Мобильный Криминалист

Современные подходы к извлечению данных из Android-устройств

Карондеев А.М.

http://www.мобильный-криминалист.рф

Самая распространенная мобильная ОС

Worldwide Smartphone Sales to End Users by Operating System in 2017 (Thousands of Units)

Operating System	2017 Units	2017 Market Share (%)	2016 Units	2016 Market Share (%)
Android	1,320,118.1	85.9	1,268,562.7	84.8
iOS	214,924.4	14.0	216,064.0	14.4
Other OS	1,493.0	0.1	11,332.2	0.8
Total	**1,536,535.5**	**100.0**	**1,495,959.0**	**100.0**

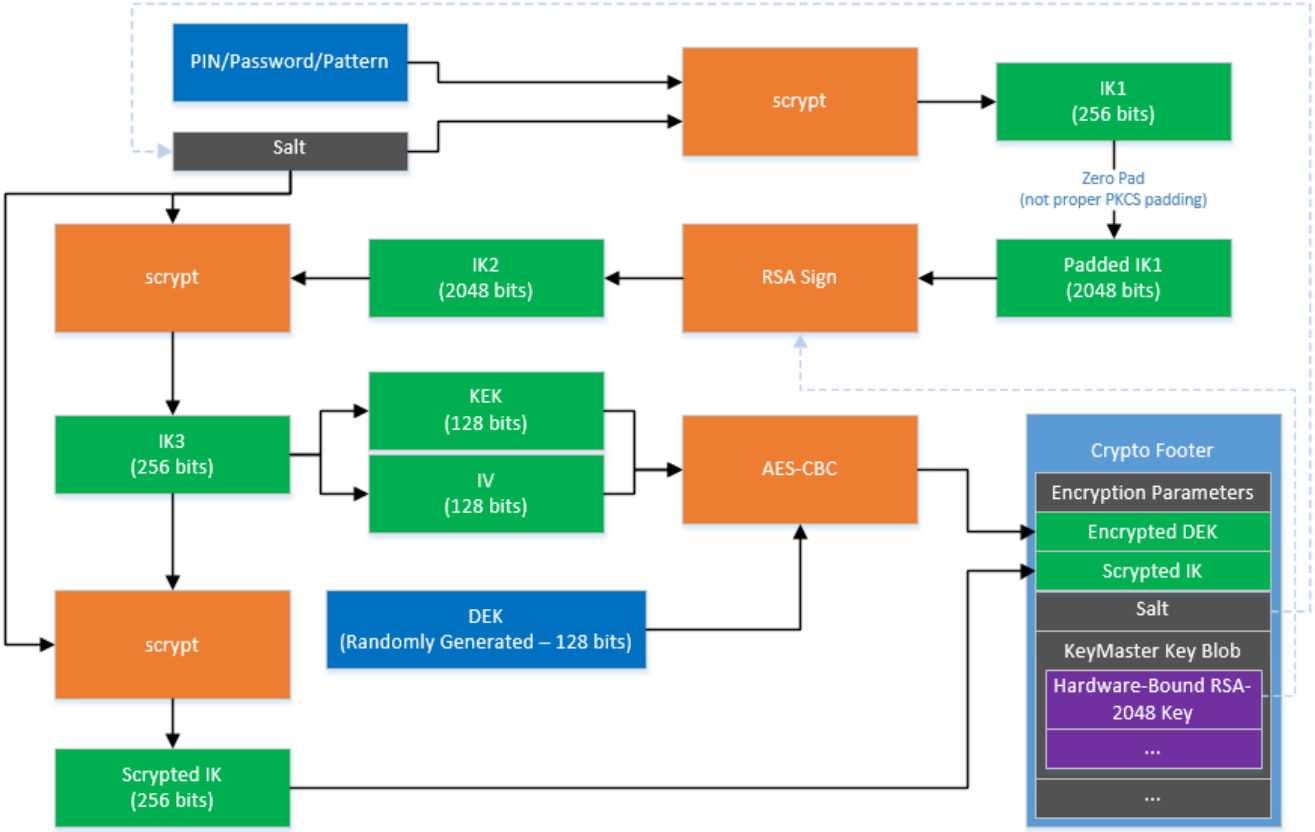
Source: Gartner (February 2018)

