Technical Procedure for Evidence Search

1.0 Purpose - The purpose of this procedure is to provide a systematic means of searching digital evidence in order to find data sought by the search authorization.

2.0 Scope - This procedure describes the steps to be taken by personnel of the State Crime Laboratory in searching computer evidence that is submitted.

3.0 Definitions

- **Forensic drive -** Hard drive containing the operating system and all the forensic software that will be used in the examination.
- **Target drive -** Drive that holds the forensic image of the suspect drive and the case file containing any evidence found on the subject drive.

4.0 Equipment, Materials and Reagents

- Forensic Tower or Portable Forensic Workstation
- Approved Forensic Software

5.0 Procedure

5.1 Read the search authorization (e.g., search warrant or consent) to ensure the scope of search is authorized by the document. Install the forensic drive and the target drive into the forensic tower.

5.2 Ensure that the forensic drive is installed as the primary master and the target drive is installed as either the primary slave, secondary master, or secondary slave.

5.3 Boot the forensic tower from the forensic drive.

5.4 Run approved software to undelete any deleted files and recover files and file fragments from unallocated space.

5.5 The forensic image of the evidence drive shall be examined for the presence of any deleted partitions on the hard drive. If any deleted partitions are noted, these partitions shall be recovered.

5.6 The forensic image of the evidence drive shall be examined for the presence of any deleted folders on the hard drive. Any deleted folders shall be recovered.

5.7 If using EnCase, a file mounter enscript shall be run to mount any zipped or compressed files so that the files contained inside can be examined.

5.8 A signature analysis shall be run on all files in the case prior to the examination of these files. The signature analysis checks the file header information to ensure that the files have not been identified with an incorrect file extension.

5.9 For Cases Involving Images

5.9.1 Computer search software or graphics thumbnail software can be used to view images on a forensic image.

5.9.2 A file search can be run to find files with graphics or movie file extensions (e.g., .jpg, .gif, .bmp, .mov, .mpg, .avi, etc.).

5.9.3 Examine files found for data sought by the search authorization and note in the FA worksheet.

5.10 Data Searches

5.10.1 Use approved forensic search software to perform keyword searches on the forensic image.

5.10.2 Enter keywords such as names, e-mail addresses, dates, or other pertinent keywords which may be used in a file containing data of evidentiary value.

5.10.3 Examine files found for data sought by the search authorization and note in the FA worksheet.

5.11 Image Restore

5.11.1 In order to review the evidence computer as it would have appeared to the user to demonstrate items such as desktop wall paper image or types and arrangement of icons and shortcuts on the desktop, it is acceptable to image the drive again with an approved DOS based imaging program such as SnapBack or to use the restore function in EnCase to restore the EnCase image to a target hard drive. This second image can then be used to boot the evidence computer.

5.12 In EnCase .asf, .max, .mpe, .mpeg, .mpg, .mov, .rm, .ram and .avi files as well as image files in unallocated space are not shown in the gallery view. These files shall be searched and viewed with external viewers.

5.13 EnCase does not display images inside of .zip files in the gallery view unless the ZIP files are first mounted. The examiner shall search for .zip files. These files shall be opened manually or with the File mounter EnScript in EnCase and any images found inside examined.

5.14 EnCase does not display images that are attached to e-mail files (e.g., Outlook Express and AOL e-mail files) prior to version 5. If an Encase version prior to version 5 is being used, the e-mail files shall be recovered to the target drive. These files can be examined by restoring the e-mails to an e-mail account on another computer so that the images attached to the e-mail can be viewed. Alternatively, the examiner may use another tool such as Forensic Tool Kit to examine the case for e-mail.

5.15 Due to the size of modern hard drives, every effort shall be made to search by relevant dates or file types and search by relevant keywords in order to find information sought by the search authorization.

5.16 Microsoft Office 2007 documents are different than previous versions. The Guidance Software website states:
"*Microsoft's Office 2007 documents are stored in what is referred to as the Office Open XML File Format. It is a ZIP file of various XML documents describing the entire document.*"

5.16.1 In order to view the contents of these files, they shall be mounted like other types of ZIP files.

5.16.2 When using version 5 of EnCase, mounting ZIP files will allow viewing of the contents of Office 2007 documents.

5.16.3 When using version 6 of EnCase, select "Mount Persistent" option inside of the File Mounter EnScript to keep the files mounted after the EnScript completes running. If not, the files will unmount as soon as the EnScript finishes running and it will be necessary to mount the files manually by right clicking and viewing file structure.

5.17 Standards and Controls - A control disk image with a known hash value is used to ensure the proper functioning of forensic computers used in casework.

5.18 Calibrations - The forensic towers used in casework shall be verified each day that they are used to ensure that the computer hardware and software are functioning properly (see the Computer Performance Verification Procedure).

5.19 Maintenance – N/A

5.20 Sampling - N/A

5.21 Calculations - N/A

5.22 Uncertainty of Measurement - N/A

6.0 Limitations - N/A

7.0 Safety - N/A

8.0 References

- EnCase Forensic User Manual
- EnCase Intermediate Analysis and Reporting Course Guide
- EnCase Advanced Computer Forensics Course Guide
- Forensic Toolkit User Guide
- Forensic Boot Camp Training Manual
- Computer Performance Verification Procedure

9.0 Records - N/A

10.0 Attachments

- Attachment A: General Flow Diagram for Computer Forensic Examination

Revision History		
Effective Date	Version Number	Reason
09/17/2012	1	Original Document

ATTACHMENT A:

General Flow Diagram for Forensic Computer Examination