A. Purpose:

To outline the steps taken to image a hard drive submitted to the CCEEU for analysis while maintaining the integrity of the evidence.

B. Responsibility:

CCEEU forensic examiners

C. Definitions:

Refer to SOP-CC-26 - Definitions and Abbreviations.

D. Procedure:

1. Connect the evidence drive to a forensic computer using an approved read-only hardware device. Document the make, model and serial#/Tag# of the write block / read-only hardware device using Laboratory Notes (QR-CC-5).
2. Connect a staging drive(s) to the forensic computer.
3. Create a folder on the staging drive to image to or access the staging partition on the server. Name the folder the specific Laboratory Case Number.
4. Using an approved hashing program (e.g. FTK Imager) and following the procedures outlined in the product manual or training documentation, obtain the pre-imaging MD5 and/or SHA1 hash values of the evidence drive prior to imaging. Document the pre-acquire hash software application version, sector count and the pre-acquire hash values in the Laboratory Notes(QR-CC-5)
5. Make a forensic image of the evidence drive saving it to the folder created on the staging drive using an approved imaging software program. Follow the imaging procedures outlined in the product manual or training documentation.
   a. If using EnCase to create the image, follow the protocols outlined in the Reference Document pertaining to the associated EnCase version. Follow the naming conventions outlined in Appendix A - EnCase Naming Conventions when filling in the acquisition information.
   b. If using FTK Imager to create the image, follow the protocols outlined in the Reference Document pertaining to the associated FTK Imager version. Follow the naming conventions outlined in Appendix A - FTK Imager Naming Conventions when filling in the acquisition information.
   c. If using TD1 Forensic Duplicator to create the image, follow the protocols outlined in the Reference Document pertaining to the associated TD1 Forensic Duplicator version. Follow the naming conventions outlined in Appendix A - TD1 Forensic Duplicator Naming Conventions when filling in the acquisition information.
6. Upon completion, document the acquisition software version, staging drive # or staging path, forensic system OS , sector count, drive capacity and the image hash values in the Laboratory

Notes(QR-CC-5). Ensure that the pre-imaging hash values and the image hash values match. If the values are identical, remove the evidence drive and proceed processing the case.

7. In instances when the hash values do not match, follow the following procedures:
   a. 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.
   b. If no read errors and/or bad sectors were encountered in the pre-hash process and in the image process, repeat steps 4 through 6. In the event that this process again fails, it is at the examiner's discretion, based on his/her knowledge, training, experience and in consultation with the Technical Lead or Unit Supervisor, to determine how to proceed. In a narrative format, document all steps taken, to include any observations made and additional steps taken during the process using Laboratory Notes (QR-CC-5).
8. When image processing failure occurs (e.g. does not complete), the image process should be retried using the current imaging software. If the second attempt fails, the imaging process should be performed using another approved imaging device or software.
9. If the third attempt fails, it is at the examiner's discretion, based on his/her knowledge, training, experience and in consultation with the Technical Lead or Unit Supervisor, to determine how to proceed. In a narrative format, document all steps taken up to this point, to include any observations made and additional steps taken during the process using Laboratory Notes (QR-CC-5).
10. If it is determined that the drive cannot be analyzed, the submitting agency should be notified and alternative options should be discussed and documented.
11. Proceed with processing the case.