A. Purpose:

To outline the steps taken to generate a new EnCase case file.

B. Responsibility:

CCEEL forensic examiners.

C. Definitions/Abbreviations:

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

D. Procedure:

1. Prepare a target drive as outlined in CC SOP-2 - Target Drive Preparation Protocol and attach this drive to a forensic computer.
2. Connect the staging drive(s) to the forensic computer.
3. Open the EnCase case file and follow the steps below that represent the method of acquisition used by the examiner.
    a. If the examiner created a new EnCase case file during the imaging process and added the acquired image file(s) directly to the new case proceed to Step 5.
    b. If the examiner created a new EnCase case file during the imaging process and did not add the acquired image file(s) directly to the new case proceed to Step 4.
    c. If the examiner has not created an EnCase case file follow the protocol outlined in the Reference Document, pertaining to the appropriate EnCase version, which outlines how to create a new case. When complete go to Step 5.
4. In order to add existing evidence files to the case follow the protocol outlined in the Reference Document pertaining to the appropriate EnCase version. When complete, proceed to Step 5.
5. Complete the below listed steps prior to any analysis of the data. Use QR-CC-6 - Analysis Notes or other appropriate QR as a documented narrative to describe actions and observations made during the process. In addition, use the Analysis Notes or other appropriate QR to document any pertinent discussions with the investigating agency pertaining to the request for analysis and the results.
    a. Check to see that all of the media to be examined is present in the case file.
    b. Account for all sectors of the physical disk(s) to ensure there are no deleted or missing partitions. Make note of any read errors, missing sectors or CRC errors.
    c. Run a virus scan.
    d. Recover lost folders unless the Operating System installed on the hard drive is Microsoft Windows Vista, Windows 7 or Windows 8. This is due to a problem in which EnCase will find multiple instances of the same files and folders, occupying the same physical locations on the media.
    e. Mount appropriate compressed files.
    f. Verify file signatures and compute hash values.

g. Account for the time zone configuration.
h. Check for any irregularities with file created, last written and last accessed dates.

6. Upon completion of Step 5 proceed with case specific tasks. Use QR-CC-6 - Analysis Notes or other appropriate QR as a documented narrative to describe actions and observations made while performing the case specific tasks. In addition, document on the Analysis Notes or other appropriate QR any pertinent discussions with the submitting agency relating to the examination.

E. Documentation:

1. EnCase user manual
2. EnCase training manual