Мобильный Криминалист

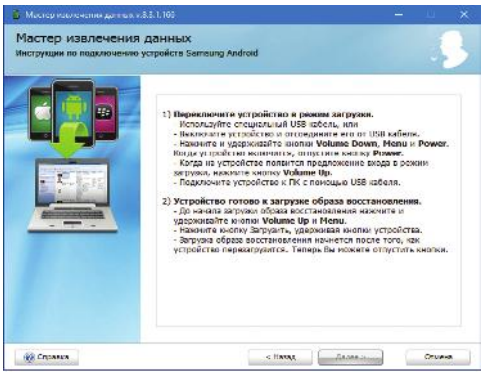
Российское ПО для экспертизы мобильных устройств

Физическое извлечение данных из устройств на ОС Android

Физические методы без использования рут-прав

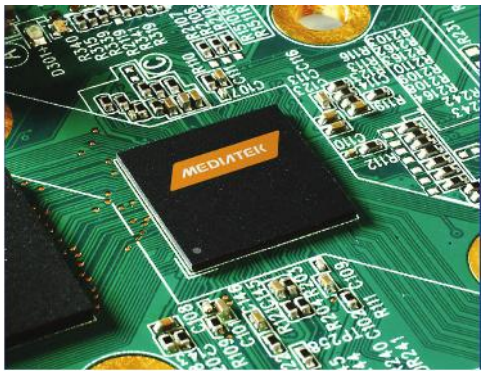
Samsung устройства

«Мобильный Криминалист» поддерживает создание физических дампов с устройств Samsung путем заливки собственного модифицированного образа восстановления. Данный подход позволяет обходить любые пароли на блокировку экрана (пароль, PIN-код, графический ключ и т.д.). Метод дает доступ ко всем данным устройства, включая удаленные записи и приложения.



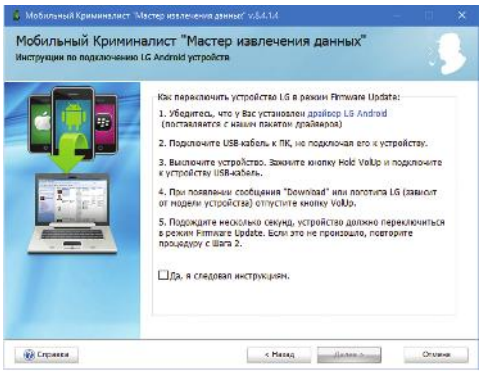
MTK и Spreadtrum устройства

«Мобильный Криминалист» дает возможность снимать физические дампы с мобильных устройств на китайских чипсетах MediaTek и Spreadtrum. Данный метод позволяет обходить любые пароли на блокировку экрана, так как устройства подключаются в выключенном состоянии. Телефон остается заблокированным и после окончания процесса чтения данных.



LG устройства

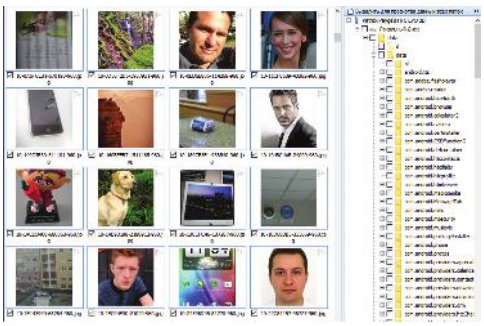
«Мобильный Криминалист» позволяет осуществлять физическое извлечение данных из устройств LG в режиме Firmware update. Метод позволяет обходить любые пароли на блокировку экрана, так как знание пароля при извлечении не требуется. При помощи этого метода можно извлечь всю файловую структуру, а также удаленные файлы и популярные приложения.



Физическое извлечение через получение рут-прав

Получение рут-прав

Функция получения прав root-доступа встроена в программу «Мобильный Криминалист. Root-права являются временными и после перезагрузки устройства отменяются. Поэтому методика полностью соответствует принципам криминалистического исследования. Применение прав root-доступа позволяет получить доступ ко всей файловой системе устройства, приложениям и удаленным записям. 100% результат применения прав root-доступа не гарантирован, но эта процедура доступна для многих устройств на платформе Android.



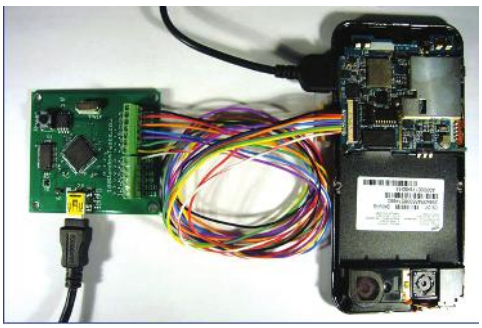
Импорт физических образов сторонних программ

Nandroid (TWRP) и (CWM) образы

Из модифицированного меню восстановления в устройстве можно сохранить физический образ Nandroid на флэш-карту и затем импортировать его в «Мобильный Криминалист».

JTAG образы

Если устройство повреждено, с него можно снять JTAG образ при помощи программаторов RIFF-box или Octopus. Анализ данных JTAG образа поддерживается в ПО «Мобильный Криминалист.



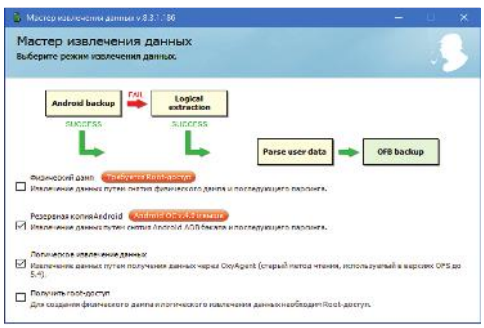
Нефизические методы

Резервная копия Android ADB

«Мобильный Криминалист» позволяет снимать резервную копию ADB с устройства Android ОС 4 и выше. Данный метод дает доступ ко многим данным, в том числе к приложениям.

Извлечение через OxyAgent

Метод работает на всех Android устройствах. При его выборе происходит загрузка утилиты OxyAgent в устройство, которая является посредником между данными устройства и программой.



www.мобильный-криминалист.рф,
Россия, 109029, Москва, ул. Нижегородская, д. 32, стр. 5, +7-495-222-9277