North Carolina State Bureau of Investigation

Computer Forensics Discipline

Technical Procedure Manual

North Carolina State Bureau of Investigation

Computer Forensics Discipline

Technical Procedure Manual

Approved By: _____ Date: _____

Reviewed By: _____ Date: _____

Reviewed By: _____ Date: _____

Table of Contents

General Flow Diagram for Forensic Computer Examination 1

General Flow Diagram Forensic Computer Crime Scene Response 2

Crime Scene / Field Response, Evidence Preservation Protocol 3

Target Drive Preparation Protocol 5

Hard Drive Removal Protocol 6

Hard Drive Imaging Protocol 7

Cable Acquisition Protocol 11

Removable Media Imaging Protocol 13

Evidence Search Protocol 15

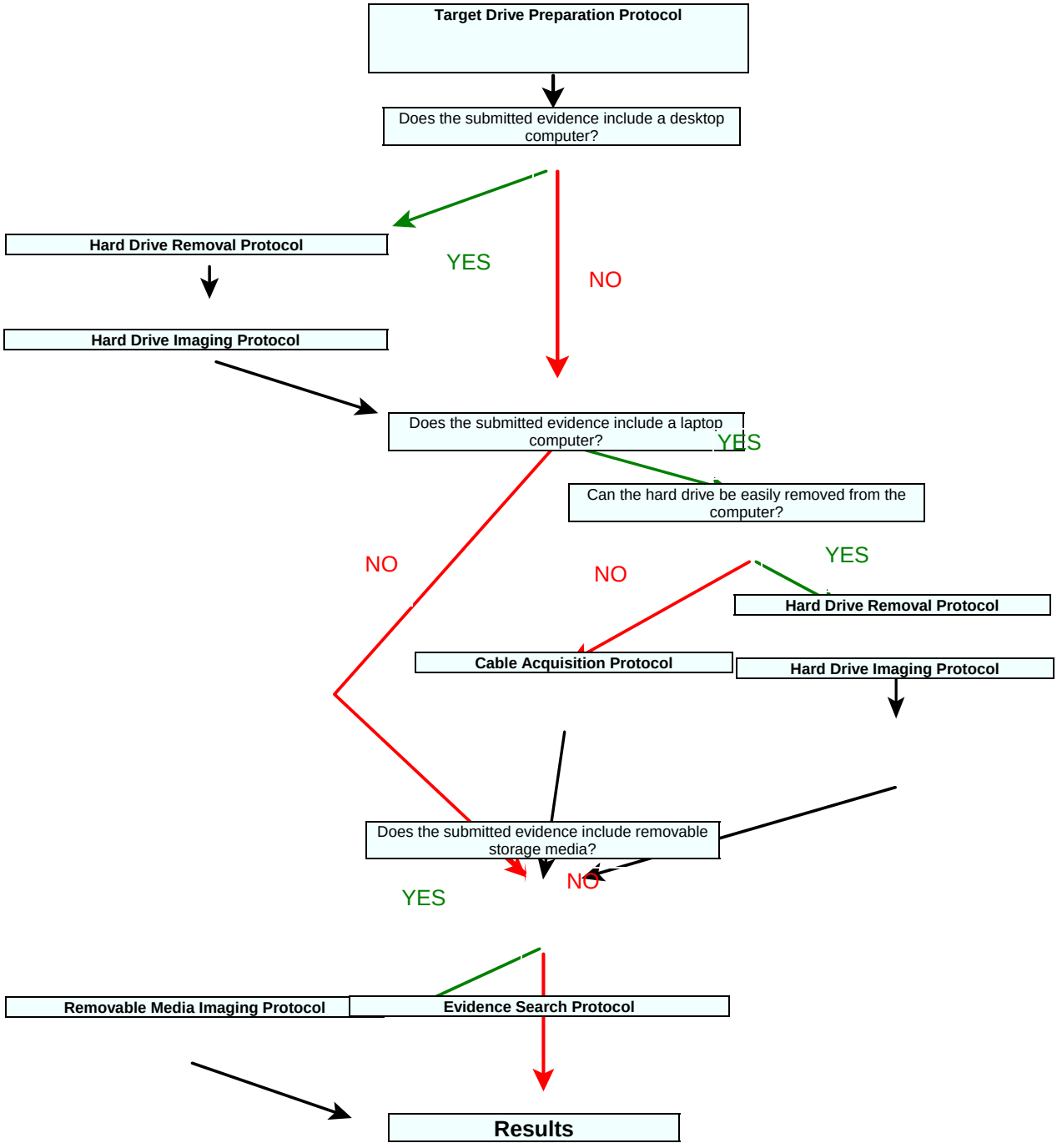
Results 17

Approved Software for Forensic Computer Examinations 19

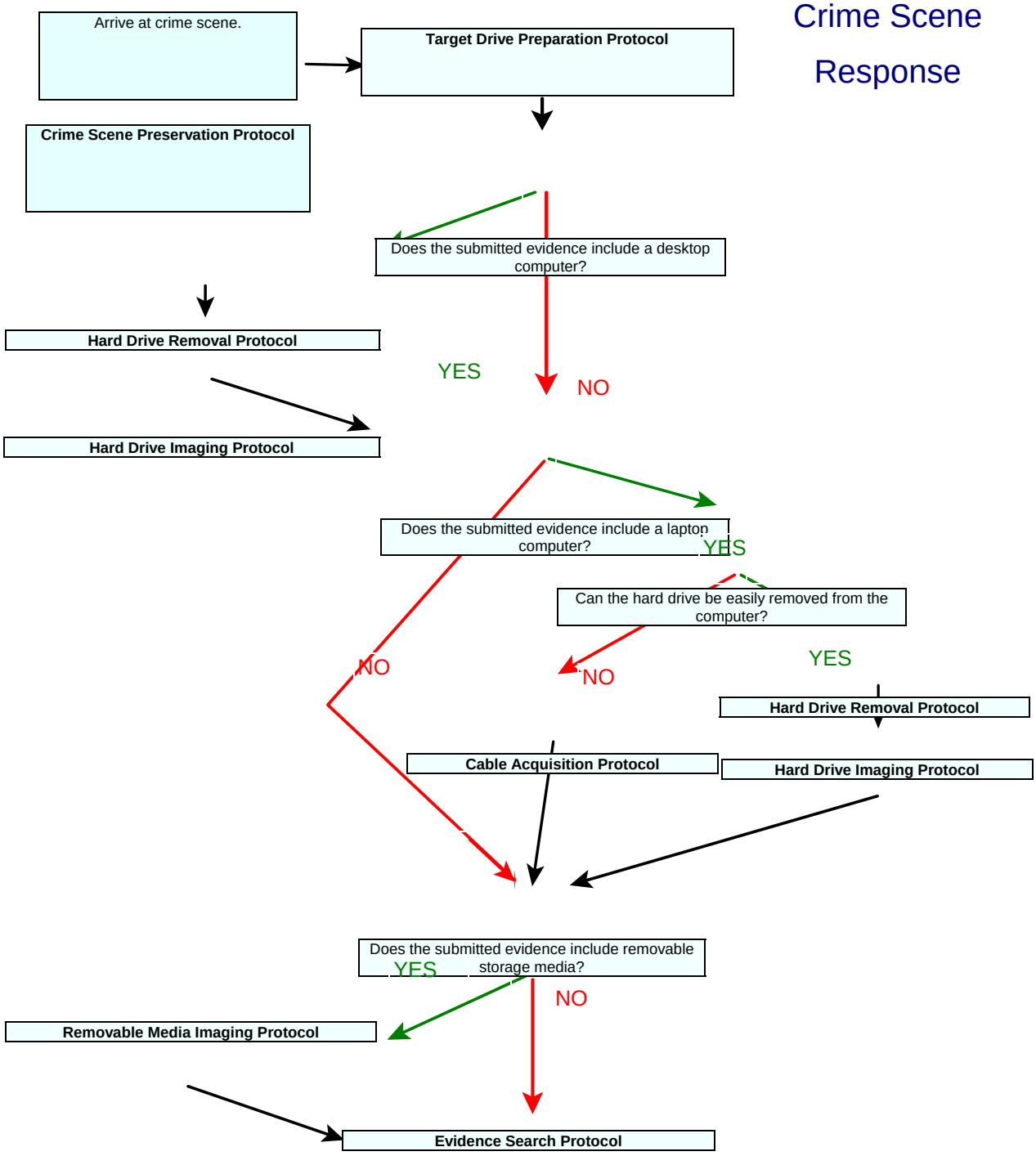
Glossary 21

References 26

General Flow Diagram for Forensic Computer Examination



General Flow Diagram for Forensic Computer Crime Scene Response



Crime Scene / Field Response, Evidence Preservation Protocol

X Upon arriving at the scene, ensure that the suspect is removed from the computer and is not allowed access to it. If the computer to be searched is on a network, ensure that all computers on the network are secured and that no one is allowed access to these computers until the crime scene search is completed.

X If computers are connected to an external network, safely remove any computer to be searched from the network.

Caution: Simply unplugging a suspect computer from a network can cause data loss and damage to the network. Assistance in safely removing the computer from the network should be sought from the system administrator, so long as the system administrator is not a suspect in the case. If the system administrator is a suspect in the case, assistance should be sought from other personnel knowledgeable in the network's operation.

