Мобильный Криминалист

Особенности извлечения данных из мобильных устройств

Карондеев А.М.

Методы извлечения данных из мобильных устройств

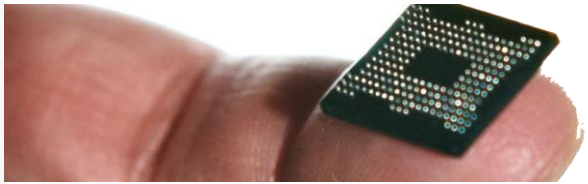
- Аппаратные (Физические)
- Программные
- Программно-аппаратные

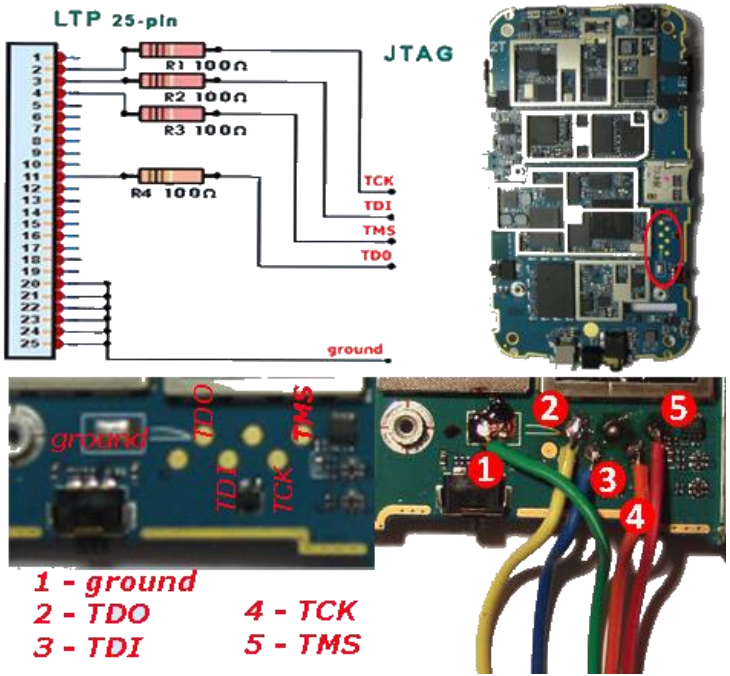
Мобильный Криминалист

http://www.мобильный-криминалист.рф

Аппаратные методы

- Chip-off
- JTAG
- ISP





Мобильный Криминалист

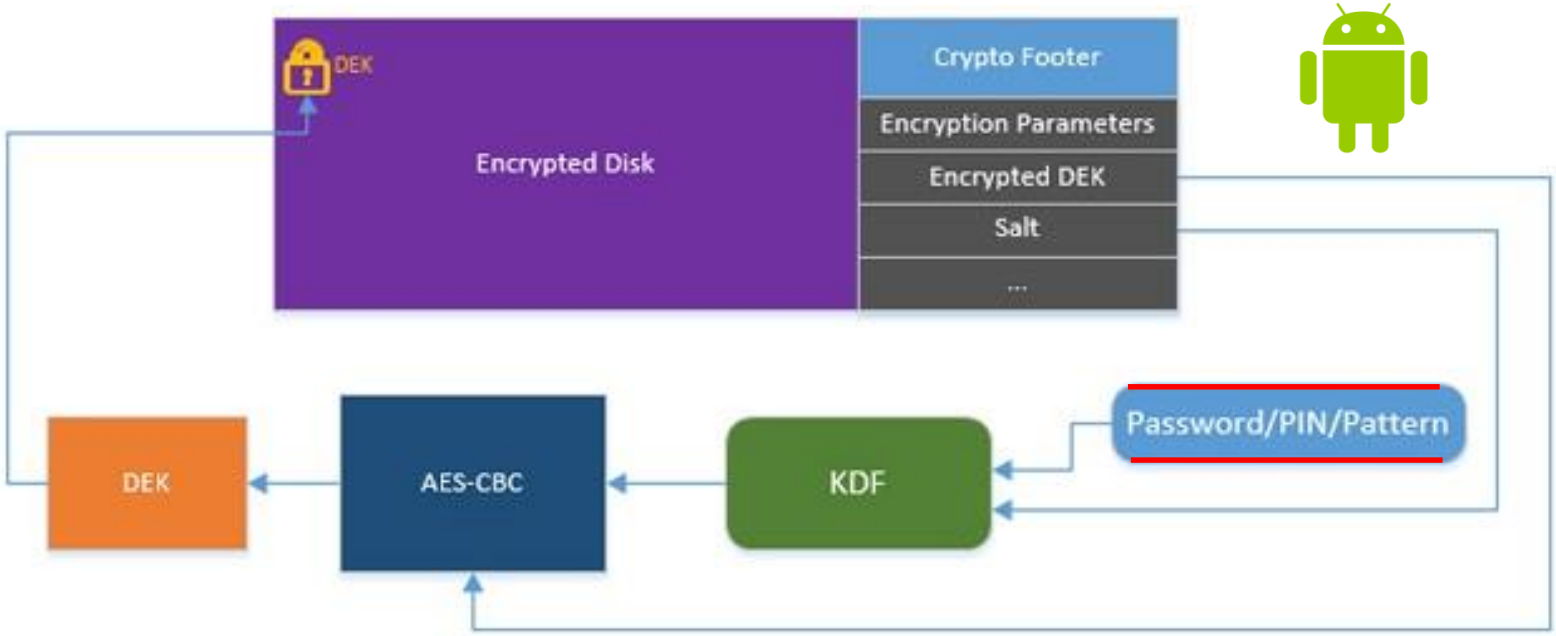
http://www.мобильный-криминалист.рф

