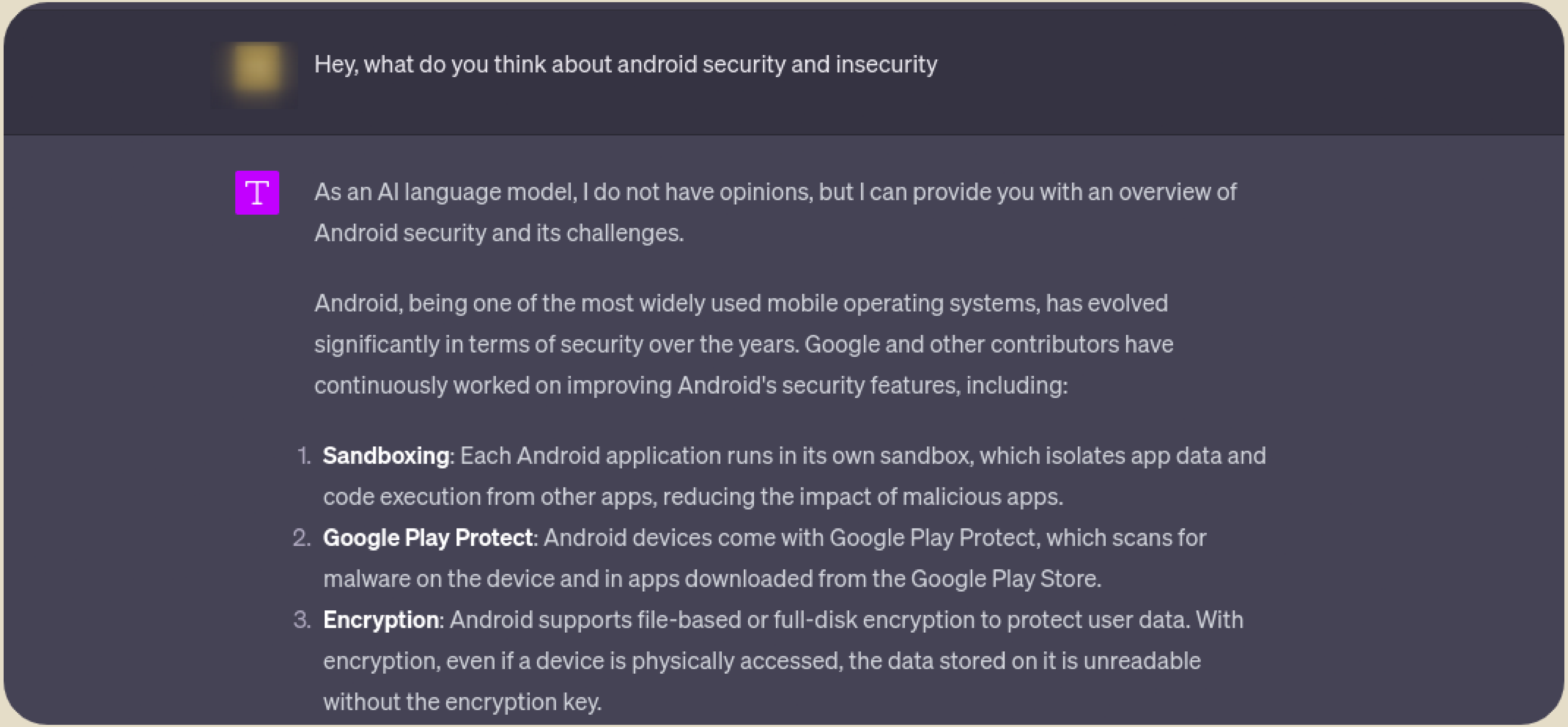
Byte By Byte:

