Mobile Device Tool Classification System (NIST)

Manual Extraction – Involves viewing the data on a mobile device. The content displayed on the screen requires the manual manipulation of the device and information may be recorded using a camera. At this level, it is impossible to recover deleted information. Can be very time consuming and the data on the device may be inadvertently modified, deleted or overwritten. Become difficult and perhaps unachievable when encountering a damaged device or when the device is configured to display a language unknown to the investigator.

Logical Extraction – Extraction of user level data via a forensic tool. Typically, deleted data is not recovered at this level. On some devices, forensic tools may extract file systems at this level. The database files may contain deleted data.

Hex Dumping and JTAG (Also referred to as Physical Extraction) – Extraction methods afford the forensic examiner more direct access to the raw information stored in flash memory. The entire physical memory is obtained and deleted data may be recovered. Joint Test Action Group (JTAG) allows for imaging devices that are locked or devices that may have minor damage and cannot be properly interfaced otherwise.

Chip-Off – Acquisition of data directly from a mobile device's flash memory. This extraction requires the physical removal of flash memory. Extensive training is required in order to successfully perform extractions at this level. Chip-Off extractions are challenging based on a wide variety of chip types, a myriad of raw data formats, and the risk of causing physical damage to the chip during the extraction process.

Micro Read – A Micro Read involves recording the physical observation of the gates on a memory chip with the use of an electron microscope. This level would require a team of experts, proper equipment, time and in-depth knowledge of proprietary information. There are no commercially available Micro Read tools.