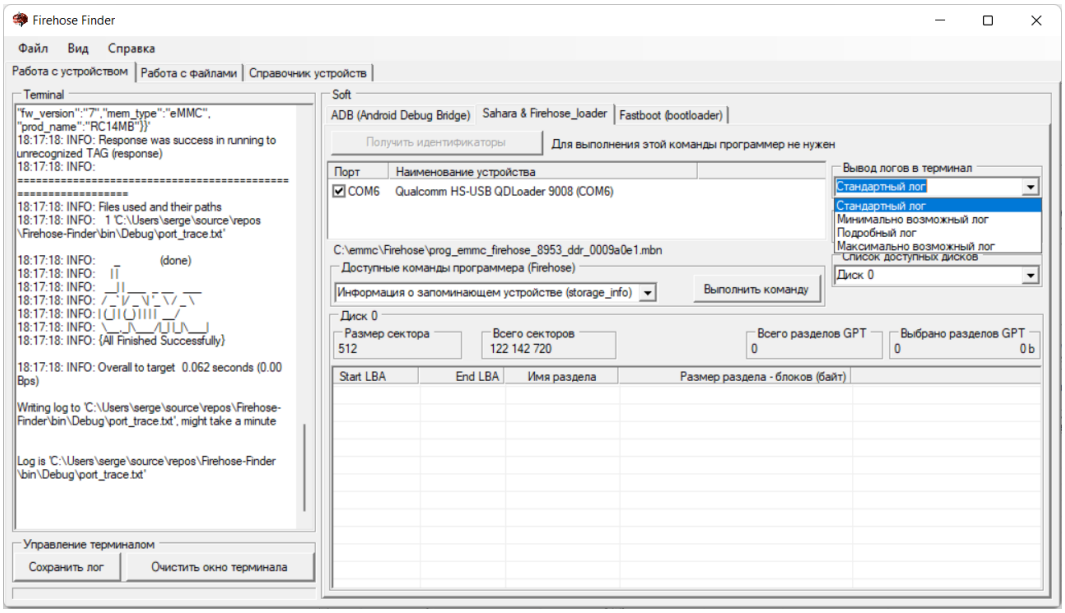


После её успешного выполнения становятся доступны и другие команды. Поле с выбором «Список доступных дисков» заполняется номерами физически доступных для работы частей флэш-памяти (в данном примере их три).

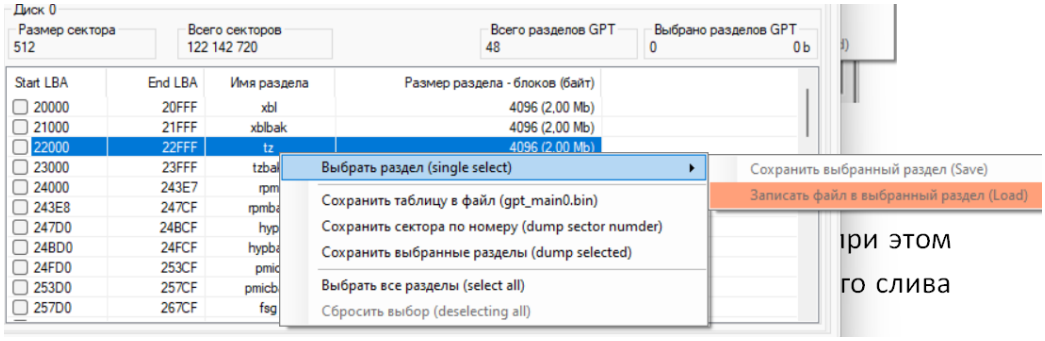


Автоматически выбирается тип памяти, но можно выбор поправить вручную, если память определилась некорректно.

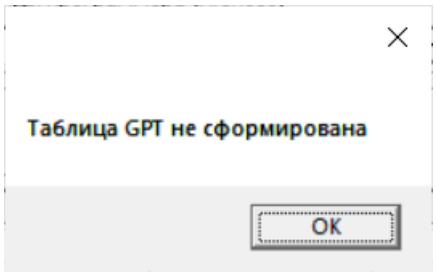
Можно выбрать четыре варианта отображения лога. По-умолчанию – «Стандартный лог»



- «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](#).

