# Mobile Phone Security

**Dr. Digvijaysinh Rathod**
**Associate Professor**
**(Cyber Security and Digital Forensics)**
**Institute of Forensic Science**
**Gujarat Forensic Sciences University**

**digvijay.rathod@gfsu.edu.in**

# Session – I

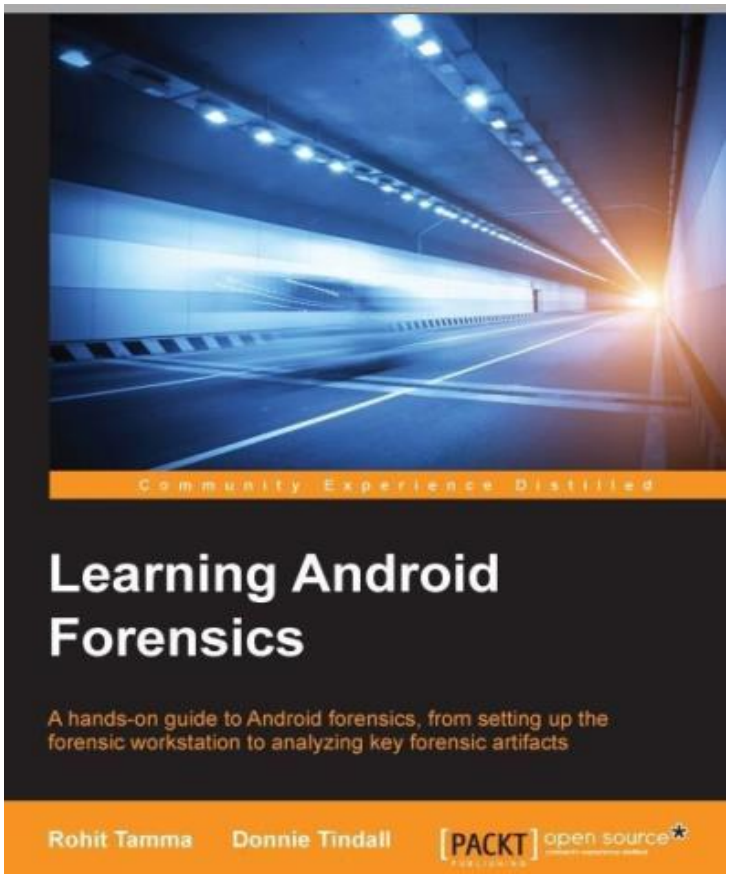
# Introduction to Android

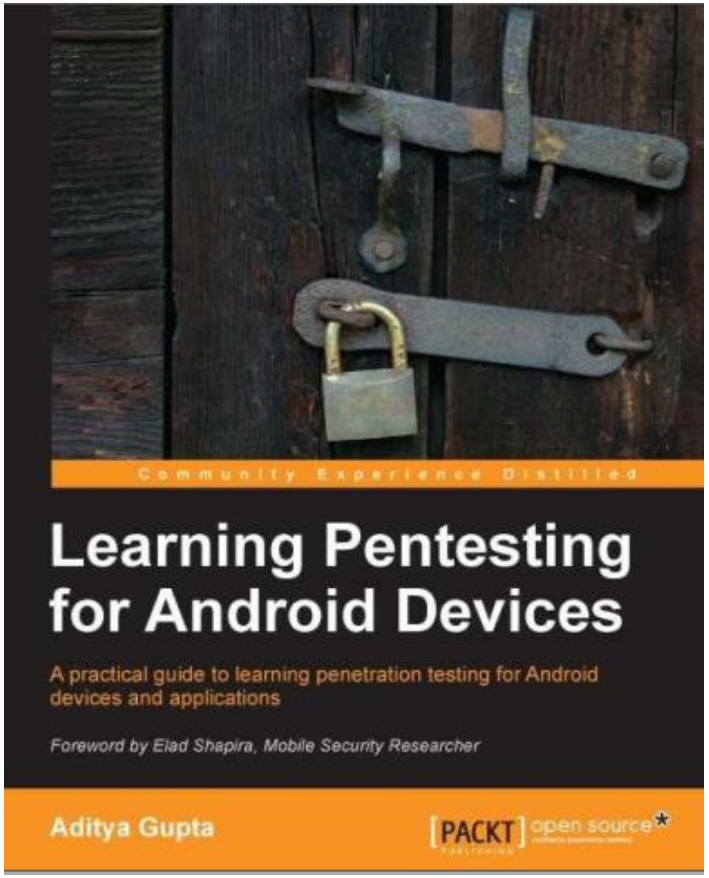
# Android Architecture

# Android Run Time

- ✓Android Application Security Pen-Testing
- ✓iOS Application Security Pen-Testing

