

**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

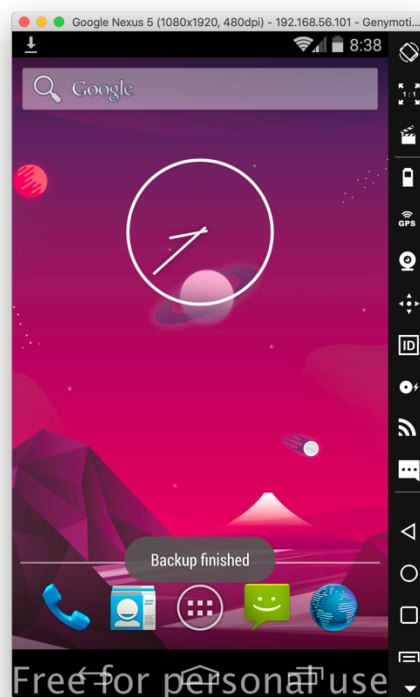


Рисунок 2 – Сообщение об успешности бэкапа

```

1  ANDROID BACKUP
2  3
3  1
4  AES-256
5  7F7EB8667413DE637D4338E640D34A8E21782367E478AB55F155A0827980451
6  8710312F10BC139BF929BB0E1AB606F351ED38C0605AB6B9A4FC45428CACE96
7  10000
8  990028C4A81CD1D9D0391EDA702ACB0D
9  CF7AAAC2489E1B6D8FF70058D35CB16D205509579DD1205763B07BC325BCC88
10 E000oy00'00c00&07#000/0ETBWe(K-WNUL0ieQ00nM00500EOTVT0$0DC3Rv$0
11 EM[0=ESCc0CAN00d0>CANXS000[0~Z0Lx0eyVB0VT0$0NAK00(>|- Fh0#000
12 ETBDC400DC40CAN000GSFDC200\SYN00FF2yKy09d0USETXRSč!o0_0&.&|0Kc0
13 RS0%FF0@DEL>kHTSpQ<70,0CAN0BEL0H"000Jnz0?00USä:
14 ESCSOH000D00"0a090BACK0SYN70DLE0U000BSRDC2,5 0$00200 0Q0?0z
15 00SUBi03w0FF0]0NUL3J00
16 0J060)0D0BEL0000'g0"BSP0S0W0f0W0n00_00d0SI0Uq}$I 00' EM?X00
17 / m0000$+100o`l(CANDC40t0 `0P]HSTXjBEL}00000^0EOT~000s00.0<0DC3
18 G000EMm
19 0 0007SUB0r00P000 0J0"&00dG*0;0`DLE000STX9IEOT<0CCHG0 00N000MS
20 DC3X00ETXZhs0i0L00+DC4J0Yo0`,gU0ETBEM0K3m00=B00ESCST0شBS+IA)~E
21 ]_lu0a000NAK00VT00DC40BS000H-w0Iu00e"0e0D00MB000fDJ00ETB000:(0
22 0.W0000US0a0P"0NUL*H0ENQ0#00RS0_^DC2B9#u}EOT0AR0C00&0<f00rP0|6
23 DLE0=0CAN0EOT00Nu20USFS7'oK0.SYN0gS0H0~+00F;00I0=fzSI00
24 !00}00"00DC4#>FF000DC10QNAKb000'SI000fA00SOH0o0s0k0DC2s000EOT`0
25 l00Aq:0DsNUL000CAN00_00DC300fxDC40LRS]0J010Q0N0RS>EGp006000"0
26 pA00t0BELr000VTan0L|00034a0k0000X^0-ESC ESC hX^00<0e0V~N筭W
27 VT~LS0000R0YQ0VTM00]_bJ000GSRsx0;Fr00000SUBS0GS00xt0M00CAN"SUB3

```

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

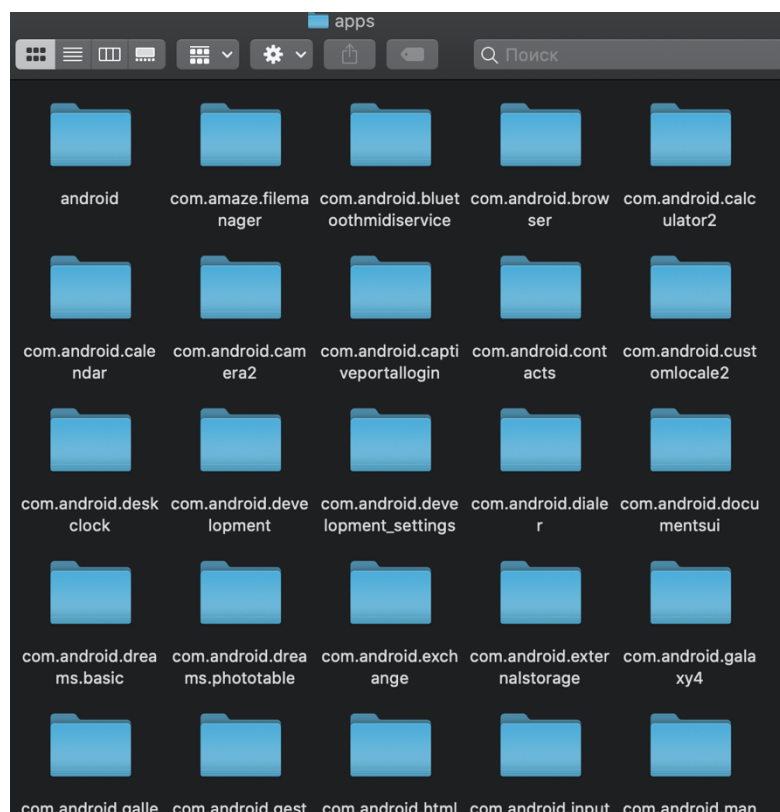


Рисунок 5 – Полученные данные бэкапа

## 2) Вывод данных из изображения

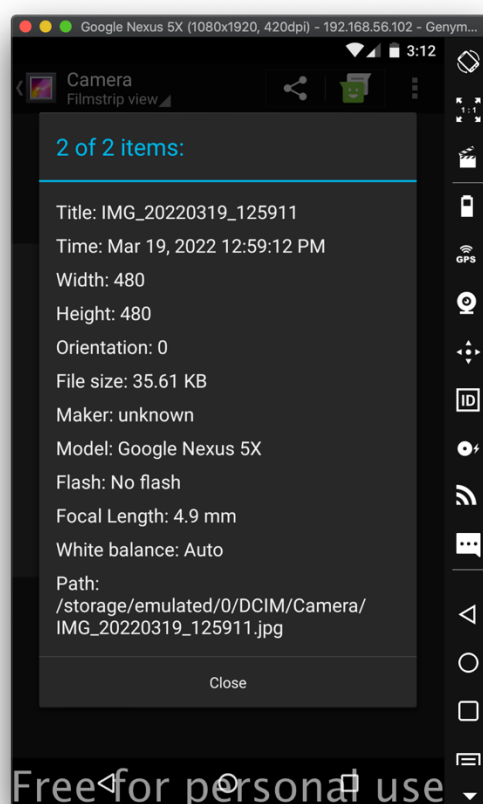


Рисунок 6 - Метаданные на устройстве

```

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 (Digit)            |600
Sub-second Time (Original)         |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 (Original)           |2022:03:18 10:26:08
Pixel X Dimension                  |480
Components Configuration           |Y Cb Cr -
Color Space                        |Uncalibrated
Exif Version                       |Exif Version 2.2
FlashPixVersion                    |FlashPix Version 1.0
-----+-----

```

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.