Полнодисковое шифрование

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Полнодисковое шифрование

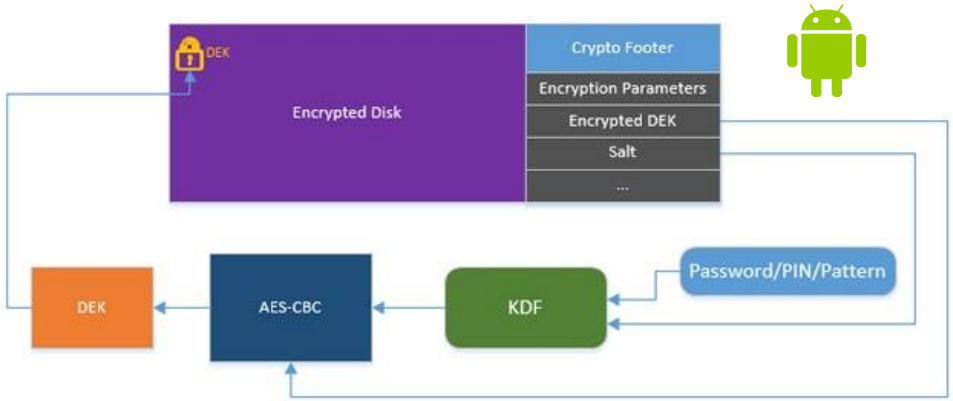


Мобильный Криминалист

http://www.мобильный-криминалист.рф

Расшифровывание данных

- Спросить пароль
- Атака грубой силой
- Словарная атака



Мобильный Криминалист

http://www.мобильный-криминалист.рф

Атака грубой силой

- Требует много времени
- Человеческий фактор
- Успех не гарантирован
  (за разумное время)

