Research - Acquisition and Analysis Guideline

1) Documentation
   a) Document the following specific information about each device (if applicable)
      i) Serial Number
      ii) Model Name
      iii) Model Number
      iv) Exterior and interior photographs of the device, showing any labels or identification numbers. Note: Pictures of the complete circuit board are very helpful.
      v) FCCID
         (1) MAC Address for each network hardware on the device (Wi-Fi, Ethernet, Bluetooth, Zigbee, etc. Typically, available through an NMAP scan.)
   b) Document timestamp of functions such as removal from network, unplugging from power source, removal of battery, and any other power or acquisition events.
   c) Document all tools used, e.g., “Philips J00 driver, pry tool”.
   d) Take photographs of each tear-down step. Capture complete logic boards and all microchip make and model identifiers.
2) Data Extractions
   a) Work through least invasive to most invasive processes that are available on the device and to you as an examiner. Common extraction methods/protocols may include ADB, UART, SPI, SWD, I2C, CAN, and chip-off.
   b) Document all tools used to include make, model, and version number.
   c) Write protect and hash (MD5 and SHA variant of choice) all extraction files.
3) Analysis (Optional)
   a) One of the goals in this project is to identify if a device does or does not store user data and if it does, how does one recover that data from the device. As such, focus analysis efforts on recovering relevant traces such as who interacted with the device, e.g., MAC address(es), when did the interaction occur, where did the action occur.
      i) Document all tools used in furtherance of the above to include make, model, and version number.
      ii) Include data storage locations and any encoding encountered.
   b) Include a summary of traces recovered, or if no traces of user activity were recovered. The absence of user data on a particular device is also helpful to the community.
4) URLs, etc. of existing research

Device

Manufacturer	
Model Name	
Model Number / Part Number	
Serial Number	
FCCID	
IC (Canadian)	
MAC Address (Wi-Fi, Bluetooth, and additional)	
Revision Number	
Build Date	
Firmware Version	
Network Connections (SSID Names)	