A. Purpose:

To outline the steps taken to generate a new case file and initiate processing in the specified forensic software application.

B. Responsibility:

CCEEU forensic examiners.

C. Definitions/Abbreviations:

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

D. Procedure:

Note: The use of a particular forensic software application will be dependent on the specifics of the case request, for this reason case initiation may include one or more of the applications listed below. Additional approved forensic tools or software applications (Approved Software QR-CC-49) may also be utilized following case initiation:

EnCase (Guidance Software)-new case file initiation and processing:

1. Prepare a target drive as outlined in CC SOP-2 - Target Drive Preparation Protocol and attach this drive to a forensic computer or access the internal drive partition on the forensic computer.
2. Connect the staging drive(s) to the forensic computer or access the designated server staging partition to access the case evidence acquisition files.
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. The file verification process which is automatically initiated upon the addition of an evidence image file can be canceled. If during the examination process (Steps 6 and 7) an "Invalid Block Checksum" error message occurs, then data corruption in the evidence file has been indicated and the integrity of the sector group(s) cannot be verified as valid. If this error condition should occur then the verification process needs to be initiated and run to completion for the associated evidence file image so that a record of the errors can be generated and documented. After data corruption errors in the evidence file image have been confirmed then acquisition procedures for the source media should be repeated (Refer to the appropriate protocol -CC SOP-05, CC SOP-06, CC SOP-12, or CC SOP-13). Use Analysis Notes (QR-CC-6) to document the errors and actions taken during the process. Proceed to Step 6.

6. Complete the below listed steps prior to any analysis of the data. Use Analysis Notes (QR-CC-6) or other appropriate QR as a documented narrative to describe actions and observations made during the process.
   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. Set-up processor options or run each of the processes below separately.
   e. Recover lost folders. (Note: EnCase version(6.x or prior) if the Operating System installed on the hard drive is Microsoft Windows Vista, Windows 7, Windows 8 or Windows 10 do not run recover lost folders. EnCase version(6.x or prior) will find multiple instances of the same files and folders, occupying the same physical locations on the media)
   f. Mount appropriate compressed files.
   g. Verify file signatures and compute hash values.
   h. Account for the time zone configuration.
   i. Check for any irregularities with file created, last written and last accessed dates.
7. Upon completion of Step 6 proceed with case specific tasks. Use Analysis Notes (QR-CC-6) or other appropriate QR as a documented narrative to describe actions and observations made while performing the case specific tasks. In addition, document in the Analysis Notes or other appropriate QR any pertinent discussions with the submitting agency relating to the examination.

FTK (AccessData)- new case file initiation and processing:

1. Prepare a target drive on the forensic computer as outlined in CC SOP-2 - Target Drive Preparation Protocol and attach this drive to a forensic computer or access the internal drive partition on the forensic computer.

2. Connect the staging drive(s) to the forensic computer or access the designated server staging partition to access the case evidence acquisition files.

3. Begin processing a case by launching the FTK application version and providing the authentication parameters (User Name and Password) that were established during the FTK database preparation.

4. Follow the protocol and guidelines established in the Reference Document, pertaining to the appropriate FTK application version to create a new case.

   a. Enter the case information; select the built-in evidence processing parameters (file signature and hash analysis, expand compound files, recover deleted files and folders, data carving, registry reports) and indexing options. Account for the time zone configuration. Create the case.

b. Add the evidence acquisition files created by imaging protocols CC SOP-05, CC SOP-06, CC SOP-12, or CC SOP-13. Note: If an error condition occurs during case initiation when using evidence acquisition files generated in Encase then verify the hash values or run the verification process in Encase. If verification fails, the acquisition procedures for the source media should be repeated (Refer to the appropriate protocol -CC SOP-05, CC SOP-06, CC SOP-12, or CC SOP-13). Use Analysis Notes (QR-CC-6) to document the errors and actions taken during the process.
c. Initiate processing and run to completion.

5. Complete the below listed steps prior to any analysis of the data. Use Analysis Notes (QR-CC-6) or other appropriate QR as a documented narrative to describe actions and observations made during the process.

