Android Application Penetration Testing

Raja Nagori

ANDROID ARCHITECTURE
&
WORKING OF APP

Android Fundamental

- Based on LINUX Operating System
  - Commands like
    - ls
    - mv
    - cd
    - whoami
    - cp
    - etc

```
1|kali:/ $ ls -al
total 3272
drwxrwxrwt  18 root   root       760 1974-03-19 08:50 .
drwxrwxrwt  18 root   root       760 1974-03-19 08:50 ..
dr-xr-xr-x 131 root   root         0 1974-03-19 08:50 acct
lrwxrwxrwx   1 root   root        11 1970-01-01 05:30 bin -> /system/bin
lrwxrwxrwx   1 root   root        50 1970-01-01 05:30 bugreports -> /data/user_de/0/com
drwxrwx---   6 system cache     4096 1974-03-19 08:50 cache
lrwxrwxrwx   1 root   root        13 1970-01-01 05:30 charger -> /sbin/charger
drwxr-xr-x   3 root   root         0 1970-01-01 05:30 config
lrwxrwxrwx   1 root   root        17 1970-01-01 05:30 d -> /sys/kernel/debug
drwxrwx--x  42 system system    4096 2021-09-04 12:46 data
lrwxrwxrwx   1 root   root        23 1970-01-01 05:30 default.prop -> system/etc/prop.d
drwxr-xr-x  20 root   root      3860 2021-12-29 22:36 dev
lrwxrwxrwx   1 root   root        11 1970-01-01 05:30 dsp -> /vendor/dsp
lrwxrwxrwx   1 root   root        11 1970-01-01 05:30 etc -> /system/etc
lrwxrwxrwx   1 root   root        20 1970-01-01 05:30 firmware -> /vendor/firmware_mnt
-rwxr-x---   1 root   root   2217040 1970-01-01 05:30 init
-rwxr-x---   1 root   root      1222 1970-01-01 05:30 init.environ.rc
-rwxr-x---   1 root   root     29936 1974-03-19 08:50 init.rc
-rwxr-x---   1 root   root      7690 1970-01-01 05:30 init.usb.configfs.rc
-rwxr-x---   1 root   root      5646 1970-01-01 05:30 init.usb.rc
-rwxr-x---   1 root   root       511 1970-01-01 05:30 init.zygote32.rc
-rwxr-x---   1 root   root       875 1970-01-01 05:30 init.zygote64_32.rc
drwxr-xr-x  12 root   system     260 1974-03-19 08:50 mnt
drwxr-xr-x   2 root   root       220 1970-01-01 05:30 odm
drwxr-xr-x   2 root   root        40 1970-01-01 05:30 oem
lrwxrwxrwx   1 root   root        19 1970-01-01 05:30 persist -> /mnt/vendor/persist
dr-xr-xr-x 547 root   root         0 1970-01-01 05:30 proc
lrwxrwxrwx   1 root   root        15 1970-01-01 05:30 product -> /system/product
drwxr-xr-x   3 root   root        60 1970-01-01 05:30 res
drwxr-x---   2 root   root       120 1974-03-19 08:50 root
drwxr-xr-x   3 root   root       320 1974-03-19 08:50 sbin
lrwxrwxrwx   1 root   root        21 1970-01-01 05:30 sdcard -> /storage/self/primary
-rw-r--r--   1 root   root   1036232 1974-03-19 08:50 sepolicy
drwxr-xr-x   5 root   root       100 2021-12-24 12:28 storage
dr-xr-xr-x  12 root   root         0 1974-03-19 08:50 sys
drwxr-xr-x  18 root   root      4096 2021-09-04 13:21 system
-rw-r--r--   1 root   root      5359 1970-01-01 05:30 ueventd.rc
drwxr-xr-x  15 root   root      4096 2009-01-01 05:30 vendor
```

Android Runtime (ART)