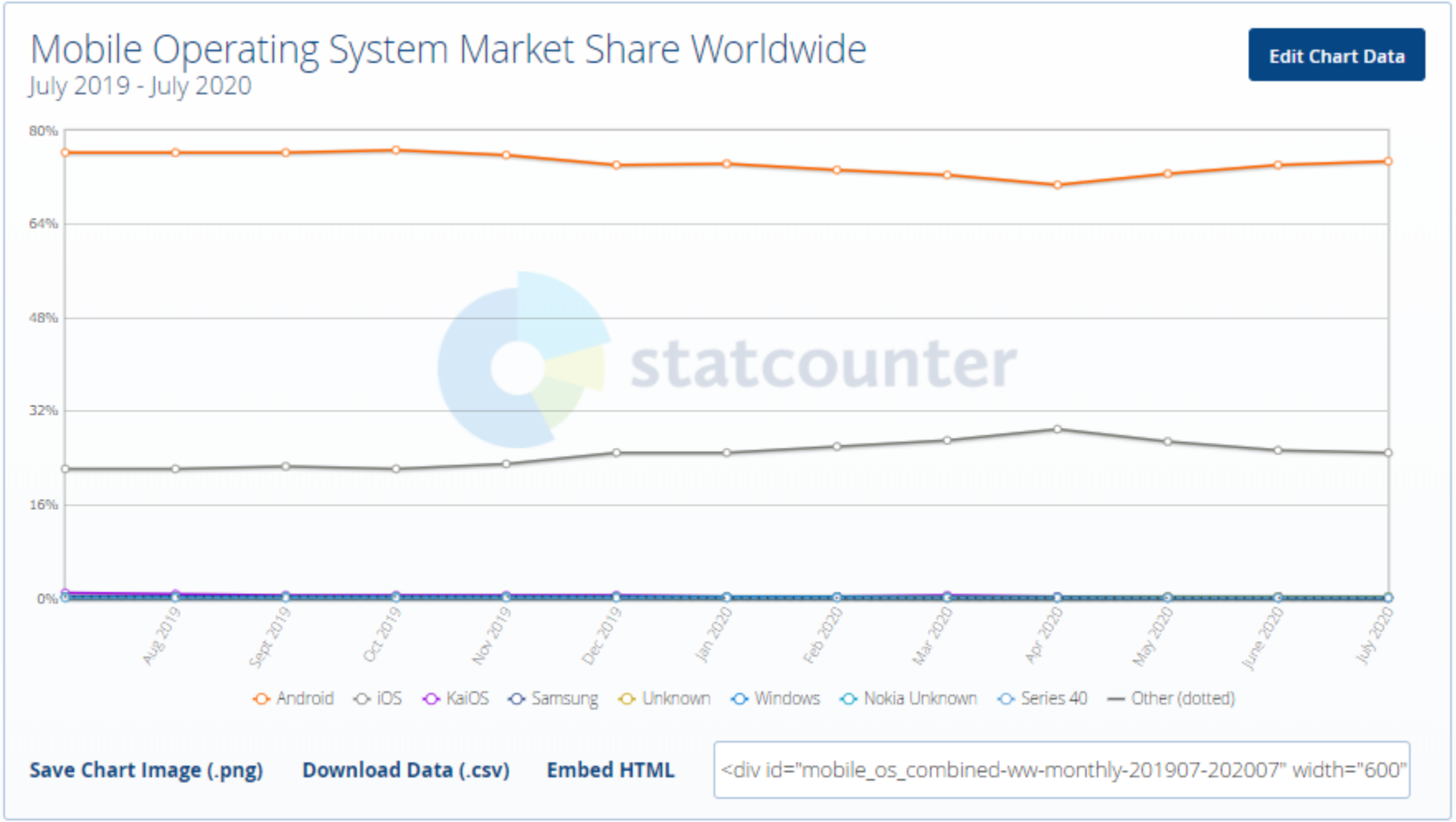
# Reference




digvijay.rathod@gfsu.edu.in

# Mobile Operating System Market Share Worldwide




Ref: https://gs.statcounter.com/os-market-share/mobile/worldwide

✓Android is an **open-source operating system** based on **Linux** with a **Java and kotlin** programming interface for mobile devices such as Smartphone (Touch Screen Devices who supports Android OS) as well for Tablets too.

✓Android was developed by the Open Handset Alliance **(OHA)**, which is led by **Google**.

✓The Open Handset Alliance (OHA) is a consortium of multiple companies like Samsung, Sony, Intel and many more to provide services and deploy handsets using the android platform.

✓In 2007, Google released a first beta version of the Android Software Development Kit (SDK) and the first commercial version of Android 1.0 (with name Alpha), was released in September 2008.

✓In 2012, Google released another version of android, 4.1 Jelly Bean.

✓In 2014, Google announced another Latest Version, 5.0 Lollipop.