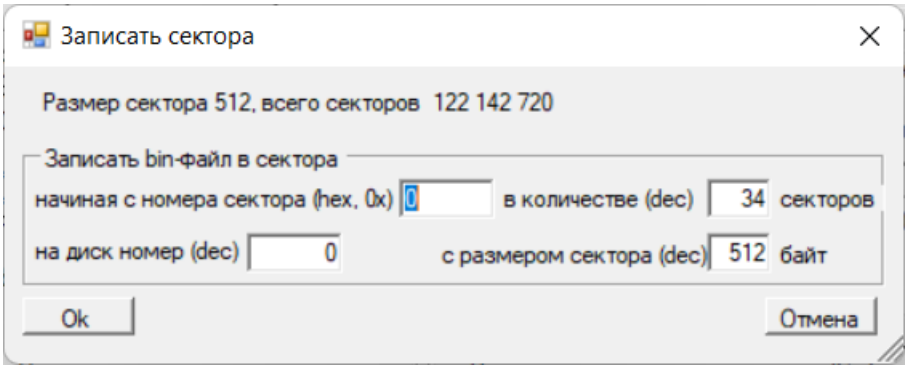


Если на диске таблица отсутствует, то будет выведено предупреждение, при этом возможность получить посекторную информацию остаётся, т.е. для полного слива информации с диска наличие таблицы разделов не обязательно.



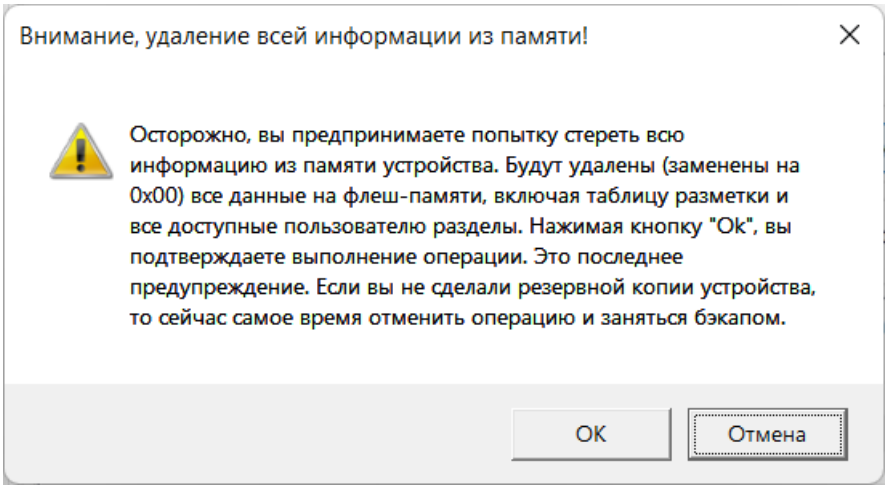
- «Перегрузить устройство в нормальный режим (reset)». Выбор данной команды позволяет перезагрузить устройство из аварийного в нормальный режим. Задержка выполнения команды перезагрузки устройства в нормальный режим – 10 секунд.

- Записать файл в сектора (load). Команда необходима для записи, например таблицы разметки. **Выполнять очень аккуратно!**

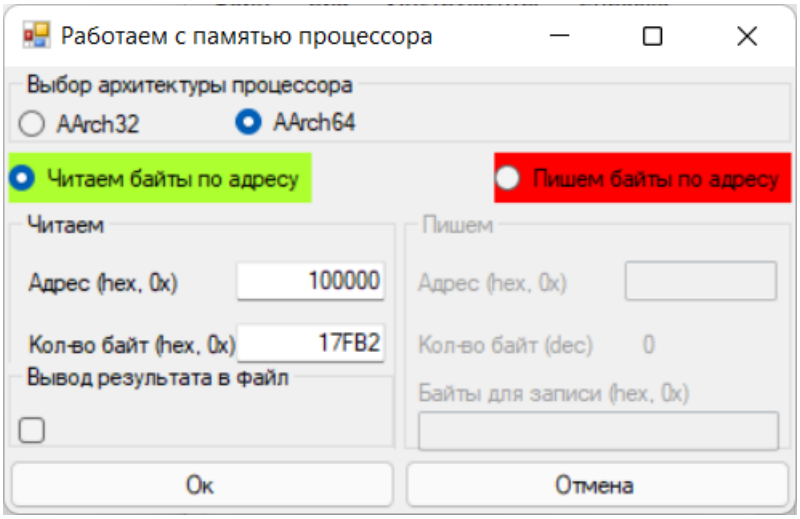


После подтверждения введённой информации будет предложено выбрать bin-файл для копирования его в память устройства по указанному адресу.