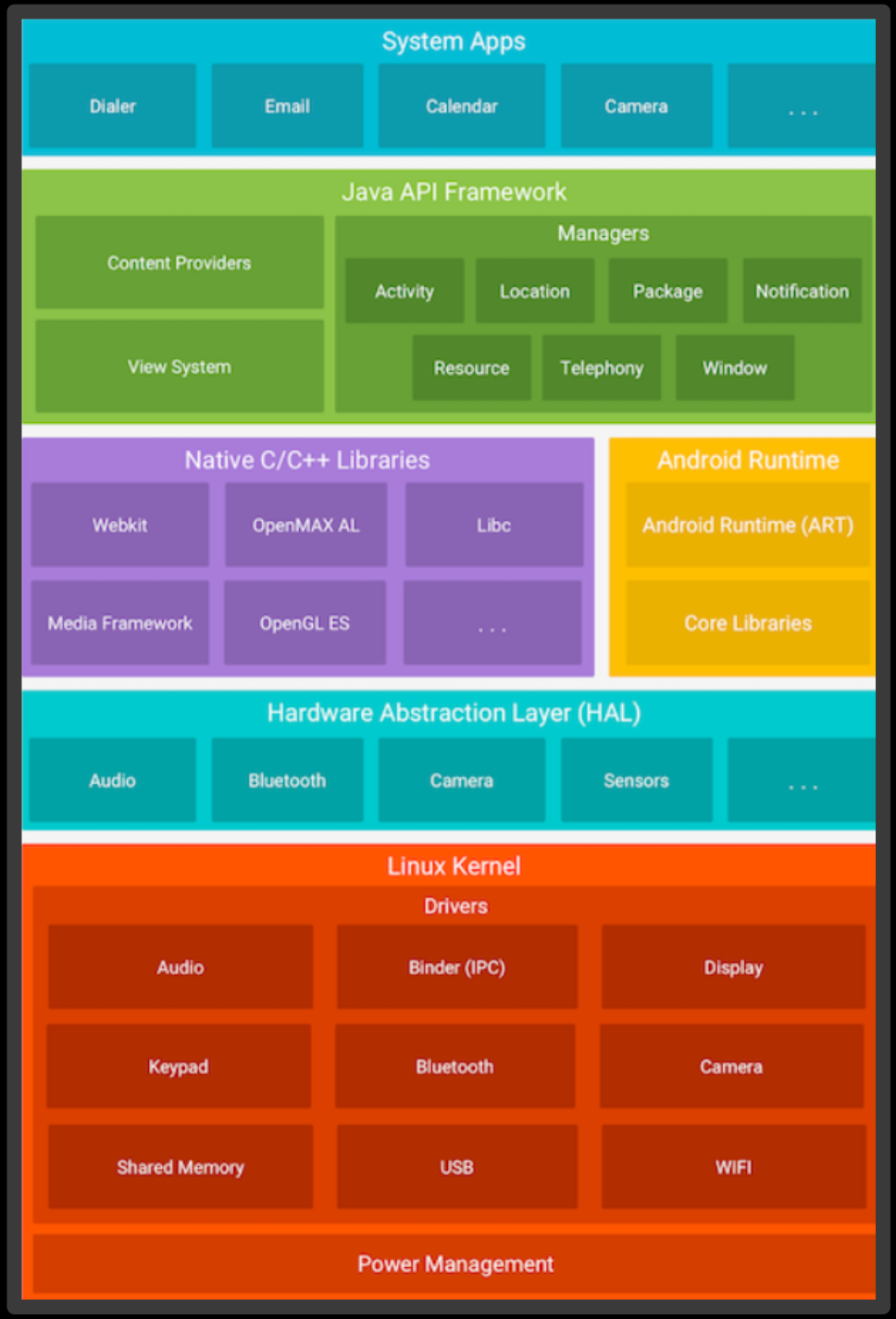
- ART is kind of a translation layer from application’s bytecode to device information.
- For every application there is a own sandbox virtual machine.
- Similarly, in the file system there is separate application system which is creating by new user for respective application.