Мобильный Криминалист

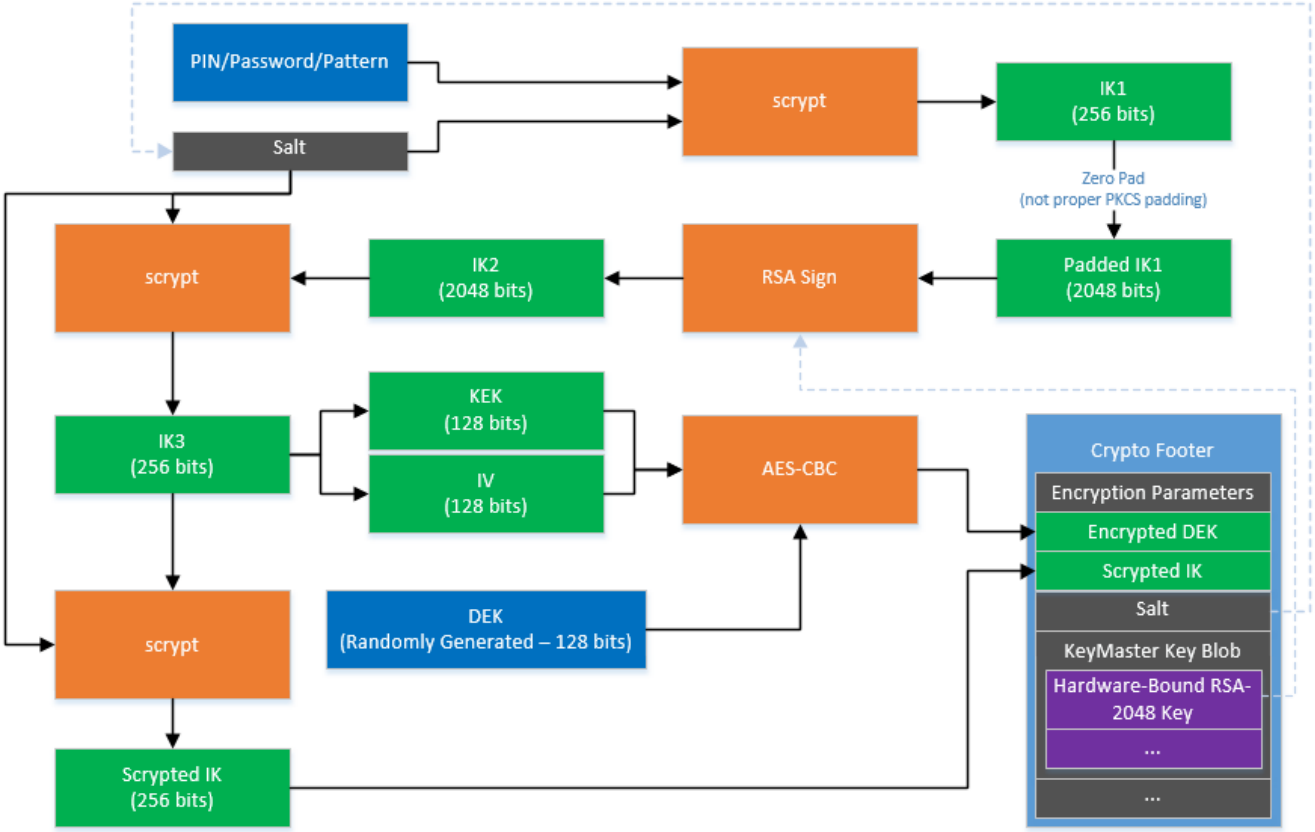
http://www.мобильный-криминалист.рф

Словарная атака

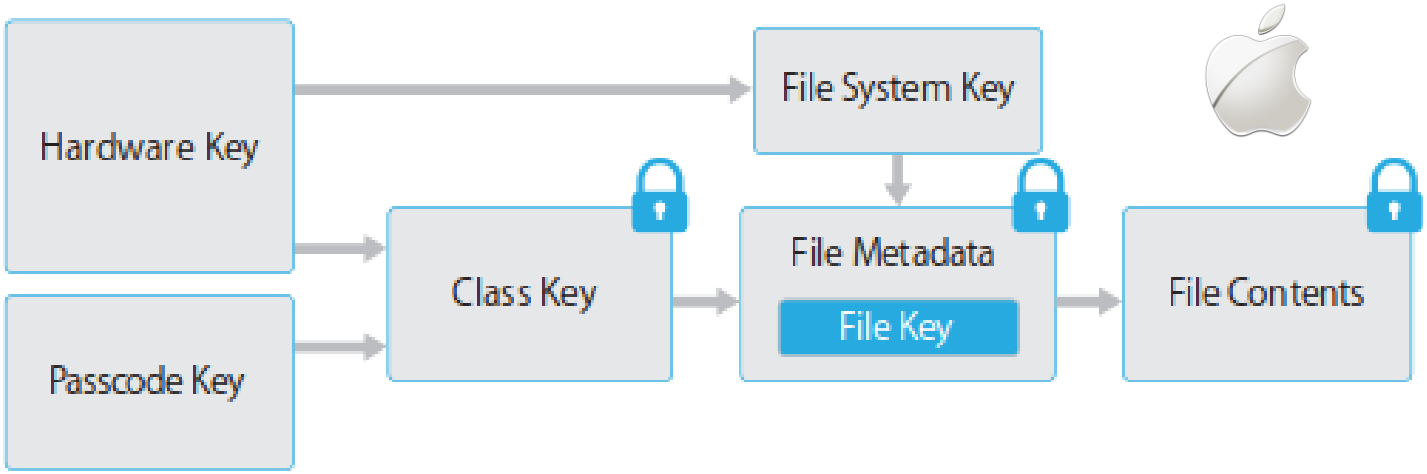
- Человеческий фактор
- Эффективность зависит от знания информации о владельце

Схожие пароли

Шифрование с аппаратным ключом



Шифрование с аппаратным ключом



Шифрование с аппаратным ключом

- Аппаратных методов недостаточно
  - Программные методы
  - Программно-аппаратные методы

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Программные методы

