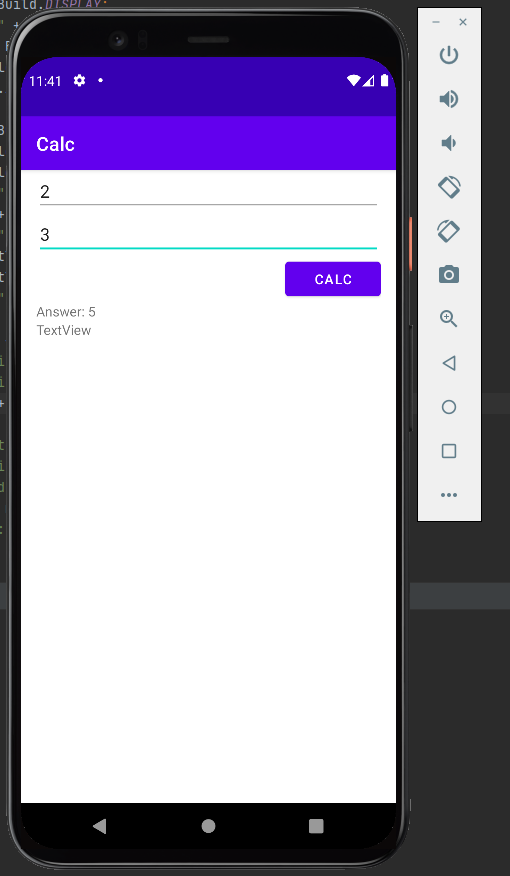
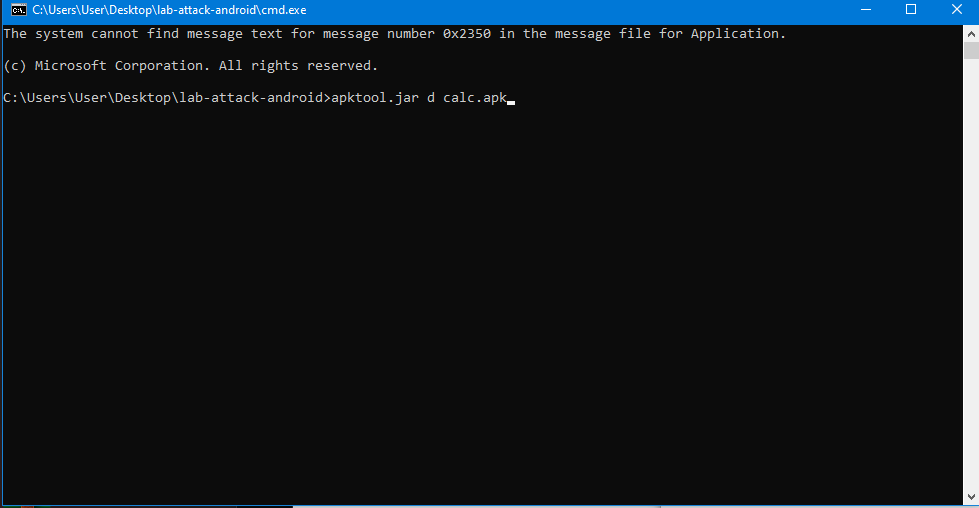
מטלת סיכום – הגנת התקפה

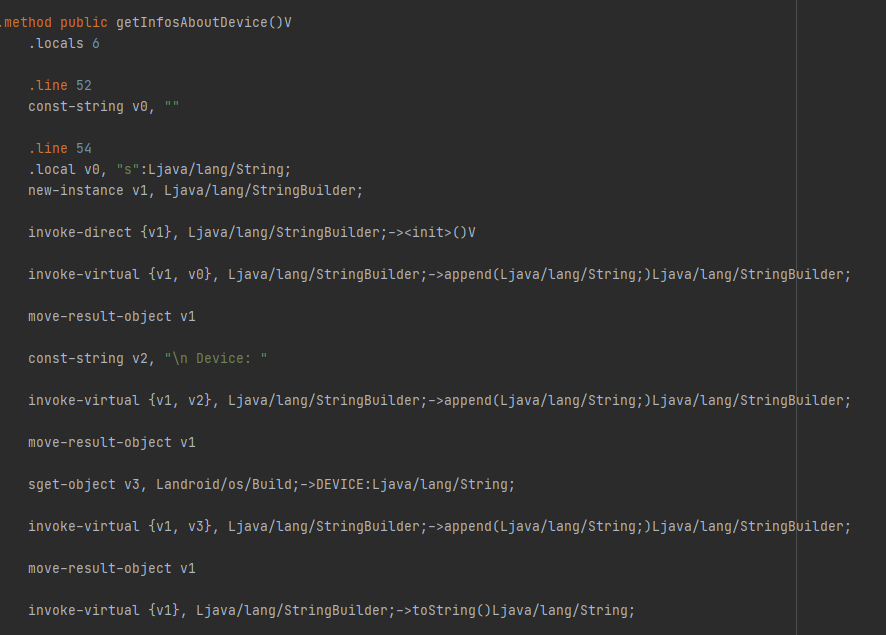
במטלה זאת קיבלנו אפליקציה בשם magicDate והתבקשנו להחדיר תוכן זדוני לצורך שליפת נתונים מן מכשיר האנדרואיד. משום שקיבלנו רק קובץ apk לעבוד איתו היינו צריכים להשתמש בapktool על מנת להפוך את הקוד לsmali.

