

## Оглавление

Часто задаваемые вопросы (ЧаВо) .....	1
Окно «Приветствие».....	2
Вкладка «Работа с файлами» (основная) .....	2
Вкладка «Работа с устройством» (скрытая) .....	4
Раздел «ADB (Android Debug Bridge)» .....	4
Раздел «Fastboot (bootloader)» .....	5
Раздел «Sahara & Firehose loader» .....	6
Команды контекстного меню .....	9
Вкладка «Справочник устройств» (скрытая) .....	10
Окно «Внести производителя, модель».....	11

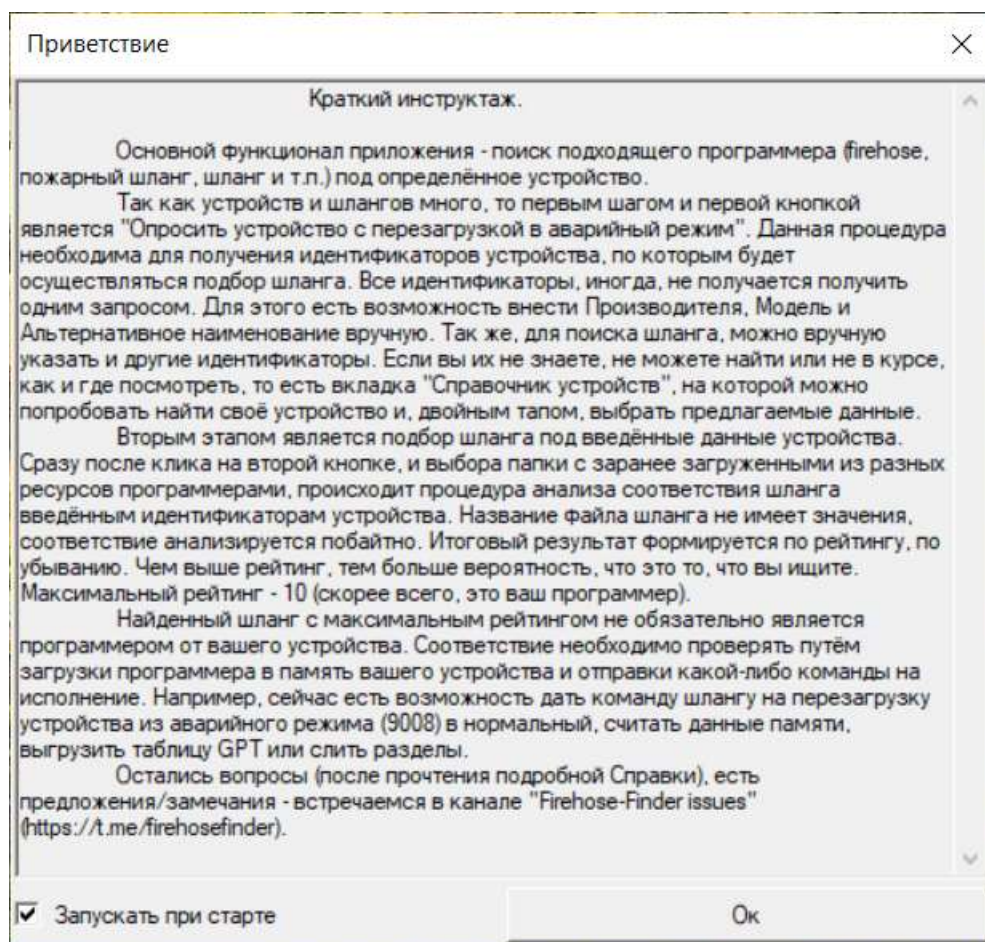
## Часто задаваемые вопросы (ЧаВо)

1. 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.
2. 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 -с 02(03,07).
3. 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).

4. q. Куда и кому отправляются, и какие именно, данные с моего устройства?
- а. Данные отправляются ботом 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 - процессор, 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.