Android Identity and Access Management

- As each application has it's own user.
  - Those user will assign an user ID which ranges from 10000 to 999999 (like u0_a178 means UID is 10178)
    - Application 1
      - /data/app/com.example.app – generic application data
      - /data/data/com.example.app – runtime storage data
      - /mnt/sdcard/Android/data/com.example.app – externally stored location for runtime
    - Application 2
      - /data/app/com.example.app – generic application data
      - /data/data/com.example.app – runtime storage data
      - /mnt/sdcard/Android/data/com.example.app – externally stored location for runtime

Android Architecture

- Layers of Android Architecture
  - Linux Kernel
  - Hardware Abstraction Layer
  - Libraries
  - Java API Framework
  - System Apps



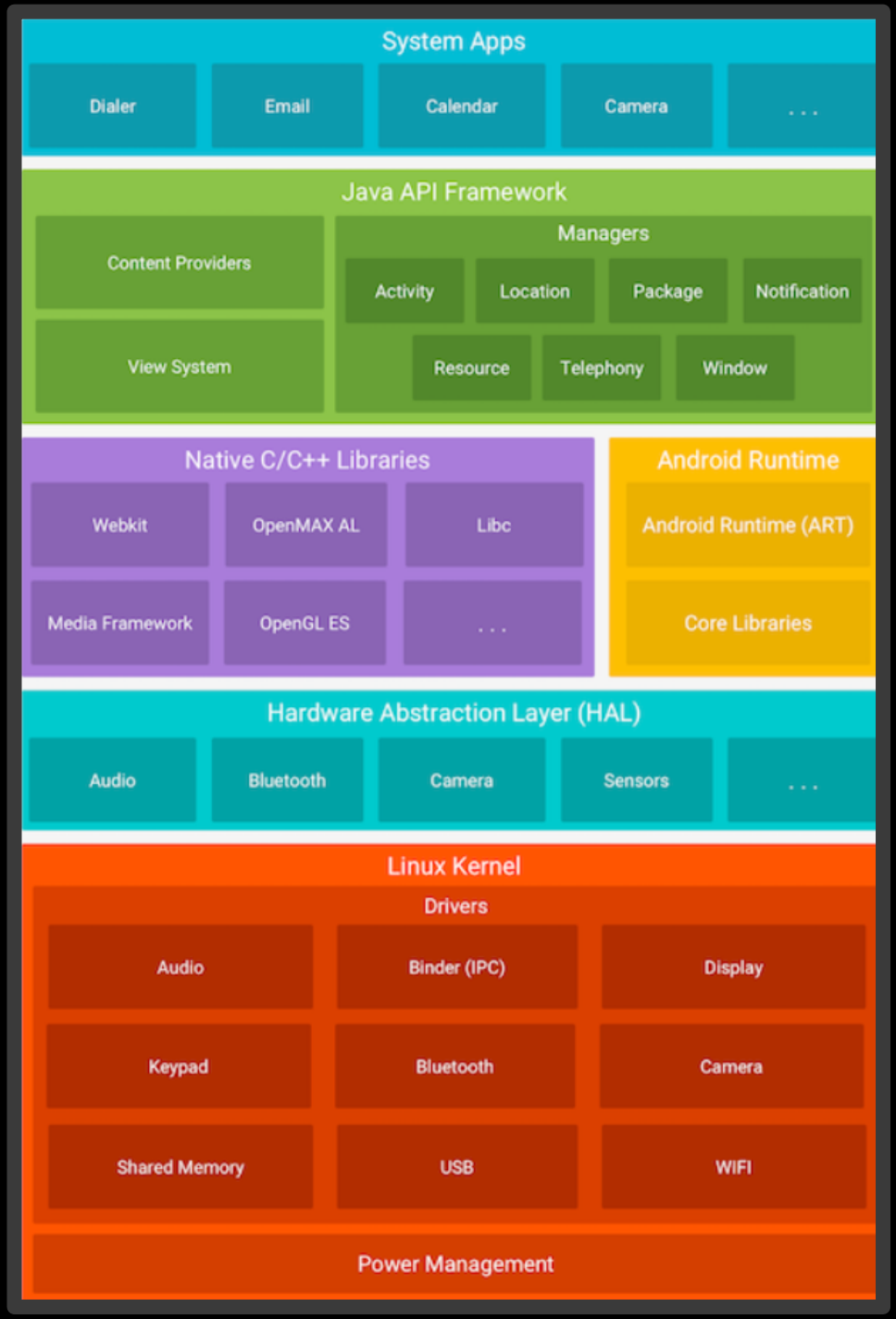
Android Architecture

Linux Kernel

- Link

- Support for different types of CPU in 32 bit and 64 bit architecture
- Android Manifest file of each application mentioned the version of the Android using at that time.