Caution: Be sure that all computers involved in search are secured and that no one is allowed access to them. Important data can be quickly damaged or destroyed if a suspect is allowed access to the computer.

X Document the condition of all computers with photographs and notes. This should include any documents that are open or information that appears on the monitor.

X Save any open documents on the computer to a floppy disk. Some other type of media such as a Zip disk should be used if the computer does not have a floppy disk drive or if the files being saved are too large to fit onto a floppy disk.

X Shut down the computer using the normal procedure for the OS used.

Caution: If at any point while securing the computer the analyst believes that evidence may be being destroyed (i.e. delete, wipe, or defrag program running or an unusual delay in the shut down of the computer), the power cord should be pulled from the **back of the computer**.

X Note the hardware connections to the computer (mouse, keyboard, phone line, external drives, etc.).

Crime Scene / Field Response, Evidence Preservation Protocol (continued)

Note: It is important to document the condition of the computer before disassembling it. It is necessary to be able to put the computer back as it was when investigators arrived at the scene.

X Search the scene for removable media such as CDs, Zip disks, Jazz disks, floppy disks, and USB thumb drives. Sometimes the evidence in a case may only be found on the removable media.

X Search the area around the computer for any passwords, account numbers, or other pertinent information which may be written down.

Note: If files on the computer are encrypted, finding the password written down near the computer may be the only way to access the information.

Target Drive Preparation Protocol

Select a hard drive that is ready to be used in a case as a forensic copy. Hard drives to be used can be either new hard drives or a hard drive that contains data from a case which has been completed. This hard drive will be referred to in the following as the target drive.

X The selected target drive should have sufficient storage capacity to hold the image files generated from the suspect's hard drive.

X Attach a label to the target hard drive with the pertinent case information.

X Use an approved wipe utility to remove the information from the previous examination from the disk. This step should also be used for new hard drives.

Caution: Failure to wipe the information from a previously used hard drive can lead to the possibility of data from old cases contaminating a new case.

X Run F-disk or G-disk on the image drive. Create the new primary DOS partition for the target drive.

X Run Format to reformat the target drive. At the end of the Format process, enter a suitable name for the drive to denote that this will be the image drive (ie. image, target, etc.).

X Directories for the hard drive or any other type of media can be created on the target drive in order to keep the evidence organized.

Note: When responding to image a computer in the field the target drives may be prepared by this procedure prior to departing the Laboratory. This will speed up the process of imaging the computer and will result in a shorter down time for the suspect computers.