## 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), 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 «Перезагрузить 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.

Backup	File	Jtag-OEM-MODEL-HASH-SW(Ver)	Peelme' max ID	Тип ПО	Может подойти для:
	mmc_firehose_8953_ide_0009ade1.mbn	0009ADE1-0043-0000-9200200F-3	10	Firehose programmer	AGM A9
	.../Sahara/commandop03.bin				
	.../Sahara/commandop07.bin				
	.../Sahara/ih_gpt_backup				
	.../Sahara/ih_loader.exe				
	.../Sahara/gpt_backup0.bin				
	.../Sahara/gpt_main0.bin				
	.../Sahara/port_trace.txt				
	.../Sahara/commandop02.bin				
	.../Sahara/QSaharaServer.exe				
	.../Sahara/sahara_help.txt				
	.../Sahara/Новый текстовый документ.txt				

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

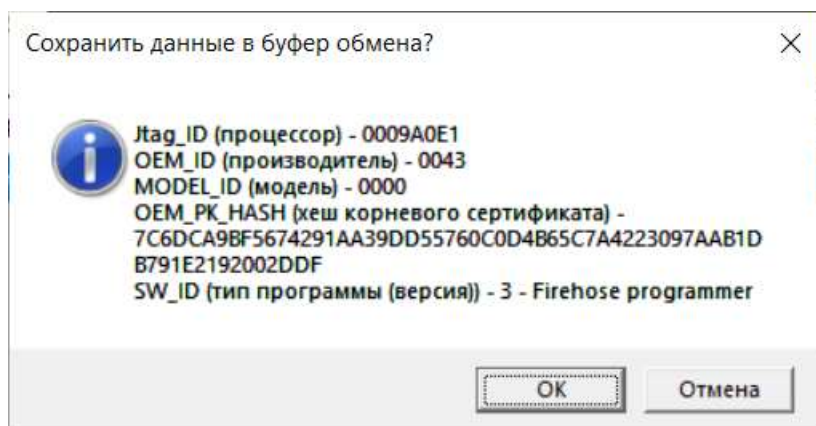
Когда данные устройства на форме заполнены (в автоматическом или ручном режиме), можно нажать кнопку «Поиск» в группе «Поиск программера» и выбрать путь к папке с коллекцией программеров. Переключателем можно выбрать область поиска:

- «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.

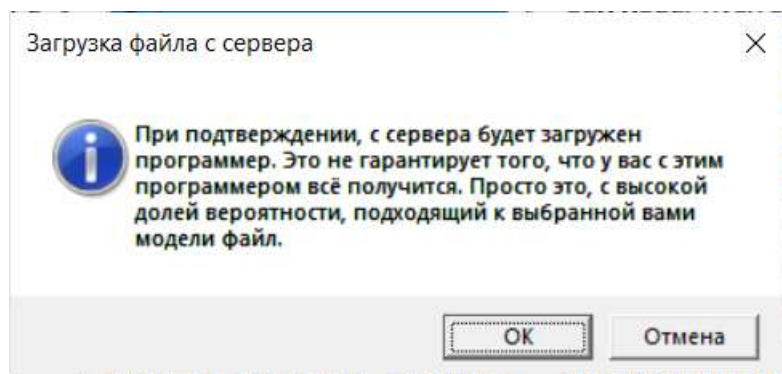
Для области «Локально» анализируется либо «только выбранная папка», либо «включая вложенные папки» – в зависимости от выбранного положения переключателя. Проверяются все файлы, находящиеся в папках. Поиск программера осуществляется не по названию, а по идентификаторам, соответственно имя файла программера 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 программмер самая высокая). Двойной тап на выбранном программмере позволяет скопировать в буфер обмена информацию об идентификаторах, которые этот программмер будет требовать при работе.



