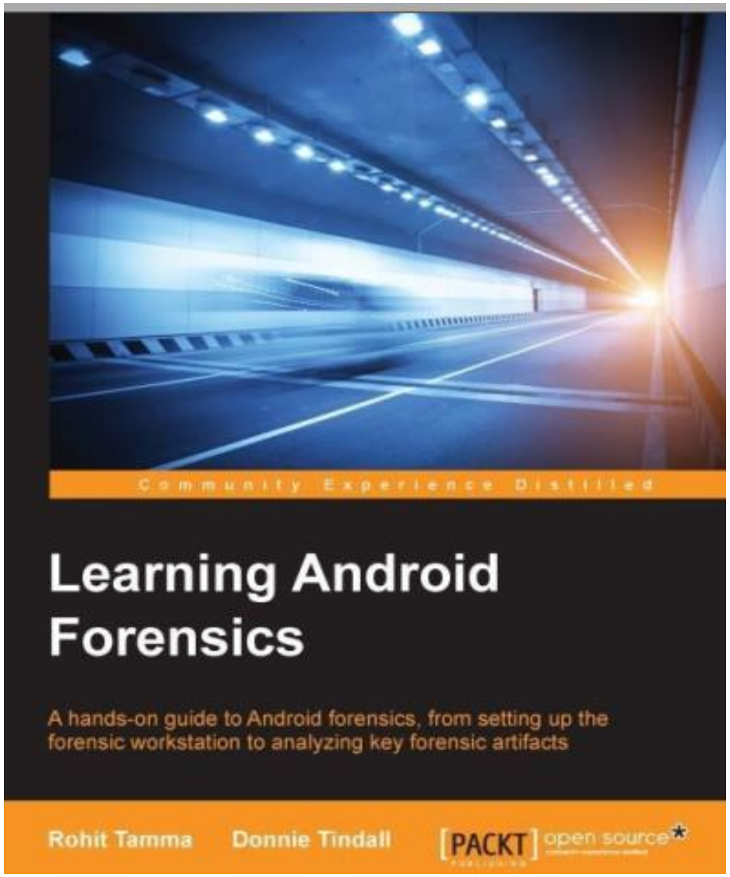
Mobile Phone Security

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

digvijay.rathod@gfsu.edu.in

Android boot process

Reference



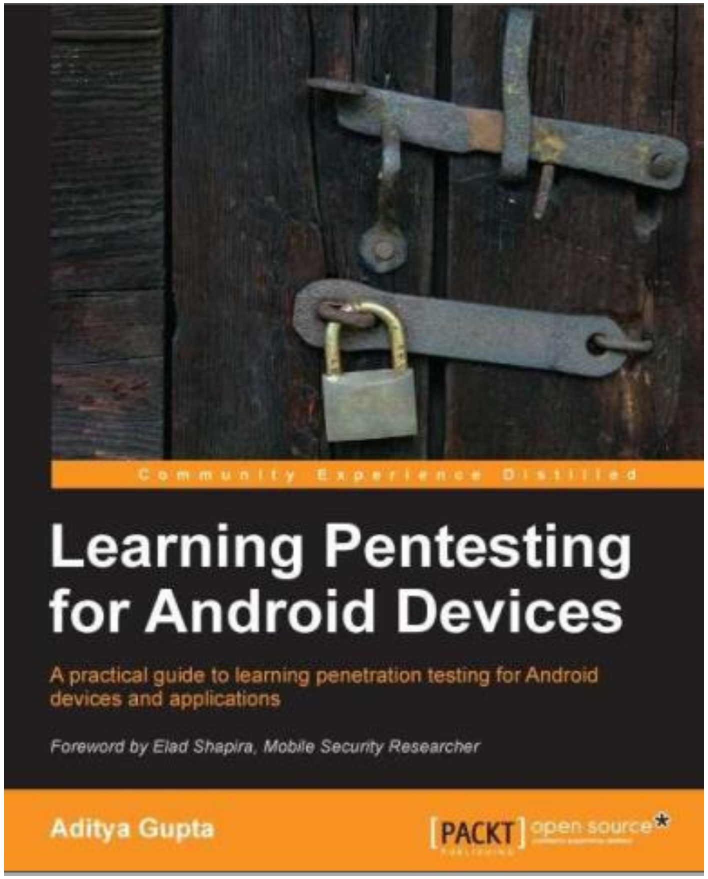
Community Experience Distilled

Learning Android Forensics

A hands-on guide to Android forensics, from setting up the forensic workstation to analyzing key forensic artifacts

Rohit Tamma Donnie Tindall

[PACKT] open source*



Community Experience Distilled

Learning Pentesting for Android Devices

A practical guide to learning penetration testing for Android devices and applications

Foreword by Elad Shapira, Mobile Security Researcher

Aditya Gupta

[PACKT] open source*

Android boot process

✓When an Android device is first powered on, there is a sequence of steps that are executed, helping the device to load necessary firmware, OS, application data, and so on into memory.

