A. Purpose:

To outline the process of imaging and acquiring evidence in preparation for examination. In some, but not all, instances, cases within the Computer Crimes Unit may be triaged and imaged/acquired by a different examiner than the analysis part of the examination.

B. Responsibility:

CCEEU forensic personnel

C. Procedure:

1. Evidence Acceptance:
    i. Verify that all tags and other case related paperwork are accurate. Refer to SOP GL 13 if any discrepancies are noticed.
    ii. Verify that the LIMS request is accurate and assigned.
    iii. Transfer evidence into custody within LIMS for examination.
2. Evidence Processing: This portion will be completed by the examiner assigned as the technician.
3. All notes or other documentation generated are to be stored inside the case jacket.
4. Photograph the outside of the submission, as well as the contents.
5. Label the sub-item or submission with the following:
    i. Lab case number
    ii. Sub-item label (Refer to appendix for labeling protocols
    iii. Initials
6. Remove any internal or external storage media including, but not limited to, hard drives, memory cards, optical discs and label in the same manner.
    i. Refer to SOP GL 4 about sub-item labeling if containerizing within LIMS.
7. Perform the acquisition; refer to the steps below based on the type of device.
8. Once acquisition is completed, the submission needs to be reassembled, packaged, and sealed appropriately.
    i. If possible, all laptop and cell phone batteries should be left disconnected.
    ii. All internal hard drives in computers should be plugged back in the way they were found originally.
9. Transfer within LIMS into the appropriate storage location.
10. If the evidence is to be fully examined at a later date, perform the following steps for virtual evidence storage. If it is to be examined by the same examiner simultaneously, this does not need to be completed.

i. Under the first piece of evidence tied to the request, create a sub-item and label it 'CC Evidence Files'.
ii. Remove the inherit and containerize options.
iii. Chain of custody will be transferred from the examiner creating the file to the location 'Computer Crimes – Virtual Evidence Storage'.
iv. Print the barcode generated and affix it to the top inside front cover of the case jacket.

11. The case jacket will be handed to the supervisor. The examination portion may be assigned for the next examiner to complete.
12. If during the imaging process it is determined that the sub-item is not able to be imaged or extracted by the unit's resources, it may be possible to outsource to a separate agency which has been pre-approved, for example, FBI CART.
    i. If an outside agency has the resources which support the capabilities at this stage, the sub-item may be outsourced.
        1. Refer to the Case Management Unit for specifics.
        2. The sub-item or submission will be transferred to Mail Transport, and the request will be changed to 'Computer Crimes Hold' for the duration. It will be indicated in the synopsis in LIMS as to the reason for the hold.
    ii. Once the evidence, as well as the evidence image is returned, analysis may begin using approved software and methods.
        1. Refer to relevant examination SOP for further guidance.
        2. At this point, the request will be changed back from Computer Crimes Hold to the original request for analysis to continue.
    iii. It is up to the examiner to ensure the data provided meets the CCEEU standard to continue with analysis. This is indicated in the analysis notes.
    iv. The final report sent to the customer must indicate the agency, which was used in the outsource, as well as what service they provided, for example, extraction of device.

See below for specific evidence types:

13. Cell Phones, Tablet, Wearable devices
    i. Use approved software/hardware available for extraction purposes.
        1. The technique used for extraction of data from cell phone should be determined by, but not limited to, the examiner's training, knowledge, and experience.

ii. Record information on QR-CC-16.
iii. All available extraction options for the chosen software will be performed. For example, logical, file system, and physical.
iv. All peripheral media will be recorded and acquired in the appropriate manner respective to it. Refer to Digital Storage Media.
    1. SIM cards and/or (micro) SD media cards
v. All original extraction files will be stored on the shared mapped network drive designated for imaging, or the examiner's mapped network drive, in a folder labeled with the lab case number and appropriate sub-item label.
vi. If the device is damaged in a way that may be repaired by a part replacement, it may be performed to allow the device to be examined.
    1. If it is determined that this is necessary to make the phone or tablet function, the examiner is to contact the submitting officer.
    2. It is up to the submitting agency to provide the necessary part(s) for replacement. While waiting, the assigned request will be changed to 'Computer Crimes Hold' for the duration until the process can be completed. It will be indicated in the synopsis in LIMS as to the reason for the hold.
        a. If it is decided not to proceed, the report will indicate no examination could be carried out.
    3. Once completed, the damaged/removed part(s) are to be returned inside the submission.

14. Digital Storage Media (computers, memory cards, etc.)
    i. Use approved software/hardware available for extraction purposes.
        1. The technique used for extraction of data from digital media should be determined by, but not limited to, the examiner's training, knowledge, and experience.
        2. Optical disks may be previewed initially for their content and only imaged if deemed necessary by the examiner.
    ii. Record information on QR-CC-5 and/or QR-CC-65.
    iii. Utilizing approved software, acquire the device (preferably E01 format) and store results on the shared mapped network drive designated for imaging, or the examiner's personal mapped network drive, in a folder labeled with the lab case number, and correct sub-item label.
    iv. Verify the acquisition. Simultaneously if possible, during the acquisition, or after if the software utilized does not allow it.

v. When image processing failure occurs (e.g. does not complete), the image process should be repeated using current imaging software and different hardware, if possible. If the second attempt fails, the imaging process should be performed using another approved software.
vi. If the third attempt fails, the analyst should consult with the Technical Lead/Unit Supervisor, to determine how to proceed and document this in the notes.
vii. If read errors and/or bad sectors were reported, document these findings.
viii. If encryption is found on the evidence, note this, and the type, if possible, on QR-CC-05.
    1. For example, if BitLocker or FileVault encryption is encountered, the examiner is to utilize any provided user login credentials or reach out to the agency for guidance on either the user account or associated key file.
    2. If a different type of encryption is encountered, the drive should be imaged fully and addressed in the notes for the examiner performing the analysis portion.

D. References:
    1. Training books and notes from applicable software
    2. Help file located either online or within the applicable software