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

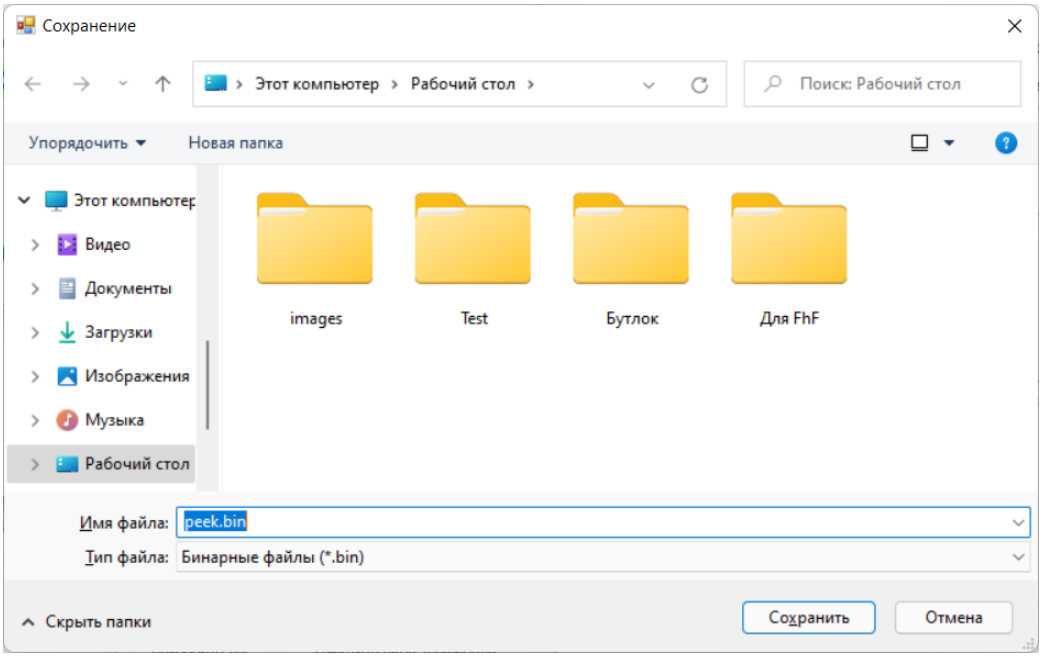


- «Читаем/пишем байты по определённому адресу (peek/poke)». Операция позволяет считать внутреннюю память (Internal memory - IMEM) процессора. Перед чтением или записью необходимо сначала уточнить адрес и количество байт для чтения/записи для вашего процессора. Адреса для архитектуры 32 и 64 байта могут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



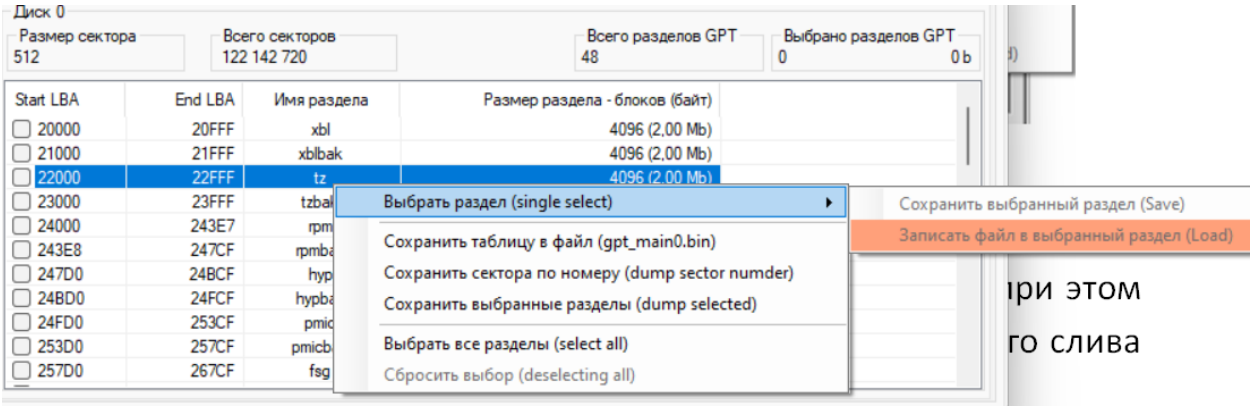
Выбор архитектуры процессора происходит автоматически, в зависимости от используемого программера. При этом, если есть необходимость, то этот параметр можно изменить (например, при ошибке «HANDLE_PEEK_FAILURE»).