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

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



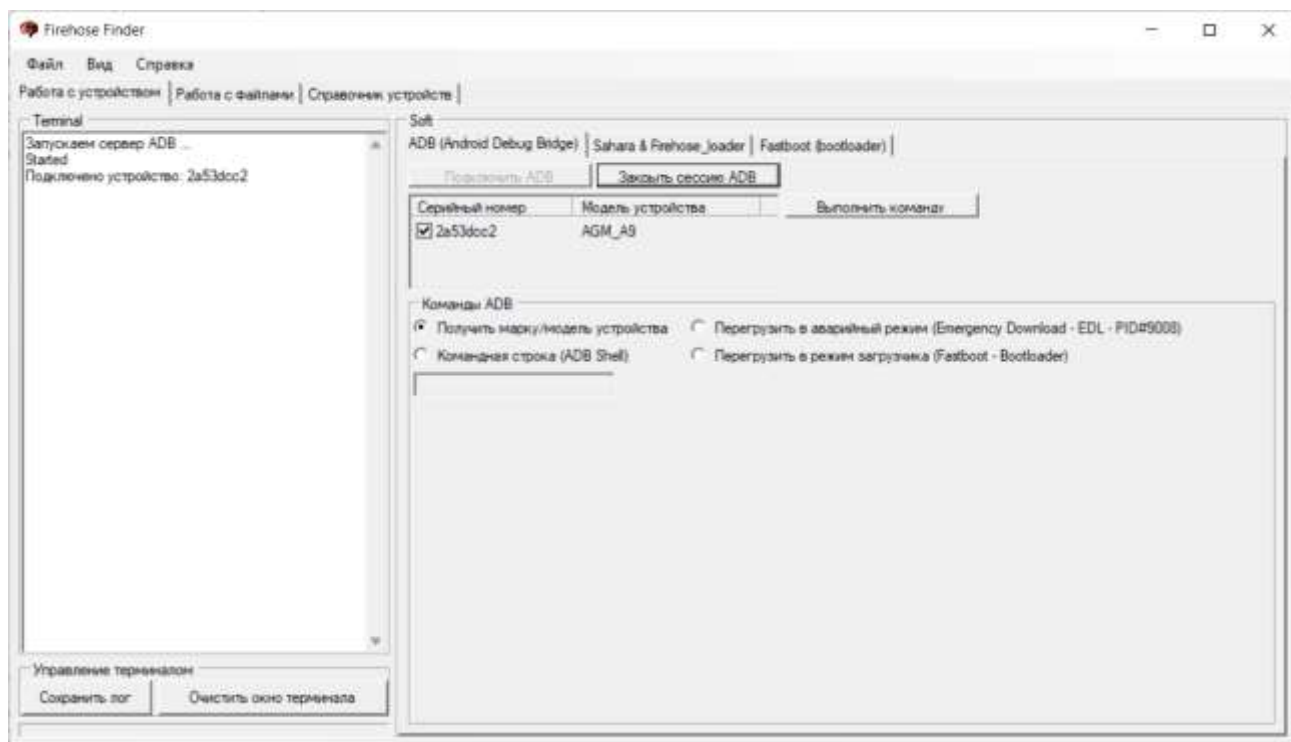
Для проверки программмеров, расположенных локально, устройство должно быть перезагружено в аварийный режим (9008) либо вручную, либо программно, со вкладки «[Работа с устройством](#)». Если устройство перед этим подключалось для получения идентификаторов, то его надо отключить от компьютера, перезагрузить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