Шифрование данных

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Шифрование данных



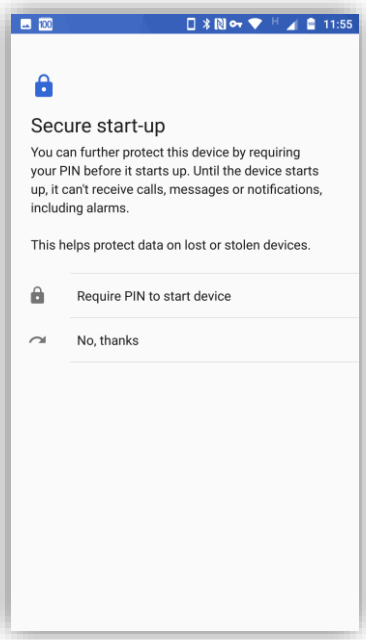
Защита от выполнения неподписанного кода

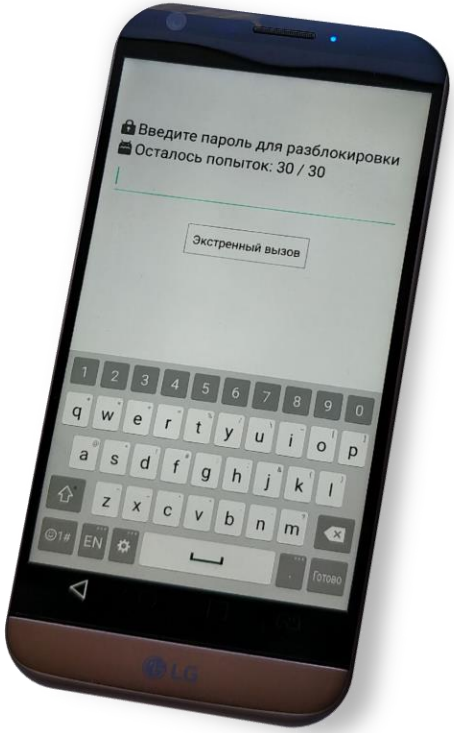
- Блокировка загрузчика
- OEM-блокировка
- qFuses
- FRP (Samsung)