   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. Note: if the image was created in a different forensic application this information should be verified within that acquisition software.
   c. Mount the evidence file image to a drive in FTK and run a virus scan.
   d. Check for any irregularities with file created, last written and last accessed dates.

6. Upon completion of Steps 4 and 5 proceed with case specific tasks. Use Analysis Notes (QR-CC-6) or other appropriate QR as a documented narrative to describe actions and observations made while performing the case specific tasks. In addition, document in the Analysis Notes (QR-CC-6) or other appropriate QR any pertinent discussions with the submitting agency relating to the examination.

<u>IEF/Axiom (Magnet Forensics)- new case file initiation and processing:</u>

1. Prepare a target drive on the forensic computer as outlined in CC SOP-2 - Target Drive Preparation Protocol and attach this drive to a forensic computer or access the internal drive partition on the forensic computer.

2. Connect the staging drive(s) to the forensic computer or access the designated server staging partition to access the case evidence acquisition files.
3. If using AXIOM for the acquisition of the submitted evidence media follow the protocol and guidelines established in the Reference Document, pertaining to the appropriate Axiom version to create a new case and begin the acquisition process. Refer to the applicable unit imaging protocols - CC SOP-05, CC SOP-06, CC SOP-12, or CC SOP-13 for specific media types. Use Laboratory

Notes (QR-CC-5) as a documented narrative to describe actions and observations made while performing the acquisition tasks.

4. Begin processing a case by launching the IEF/Axiom application version and selecting the source media type - drive(write blocked), image, files and folders, volume shadow copies or mobile. Check to see that all of the media to be examined is present in the case file.

5. Follow the protocol and guidelines established in the Reference Document, pertaining to the appropriate IEF version or Axiom version to create a new case. Use Analysis Notes (QR-CC-6) or other appropriate QR as a documented narrative to describe actions and observations made during the process.

    a. Select the processing parameters for each source media type loaded in the case.
    b. Select the artifacts to be processed and parsed.
    c. Setup the Case Folder on the designated Target Drive and enter the case information.
    d. Initiate processing and run to completion.

6. Upon completion of Steps 4 and 5 proceed with case specific tasks. Use Analysis Notes (QR-CC-6) 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 (QR-CC-6) or other appropriate QR any pertinent discussions with the submitting agency relating to the examination.

<u>NetClean Analyze (Griffeye)- new case file initiation and processing:</u>

1. Prepare a target drive on the forensic computer as outlined in CC SOP-2 - Target Drive Preparation Protocol and attach this drive to a forensic computer or access the internal drive partition on the forensic computer.

2. Connect the staging drive(s) to the forensic computer or access the designated server staging partition to access the case evidence acquisition files.

3. Begin processing a case by launching the NetClean Analyze version.

4. Follow the protocol and guidelines established in the Reference Document, pertaining to the appropriate NetClean Analyze version to create a new case. Use Analysis Notes (QR-CC-6) or other appropriate QR as a documented narrative to describe actions and observations made during the process.

    a. Verify that the hash databases have been connected and enabled in the settings menu.
    b. Create a new case.

c. Select the source media to import- forensic image, C4All XML or folder contents. Check to see that all of the media to be examined is present in the case file.
d. Select the import options and filters.
e. Initiate processing and run to completion.

5. Upon completion of Steps 3 and 4 proceed with image/video categorization. Update the child abuse hash library upon completion of categorization. Use Analysis Notes (QR-CC-6) 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 (QR-CC-6) or other appropriate QR any pertinent discussions with the submitting agency relating to the examination.

E. References:
1. Guidance Software -EnCase user manual
2. Guidance Software -EnCase training documentation.
3. Access Data - Forensic Toolkit user manual
4. Access Data - Forensic Toolkit training documentation.
5. Magnet Forensics - Internet Evidence Finder - user manual
6. Magnet Forensics Internet Evidence Finder - training documentation.
7. Magnet Forensics Axiom – Axiom Examinations (AX200) – training documentation
8. Griffeye - NetClean Analyze- user manual.
9. Griffeye - NetClean Analyze- training documentation.