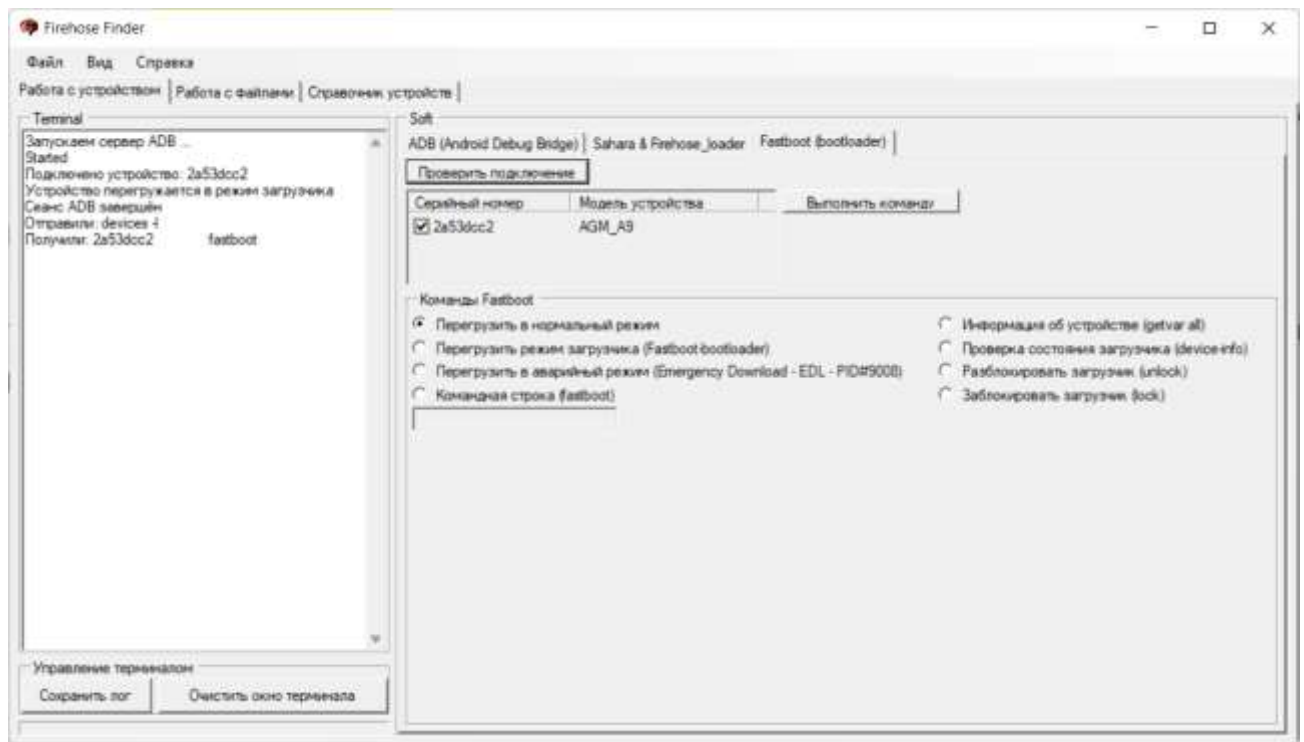
На текущий момент в списке доступно четыре команды для ADB:

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` 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 -l /system/bin` или `ls -l /system/xbin`
4. Перегрузить в режим загрузчика. Сеанс ADB завершается, открывается вкладка «Fastboot (bootloader)», устройство принимает только команды загрузчика.

