Cyber Sleuth Science Lab
Basic Mobile Device Examination Process

Mobile device technology is evolving rapidly, making it difficult to keep up with changes in operating system, native applications, and 3rd party applications. How can you keep up with new technology and applications, and reduce the risk of missing valuable digital evidence? No single tool can solve this challenge – it is necessary to follow a methodical process each time you perform a forensic examination of a mobile device.

This process is provided for forensic examination of any mobile device, including Android, iOS, and IoT devices, even when you are not familiar with the particular file system structure and applications. This process is independent of specific tools, but illustrative examples involving various tools may be included to demonstrate certain steps.

This process connects with the forensic concepts of reliability, repeatability and documentation.

1) **Inspect Device & Account Details**
   a) Inspect device details: What type of device, version, phone number, etc.
   During the initial stages of an investigation, it might not be clear who used which mobile device, or which device was in active use during the time of interest. Furthermore, when a case involves multiple mobile devices of the same type, one device might be mistaken for another. As a result, there is a risk that a given mobile device is not the one that was expected, or does not contain information from the time of interest. Therefore, as a first step, inspect phone information and user account details to confirm that the mobile device is consistent with the individuals or case you are investigating. The sooner you realize that the device is not the one you expected, the more likely you will be able to resolve the issue. For instance, checking the phone number and contacts can provide a quick verification that a specific individual used the mobile device. In addition, checking the dates of activities on the device can verify that the device was in use when the offense occurred.

   b) Review user accounts
   The user accounts configured on a mobile device can give a good indication of who used the device. Most mobile devices have a location where multiple user accounts are stored, such as the iOS Accounts database and the Blackberry Service Book. User account information can also be useful for recognizing online data sources such as webmail and cloud storage, which might require legal authorization to obtain related digital evidence.

2) **Survey Installed Applications**
   Carefully inspect a list of applications that are installed, or were used, on the mobile device. Mobile device forensic tools may provide a list of installed applications,

including the permissions assigned to each application provide clues about its capabilities, including the ability to use the camera and make phone calls.

3) **Survey File System**

Perform a preliminary inspection of the file system on the mobile device to find areas that may contain user created data. Look for recently modified files that may have resulted from user activities on the mobile device, large files that contain communications and multimedia, and deleted files that the user may have attempted to destroy prior to the mobile device being seized as evidence.

a) <u>Look at recently created or modified files</u>

Use a forensic tool to examine a list of all files, sorted in chronological order by creation or last modification date, and inspect these files to determine what activities and applications were performed on the mobile device most recently.

b) <u>Look at very large files</u>

Use a forensic tool to examine a list of all files, sorted by size, and inspect the largest files to determine whether they contain information of probative value.

c) <u>Look at recently deleted files</u>

Use a forensic tool to examine a list of all deleted files that are recoverable within the file system, and inspect them to determine whether they contain information of probative value.

4) **Perform Keyword Searches**

Conduct keyword searches to determine where specific terms of interest are stored on the device. For instance, if a username or phone number is known, determine where this information is stored on the device. Once found, perform further analysis to determine whether there is more information of interest in the application or area that contains the keyword hits.

5) **Examine Pictures and Videos**

Use a forensic tool to examine pictures and videos on mobile device to determine whether they contain relevant information.

6) **Forensic Reconstruction**

Any new information found during forensic examination should be incorporated into the overall forensic reconstruction (timelines, link diagrams, etc.) and used for keyword searching. Steadily building this reconstruction of events continues until digital investigators are satisfied that they have a sufficient understanding of the crime.