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.

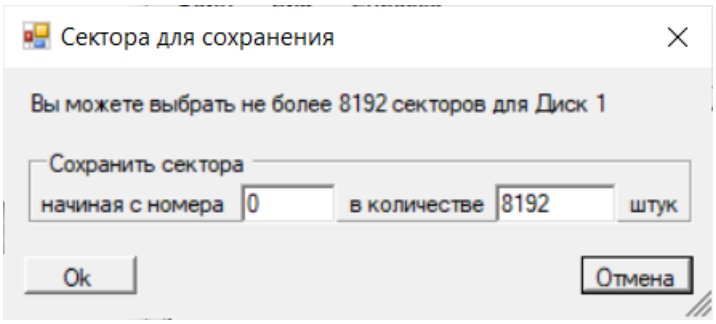


- «Выбрать раздел». При выборе сбрасываются все флажки на разделах, и остаётся только на одном – текущем. При этом становятся активны пункты меню для одиночной работы с разделом. Множественный выбор разделов не допускается.

  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 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.

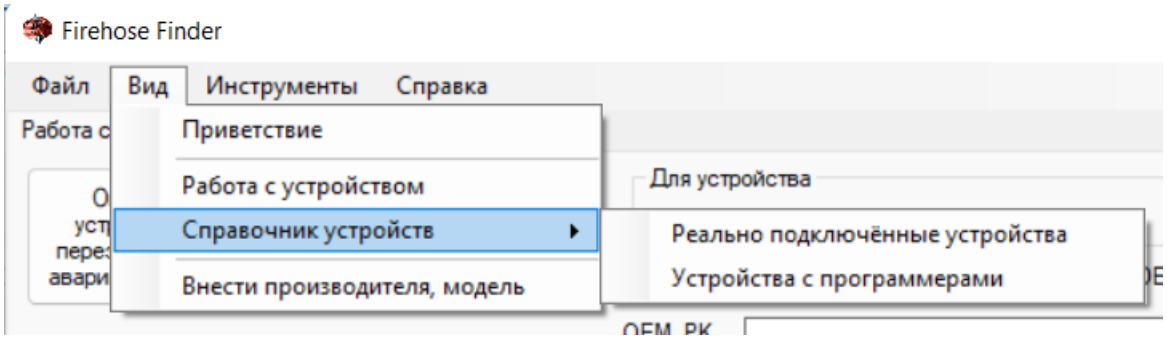


- «Сохранить выбранные разделы (dump)». Мультисекторный дамп разделов. Можно выбрать один, несколько или все разделы для сохранения. Стоит обратить внимание на достаточность места на локальном диске для дампа выбранных разделов. Обычно, раздел **«userdata»** несёт в себе большинство пользовательских данных, **является самым большим и**, при сохранении резервной копии, **не копируется из-за размера.**

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

Вкладка «Справочник устройств» (скрытая)

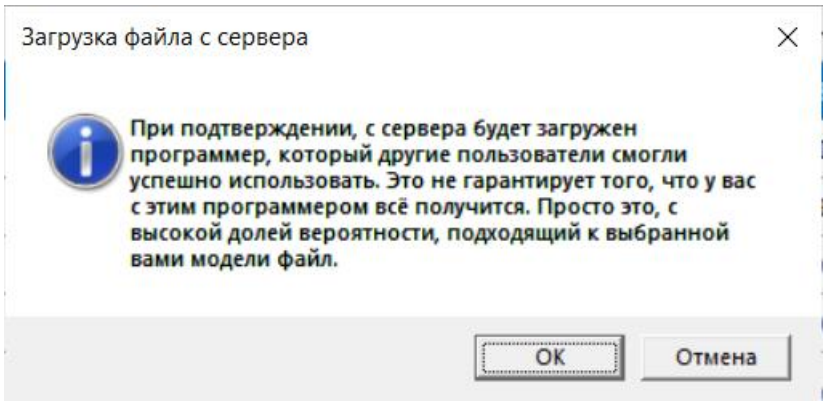
Активизировать вкладку можно из меню «Вид». «Справочник устройств» содержит фильтр «полностью подтверждённые устройства» - это список устройств, с которых все идентификаторы были получены в автоматическом режиме (без ручного ввода).



