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 all tags and other case related paperwork are accurate. Refer to SOP GL 13 if any discrepancies are found.
   ii. Verify 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 disks 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 back into the appropriate storage location.
10. The case jacket will be handed into the supervisor. The examination portion may be assigned for the next examiner to complete.

State of Connecticut Department of Emergency Services and Public Protection
Division of Scientific Services
Documents outside of the QMS are considered uncontrolled.

See below for specific evidence types:

11. 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.
12. 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.
    iii. Perform a pre-hash analysis on each sub-item, using approved software and record all appropriate data in the notes.
        1. Note, in certain instances, such as with Paladin and Recon, this is not able to be performed.
    iv. Utilizing an 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.
    v. 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

State of Connecticut Department of Emergency Services and Public Protection
Division of Scientific Services
Documents outside of the QMS are considered uncontrolled.

passwords, 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.

    vi. In instances when the hash values do not match, perform the following:

1. If read errors and/or bad sectors were encountered in the pre-hash process and/or in the imaging process, document these findings. It is not necessary to attempt the image process again.
2. If no read errors and/or bad sectors were encountered in the pre-hash process and in the image process, repeat steps iii and iv.
3. When image processing failure occurs (e.g. does not complete), the image process should be repeated using the current imaging software and different hardware, if possible. If the second attempt fails, the imaging process should be performed using another approved imaging software.
4. 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.

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

State of Connecticut Department of Emergency Services and Public Protection
Division of Scientific Services
Documents outside of the QMS are considered uncontrolled.