✓Latest release10/August 3, 2020 and on the way to release Android 11

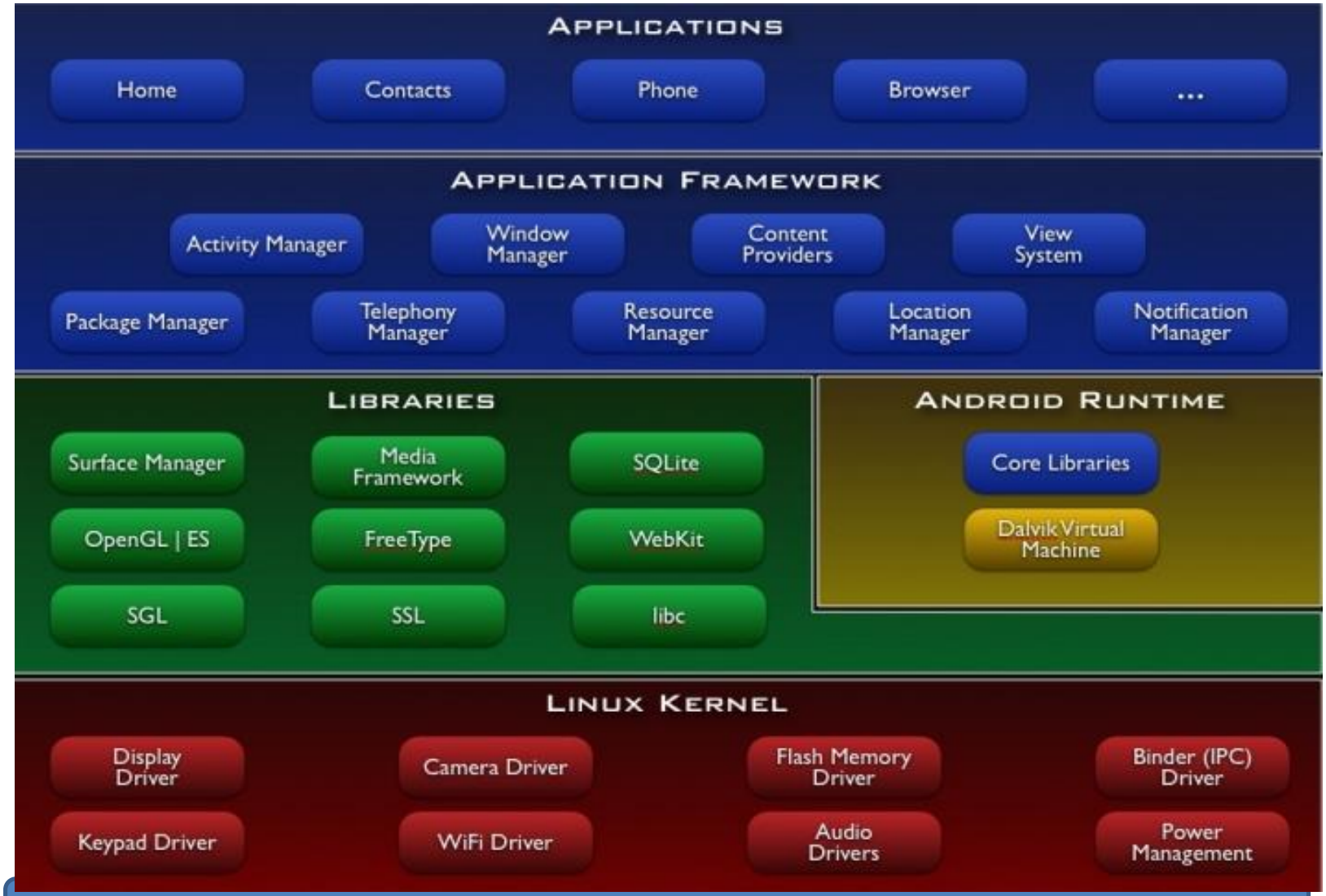
# The Android architecture

✓Any operating system (desktop or mobile) takes responsibility for **managing the resources** of the system and provides a way for **applications to talk to hardware or physical components** in order to accomplish certain tasks.

✓ OS manage mobile phones, manages **memory** and **processes, enforces security**, takes care of networking issues

# The Android architecture

✓The Android operating system consists of a stack of layers running on top of each other.



## ✓The Linux kernel:

✓Provides a level of **abstraction** between the device hardware and the upper layers.

✓Kernel contains **drivers to understand the hardware instruction.**

✓The drivers in the kernel control the underlying hardware.

✓As shown in the preceding figure, the kernel contains drivers related to Wi-Fi, Bluetooth, USB, audio, display, and so on.

✓Such as **process management, memory management, security, and networking, are managed** by Linux kernel

## ✓Libraries:

✓On top of Linux kernel are Android's native libraries.