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.

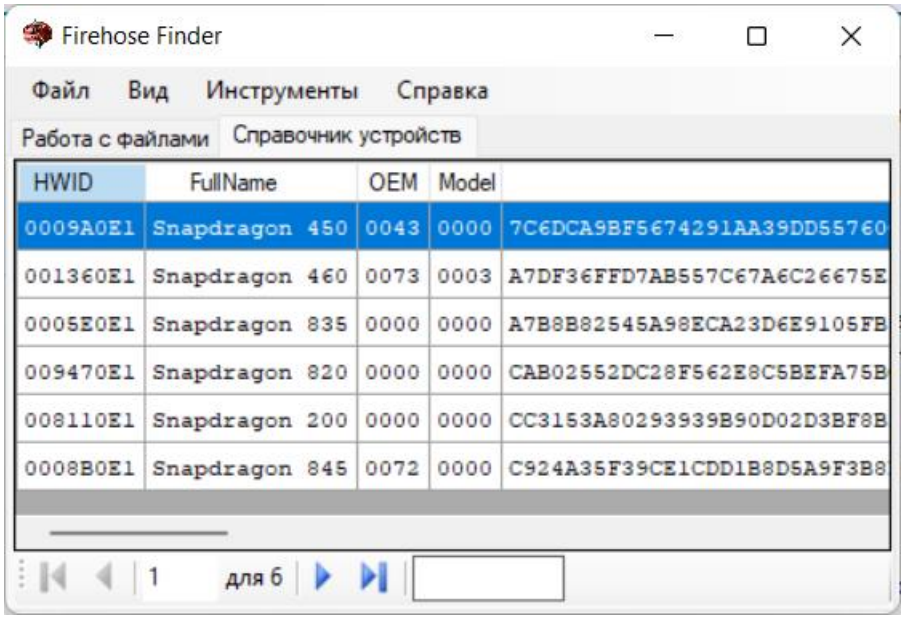
При двойном клике на строке с выбранным устройством произойдёт автозаполнение данных на вкладке «Работа с файлами» и будет предложено загрузить программер с сервера.



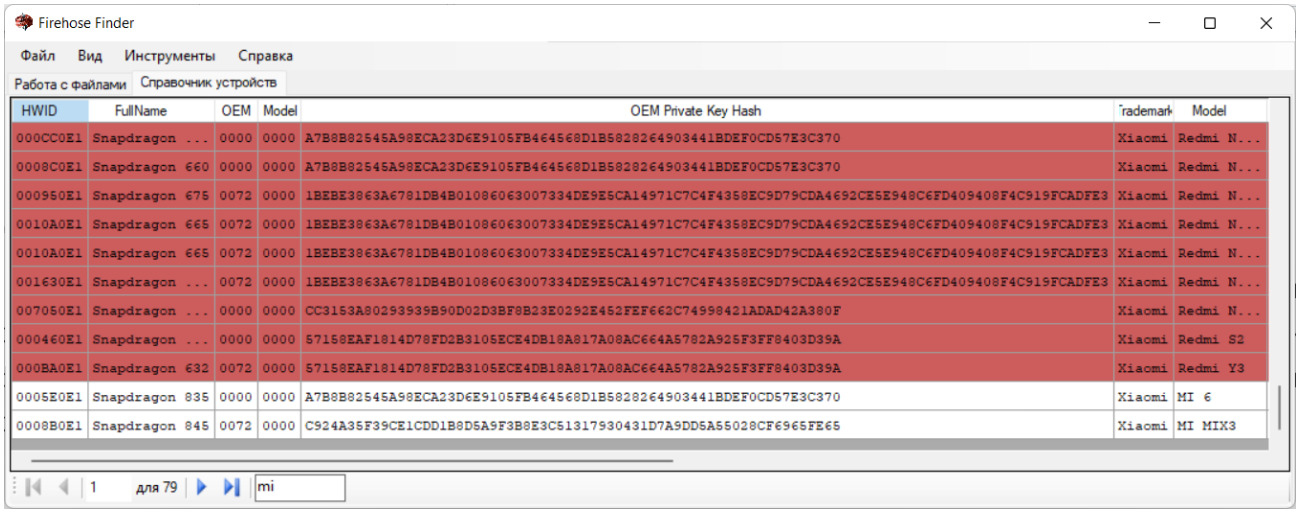
В полном списке соответствие программера устройству может оказаться далеко не у всех. Некорректные или отсутствующие данные в «Справочнике устройств», с согласия пользователя

