Mobile Forensics Day 2020
Сентябрь 2020, Москва

ELCOMSOFT

Мастер-класс: извлечение данных из Apple iPhone

Извлечение данных из iPhone

С чего начать?

- **Документировать все шаги!**
- Отключить автоматическую блокировку экрана, если разблокирован
- Если заблокирован, проверить наличие пасскода (не использовать Touch ID / Face ID!)
- Перевести телефон в авиарежим, если возможно (если нет, поместить в клетку Фарадея)
- **Не вытаскивать сим-карту**
- Не выключать, если включен
- Определить модель (Axxx на задней крышке; *может не соответствовать действительности*)
- Если пасскод неизвестен, выяснить доступность компьютеров, с которыми могли быть установлены доверенные отношения
- Определить серийный номер и IMEI, если аппарат выключен:

  https://blog.elcomsoft.ru/2020/02/rol-speczialnyh-rezhimov-ios-v-mobilnoj-kriminalistike-dfu-recovery-i-sos/
- Возможно запросить данные у Apple (из iCloud), по серийному номеру или IMEI
- *Собрать максимум данных о владельце телефона*

Извлечение данных из iPhone

Что можно сделать?

- iPhone 4, iPhone 4s, iPhone 5, iPhone 5c: практически всё ☺
- iPhone 5s, iPhone 6, iPhone 6s, iPhone SE, iPhone 7, iPhone 8, iPhone X:
  - работает эксплойт checkm8
  - возможно частичное извлечение при неизвестном пасскоде
  - совместимость от iOS 12.3 (и до 13.7), иначе общий случай
- iPhone 5s .. iPhone X, iOS 9.0 .. 12.2: извлечение с помощью агента (12.3 – 12.4.8 тоже поддерживаются)
- iPhone Xr, iPhone Xs, iPhone 11, iPhone SE 2020: извлечение с помощью агента (iOS 13.0 .. 13.5)

Извлечение данных из iPhone

iPhone 5s .. iPhone 11

- iPhone 5s .. iPhone X, iOS 12.3+: извлечение checkm8 (рекомендуется Oxygen) или checkra1n
- checkra1n: некоторые особенности и рекомендации
  - Ввод в DFU через Recovery
  - Никаких хабов
  - Кабель Lightning to USB-A (желательно оригинальный)
  - Достаточный заряд (20%+, не в режиме энергосбережения)
  - Может понадобиться несколько попыток (на разных компьютерах с разными кабелями)
  - Может понадобиться перезагрузка компьютера и/или телефона
- Извлечение агентом
  - Рекомендуется учётка разработчика
  - Обычная учётная запись: только macOS; необходимо ограничить сетевые соединения
- **Обязательно извлечь keychain**

Извлечение данных из iPhone

iPhone 5s .. iPhone 11

DEMO

Извлечение данных из iPhone

iPhone 5/5c – взлом пасскода

- Поддерживаются все версии iOS (от 6.0 до 10.3.4)
- Скорость перебора около 15 п/с
  - 4 цифры: около 10 минут
  - 6 цифр: около 20 часов
- Перебор возможен, даже если устройство заблокировано после 10 попыток
  - *отключение блокировки возможно*
- Полное извлечение файловой системы в процессе реализации
- Поддержка iPhone 4s будет
- *iPhine 5s+: нет, этот метод не сработает*

Извлечение данных из iPhone

iPhone 5/5c – взлом пасскода

DEMO

Вопросы?

Vladimir Katalov, ElcomSoft Co. Ltd.

http://www.elcomsoft.ru
https://blog.elcomsoft.ru

Facebook: ElcomSoft
Twitter: @elcomsoft