ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

Дисциплина:

«Обеспечение информационной безопасности мобильных устройств»

ОТЧЕТ ПО ЛАБАРАТОРНОЙ РАБОТЕ №5

«Форензика в области безопасности мобильных приложений и используемый для этого инструментарий»

Выполнил:

Гаврилова В. В., студент группы N33471

(подпись)

Проверил:

Федоров Иван Романович

24.03.2022

(отметка о выполнении)

(подпись)

Санкт-Петербург

2022г.

Содержание

1. Цель работы

Ознакомиться с форензикой в области безопасности мобильных приложений и используемыми для этого инструментарий.

2. Основная часть

1) Извлечение данных из эмулятора

```
MBP-Veronika:~ veronikagavrilova$ adb backup -apk -shared -all -system
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
MBP-Veronika:~ veronikagavrilova$
```

Рисунок 1 – Физический бэкап через adb shell

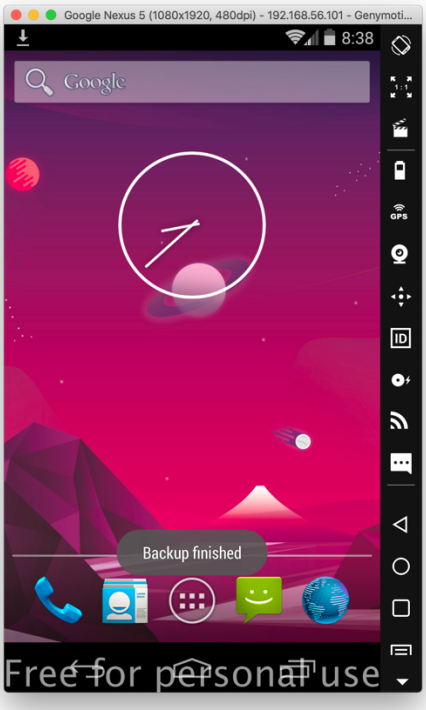

Рисунок 2 – Сообщение об успешности бэкапа

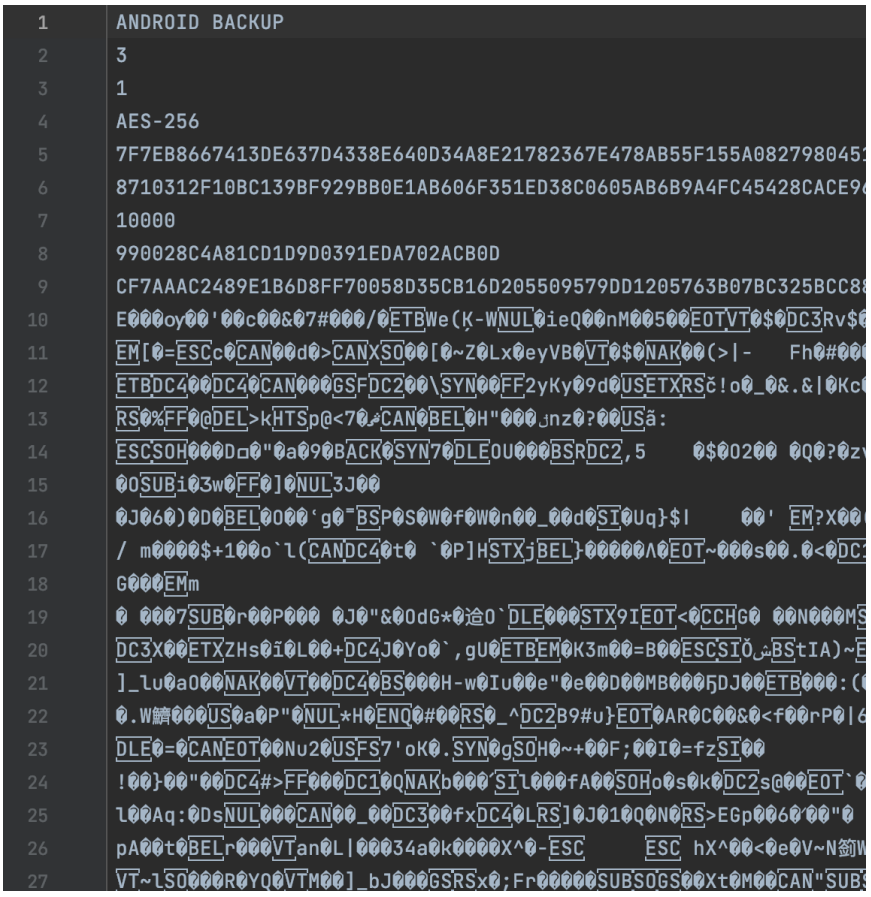

Рисунок 3 – Файл бэкапа отрытый в Android Studio

```
[MBP-Veronika:executable veronikagavrilova$ adb devices
 List of devices attached
 192.168.56.102:5555     device

[MBP-Veronika:executable veronikagavrilova$ adb connect 192.168.56.102
 already connected to 192.168.56.102:5555
[MBP-Veronika:executable veronikagavrilova$ adb backup -apk -shared -all -system
 WARNING: adb backup is deprecated and may be removed in a future release
 Now unlock your device and confirm the backup operation...
[MBP-Veronika:executable veronikagavrilova$ java -jar abp.jar unpack backup.ab backup.tar 2002
[MBP-Veronika:executable veronikagavrilova$ java -jar abp.jar unpack backup1.ab backup1.tar 2002
[MBP-Veronika:executable veronikagavrilova$ tar -xvf backup.tar
 x apps/android/_manifest
```