אף על פי שלא למדנו smali עדיין ישנה דרך לכתוב בsmali בדרך עקיפה.

האפליקציה magicDate היא מחשבון רנדומלי בעל 2 כפתורים – "calculate","random". אנו התבקשנו שכאשר משתמש ילחץ על כפתור הrandom התוכנית למעשה תשאב את כל המידע שיש על הטלפון ותדפיס אותו לקובץ information.txt בתוך הstorage של הטלפון.

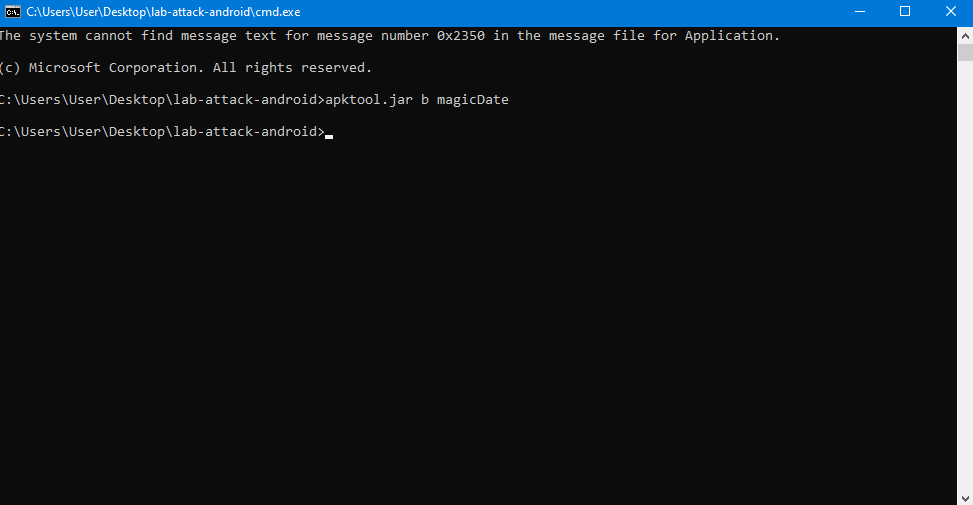
בהתחלה הכנתי תוכנית באנדרואיד סטודיו של מחשבון פשוט בעל כפתור אחד אשר מחשב x+y=sum אך כאשר הוא לוחץ sum למעשה הפונקציה הזדונית שכתבתי "getInfosAboutDevice()" מופעלת, ונשמר בstorage של הטלפון כל הפרטים על גבי הטלפון עצמו. 

כעת, המרתי את הapk של התוכנית שלי לקוד בsmali על ידי שימוש בapktool  וחיפשתי את שם הפונקציה בין התיקיות עד שמצאתי שורת קוד אחת לקריאה לפונקציה ומקבץ גדול של שורות קוד של הפונקציה עצמה.