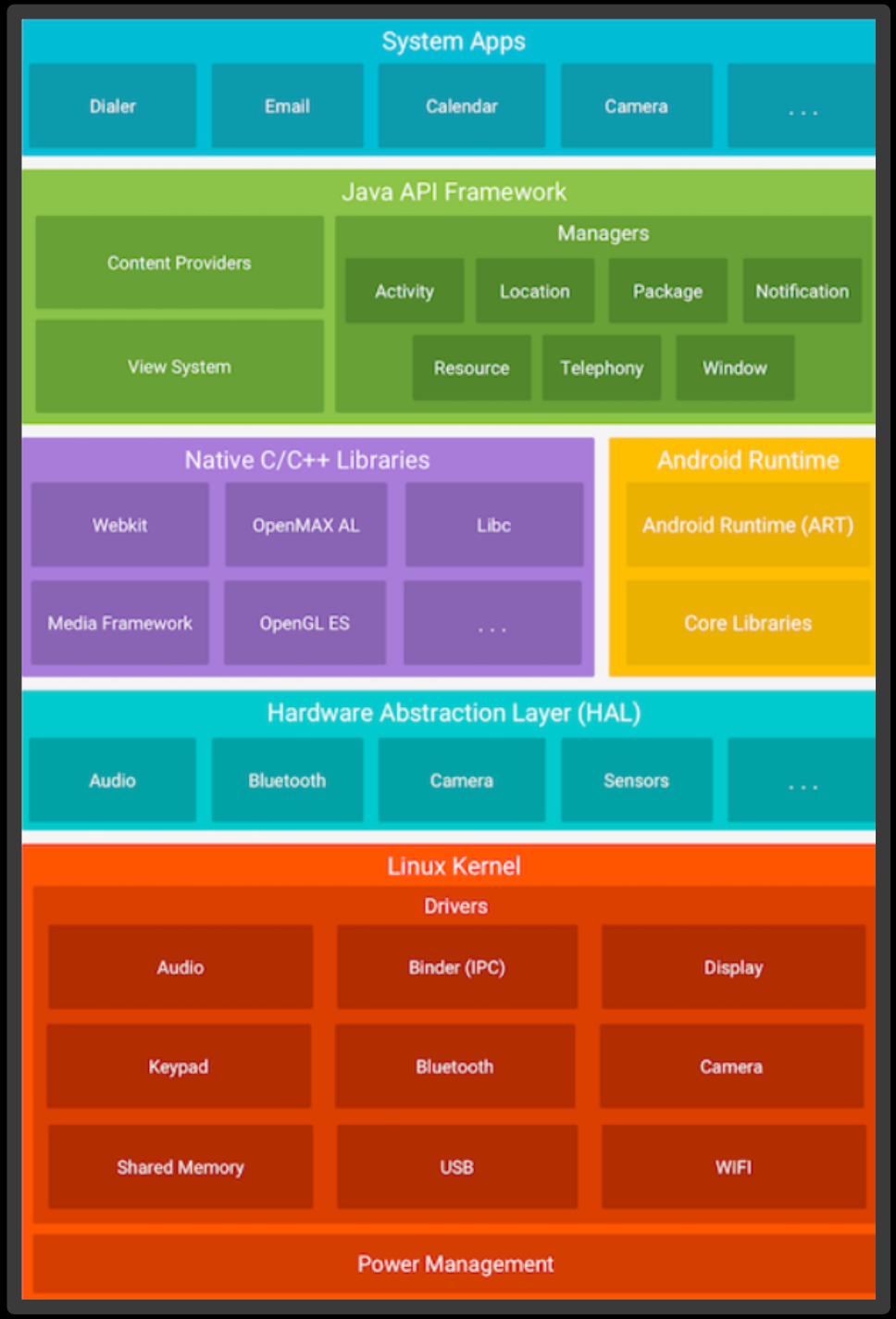
  In short SDK version of the APK



Android Architecture

Hardware Abstraction Layer

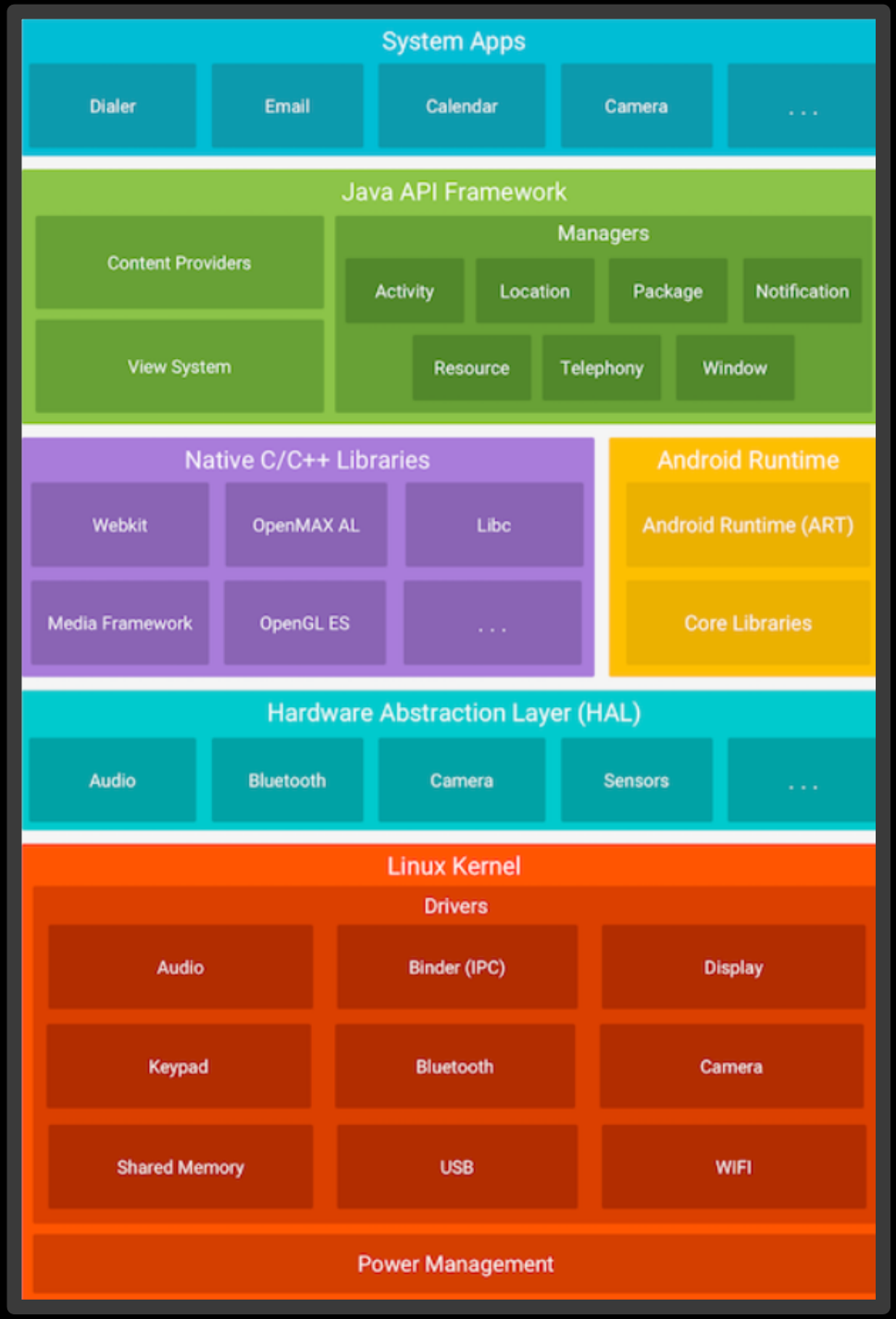
- Layer allows to access the hardware component of the device
  - For example
    - QR code scan to initiate the payment process
    - To scan a document using the built in camera in mobile device.
    - If you using snapchat 😄 then you allow the location to the application.
    - The NFC card again such a great service in TODAY's devices
    - And many other things….