Android Security and Insecurity

Mark Tanui



Hey, what do you think about android security and insecurity

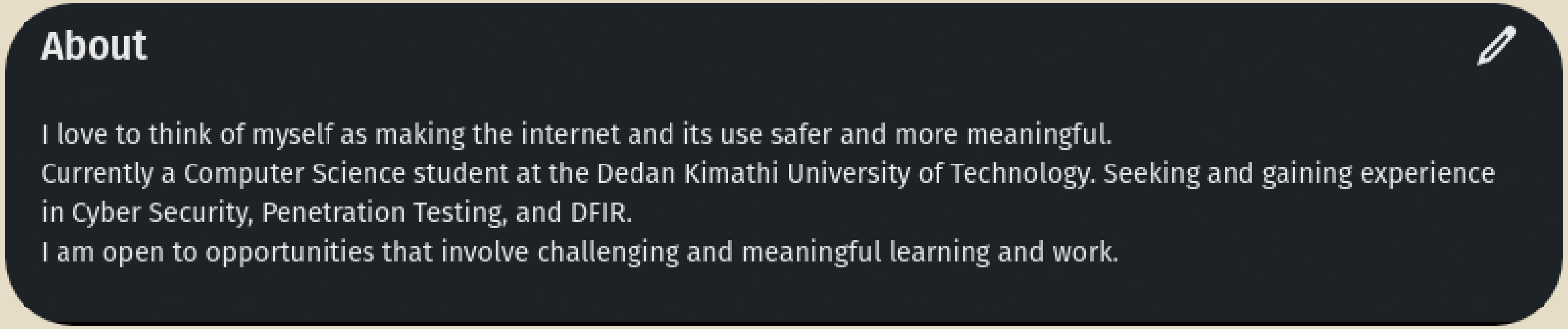
As an AI language model, I do not have opinions, but I can provide you with an overview of Android security and its challenges.

Android, being one of the most widely used mobile operating systems, has evolved significantly in terms of security over the years. Google and other contributors have continuously worked on improving Android's security features, including:

1. **Sandboxing**: Each Android application runs in its own sandbox, which isolates app data and code execution from other apps, reducing the impact of malicious apps.
2. **Google Play Protect**: Android devices come with Google Play Protect, which scans for malware on the device and in apps downloaded from the Google Play Store.
3. **Encryption**: Android supports file-based or full-disk encryption to protect user data. With encryption, even if a device is physically accessed, the data stored on it is unreadable without the encryption key.

