101 REVERSING ANDROID MALWARE

Hugo Gonzalez

The Honeynet Workshop - Jun 4, 2025

CONTENT

- Whoami
- Objective
- Why reversing
- Android introduction
- Tools
- Crackmes (3)
- SMSStealer - find url
- Scareware - find the password
- New one ???
- Conclusions

WHOAMI

OBJECTIVE

Give a brief introduction about Android platform and how to reverse engineering APKs to find the malicious or interesting part using open source tools.

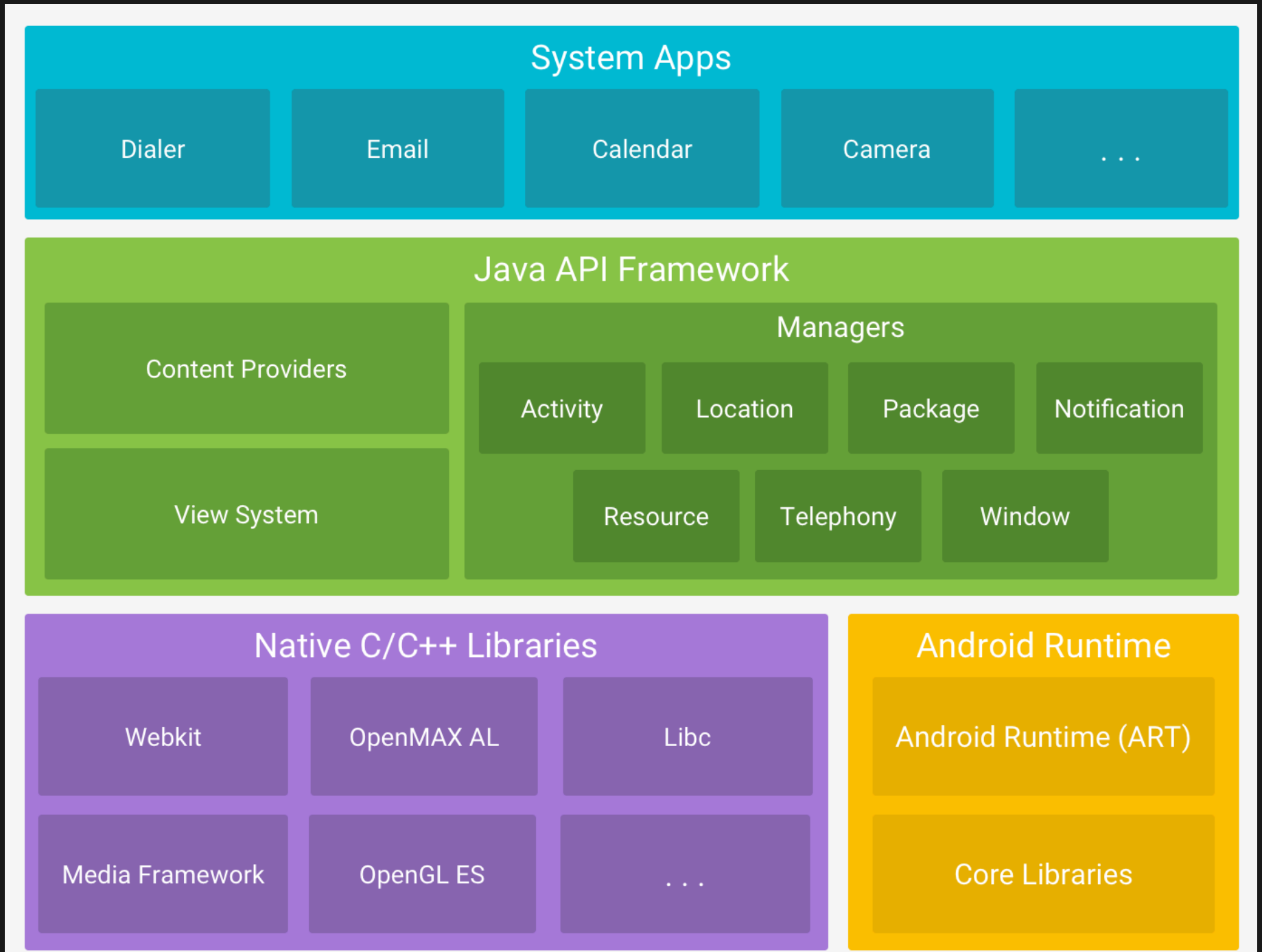
WHY REVERSING

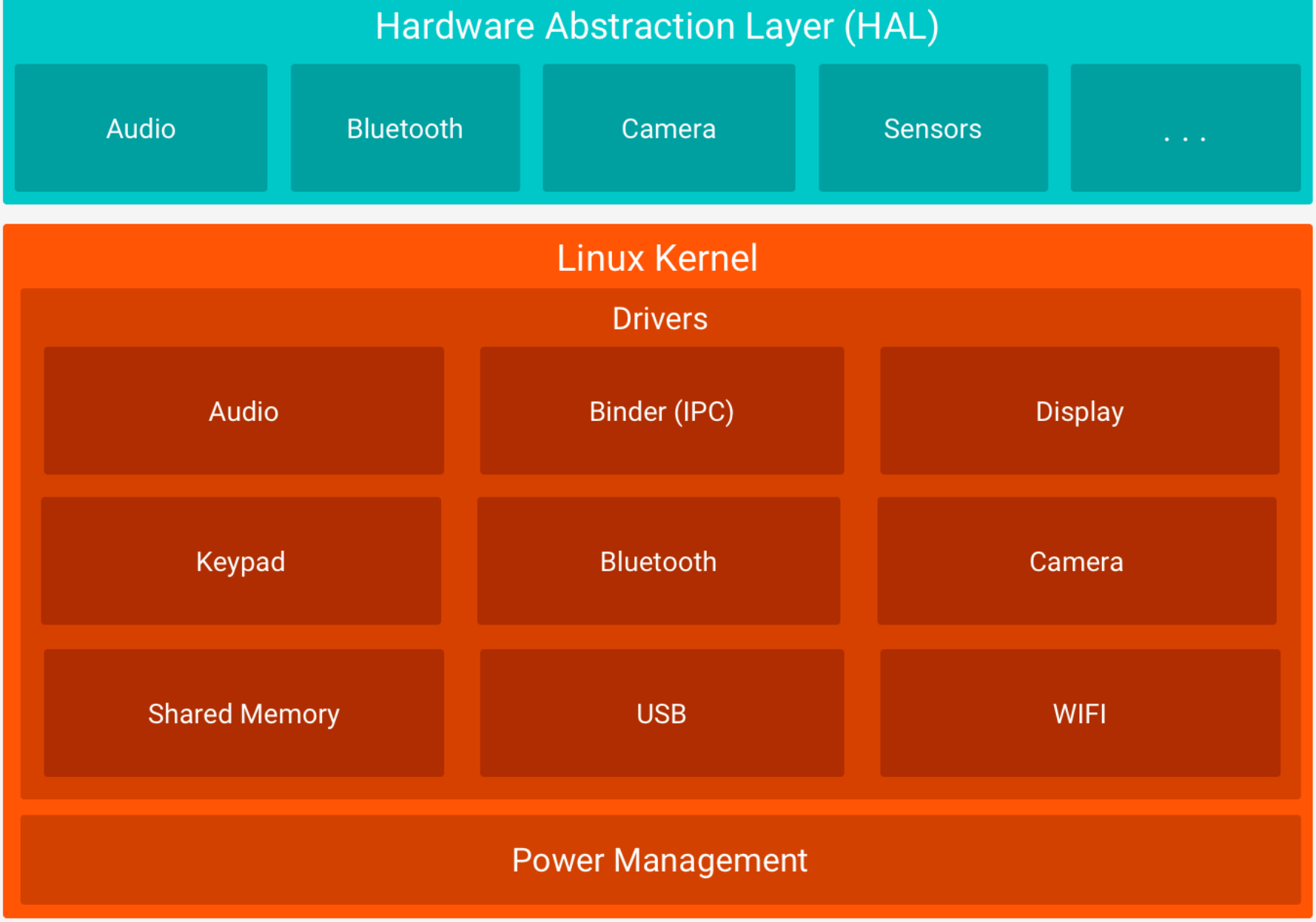
- Open question

WHY REVERSING

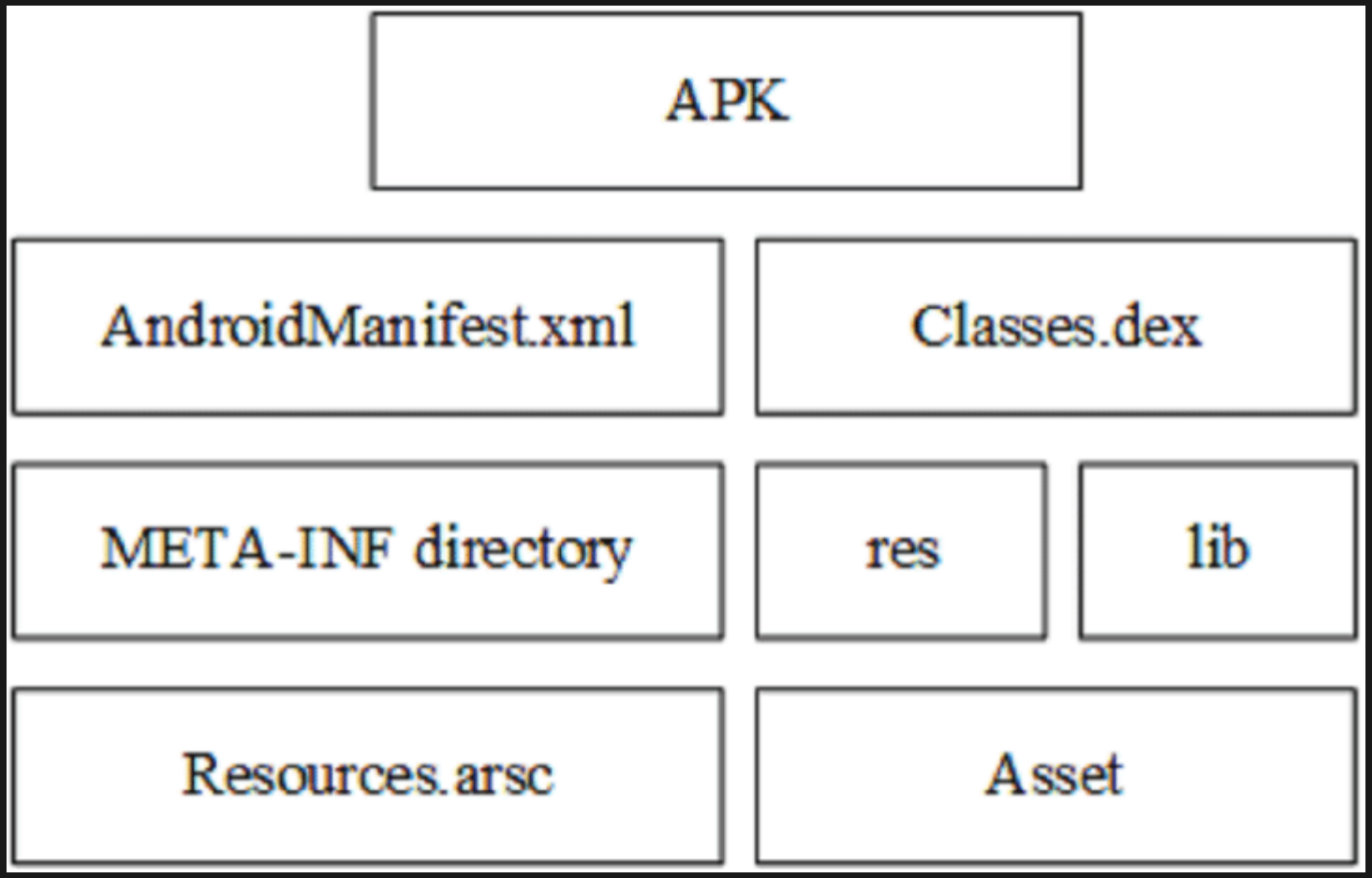
1. Understand malware behaviour
2. Develop detection signatures
3. Identify vulnerabilities
4. Attribution
5. Threat Intelligence (IoCs)
6. Help in incident response

ANDROID


System Apps
Dialer
Email
Calendar
Camera
. . .
Java API Framework
Content Providers
View System
Managers
Activity
Location
Package
Notification
Resource
Telephony
Window
Native C/C++ Libraries
Webkit
OpenMAX AL
Libc
Media Framework
OpenGL ES
. . .
Android Runtime
Android Runtime (ART)
Core Libraries


Hardware Abstraction Layer (HAL)
Audio
Bluetooth
Camera
Sensors
. . .
Linux Kernel
Drivers
Audio
Binder (IPC)
Display
Keypad
Bluetooth
Camera
Shared Memory
USB
WIFI
Power Management

