

**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

2. Основная часть

3. Выводы

## 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

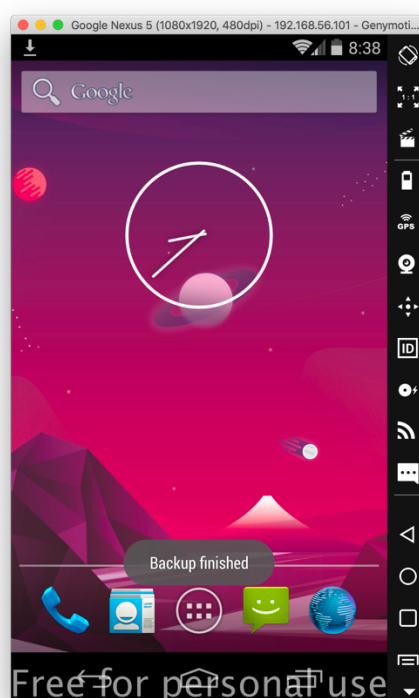


Рисунок 2 – Сообщение об успешности бэкапа

```
[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 3 – Распаковка

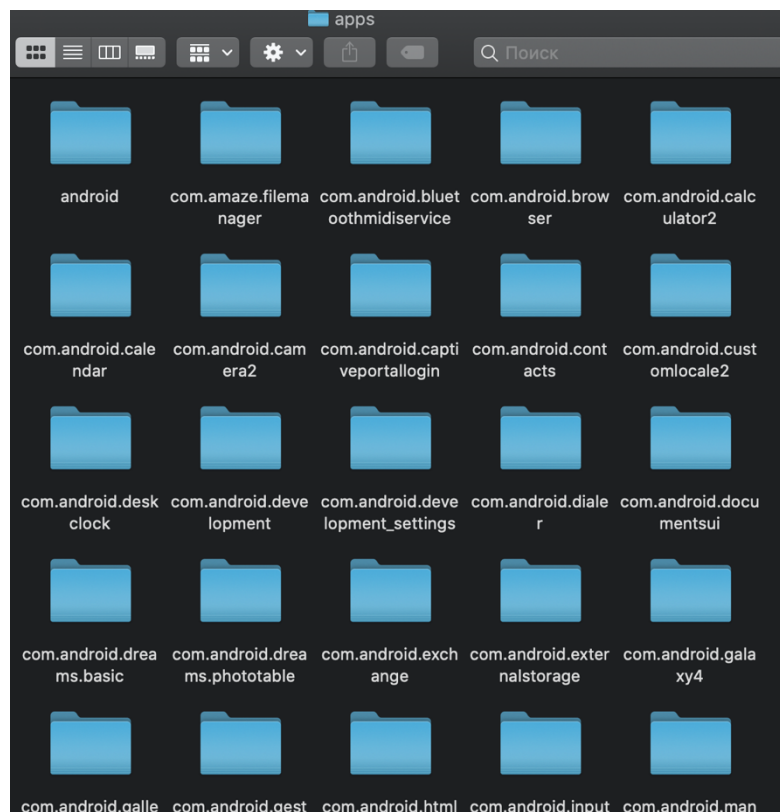


Рисунок 4 – Полученные данные бэкапа

## 2) Вывод данных из изображения

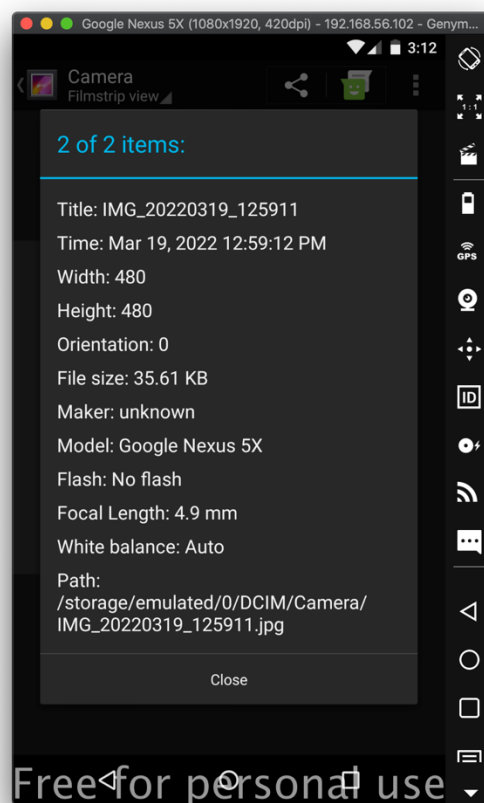


Рисунок 5 - Метаданные на устройстве