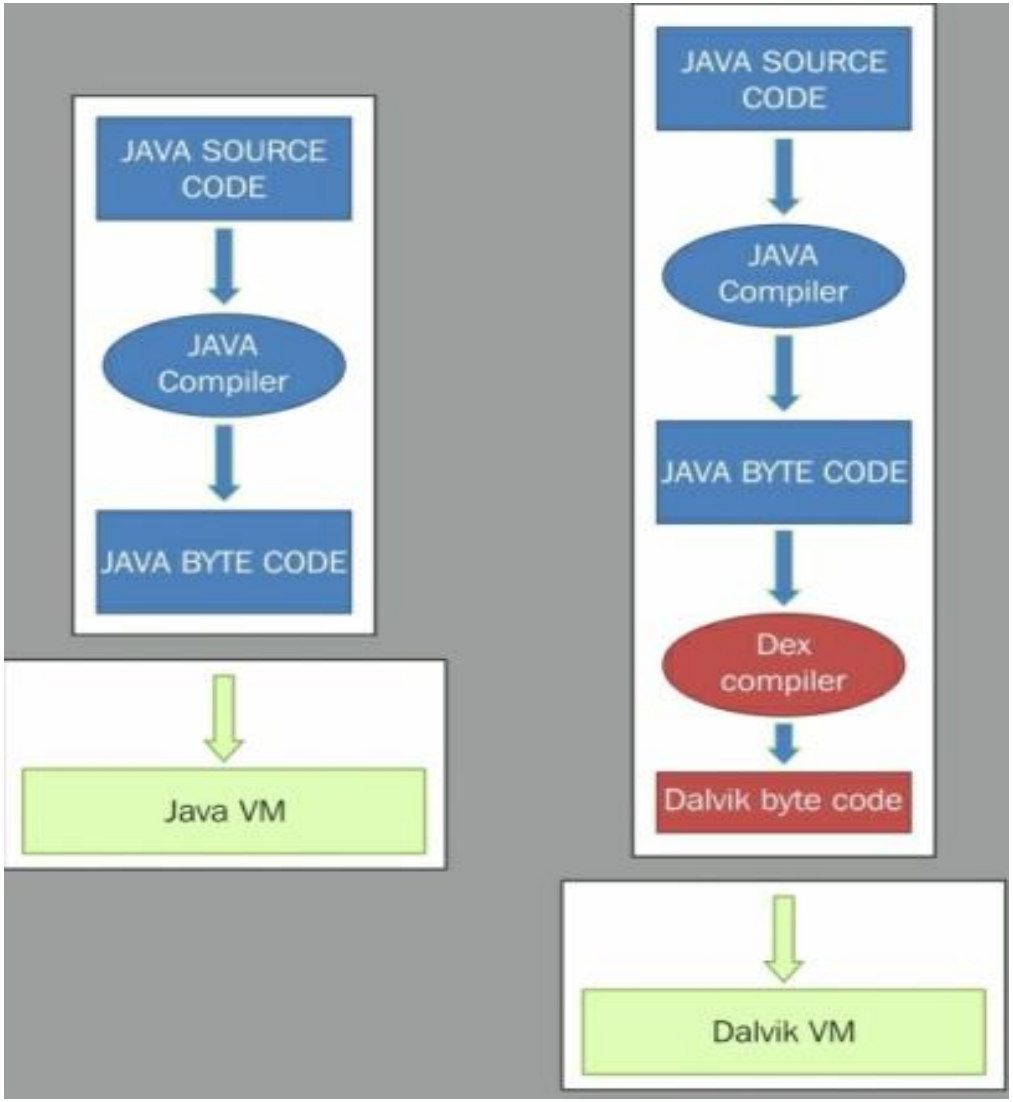
✓It is with the help of these **libraries that the device handles different types of data**.

✓These libraries are written in the **C or C++ programming languages** and are specific to a particular hardware.

✓For example, the media framework library supports the recording and playback of audio, video and picture formats.