Stack

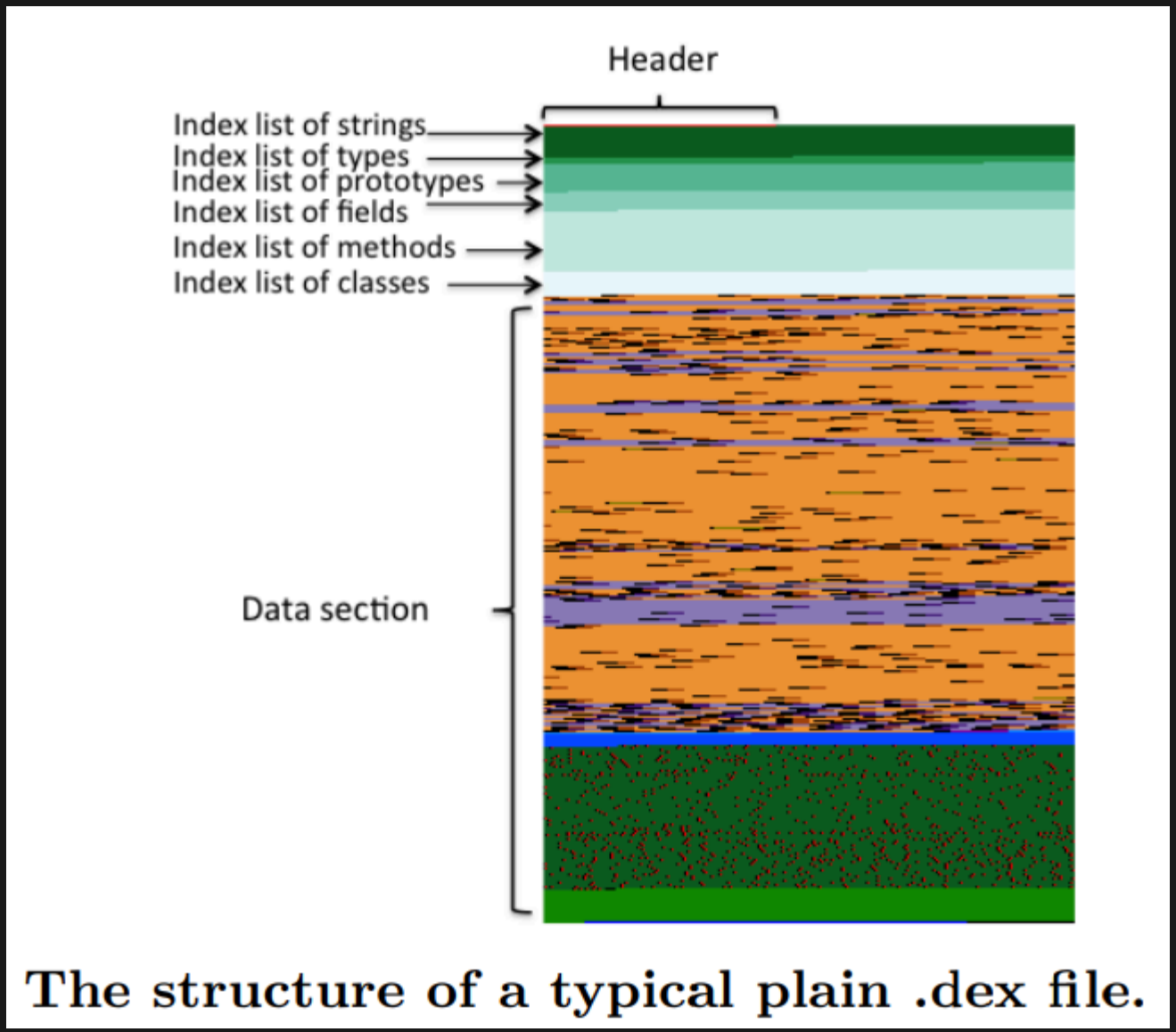

APK
AndroidManifest.xml
Classes.dex
META-INF directory
res
lib
Resources.arsc
Asset

Apkfile

header	Structural information
string_ids	Offset list for strings
type_ids	Index list into the string_ids for types
proto_ids	Identifiers list for prototypes
field_ids	Identifiers list for fields
method_ids	Identifiers list for methods
class_defs	Structure list for classes
data	Bytecode and data
link_data	Data for statically linked files.

Figure 1: The layout of a .dex file

Conceptual dexfile



The structure of a typical plain .dex file.

Dexfile

WHERE TO START?


<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.program1.buttons"
android:versionCode="1"
android:versionName="1.0" >
<uses-sdk
android:minSdkVersion="8"
android:targetSdkVersion="17" />
<application
android:allowBackup="true"
android:icon="@drawable/ic_launcher"
android:label="@string/app_name"
android:theme="@style/AppTheme" >
<activity
android:name="com.program1.buttons.MainActivity"
android:label="@string/app_name" >
<intent-filter>
<action android:name="android.intent.action.MAIN" />
<category android:name="android.intent.category.LAUNCHER" />
</intent-filter>
</activity>
</application>
</manifest>

Manifest

- Main Activity
- Receivers
- Filters
- Intents

WHERE TO GET APKS?

TOOLS

- Android Studio
- Android Emulator
- Apktool
  - Smali
- dex2jar
- smali_emulator

BASICS OF STATIC ANALISYS

- unpack
- Manifest
  - Entries
- Strings
- Permissions
- Specific Code

CRACKME 1

CRACKME 2

CRACKME 3

SMSSTEALER

SCAREWARE

FRESH SAMPLE MALWARE

- Crocodilus

CONCLUSIONS

CONTACT INFO

- @hugo_glez
- hugo.gonzalez@upslp.edu.mx
- linkedin.com/in/hugoxglez