Рисунок 4 – Распаковка

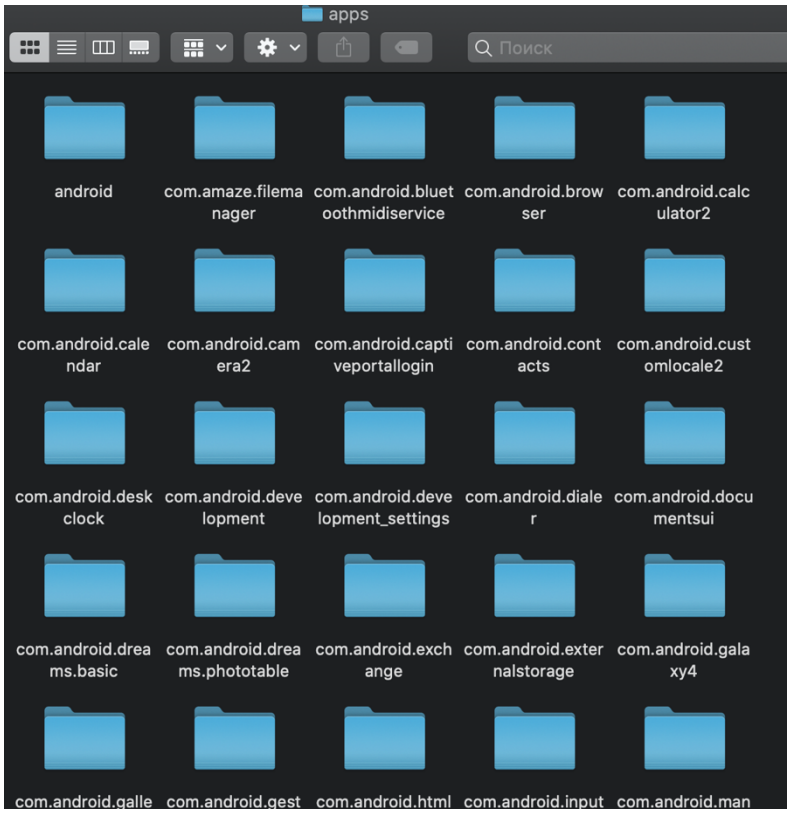

Рисунок 5 – Полученные данные бэкапа

2) Вывод данных из изображения

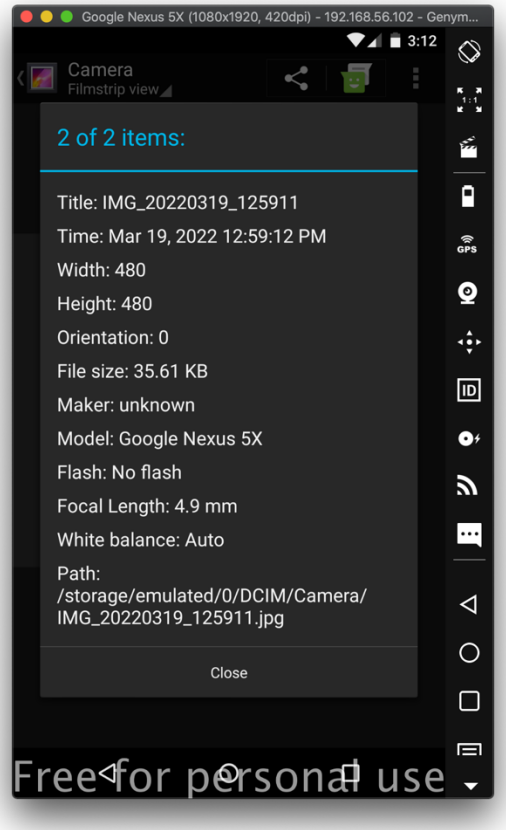

Рисунок 6 - Метаданные на устройстве