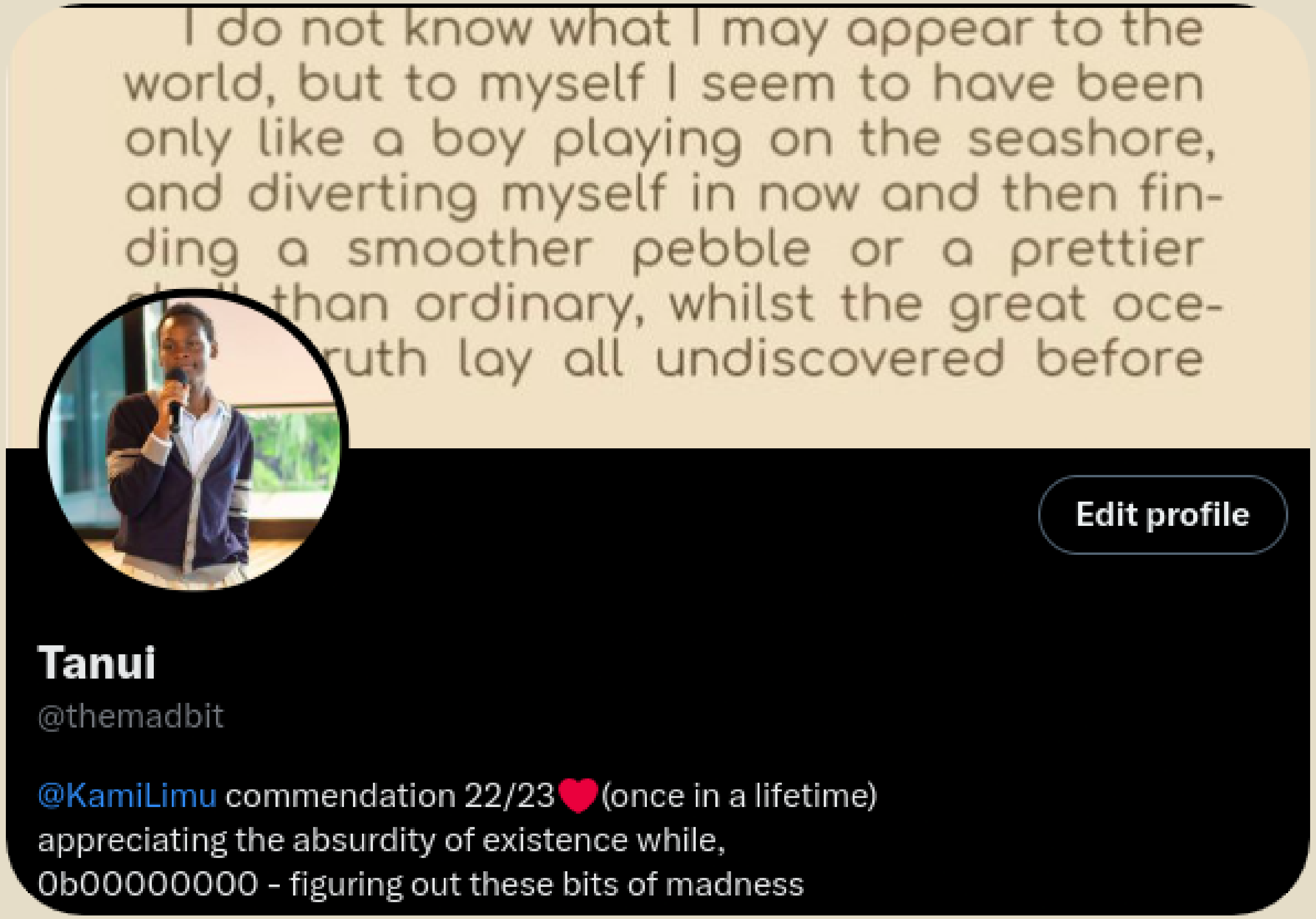
• • •

WHO AM I ?



About

I love to think of myself as making the internet and its use safer and more meaningful.
Currently a Computer Science student at the Dedan Kimathi University of Technology. Seeking and gaining experience in Cyber Security, Penetration Testing, and DFIR.
I am open to opportunities that involve challenging and meaningful learning and work.



I do not know what I may appear to the
world, but to myself I seem to have been
only like a boy playing on the seashore,
and diverting myself in now and then fin-
ding a smoother pebble or a prettier
than ordinary, whilst the great oce-
ruth lay all undiscovered before

Tanui
@themadbit

@KamiLimu commendation 22/23❤️(once in a lifetime)
appreciating the absurdity of existence while,
0b00000000 - figuring out these bits of madness

@themadbit

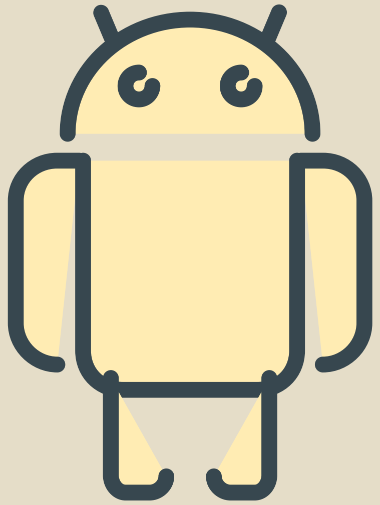
linkedin.com/in/marktanui/

marktanui.github.io

LESSON OBJECTIVES

Intro to Android

How are Android applications packed & what technologies power it's development.



Android Security

Fundamental concepts of security as it pertains to Android, permissions, and user data protection.