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Secure Start-Up

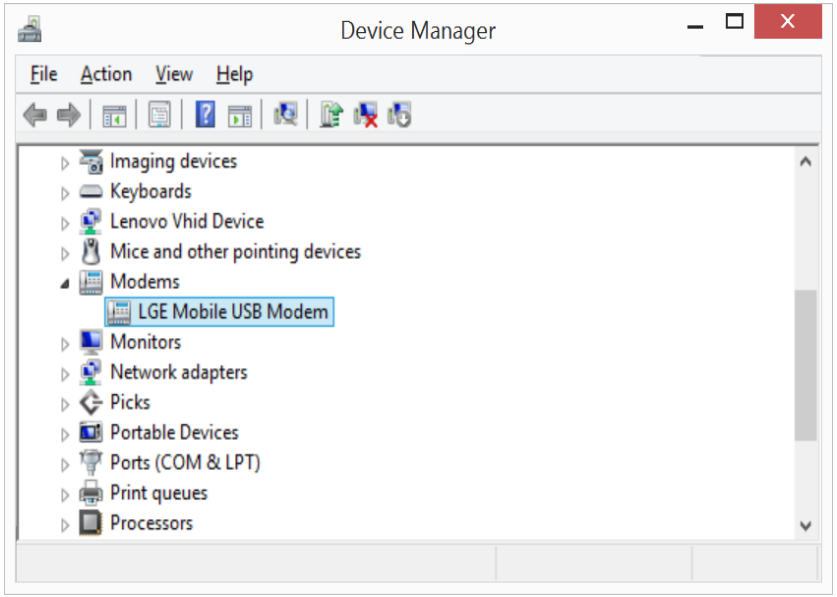




Мобильный Криминалист

http://www.мобильный-криминалист.рф

Уязвимость модема LG



Мобильный Криминалист

http://www.мобильный-криминалист.рф

LG Firmware Update Mode

- Чтение/Запись ROM
- root shell

Мобильный Криминалист

http://www.мобильный-криминалист.рф

LG Firmware Update Mode

- Модификация System
- Дамп KeyStore data
- bruteforce
- Восстановление System

Мобильный Криминалист

http://www.мобильный-криминалист.рф

LG Firmware Update Mode

- Чтение текущего состояния
- Подбор пароля
- Восстановление состояния
- Подбор пароля

…

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Уязвимость в загрузчике Motorola

CVE-2016-10277

Bootloader Kernel
cmdline Injection

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Samsung custom recovery

- В международной версии по умолчанию разблокирован загрузчик
- Дамп KeyStore data
- bruteforce

Samsung custom recovery

- Octoplus box
- отключение FRP
- UART mode
- прошивка специального boot

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Samsung T-Flash Bootloader Buffer Overflow