(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.



В результате поиска будут отображены все модели устройств, которые содержат введёные 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.

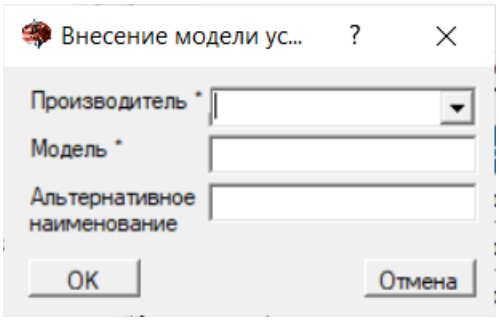


При стирании символов в окне поиска результаты будут сброшены и вывод отобразит данные в соответствии с выбором в меню.

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.



Пункт меню «Инструменты»

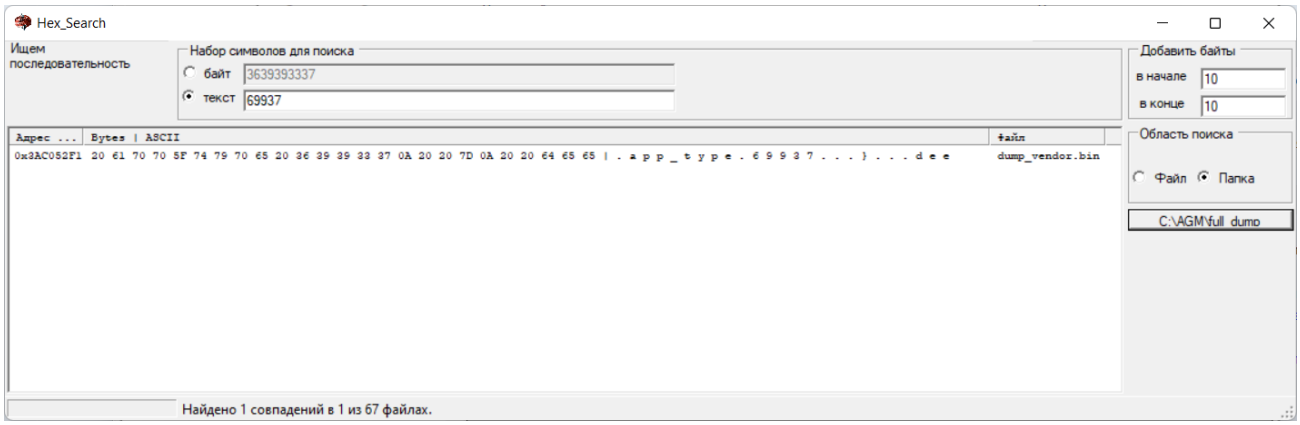
В этом меню собраны инструменты, которые могут помочь при распаковке прошивки и при поиске информации в сохранённых с устройства файлах.

Раздел «Бинарный поиск по маске»

Инструмент «Бинарный поиск по маске» 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).