Android Architecture

Native C/C++ Libraries

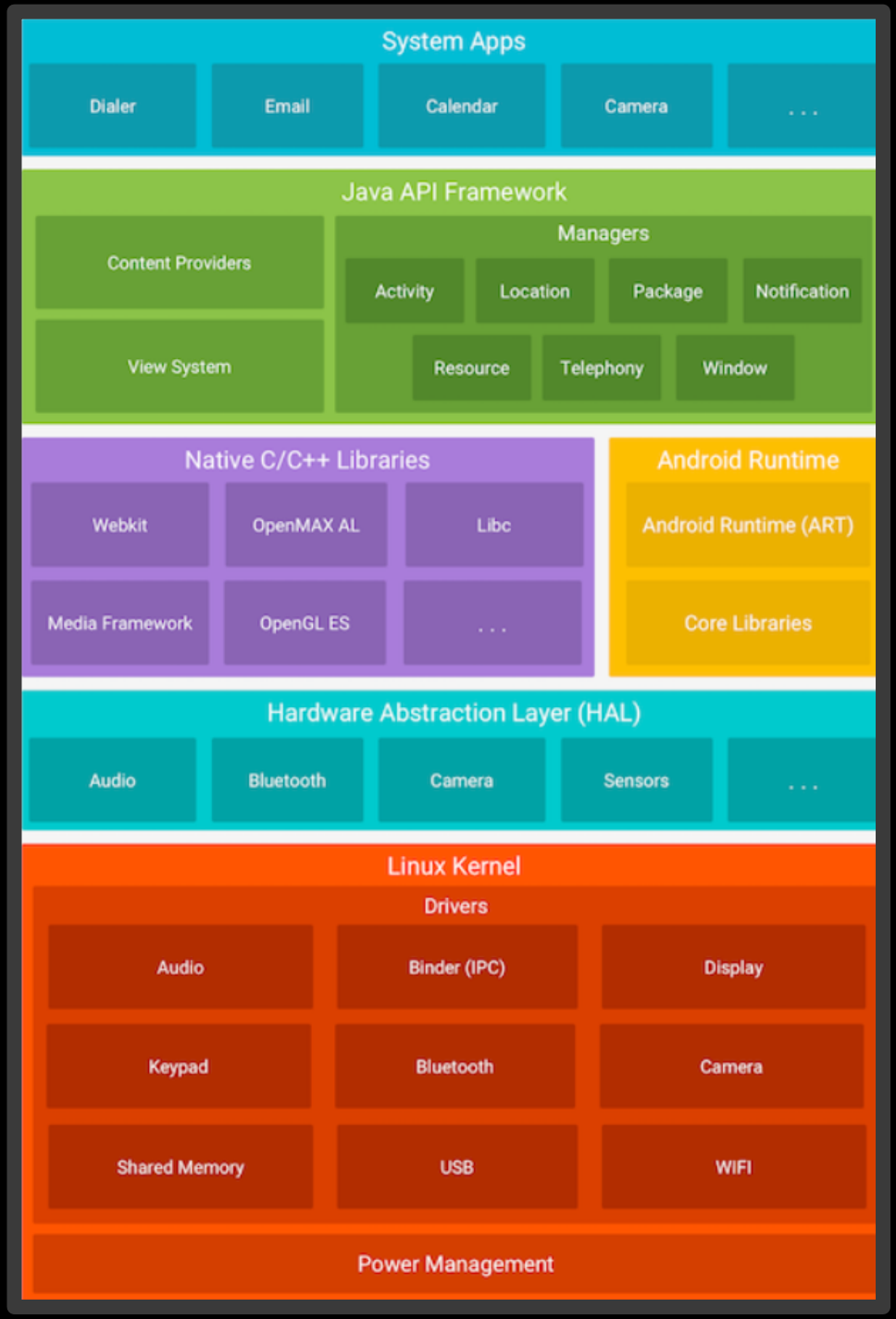
- Webkit : A built in web browser for the application
  - For example any mutual fund application.
- Media Framework
- OpenGL and OpenMAX AL these are the UI framework for 2D and 3D model or design