Android Insecurity

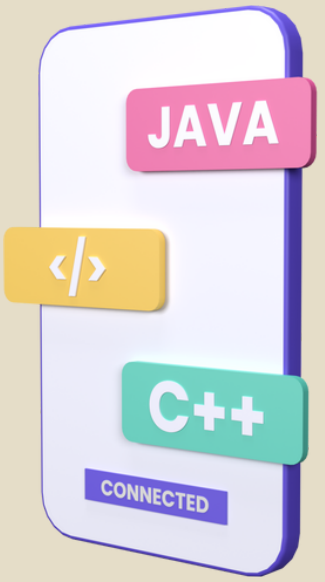
Security reversed?

3.553 million -
Mobile apps accessible for Android users to download.

The code is in your pocket. (Readable or not)

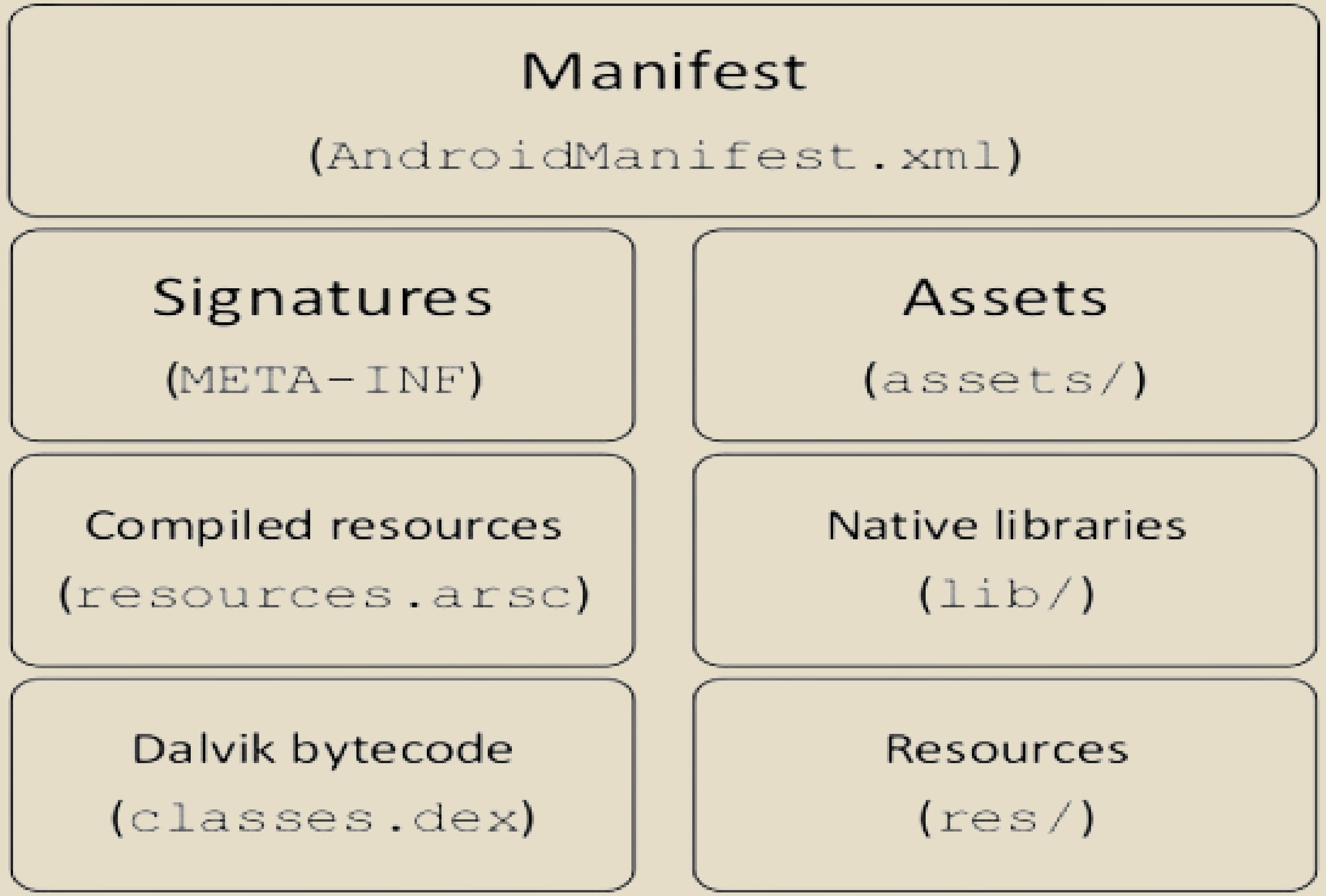
INTRODUCTION TO ANDROID

Android development is niched. Native & Hybrid Technologies (Java/Kotlin/Flutter/Dart et al)



APKs: ZIP file with a bunch of metadata, all the application's assets & config files, and binary files(dex), which contain the compiled application.

APPLICATION STRUCTURE. (APK)



Manifest

(AndroidManifest.xml)

Signatures

(META-INF)

Assets

(assets/)

Compiled resources

