**Cyber Sleuth Science Lab**

**Basic Mobile Device Examination**

**DEVICE OWNER: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**DEVICE TYPE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**PHONE NUMBER: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Complete this for each device you investigate)

**1. Inspect Device & Account Details**

* Inspect device details: What type of device, version, phone number, etc.
* Review user accounts: Include online data sources such as webmail and cloud storage

**2. Survey Installed Applications -** List applications installed and used along with their capabilities.

**3. Survey File System**

* List recently created or modified files
* List large files
* List recently deleted files

**4. Perform Keyword Searches -** Using know information search as keywords and list any additional information of interest in the application or area that contains the keyword hits.

**5. Examine Pictures and Videos -** List any additional relevant information contained in the pictures and videos relating to the investigation.

**6. Forensic Reconstruction -** Continue to reconstruct events until satisfied you have sufficient understanding of the incident.