Android boot process

✓The sequence of steps involved in Android boot process is as follows:

✓1. Boot ROM code execution

✓2. The boot loader

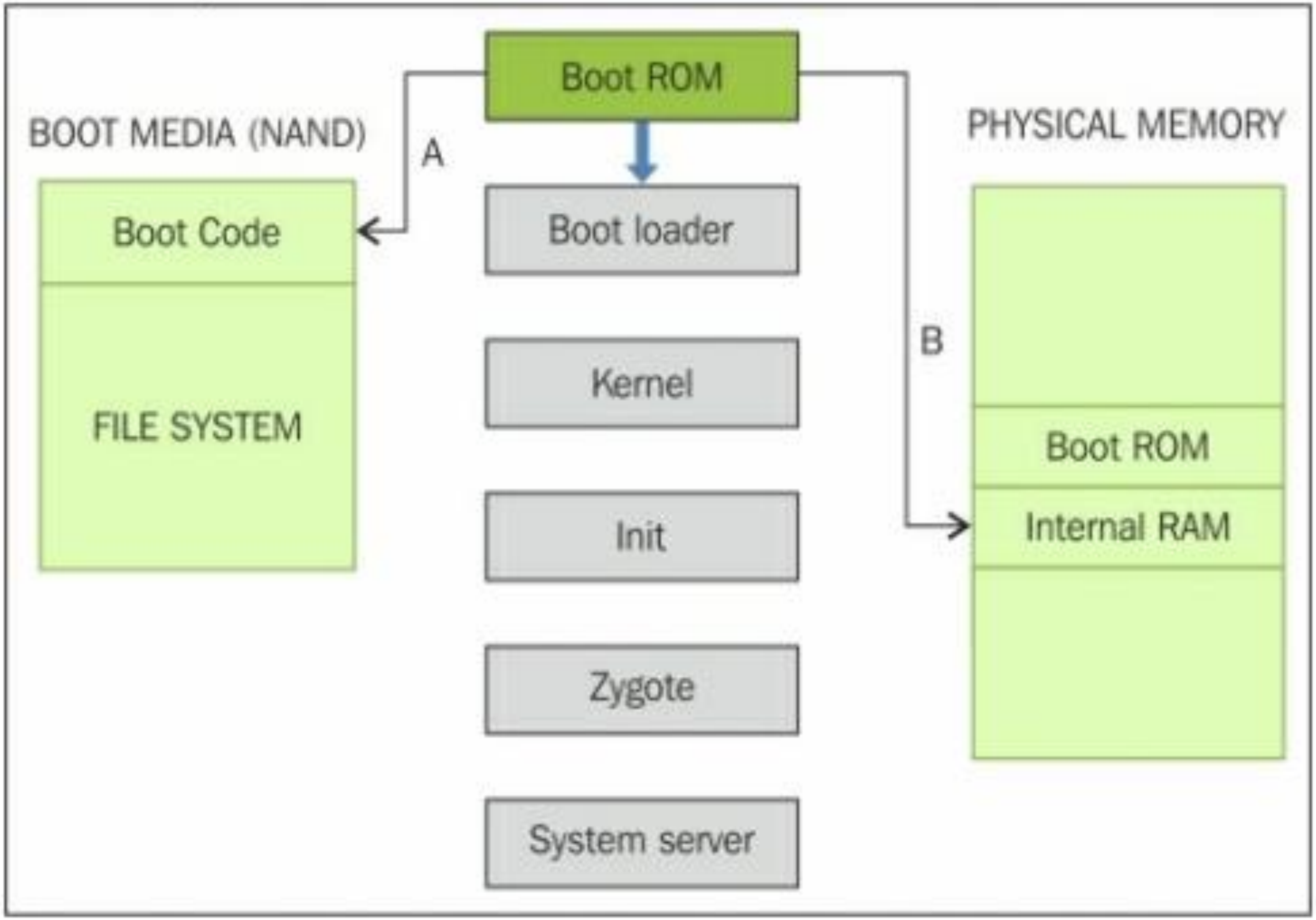
✓3. The Linux kernel

✓4. The init process

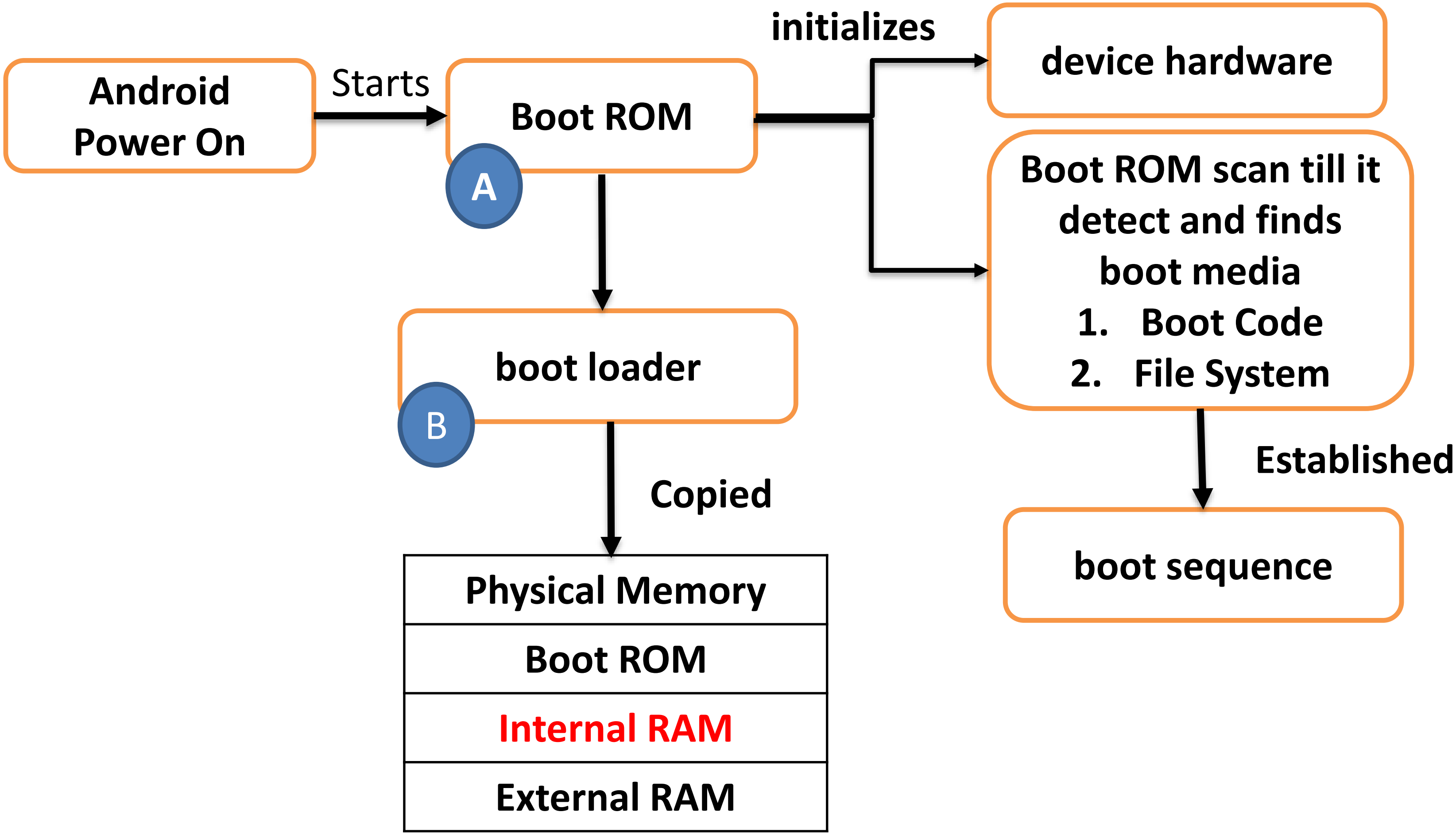
✓5. Zygote and Dalvik

✓6. The system server

Android boot process



Android boot process

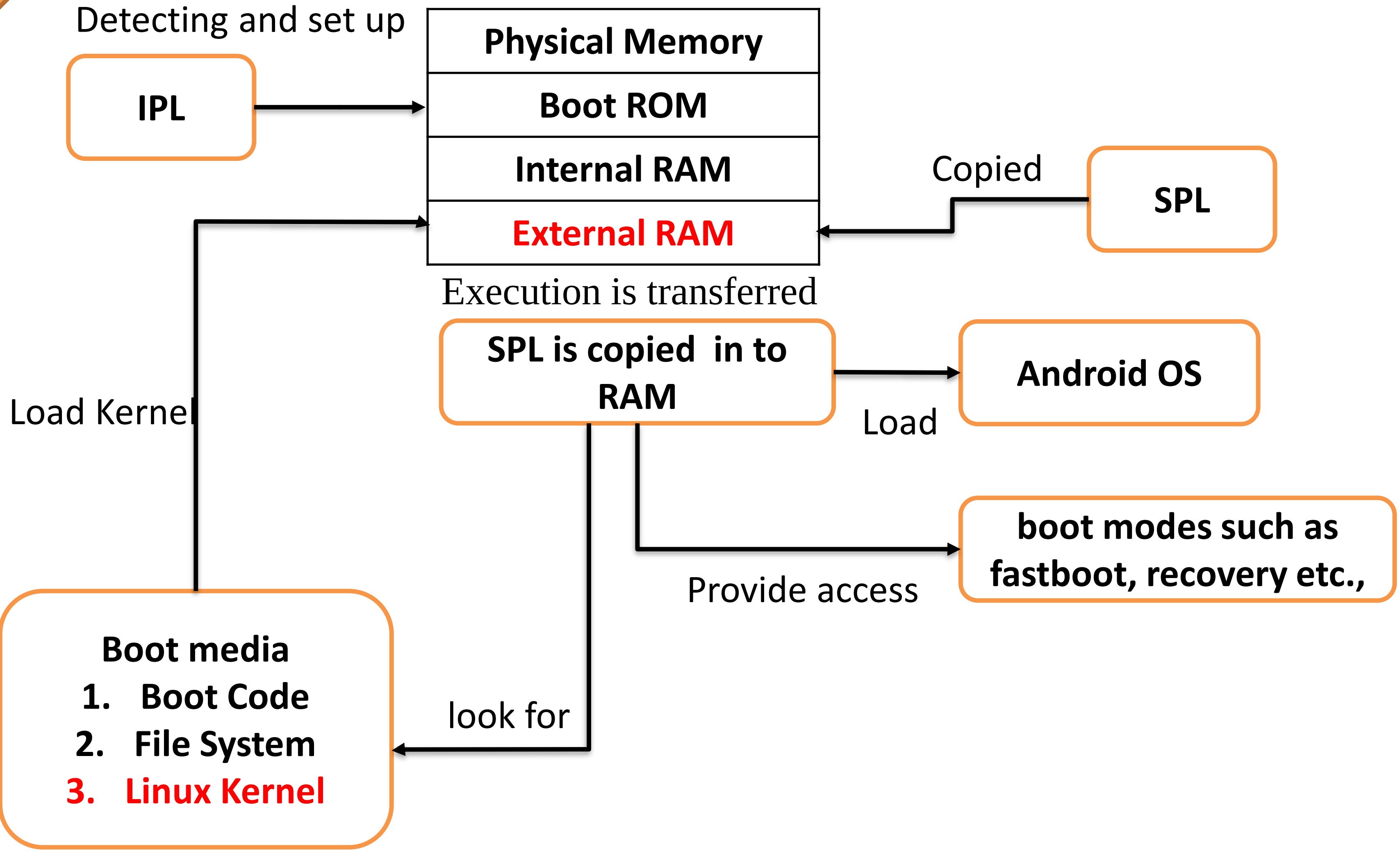


execution shifts to the code loaded into the RAM.

Android boot process – Boot Loader

- ✓The boot loader is a piece of program that is executed before the operating system starts to function.
- ✓there are two stages—
  - ✓initial program load (IPL)
  - ✓second program load (SPL).

Android boot process – Boot Loader



Detecting and set up

IPL

Physical Memory
Boot ROM
Internal RAM
External RAM

Copied

SPL

Execution is transferred

SPL is copied in to RAM

Load

Android OS

Load Kernel

Provide access

boot modes such as fastboot, recovery etc.,