(resources.arsc)

Native libraries

(lib/)

Dalvik bytecode

(classes.dex)

Resources

(res/)

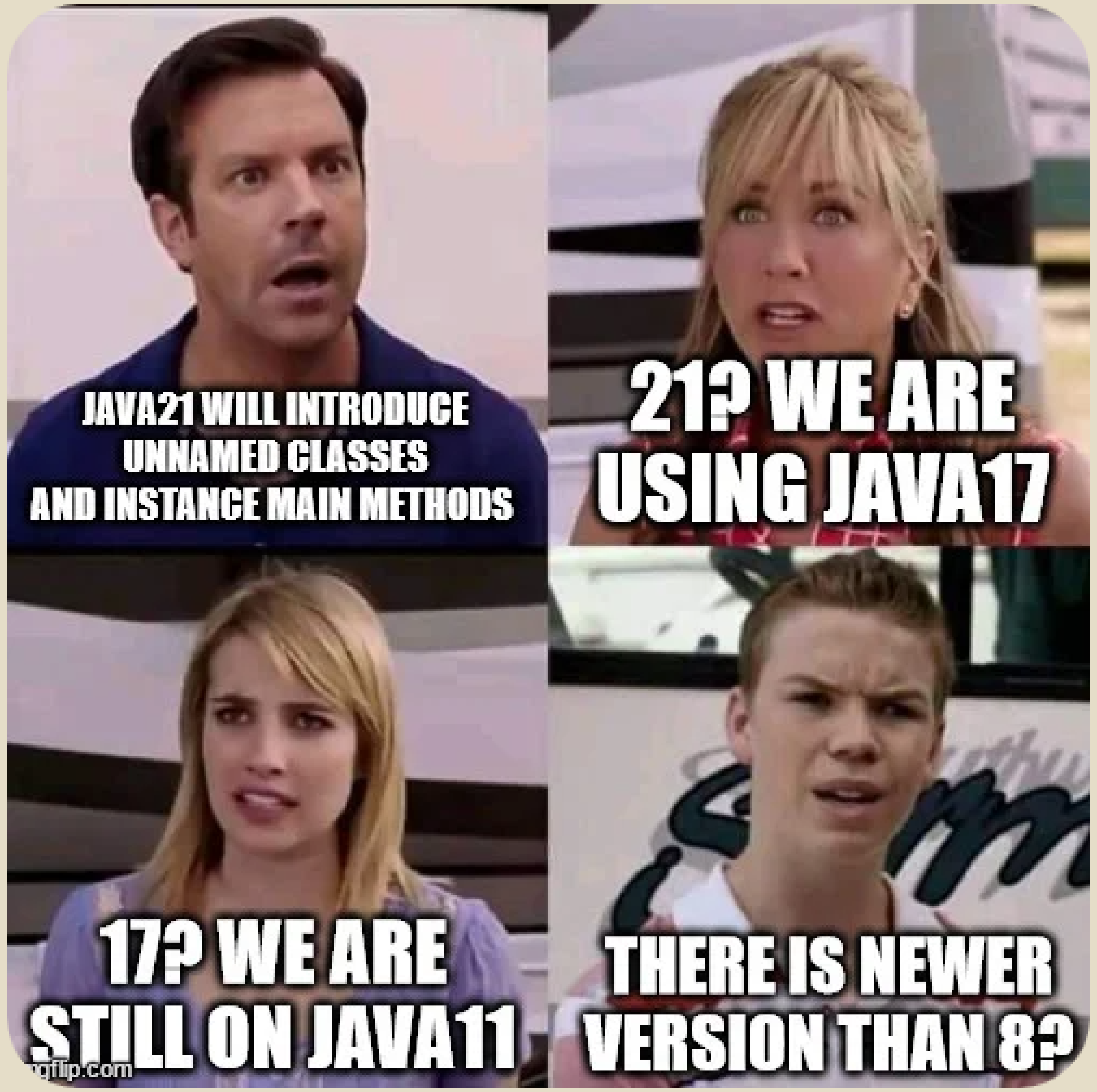
- AndroidManifest.xml: the manifest file in binary XML format.
- classes.dex: application code compiled in the dex format.
- resources.arsc: contains precompiled application resources, in binary XML.
- res/: folder containing resources not compiled into resources.arsc
- assets/: optional folder containing applications assets.
- lib/: optional folder containing compiled code - i.e. native code libraries.
- META-INF/: folder containing the MANIFEST.MF file, which stores meta data