- SVE-2016-7930
- Запуск неподписанного образа с внешней SD-карты
- KNOX Safe

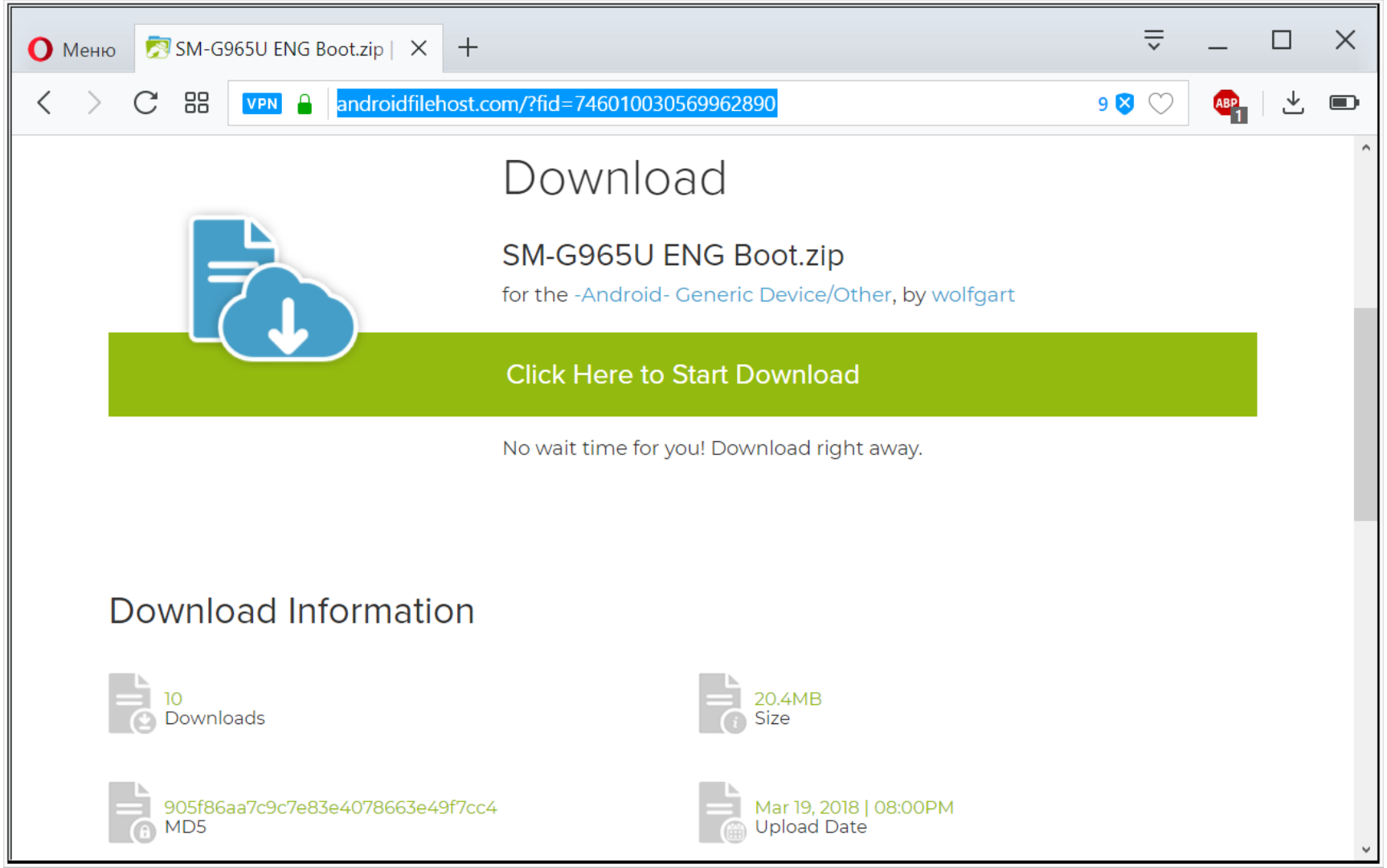
Мобильный Криминалист

http://www.мобильный-криминалист.рф

Samsung ENG BOOT

- Включен ADB
- root shell

Мобильный Криминалист

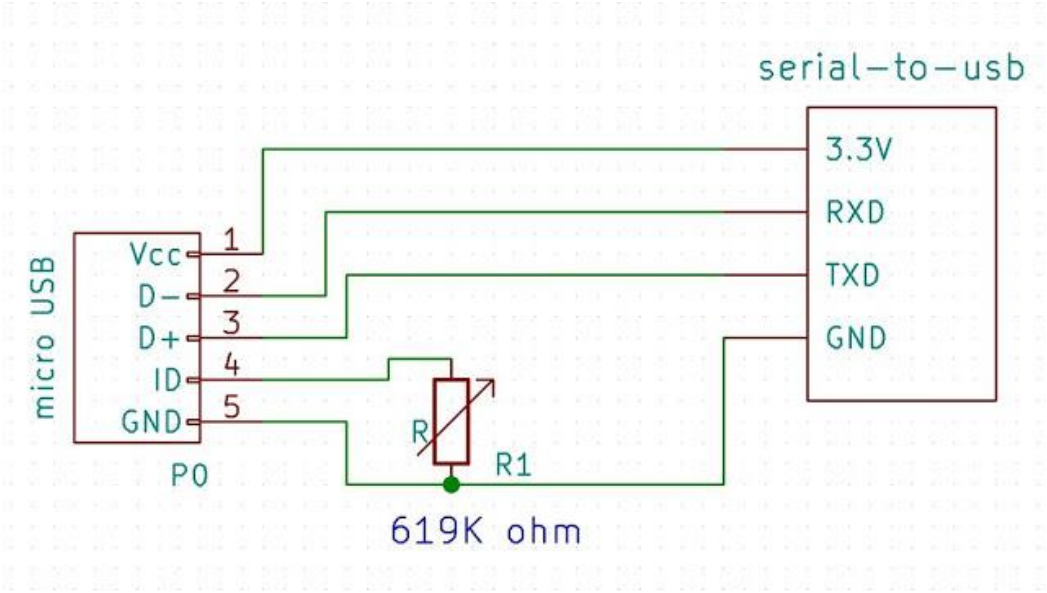

Меню
SM-G965U ENG Boot.zip |
VPN
androidfilehost.com/?fid=746010030569962890
Download
SM-G965U ENG Boot.zip
for the -Android- Generic Device/Other, by wolfgart
Click Here to Start Download
No wait time for you! Download right away.
Download Information
10
Downloads
20.4MB
Size
905f86aa7c9c7e83e4078663e49f7cc4
MD5
Mar 19, 2018 | 08:00PM
Upload Date

