Mobile Forensics

1.1 Mobile Devices

A mobile device is a portable computing platform characterized by integrated sensors (e.g., GPS, accelerometer, biometrics) and wireless connectivity (e.g., LTE/5G/Wi-Fi). Common example include smartphones, tables, and feature phones.

Memory. Mobile devices contain two main types of memory: volatile and non-volatile.

- *Volatile*: Volatile memory (or RAM) temporarily holds running processes, transient data, and essential information like cryptographic session keys. Its contents are lost immediately upon power-off. Consequently, live RAM extraction is a highly challenging forensic procedure on modern mobile devices, often requiring prior device compromise.
- *Non-Volatile*: Non-volatile memory is persistent, meaning its contents remain intact even when power is lost or the device is rebooted. This memory stores the Operating System, installed applications, and all user data. Contemporary devices rely on encrypted NAND-based storage for this persistence.

Feature	**NOR**	**NAND**
Cell Connection	Parallel	Serial (Block-based)
Read Speed	Very fast (ideal for code execution)	Slower for random access
Write/Erase Speed	Slower	Faster
Storage Density	Lower	High
Cost per bit	Higher	Cost-efficient

Table 1 / Comparison between NOR and NAND flash memory architectures.

Early feature phones often employed NOR flash for the operating system due to its fast read speeds, alongside RAM for temporary data. As storage needs increased, smartphones transitioned to NAND flash for higher capacity and performance. Modern smartphones now use NAND flash exclusively for storage, paired with RAM for temporary data, driven by the need for superior speeds, greater storage density, and better cost efficiency.

To manage the NAND memory, two main packaged solutions are used:

- *eMMC (embedded MultiMediaCard)*: This is a flash storage solution that combines the NAND memory and a controller into a single package. It simplifies device design and is cost-efficient, typically found in older or lower-end devices.
- *UFS (Universal Flash Storage)*: This represents a high-performance, advanced flash storage standard. A key advantage of UFS is its support for full-duplex operations, allowing it to read and write data simultaneously, which significantly improves overall device performance compared to eMMC.

File Systems. The underlying operating system dictates the file system structure. Since Android is based on the Linux kernel, it traditionally utilizes Linux-based file systems. However, in modern devices, manufacturers like Samsung have introduced F2FS (Flash-Friendly File System). F2FS is optimized for NAND flash memory, featuring mechanisms like checkpointing and reduced write amplification, which extends the lifespan of the NAND cells. iOS utilizes the Apple File System (APFS), which succeeded the older HFS+. APFS is optimized for modern iOS devices, providing native support for features critical in forensics, such as strong encryption and snapshots.

1.2 SIM Cards.

SIM cards are secure microcontroller-based devices. They securely store elements (like subscriber identity and authentication material) that are essential to enable communication in GSM networks. As today, most user data is no longer stored on the SIM. Only identity and authentication remain critical. The content is a processor, persistent electronically erasable programmable read only memory (EEPROM) between 16 and 128 KB, RAM for program execution, ROM for the operating system, user authentication, data encryption algorithms and other applications. Software-side, we can refer to them with the term Universal Integrated Circuit Card (UICC). They securely store elements that are essential to enable communication in GSM networks. The International Mobile Subscriber Identity (IMSI) is a number that uniquely identifies a mobile user on the network (64 bit). It consists of MCC, MNC and MSIN. The ICCID is the unique serial number assigned to, maintained within, and usually imprinted on the UICC (19-20 chars). Cryptographic keys used to secure communication and authenticate the subscriber and the network in mobile communication systems.