# Анализ шифрования резервной копии Huawei

Дина Дмитриевна Фунт, 17.Б11-мм

Научный руководитель: доц., к.т.н. Ю.В. Литвинов
Консультант: разработчик ПО, ООО “Белкасофт” М.В. Виноградов

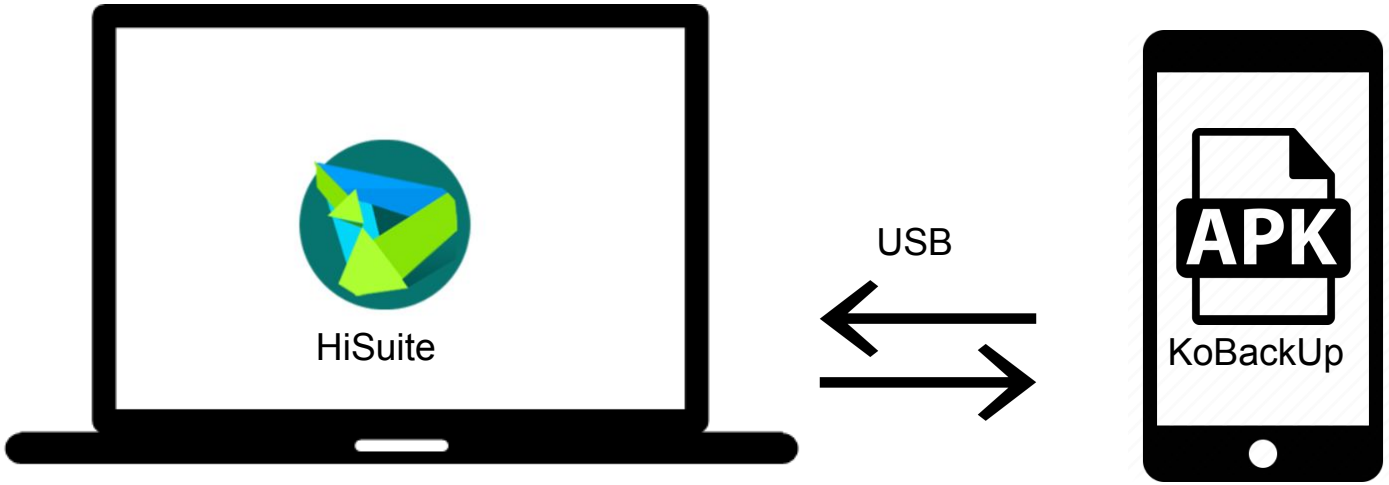
# Введение

- Цифровая криминалистика
- Доля устройств Huawei на рынке велика
- Извлечение данных из резервных копий

# Создание резервной копии Huawei

Резервное копирование с шифрованием:

1. На основе пароля, введенного пользователем
2. Без пользовательского пароля



# Основополагающее исследование [1]

- Описаны алгоритмы шифрования в случае шифрования с пользовательским паролем
- Предложены алгоритмы дешифрования
- Не описан случай, когда пароль не задан

| Encryption Algorithm |
| --- |
| AES128-CTR(*P*, *Key*, *Counter*) |
| AES256-CTR(*P*, *Key*, *Counter*) |

[1] “Decrypting password-based encrypted backup data for Huawei smartphones” / Myungseo Park, Giyoon Kim, Younjai Park et al.