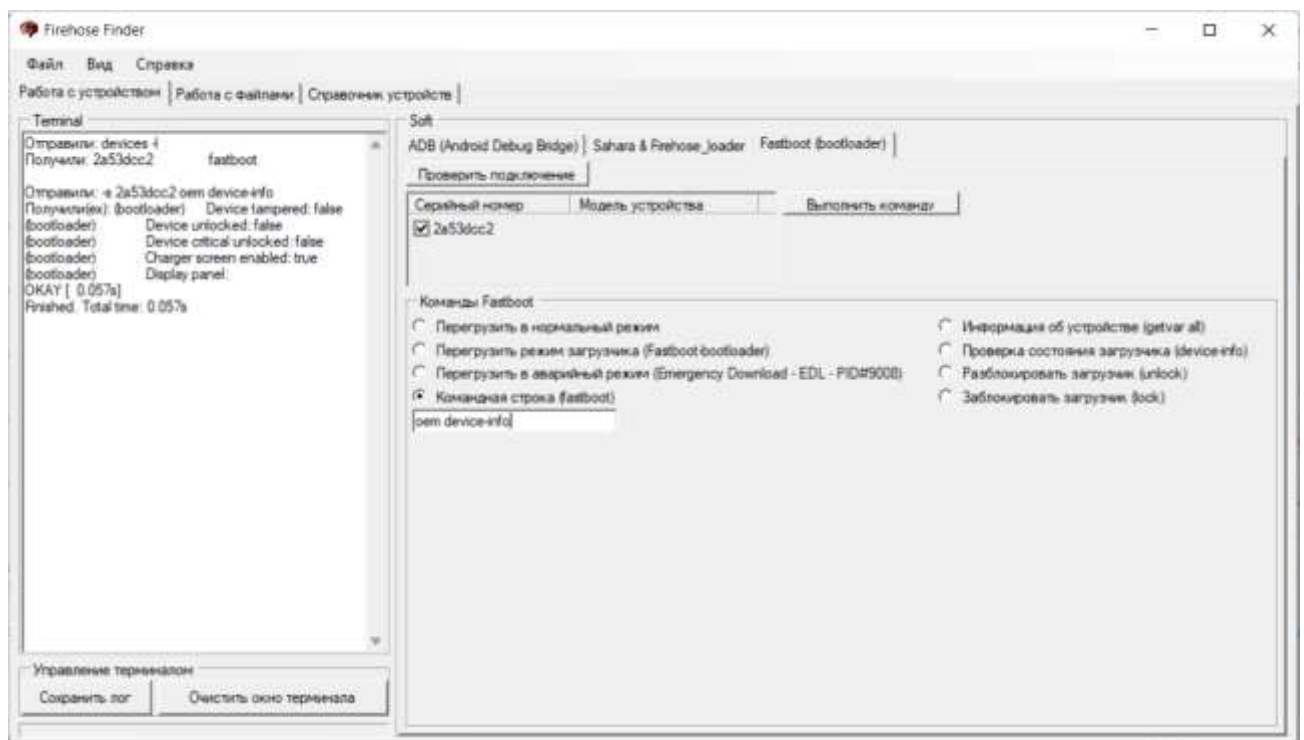
## Раздел «Fastboot (bootloader)»