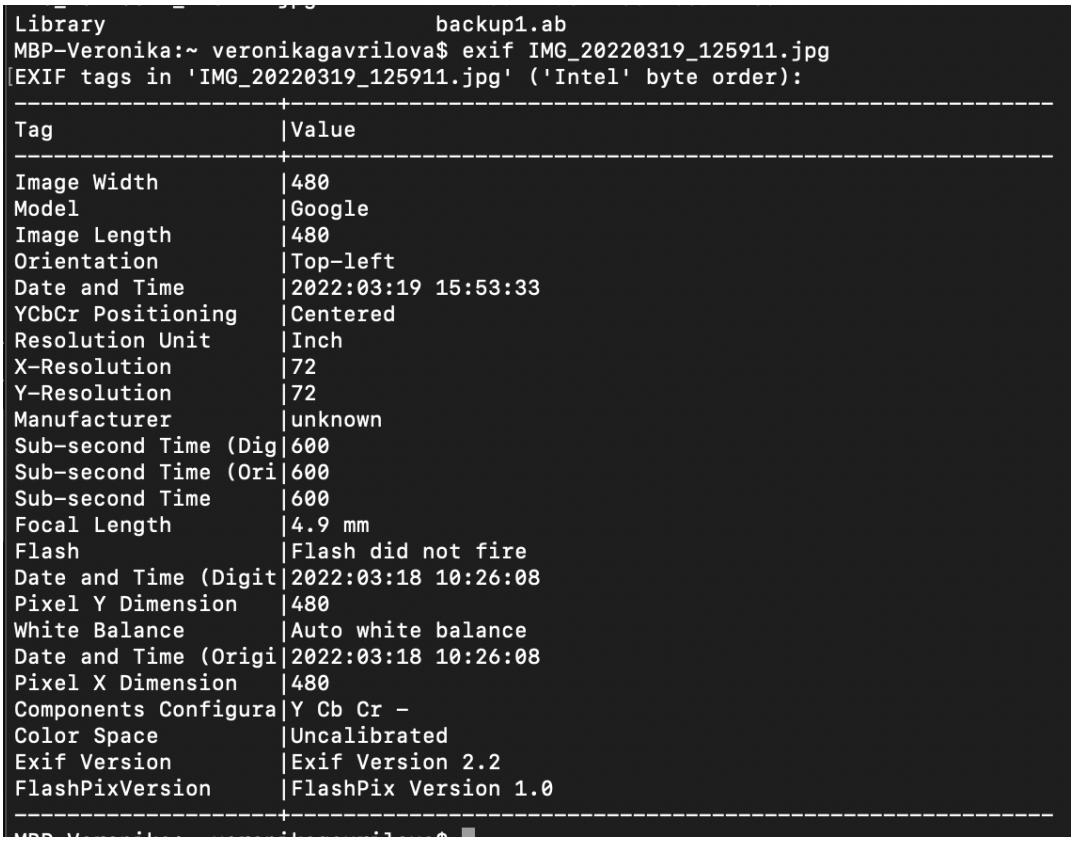

Рисунок 7 – Метаданные полученные утилитой exif

3. Вывод

В результате выполнения работы я ознакомилась с форензикой в области безопасности мобильных приложений и используемыми для этого инструментарий.