Уязвимость Samsung SBOOT

Мобильный Криминалист

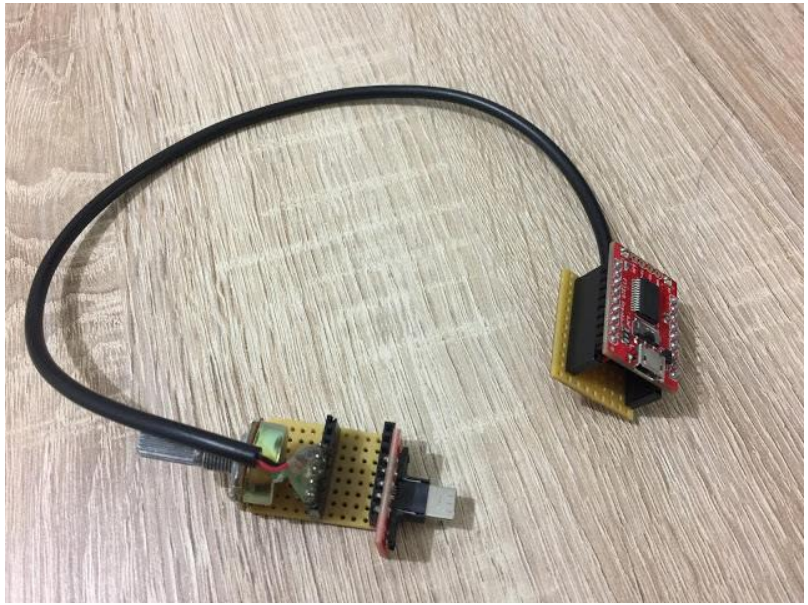
http://www.мобильный-криминалист.рф

Уязвимость Samsung SBOOT



Мобильный Криминалист

Уязвимость Samsung SBOOT



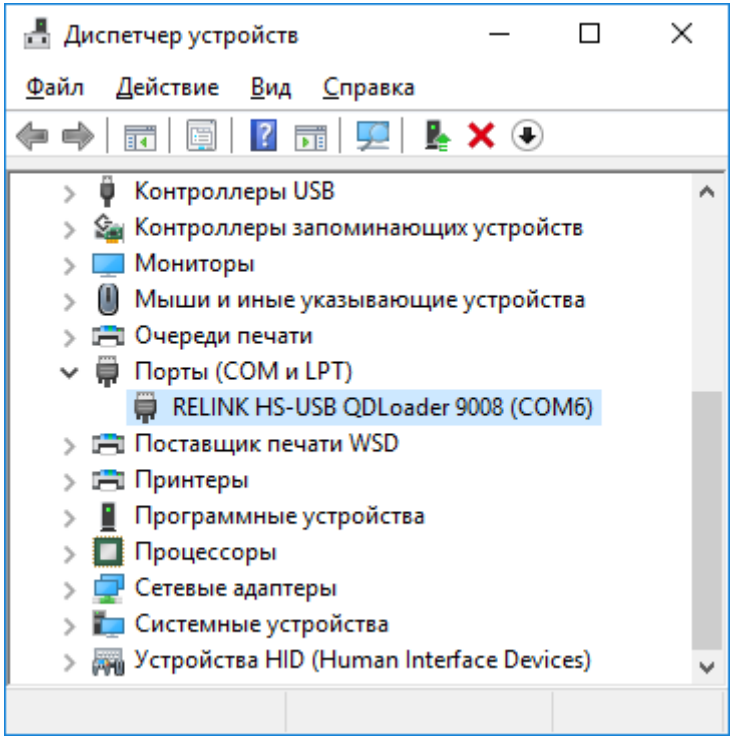
Китайские MTK/SPD Android-устройства

- Проприетарные протоколы Чтения/Записи
- Не у всех устройств есть поддержка шифрования

Мобильный Криминалист

Qualcomm EDL режим

- Протоколы
  Firehose, Sahara



Мобильный Криминалист

Современные подходы к извлечению данных из Android-устройств

- Уязвимости в загрузчике
- Уязвимости в проприетарных протоколах

Что осталось за кадром

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Мобильный Криминалист

Спасибо за внимание!
Вопросы?

Карондеев Андрей Михайлович
karondeev@oxygensoftware.com