Technical Procedure for Approved Software for Forensic Computer Examinations

1.0 Purpose – This list contains the software currently approved for use in computer forensic examinations by State Crime Laboratory personnel. Specific versions of the software used shall be recorded within the Forensic Advantage worksheet by the examiner.

2.0 Scope – This list is to be used by personnel of the State Crime Laboratory as a guide in determining which pieces of software have been validated for use in casework and generating case results.

3.0 Definitions – N/A

4.0 Equipment, Materials and Reagents – N/A

5.0 Procedure

5.1 Hard Drive Imaging

- EnCase
- SnapBack
- Forensic Tool Kit
- DD/DCFLDD/SDD
- DEFT 8
- Get Data Back

5.2 Anti-Virus Software

- Trend Micro OfficeScan
- Symantec Norton Anti-Virus

5.3 Deleted File Recovery

- EnCase
- Norton Unerase
- Forensic Took Kit
- Internet Evidence Finder

5.4 Slack and Unallocated Space Recovery

- EnCase
- Norton DiskEdit
- Forensic Tool Kit
- Get Data Back

5.5 Password Recovery

- Ultimate Took Kit

5.6 Optical Media Processing

- CD/DVD Inspector

5.7 System Image Creation/Restoration

- Symantec/Norton Ghost
- Image for Windows

5.8 Data Carving

- EnCase
- Forensic Tool Kit
- DataLifter

5.9 Text String Searches

- EnCase
- Windows 'Find' Function
- Forensic Tool Kit

5.10 Text Viewers

- EnCase
- Quick View Plus
- Microsoft Word
- Wordpad
- Notepad
- Outlook Express
- Adobe Acrobat
- AOL
- Forensic Tool Kit
- Internet Evidence Finder

5.11 Graphics Viewers

- EnCase
- Thumbs Plus
- Quick View Plus
- Outlook Express
- AOL
- Irfanview
- Xnview
- Forensic Tool Kit
- Internet Evidence Finder

5.12 Movie Viewers

- Windows Media Player
- VLC
- Quicktime

5.13 Internet/IM History Analysis

- EnCase
- NetAnalysis
- Neda-Nama Yahoo Messenger Archive Decoder
- Internet Evidence Finder

5.14 Data Wiping Utilities

- EnCase
- GDisk (Hard Drives only)

5.15 Taser Data Recovery

- **SYNC**
- **Dataport**

6.0 Limitations – N/A

7.0 Safety – N/A

8.0 References – N/A

9.0 Records – N/A

10.0 Attachments – N/A

Revision History		
Effective Date	Version Number	Reason
09/17/2012	1	Original Document
02/01/2013	2	Documentation on version numbers of software while working cases added to 1.0
10/31/2013	3	Added issuing authority to header
01/24/2014	4	Added Deft 8 to 5.1; created 5.15
08/29/2014	5	Added Get Data Back to 5.1 and 5.4 Added Internet Evidence Finder to 5.3, 5.10, 5.11, and 5.13