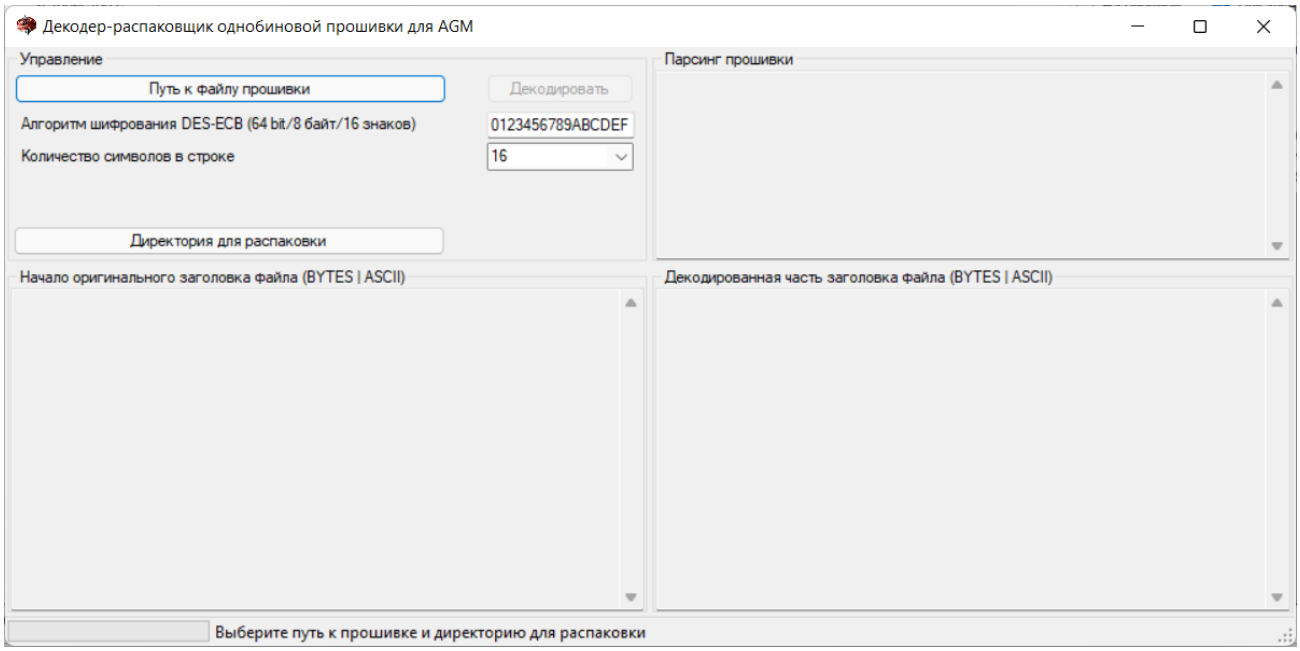
Двойной клик на строке с результатами поиска позволяет сохранить в буфер обмена адрес начала последовательности байт для поиска. Это можно использовать при открытии файла в хекс-редакторе и переходе по адресу, вставленному из буфера обмена, для редактирования этого файла. Имя файла, в котором найдена требуемая последовательность, указано в конце строки результатов поиска. Если результатов несколько, то они группируются по имени файла и отсортированы по адресу по возрастанию.



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».