look for

Boot media

1. Boot Code
2. File System
3. Linux Kernel

Dr. Digvijaysinh Rathod

Android boot process – Linux Kernal

- ✓The Linux kernel is the heart of the Android operating system and is responsible for **process management, memory management,** and enforcing security on the device.
- ✓After the kernel is loaded,
- ✓it mounts the root file system (rootfs) and provides access to system and user data.

Android boot process – Linux Kernal

1. When the memory management units and **caches have been initialized**, the system can use virtual memory and launch user space processes.
2. The kernel will look in the **rootfs for the init process** and launch it as the **initial user space process.**

Android boot process – The init process

1. The **init** is the very **first process** that starts and is the root process of all other processes - (**init.rc**).
2. The init process will **parse** the **init.rc** script and launch the system service processes.
3. At this stage, you will see the **Android logo** on the device screen.

Android boot process – Zygote and Dalvik

- ✓ Zygote is one of the first init processes created after the device boots.
- ✓ It initializes the Dalvik virtual machine and tries to create multiple instances to support each android process.
- ✓ Zygote facilitates using a shared code across the VM, thus helping to save the memory and reduce the burden on the system.

Android boot process – System server

- ✓ All the core features of the device such as telephony, network, and other important functions, are started by the system server

Android boot process – System server

- ✓ The following core services are started in this process:
- ✓ Start Power Manager
- ✓ Create Activity Manager
- ✓ Start Telephony Registry
- ✓ Start Package Manager
- ✓ Set Activity Manager Service as System Process
- ✓ Start Context Manager etc.,

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