

A Lawyer's Guide To Understanding Mobile Devices and Forensics
Defender Services Office Training Division: Winning Strategies Seminar
May 19-21, 2016, Denver, Colorado
John C. Ellis, Jr.

Presentation Outline

1. What Is A Mobile Device

- a. Mobile device features are constantly changing, so it is difficult to define the term “mobile device”. However, as features change, so do threats and security controls, so it is important to establish a baseline of mobile device features. The following hardware and software characteristics collectively define the baseline for the purposes of this publication:
 - i. A small form factor;
 - ii. At least one wireless network interface for network access (data communications);
 - iii. This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the Internet or other data networks;
 - iv. Local built-in (non-removable) data storage;
 - v. An operating system that is not a full-fledged desktop or laptop operating system;
 - vi. Applications available through multiple methods (provided with the mobile device, accessed through web browser, acquired and installed from third parties).

[Guidelines for Managing the Security of Mobile Devices in the Enterprise](#)

- 2. Binary—describes a numbering scheme in which there are only two possible values for each digit: 0 and 1. This is the foundation of digital data.
 - a. Bits and Bytes
 - i. A bit is the smallest measurement: either a 1 or a 0.
 - ii. A byte contains 8 bits.

1. Example

D	00001101
e	00001110
f	00001111
e	00001110
n	01101110
d	00001101
e	00001110
r	01110010

2. Using the above example, if “Defender” was saved as a text file, the file size would be 8 bytes.

3. Metadata—a set of data that describes and gives information about other data.

a. Examples

- i. The time and date a photograph was created;
- ii. The data an application was downloaded; and
- iii. The last time a file was accessed.

4. How Digital Data is Stored—data is stored in unallocated space, and once stored, the space is allocated.

- a. Unallocated Space—is logical space in a digital device’s operating system can place data.
- b. Allocated space—is the space in a digital device’s operating system has already placed data.

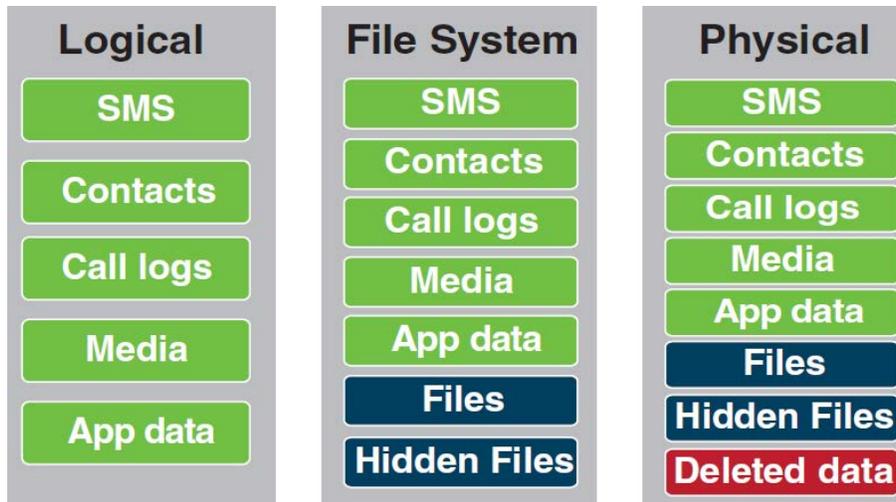
5. Mobile Forensics

- a. Acquiring Data—Acquisition is the process of imaging or otherwise obtaining information from a mobile device and its associated media. Performing an acquisition at the scene has the advantage that loss of information due to battery depletion, damage, etc. during transportation and storage is avoided. Off-site acquisitions unlike a laboratory setting may be challenging in finding a controlled setting in which to work with the appropriate equipment while satisfying additional prerequisites. For the purpose of this discussion, a laboratory environment is assumed throughout this chapter.

The forensic examination begins with the identification of the mobile device. The type of mobile device, its operating system, and other characteristics determine the route to take in creating a forensic copy of the contents of the device. The type of mobile device and data to be extracted generally dictates which tools and techniques should be used in an investigation.

i. Types of Acquisitions (or Extractions):

1. Logical Extraction— acquires a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical storage (e.g., a file system partition). Logical acquisition has the advantage that system data structures are easier for a tool to extract and organize. Logical extraction acquires information from the device using the original equipment manufacturer application programming interface for synchronizing the phone's contents with a personal computer. A logical extraction is generally easier to work with as it does not produce a large binary blob. However, a skilled forensic examiner will be able to extract far more information from a physical extraction.
2. File System Extraction—acquires data by relying on software to access the device's memory; however, rather than obtain a bit-for-bit image including unallocated space, the software extracts only the device file system.
3. Physical Extraction—acquires data from both allocated and unallocated space, including logical data, deleted data, and hidden data.



[What Happens When You Press The Button? Explaining Cellebrite UFED Data Extraction Processes.](#)

- b. **Reviewing Data**—the examination process uncovers digital evidence, including that which may be hidden or obscured. The results are gained through applying established scientifically based methods and should describe the content and state of the data fully, including the source and the potential significance. Data reduction, separating relevant from irrelevant information, occurs once the data is exposed. The analysis process differs from examination in that it looks at the results of the examination for its direct significance and probative value to the case. Examination is a technical process that is the province of a forensic specialist. However, analysis may be done by roles other than a specialist, such as the investigator or the forensic examiner.

The examination process begins with a copy of the evidence acquired from the mobile device. Fortunately, compared with classical examination of personal computers or network servers, the amount of acquired data to examine is much smaller with mobile devices. Because of the prevalence of proprietary case file formats, the forensic toolkit used for acquisition will typically be the one used for examination and analysis. While interoperability among the acquisition and examination facilities of different tools is possible, only a few tools support this feature. Examination and analysis using 3rd party tools are generally accomplished by importing a generated

mobile device memory dump into a mobile forensics tool that supports 3rd party mobile device images.

The forensic examiner will need information about the case and the parties involved to provide a starting point for potential evidence that might be found. Conducting the examination is a partnership between the forensic analyst or examiner and the investigator. The investigator provides insight into the types of information sought, while the forensic examiner provides the means to find relevant information that might be on the system.

The understanding gained by studying the case should provide ideas about the type of data to target and specific keywords or phrases to use when searching the acquired data. Depending on the type of case, the strategy varies. For example, a case about child pornography may begin with browsing all of the graphic images on the system, while a case about an interrelated offense might begin with browsing all Internet history files.

[Guidelines on Mobile Device Forensics.](#)

6. Hash Values—is a numeric value of a fixed length that uniquely identifies data. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures. You can sign a hash value more efficiently than signing the larger value. Hash values are also useful for verifying the integrity of data sent through insecure channels. The hash value of received data can be compared to the hash value of data as it was sent to determine whether the data was altered.
7. Reliance on Mobile Forensic Programs—with all digital forensic tools and techniques, an examiner should not rely on a single tool to interpret the data. The forensic program makes it possible for a trained and experienced examiner to validate data, but only after comparing the data with the investigation and/or other forensic programs.

[Will Your Mobile Evidence Stand Up In Court? 4 Questions to Ask When Evaluating the Forensic Soundness of Mobile Forensics Tools.](#)