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**

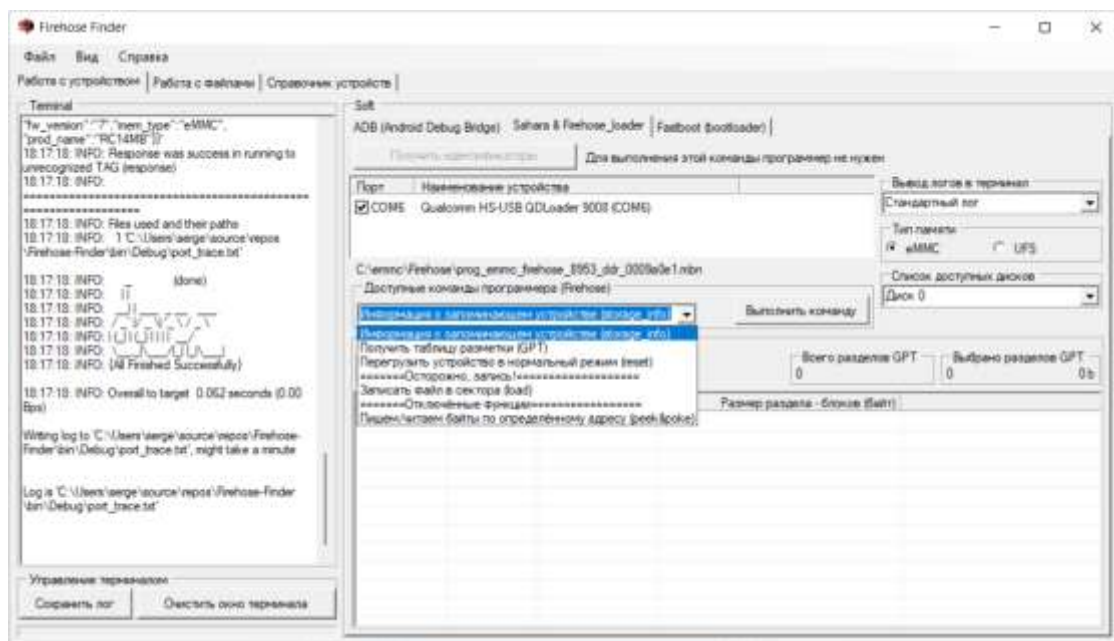


## Раздел «Sahara & Firehose loader»

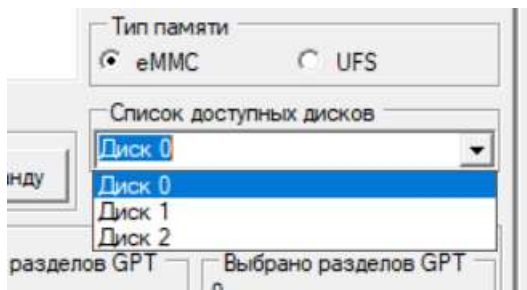
Команды для Sahara становятся активными после перезагрузки устройства в аварийный режим (9008). Порт устройства определяется автоматически, но, при необходимости, также может

быть выбран и вручную, из списка доступных 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. 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)».

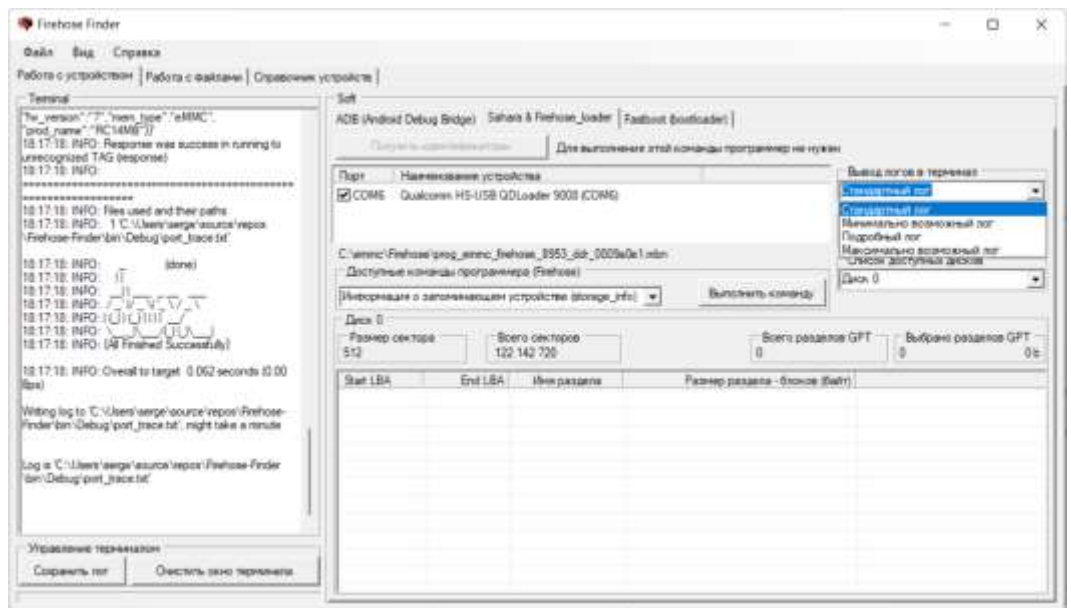


После её успешного выполнения становятся доступны и другие команды. Поле с выбором «Список доступных дисков» заполняется номерами физически доступных для работы частей флэш-памяти (в данном примере их три).