TOOLS OF TRADE:

Java Development Kit
(The engine)

Jadx-Gui
(Blueprint and Schematics)

Emulators/Rooted Devices
(The Test Track)


JAVA21 WILL INTRODUCE UNNAMED CLASSES AND INSTANCE MAIN METHODS
21? WE ARE USING JAVA17
17? WE ARE STILL ON JAVA11
THERE IS NEWER VERSION THAN 8?
imgflip.com

adb
(Pit Crew Tools)

Frida
(The Tuning Equipment)

SECURITY & INSECURITY JUXTAPOSED

01	**Permission** Identifying necessary permissions, as requested by applications.	01	**Permissions?** When are the permissions needed? Once?/ Always on?
02	**DataBase(s)** Sure, we need to persist data. How do we do it?	02	**Secured DataBase(s)?** Is the database secure? Is data stored locally encrypted?
03	**Strings** strings.xml - Centralize all the text strings in one place.	03	**What strings?** What are the contents of your strings.xml file?

CONTD...

04 Secure Communication

Communication between an Android app and remote servers through SSL/TLS

05 Anti-reverse Engineering

Protect Android apps from reverse engineering, such as code obfuscation and tamper detection

06 Anti-Rooting

Detect and protect applicatons against running on rooted devices

04 SSL/Cert Pinning?

Can the application verify the legitimacy of the certs?

05 Reverse Engineered!

The code is in our pocket yes, but can we make it harder for anyone to know our logic?

06 Anti-Rooting Bypass!

Security must be a myth.?!

DEMO

- Live Demo
- Written Demo

WHAT NEXT DROID?

MAS Crackmes

TryHackMe - Android Hacking 101

Android RE - Maddie Stone

Read Security bulletins & article

WHO TO FOLLOW!

SheHacks KE

A community of women cyber warriors

@shehacks_ke

Maddie Stone

Security Researcher - Google Project Zero

@maddiestone

Chalie

Mobile AppSec Engineer

@chaliewizz

> “
>
> WHEN YOU PLUG INTO THE WORLD IT'S EASY TO FORGET THAT THE WORLD IS ALSO PULGED INTO YOU

~ NetworkBox.

Buy me a coffee