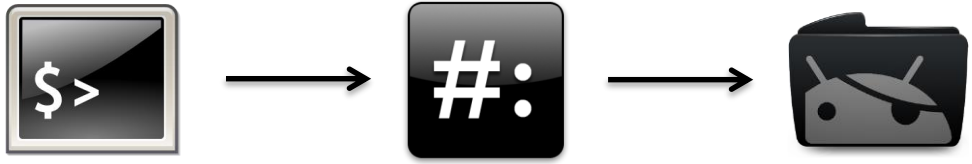
- Уязвимости в ОС
- Кастомный recovery

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Уязвимости в ОС

- Получение доступа Linux shell
- Повышение привилегий
- Чтение памяти

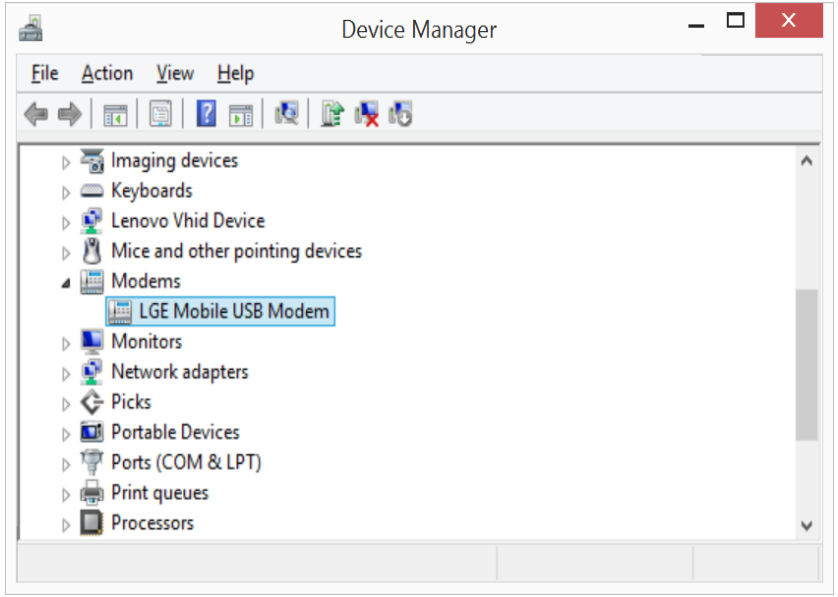


Получение доступа Linux shell

- Screen Lock

Мобильный Криминалист

Уязвимость модема LG



Мобильный Криминалист

http://www.мобильный-криминалист.рф

Уязвимость MTP Samsung

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Уязвимость интерфейса Android