```

Library backup1.ab
MBP-Veronika:~ veronikagavrilova$ exif IMG_20220319_125911.jpg
[EXIF tags in 'IMG_20220319_125911.jpg' ('Intel' byte order):]
-----+-----
Tag | Value
-----+-----
Image Width | 480
Model | Google
Image Length | 480
Orientation | Top-left
Date and Time | 2022:03:19 15:53:33
YCbCr Positioning | Centered
Resolution Unit | Inch
X-Resolution | 72
Y-Resolution | 72
Manufacturer | unknown
Sub-second Time (Dig | 600
Sub-second Time (Ori | 600
Sub-second Time | 600
Focal Length | 4.9 mm
Flash | Flash did not fire
Date and Time (Digit | 2022:03:18 10:26:08
Pixel Y Dimension | 480
White Balance | Auto white balance
Date and Time (Orig | 2022:03:18 10:26:08
Pixel X Dimension | 480
Components Configura | Y Cb Cr -
Color Space | Uncalibrated
Exif Version | Exif Version 2.2
FlashPixVersion | FlashPix Version 1.0
-----+-----

```

Рисунок 6 – Метаданные, полученные утилитой exif

The screenshot shows the Magnet AXIOM Examine v4.10.0.23663 interface. The main window displays a list of evidence items under the 'EVIDENCE (299)' tab. The selected item is 'IMG\_20220319\_155333.jpg'. The right-hand pane shows detailed metadata for this file, including file extension, last modified date/time, size, skin tone percentage, original width/height, exif extraction status, created/modified dates, make/model, exif data, MD5 hash, and SHA1 hash.

Item	Type
16477052...	Pictures
IMG_2022...	Pictures
IMG_2022...	Pictures
1619	Pictures
1078	Pictures
1548	Pictures
1748	Pictures
1028	Pictures
1290	Pictures
5069	Pictures
1749	Pictures
1770	Pictures
2062	Pictures
2042	Pictures
2033	Pictures
2014	Pictures

Property	Value
File Extension	.jpg
Last Modified Date/Time	19.03.2022 15:53:33
Size (Bytes)	3923
Skin Tone Percentage	0.0
Original Width	480
Original Height	480
Exif Extraction Status	Complete
Created Date/Time - Local Time	18.03.2022 10:26:08 (Local time)
Modified Date/Time - Local Time	19.03.2022 15:53:33 (Local time)
Make	unknown
Model	Google
Exif Data	Extraction Result: Complete ImageWidth: 480 ImageHeight: 480 DateTimeOriginal: 03/18/2022 10:26:08 CreateDate: 03/18/2022 10:26:08 ModifyDate: 03/19/2022 15:53:33 Make: unknown Model: Google
MD5 Hash	8bd808cee5ea818087b2d5cb1c6c0f8e
SHA1 Hash	b6bfd00fce453c7d1a49cfe5d066f273683b5

Рисунок 7 – Метаданные в Аxiom

Далее необходимо извлечь информацию об устройстве по фото из hex данных. Откроем бэкап в hex-редакторе Hex Fiend.

Для того чтобы узнать jpeg файл в hex редакторе, необходимо узнать его сигнатуру. Обратимся к статье <https://www.file-recovery.com/jpg-signature-format.htm> :





Размеры: 480 x 480  
Изготовитель устройства: unknown  
Модель устройства: Google  
Цветовое пространство: RGB  
Цветовой профиль: sRGB IEC61966-2.1  
Фокусное расстояние: 4,9 мм  
Альфа-канал: Нет  
Красные глаза: Нет

▼ Имя и расширение:

Untitled.jpeg

☐ Скрыть расширение

▼ Комментарии:

> Открывать в приложении:

▼ Просмотр:

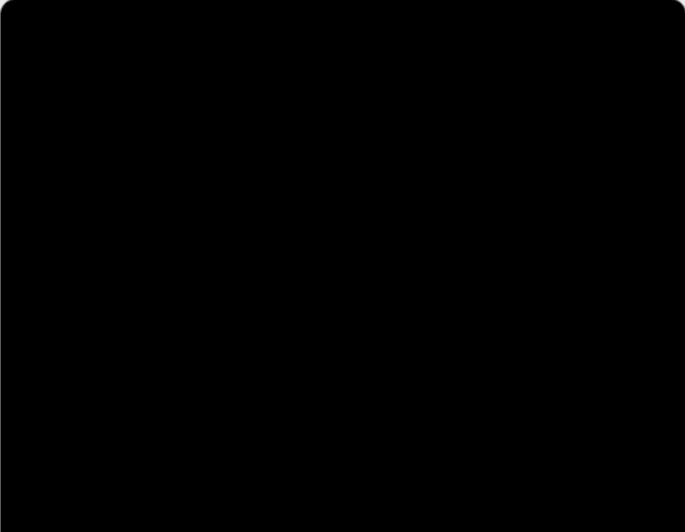


Рисунок 11 – Свойства нового изображение, по которым мы можем определить модель устройства

### 3. Вывод

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