

# 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

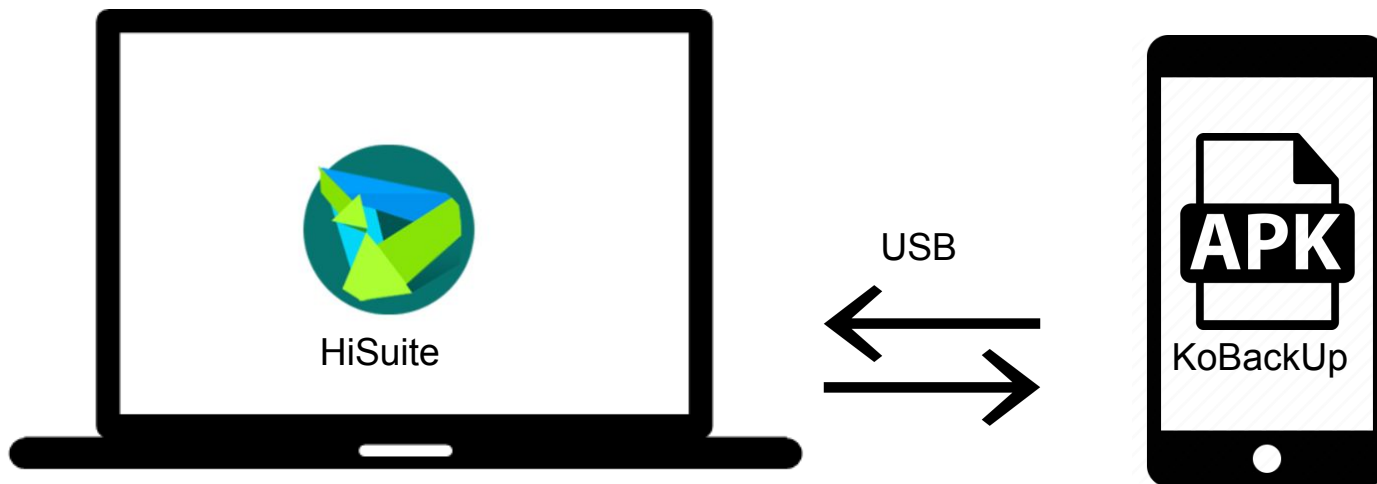
# Введение

- 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 зашифрованные
- Анализ HiSuite
  - отсутствие отладочных СИМВОЛОВ
  - код обфусцирован

```
86 6D 31 DE F3 A5 D3 35 19 63 F8 B6 DE F2 D0 BB  tmlЮyГY5.смЮтP»
35 63 90 00 A2 42 31 81 4F 00 6B C6 DA 29 44 AE  5сЪ.ÿB1ГO.кЖЪ)D@
75 A4 A2 59 F0 21 53 FC C4 24 B3 93 43 89 29 28  uкÿYp!СьД$i"С%) (
D4 05 CA 04 92 18 83 F3 26 C5 51 3E DD 07 E7 BF  ф.К.' .fy&EQ>Э.зі
CF C4 74 39 B3 46 62 DF 20 98 57 DA 08 F3 FA C9  ПДт9iFbЯ .WЪ.уьЙ
BD 43 91 68 A2 8E B2 9A 3F B0 A8 95 51 44 1F 75  SC`hÿhIъ?°Ë•QD.u
```

```
1b 00 a0 69 7c 78 81 c2 ff ff 00 00 00 00 09 00  ...i|x.. .....
01 01 00 0a 00 81 03 00 5e 00 00 f3 a5 d3 35 19  ..... ^.....5.
63 f8 b6 de f2 d0 bb 35 63 90 00 a2 42 31 81 4f  c.....5 c...B1-0
00 6b c6 da 29 44 ae 75 a4 a2 59 f0 21 53 fc c4  .k..)D.u ..Y.!S..
24 b3 93 43 89 29 28 d4 05 ca 04 92 18 83 f3 26  $.-C.)(. .....&
c5 51 3e dd 07 e7 bf cf c4 74 39 b3 46 62 df 20  .Q>..... -t9.Fb.
98 57 da 08 f3 fa c9 bd 43 91 68 a2 8e b2 9a 3f  .W..... C.h....?
```

# 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 KoVascur

- 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

Backup Data Viewer

decrypt  
db  
  calllog.db  
  sms.db

addresses\_tb  
sms\_tb  
threads\_tb

|  | address     | read | date_sent   | subje | sub_id | reply_patr | type | body                         |
|--|-------------|------|-------------|-------|--------|------------|------|------------------------------|
|  | MegaFon OFD | 0    | 15821960... |       | 0      | 0          | 1    | Оплата связи 10 руб. Чек...  |
|  | MegaFon     | 1    | 15821951... |       | 0      | 0          | 1    | Платеж от 20.02.2020 в 1...  |
|  | MCHS        | 0    | 15784023... |       | 0      | 0          | 1    | ФГБУ «Северо-Западное ...    |
|  | 5016        | 0    | 15774664... |       | 0      | 0          | 1    | Смотрите новые шоу и дн...   |
|  | 2019        | 0    | 15725224... |       | 0      | 0          | 1    | 31 октября 5 000 000 рубл... |
|  | MegaFon     | 1    | 15723534... |       | 0      | 0          | 1    | Отличная новость! Вы в з...  |
|  | 5016        | 0    | 15721904... |       | 0      | 0          | 1    | Совершай покупки в инте...   |
|  | 2019        | 0    | 15720881... |       | 0      | 0          | 1    | 31 октября 5 000 000 рубл... |
|  | MegaFon     | 1    | 15707937... |       | 0      | 0          | 1    | Хотите проверить баланс...   |
|  | MegaFon     | 1    | 15707933... |       | 0      | 0          | 1    | Хотите проверить баланс...   |
|  | MegaFon     | 1    | 15707937... |       | 0      | 0          | 1    | Хотите проверить баланс...   |
|  | MegaFon     | 1    | 15707937... |       | 0      | 0          | 1    | Платеж от 11.10.2019 в 1...  |

New

# 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>)