# The Android Run Time

## ✓Dalvik virtual machine:




.Class

.dex
Dalvik Executable

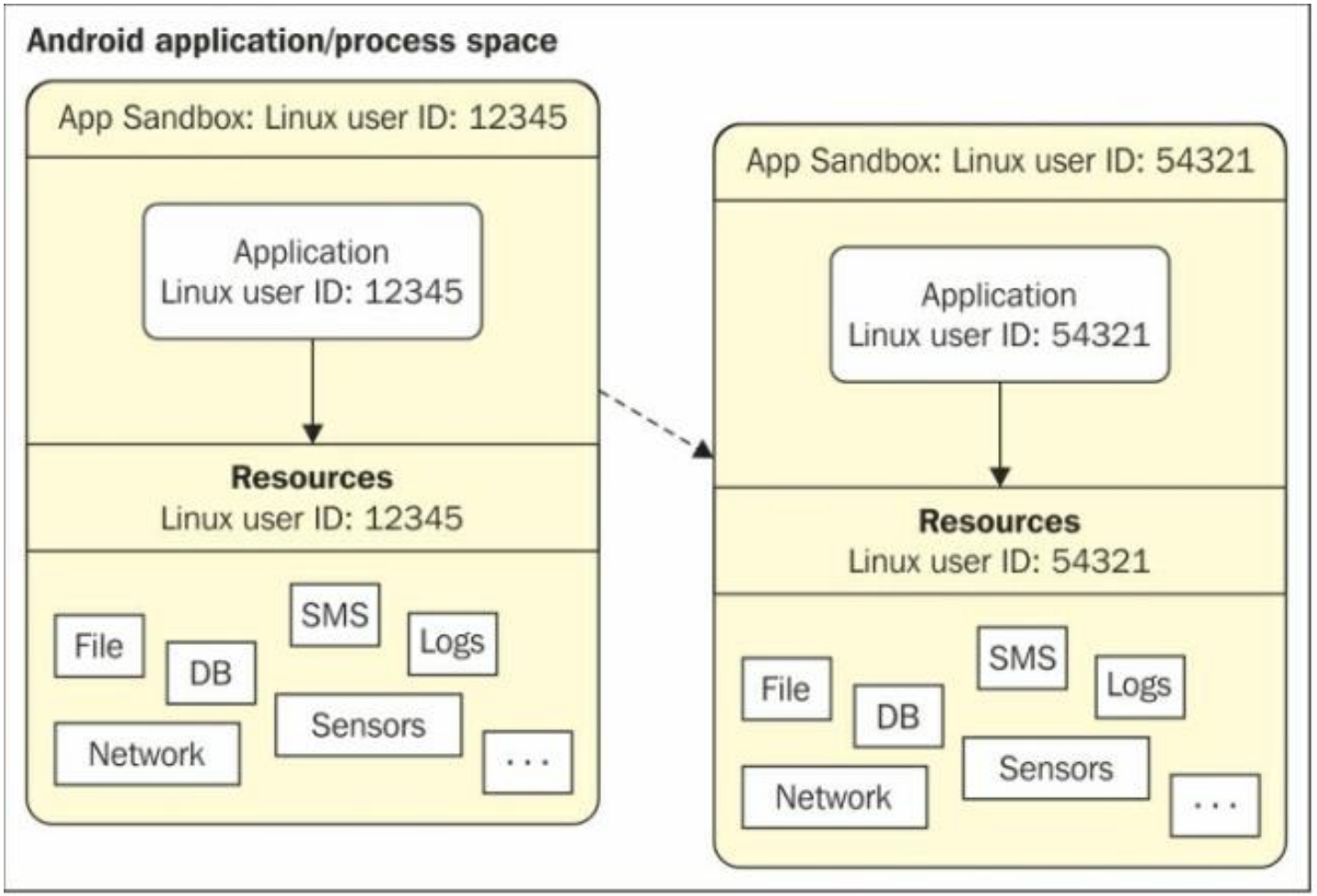
## ✓Dalvik byte code :

✓Dalvik byte code is an **optimized byte code** suitable for low-memory and low-processing environments.

✓Also, note that JVM's byte code consists of **one or more .class files**, depending on the number of Java files that are present in an application,

✓but Dalvik byte code is composed of **only one .dex file.**

## ✓Application sandboxing :




*Two applications on different processes on with different UID's*

## ✓Application sandboxing :

✓In order to isolate applications from each other, Android takes advantage of the Linux user-based protection model.

✓In Linux systems, each user is assigned a unique user ID (UID) and users are segregated so that one user does not access the data of another user.

✓All resources under a particular user are run with the same privileges. Similarly, each Android application is assigned a UID and is run as a separate process.

✓**This application sandboxing is done at the kernel level. it applies to both native applications and OS applications**

# Mobile Phone Security

**Dr. Digvijaysinh Rathod**
**Associate Professor**
**(Cyber Security and Digital Forensics)**
**Institute of Forensic Science**
**Gujarat Forensic Sciences University**

**digvijay.rathod@gfsu.edu.in**