Android Architecture

Java API Framework

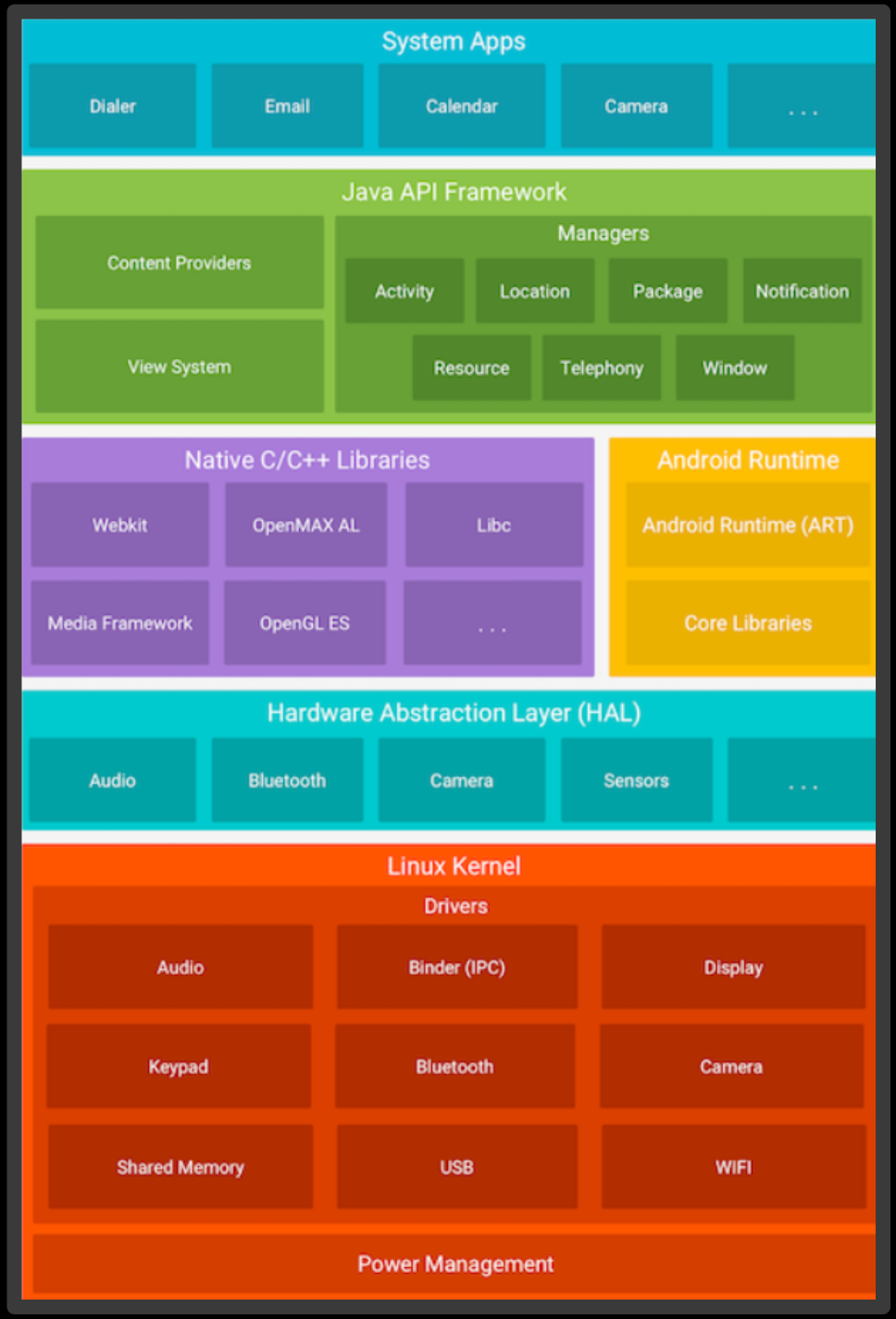
- Basically it allow your application to interact with the other application or services running in your mobile devices
  - Content providers
  - Activity
  - Intent
  - Location
  - Package



Android Architecture

System Apps

- Well system application are those which is pre install in the mobile devices
  - Phone
  - Email or Gmail
  - Camera
  - Calendar
  - Etc



See you on next chapter of this series