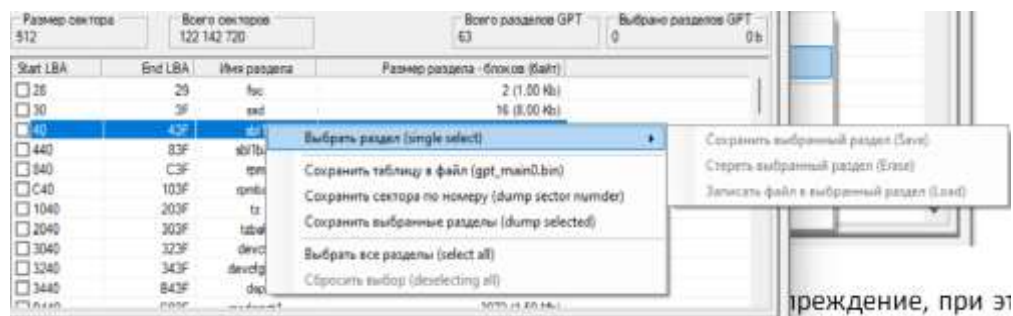


Автоматически выбирается тип памяти, но можно выбор поправить вручную, если память определилась некорректно.

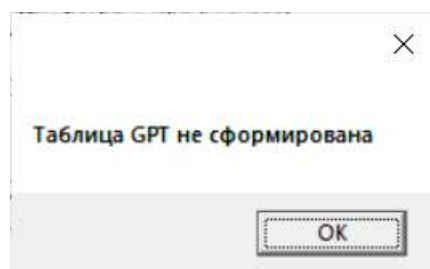
Можно выбрать четыре варианта отображения лога. По-умолчанию – «Стандартный лог»



- «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](#).



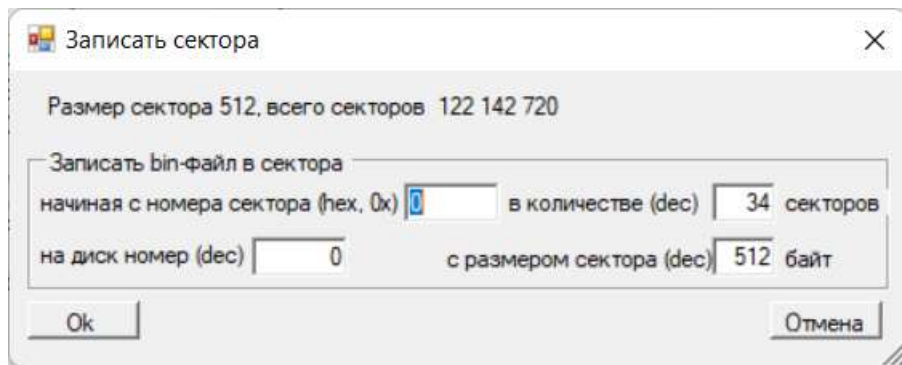
Если на диске таблица отсутствует, то будет выведено предупреждение, при этом возможность получить посекторную информацию остаётся, т.е. для полного слива информации с диска наличие таблицы разделов не обязательно.



- «Перезагрузить 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.

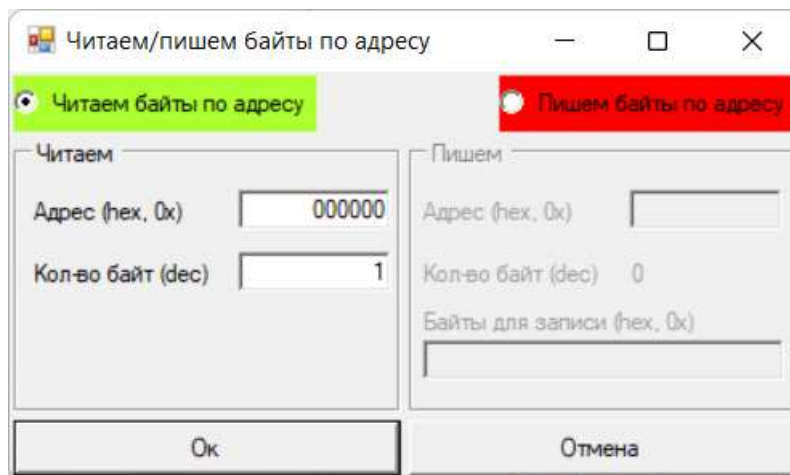


- Записать файл в сектора (load). Команда необходима для записи, например таблицы разметки. **Выполнять очень аккуратно!**