# Поставленные задачи

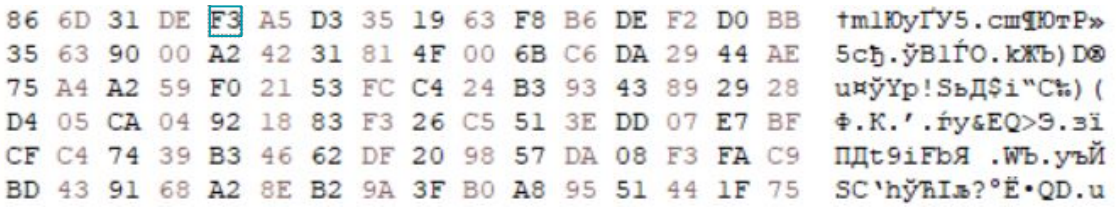
**Цель**: Исследовать механизм создания резервных копий телефонов Huawei в случае, когда пароль не задан пользователем

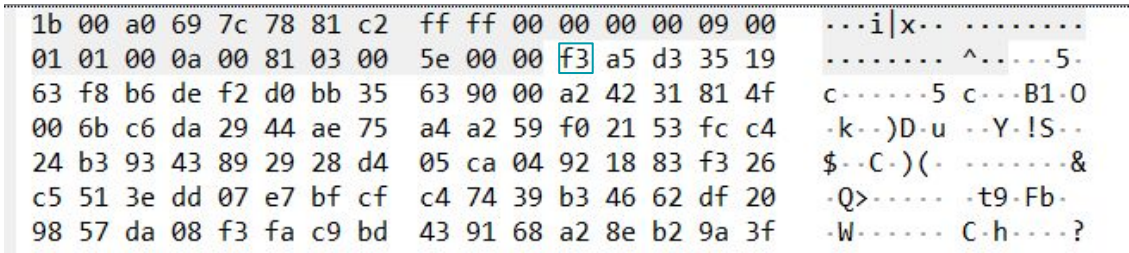
**Задачи**:

1. Проанализировать приложение для компьютера
2. Проанализировать приложение на смартфоне с целью выявления применяемых алгоритмов шифрования
3. Проанализировать USB трафик между ними
4. Разработать инструмент, дешифрующий данные резервной копии

# Исследования. HiSuite для Windows

- Анализ USB трафика
  - запросы шифрованные
- Анализ HiSuite
  - отсутствие отладочных символов
  - код обфусцирован



# Исследования. HiSuite для Mac OS

- Анализ USB трафика
  - аналогичен трафику на Windows
- Анализ HiSuite
  - имеет отладочные символы
  - не обфусцирован
  - возможность преобразования в псевдокод на Objective-C
  - обнаружен метод, устанавливающий пароль