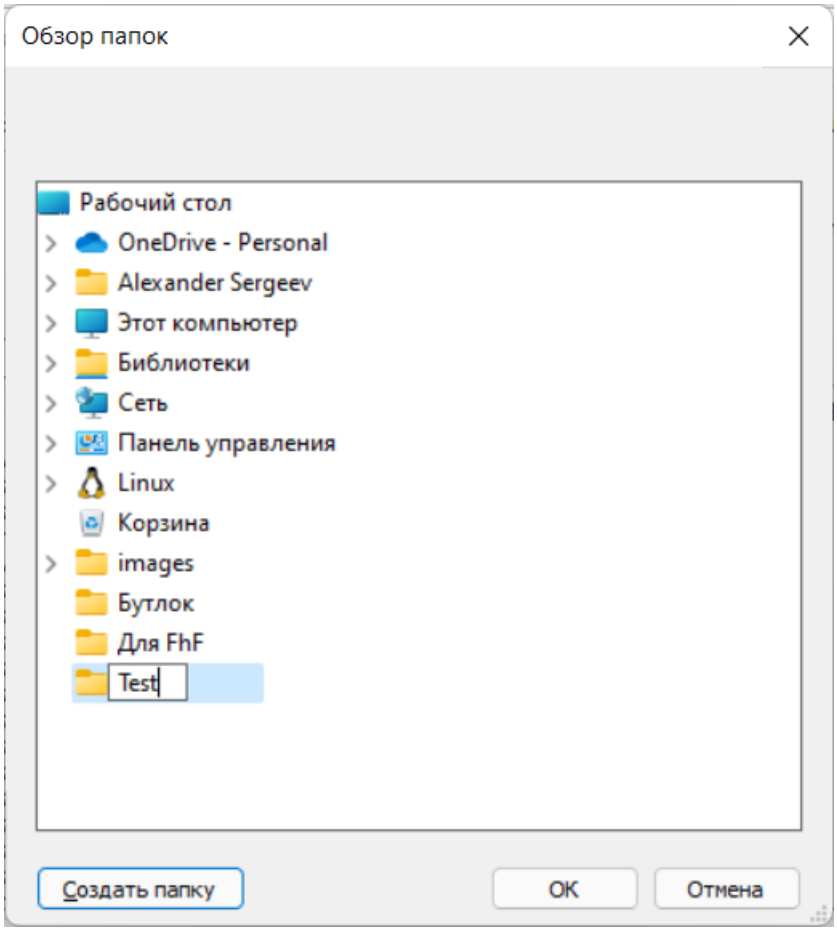


Для декодирования прошивки необходимо указать путь к однобиновому файлу, нажав соответствующую кнопку. После указания файла сразу же начнётся его считывание. На форму выводится не весь блок информации шапки прошивки, а только часть, для оптимизации скорости работы программы. Информация выводится в оригинальном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

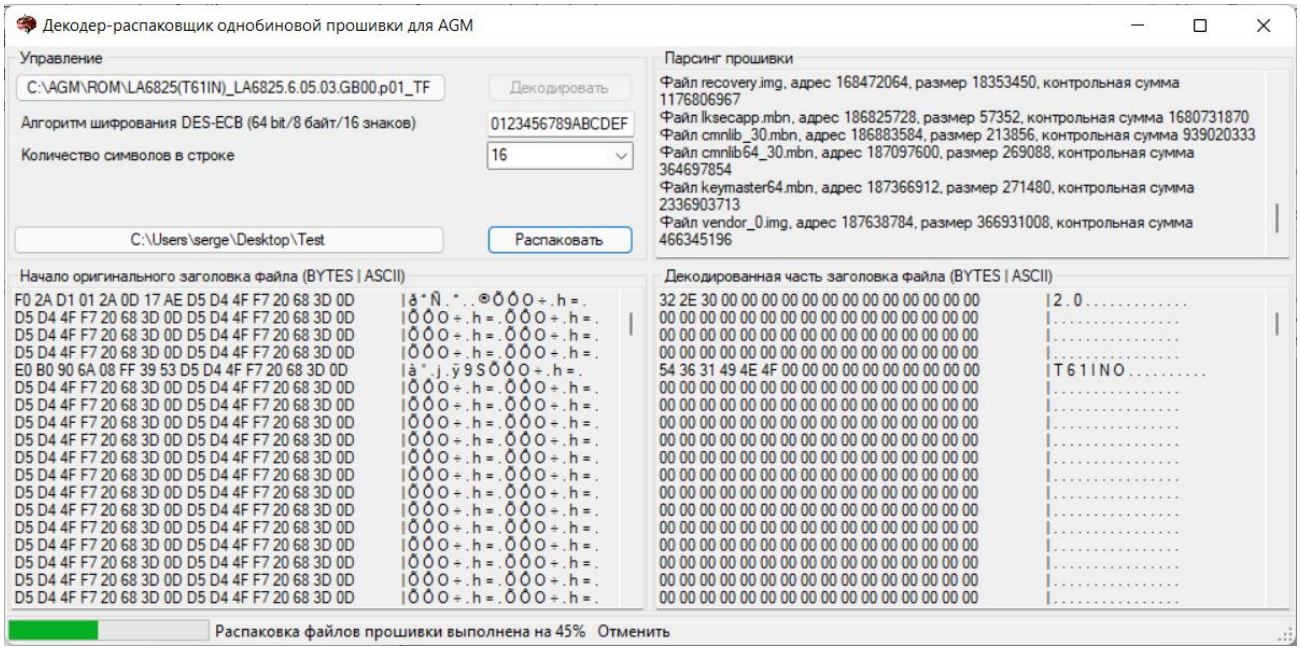
После считывания шапки прошивки становится активна кнопка «Декодировать». Для декодирования необходимо указать код кодировки. По-умолчанию выставлен «0123456789ABCDEF». Также можно выбрать, сколько символов отображать в строке для удобства оценки корректности декодирования. Справа внизу на форме будет 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).

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.

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.