תיאור התהליך – הפיכת MagicData לאפליקציה שמושכת מידע מהמכשיר כאשר לוחצים על כפתור Random :

שלבי התהליך :

1.**כתיבת הקוד הזדוני** בandroid studio – כתבתי class שנקרא GatherData וconstructor שלו הכנסתי את כל הקוד שמוציא מידע על המכשיר . זאת כדי שיהיה קל אחרי זה להכניס את הקובץ כולו לאפליקציית הבסיס. לאחר מכן, כתבתי ב MainActivity מופע של הclass הנ"ל (כדי שהconstructor יקרא)

2.**יצירת קובץ APK** של הפרויקט שכתבתי – ע"י לחיצה על Build->Generate Signed bundle/APK... .

3.פתיחה של הKALI שלי – שם הורדתי apktool, ופתחתי את Base_app.apk ע"י הפקודה

apktool d Base_app.apk

ועשיתי אותם שלבים גם לקובץ הAPK עם הקוד הזדוני.

4.כעת, נכנסתי לקבצי **הsmali** של אפליקציית הבסיס וחיפשתי איפה יש קריאה למשהו עם המילה random. מצאתי את השורות הנל :

```
2528    goto :goto_0
2529
2530    .line 137
2531    .end local v0    # "tmpAnzahl":Ljava/lang/String;
2532    :pswitch_1
2533    invoke-direct {p0}, Lcom/MagicDate/MagicDate;→getRandom()V
2534
2535    .line 138
2536    new-instance p1, Lcom/MagicDate/GatherData;
2537
2538    invoke-virtual {p0}, Lcom/MagicDate/MagicDate;→getApplicationContext()Landroid/content/Context;
2539
2540    move-result-object v0
```

לקחתי מקבצי הsmali של הקוד הזדוני את החלק בקוד בMainActivity שבו יש את היצירה של המופע של GatherData והעתקתי אותו מתחת ל()getRandom, תחת השורה :"line 138." כי getRandom היא בשורה 137 כפי שניתן לראות .

5.את הקובץ של הclass של GatherData **העתקתי** במלואו ללא שינוי לתקייה של MagicData .

6.על התקייה של MagicData הרצתי את הפקודה **apktool b Base_app** .

7.כעת, בwindows שלי בcmd הרצתי את 2 הפקודות הבאות :

C:\Program Files\Java\jdk-17.0.1\bin\keytool.exe" -alias bob -genkey -v -keystore mykey.keystore -" keyalg RSA – **יצירת מפתחות לחתימה**

C:\Program Files\Java\jdk-17.0.1\bin\jarsigner.exe" -signedjar "out.apk" -keystore mykey.keystore " bob "Base_app.apk" – **חתימה על הקובץ APK המתאים**

8.**הרצה של הקובץ החתום באימולטור** – גרירה של הקובץ לתוך המכשיר ... וכפי הניתן לראות בסרטון האפליקציה עובדת ומוציאה מידע לקובץ information.txt .