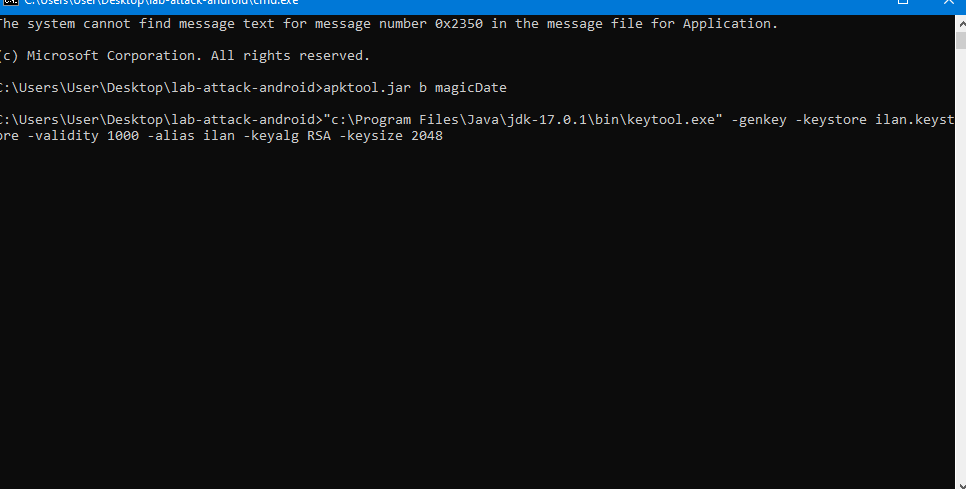


לאחר מכן העתקתי את כל הפונקציה בsmali לתוך הsmali של magicDate בנוסף העתקתי את שורת הקריאה לפונקציה בתוך הפונקציה getRandom אשר מופעלת בעת לחיצה על כפתור הrandom וככה למעשה השתלתי את הפונקציה הזדונית שיצרתי במחשבון הפשוט שלי.

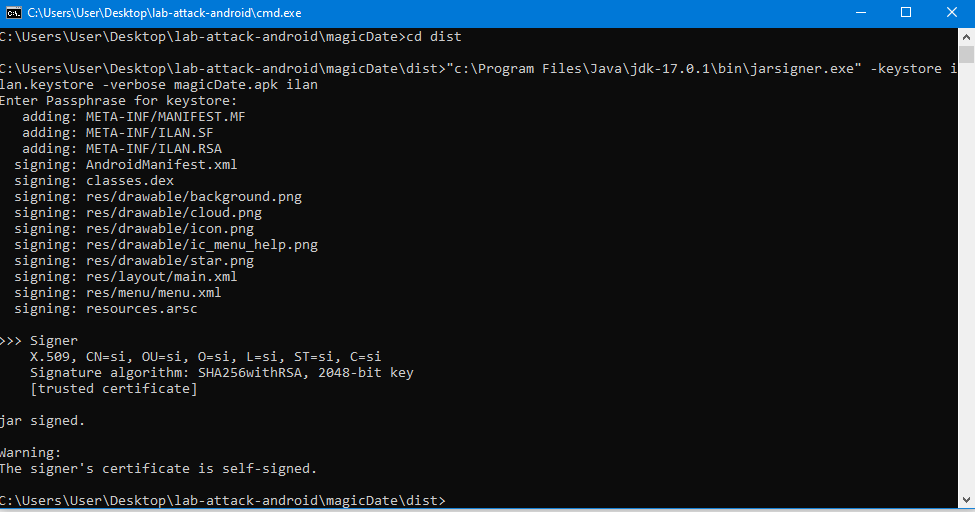
לאחר מכן בשביל להשיג את הapk החדש של magicDate יש להשתמש שוב בapktool



בנוסף לכך צריך ליצור מפתח יחודי

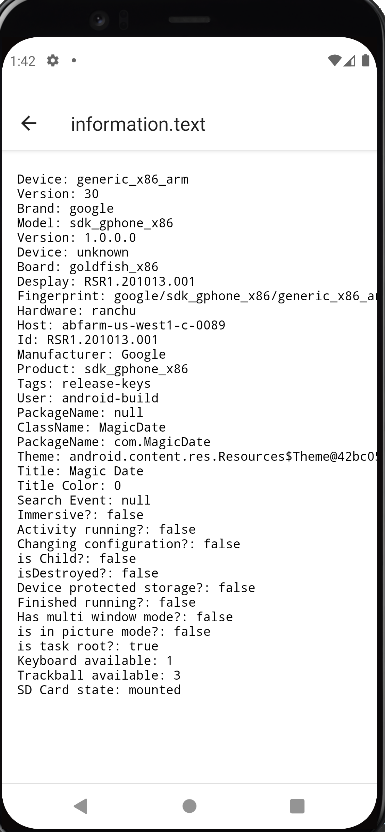


ולהשתמש בjarsigner עם המפתח היחודי שיצרנו



לאחר מכן הmagicDate.apk מוכן לשימוש – נגרור אותו אל תוך הטלפון לצורך התקנה , נפתח את האפליקציה ונלחץ על כפתור הrandom .

בשביל לראות אם הפעולה הזדונית שכתבנו אכן עבדה ניתן לגשת לתיקיית הFiles>Android>data>com.MagicDate>This\_dir>information.txt



בנוסף להכל התבקשנו לצלם סרטון וידאו שניתן להוציא את הקובץ information.txt החוצה אך לאחר מספר רב של ניסיונות לא צלחתי



את קובץ הטקסט העתקתי בדרך אחרת אשר לא מוצגת בסרטון הנל.