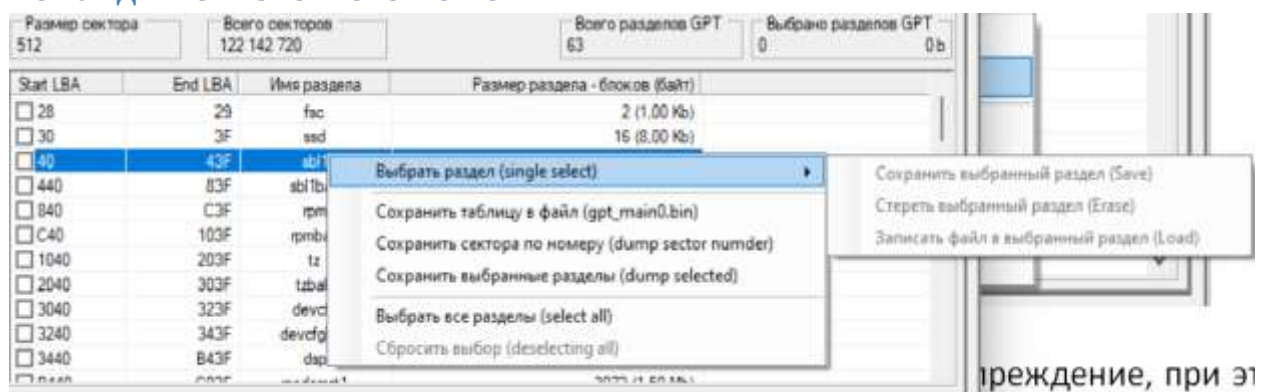


После подтверждения введённой информации будет предложено выбрать bin-файл для копирования его в память устройства по указанному адресу.

- «Пишем/читаем байты по адресу». Команда реализована, но при этом не поддерживается текущей версией лоадера, т.ч. оставлена просто, чтоб не удалять.



## Команды контекстного меню

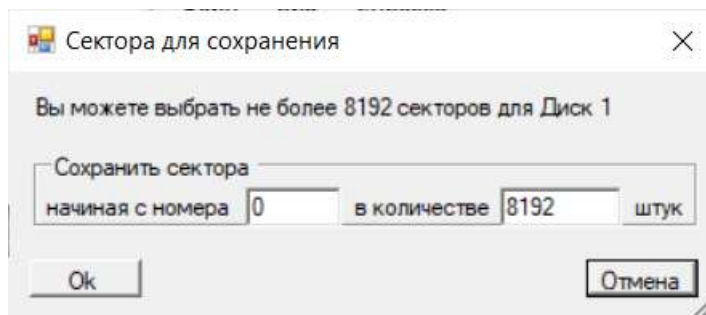


- «Выбрать раздел». При выборе сбрасываются все флажки на разделах и остаётся только на одном – текущем. При этом становятся активны пункты меню для одиночной работы с разделом. Множественный выбор разделов не допускается.

Одиночный раздел можно сохранить, стереть и на его место записать bin-файл.

**Стирание и запись необходимо осуществлять с особой внимательностью.**

- «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/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	105 074 645 (50,10 Gb)
<input type="checkbox"/>	7403FD5	747BFDE	grow	491 530 (240,00 Mb)

- 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 «(с программерами)», а также «Полный список». «Справочник устройств (с программерами)» - это данные, которые 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.



Внесение модели ус... ? X

Производитель \*

Модель \*

Альтернативное наименование

OK Отмена