# Исследования. Анализ KoBackup

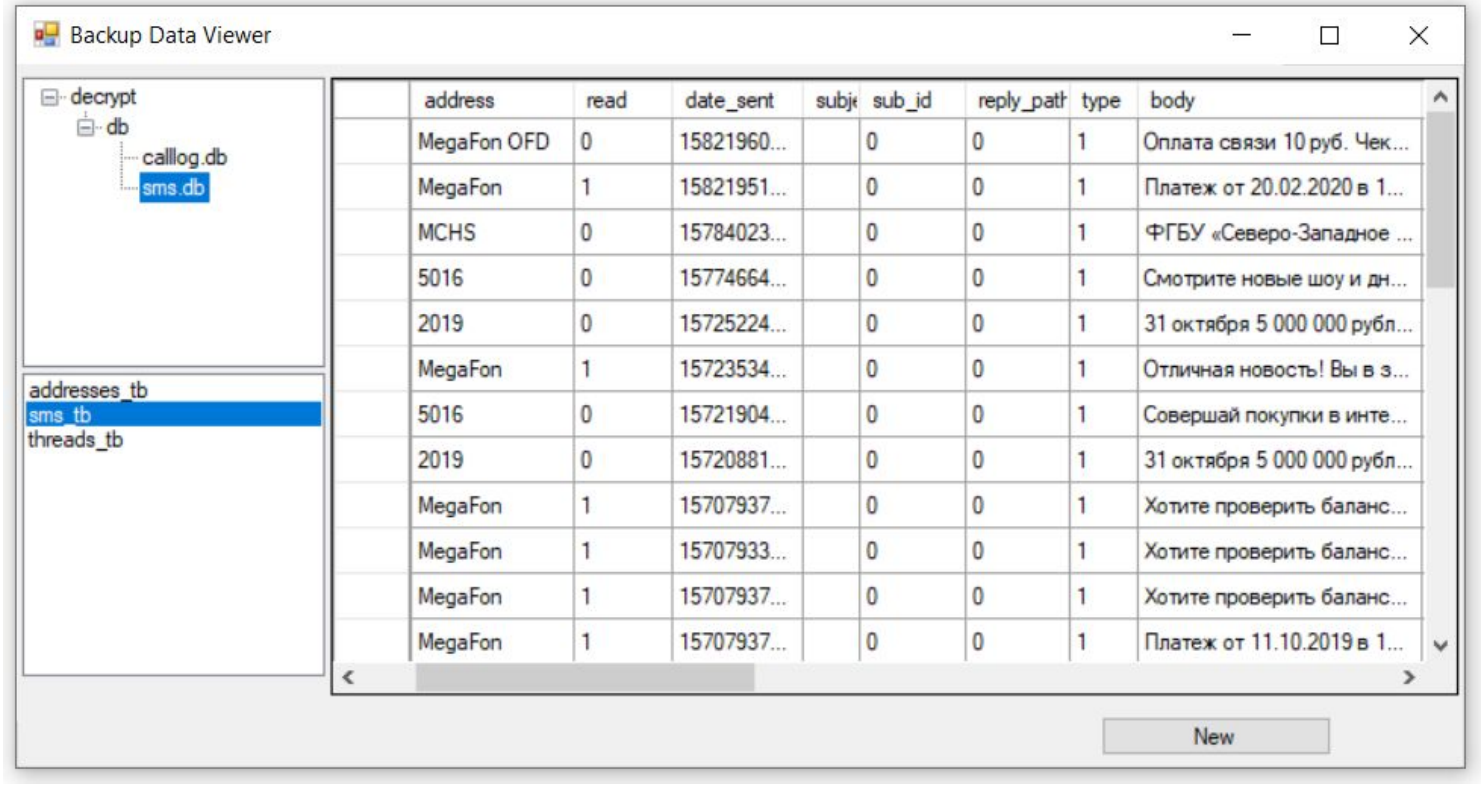
- Анализ кода приложения
  - определен метод шифрования
  - обнаружен метод, устанавливающий пароль
- Дизассемблирование приложения
  - инструмент apktool
  - получен код на smali
- Модификация, сборка
  - добавлен метод android.util.Log.e()
  - инструмент apktool

# Исследования. Установка KoBackup

- Установка
  - ADB
  - проблема несовместимости сертификатов
  - отключение проверок безопасности Android (Lucky Patcher)
- Вывод пароля в журнал

```
03-26 11:48:33.786  2079  7175 W BackupModule: delete file fail : /storage/emulated/0/Android/data/com.huawei.hisuite/cache/MicroMsg

03-26 11:48:33.789  7392  7406 E HwBackup8.0.1.306_OVE: [BackupPasswordHere]: 123456

03-26 11:48:33.797  7392  7406 I HwBackup8.0.1.306_OVE: [BackupLogicService]: handleMessage callback,msg.what=28, msg.arg1=0, msg.arg2=0,

03-26 11:48:33.797  7392  7406 I HwBackup8.0.1.306_OVE: [PMSUtil]: finishBackupSessionMethod :true

03-26 11:48:33.797  7392  7406 I HwBackup8.0.1.306_OVE: [BackupObject]:  moduleName = sms
```

# Проверка результатов



# Результаты

1. Определены алгоритмы шифрования, используемые в создании резервных копий без пользовательского пароля

2. Получена строка, используемая в качестве пароля

3. Предложены алгоритмы для расшифровки резервных копий

4. Реализовано тестовое приложение для дешифрации данных, с использованием предложенных алгоритмов

(https://github.com/DinaFunt/HuaweiBackupViewer)