- https://www.youtube.com/watch?v=J-pFCXEqB7A
- https://geektimes.ru/post/262574/

Мобильный Криминалист

Уязвимость интерфейса iOS

- https://xakep.ru/2016/11/18/ios-lockscreen-bypass-2/
- https://www.youtube.com/watch?v=LWJG5I8xCDU

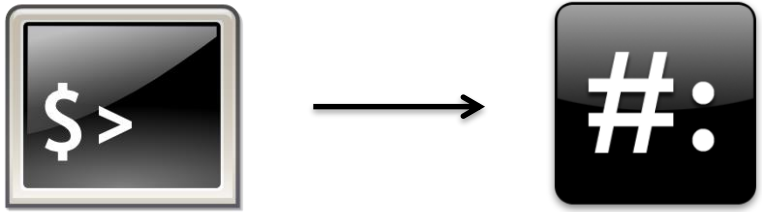
Уязвимость интерфейса iOS

- https://xakep.ru/2016/12/02/activation-lock-bypass/
- https://www.youtube.com/watch?v=yygvBJBFy4s

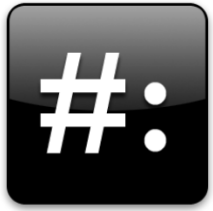
Мобильный Криминалист

Повышение привилегий

- CVE-2014-3153
- CVE-2015-3636
- CVE-2015-1805
- CVE-2016-5195



Кастомный recovery



Проприетарные протоколы

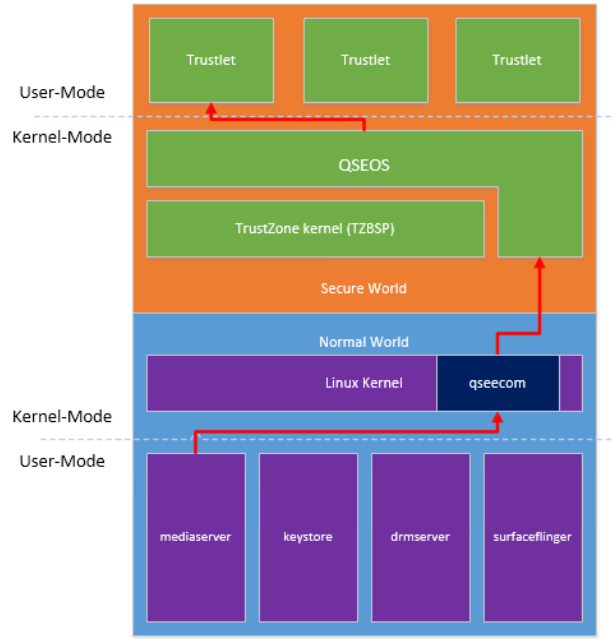
- Download Mode MTK
- Download Mode Spreadtrum
- Firmware Update Mode LG
- Advanced Logical iOS < 8.3

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Программно-аппаратные методы

- Аппаратные уязвимости
- CVE-2015-6639
- CVE-2016-2431



Подведем Итоги

Рассмотрены различные методы извлечения данных из мобильных устройств, а также особенности их использования с учетом современных методов защиты таких как Screen Lock и Full Disk Encryption

Мобильный Криминалист

http://www.мобильный-криминалист.рф

Спасибо за внимание!
Вопросы?

Карондеев Андрей Михайлович
karondeev@oxygensoftware.com