Digital Storage Media Analysis

A. Purpose:
   To outline the steps taken for examination of digital storage media
B. Responsibility:
   CCEEU forensic examiners
C. Procedure:
   1. The digital storage media will already have been acquired and the evidence file(s) will be present on the network storage (Refer to CC-SOP-50 – Device Imaging SOP).
   2. If the case was acquired by a different examiner than the one performing analysis, follow steps a.-c.
      a. Transfer the evidence item 'CC Evidence Files' from its current location to your custody in LIMS when the examination is started.
      b. Once the case is completed and marked as draft complete, transfer the sub-item back into 'Computer Crimes – Virtual Evidence Storage'.
      c. If during the technical review further examination is warranted, the sub-item will be transferred into the examiner's custody in the same manner.
   3. Open or create a new case record using "QR-CC-6 – Analysis Notes".
      a. Ensure the necessary sections are filled in.
      b. The forensic system used shall be included in the section regarding forensic tools. This is to include the system name, unique identifier (serial number or DPS tag, and installed operating system).
      c. Examination results shall include any specific case details and findings as determined by the examiner.
   4. The examiner will review the search warrant/consent form for the appropriate date range or artifact type to provide, if present.
   5. For all evidence, the following information will be examined and documented prior to the case specific examination:
      a. Physical disk space and any discrepancies.
      b. If applicable, time zone settings.
      c. Any irregularities with the file created, last written, and last accessed date and time stamps.
      d. If applicable, registry information regarding connected devices, operating system and user installations, drive lettering, and network attached storage devices.

6. The evidence is to be examined based upon the request of the submitting agency using approved software.
    a. For CSAM related examinations, utilize the related quality record "QR-CC – CSAM Guidelines" for additional specific examination procedures.
    b. If the examination involves the review of images and/or videos, the unit maintained hash database is to be utilized for efficiency.
7. A virus scan should be run against any media which has been determined to contain any artifacts of evidentiary value and results recorded in the notes.
    a. Utilize the current lab accepted software and procedures for virus protection.
    b. Ensure the software is updated to the most current version before processing.
    c. If the sub-item has been examined and determined to contain nothing to report, a virus scan does not need to be performed.
8. Optical disks can be examined in the same manner as other digital storage media. It may not be necessary to acquire or hash this type of media.
    a. Preview the media using either an approved forensic software or Windows Explorer. Depending on what data is seen on the media, an acquisition of the media may be required. For example, a DVD containing suspected CSAM images and videos.
    b. Document, and include any artifacts of evidentiary value, if present, in the report.
9. In addition to using techniques for analysis based upon, but not limited to, the examiners' training, knowledge, and experience, other protocols can be found outlined and explained in the forensic software utilized.
    a. If a request is outside of the trainings/scope of the Unit, the technical lead and Manager will be contacted to determine which type of analysis may be conducted.
10. For instances where images and/or videos are to be sent to NCMEC for a CRIS review, or are identified as a possible new victim, refer to "CC SOP-32 – NCMEC Requirements".
11. Upon completion of the examination, proceed with "CC SOP-9 – Laboratory Report Protocol" to produce the report(s) and mark the case as draft complete.
    a. Refer to "GL 4 – LIMS" for further guidance.

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