Hard Drive Removal Protocol

X Record the system information from the suspect's computer on the notes sheet.

X If necessary, photograph the condition of the suspect's computer prior to opening the case. Add photograph to the case notes.

Note: The hard drive from many laptop computers can be removed and by using an adapter, imaged with the same procedures as the hard drives removed from desktop computers. With some laptop computers however, the hard drives are very difficult to remove and are designed to only be removed by trained service personnel. It is permissible to image laptop computers without removing the hard drives by using the Cable Acquisition Protocol.

X Open the case on the suspect's computer.

X If necessary, photograph the internal contents of the suspect's computer prior to removing the hard drive(s). Add photograph to the case notes.

X Mark the cords connecting the hard drive to the suspect□s computer. These markings will enable the analyst to reassemble the computer correctly.

X Remove the hard drive(s) from the suspect's computer.

X Label the suspects hard drive as the original hard drive in order to prevent evidence contamination. The label should contain the case number, item number, date and the analyst□s initials.

X Record the drive information including make, model, serial number, number of sectors, number of heads, and jumper settings on the notes sheet.

X The date and time used by the suspect□s computer may become important in an investigation. In order to check the date and time information, the computer can be booted from a DOS boot floppy disk with the hard drive removed. During the boot process, enter the BIOS and note the date and time and compare to the actual date and time. Record the date and time information on the EnCase notes sheets.

Hard Drive Imaging Protocol

Note: Making an image of the suspect□s hard drive is not the same as making a copy of the suspect□s hard drive. When a hard drive is copied, only the logical files are written onto the target drive. When an image is created of a drive, all of the information on the suspect hard drive is written to the target drive, including slack space, unallocated space, and deleted files.

X Insert the suspect hard drive and the target drive into the computer.

Note: When working with the hard drive from a laptop computer, the smaller laptop hard drive can be imaged by using the adapter to connect it to the standard IDE connector. The same imaging procedures are used.

X Depending on the hardware used to image the suspect drive, the drive can be imaged in either the Windows or DOS environment.

Note: In most situations, the Windows acquisition is preferable if the hardware allows it. Imaging in Windows is much faster than imaging in DOS.

DOS Imaging Procedure

X The DOS imaging procedure **must** be used to image a hard drive when hardware to write protect the hard drive is not used.

Caution: While the suspect's hard drive is in the computer and the hard drive is not write protected, the computer must not be booted in Windows mode. Booting in Windows can change files on the suspect's hard drive. While the suspect's hard drive is in the computer, the computer must only be booted in DOS.

X Boot the computer in DOS using an EnCase Boot Disk.

X Make a forensic image copy of suspect's hard drive onto the target drive using the DOS EnCase program located on the EnCase Boot Disk.

X In EnCase, ensure that the suspect□s drive is locked and unlock the target drive.

Caution: Locking the suspect□s hard drive ensures that the target drive cannot be accidentally copied onto the suspect□s hard drive. Ensure that the

suspect□s hard drive is locked.

Hard Drive Imaging Protocol (Continued)

X Image the suspect□s hard drive by choosing the Acquire button at the bottom of the screen. On the Acquire Evidence screen, choose the drive letter of the suspect□s hard drive.

X On the Evidence File Path screen, enter the correct path in order to have EnCase image the suspect□s drive to the target drive.

X Enter the case information that the program requests. This information will be used by the program in preparing the EnCase report.

X EnCase asks if you would like to compress the file. Compression may be used in the imaging of larger hard drives in order to require less CDs or DVDs to store the image at the completion of the analysis.

Note: Using compression has NO damaging effects on the evidence. The files created are two to three times smaller than uncompressed files. However, creating compressed images may take fives times longer than creating uncompressed images.

X When asked if you would like to do a MD5 hash, choose YES. EnCase uses this hash to verify that the target drive is an exact forensic image of the suspect□s hard drive.

X EnCase offers the ability to password protect the image. The decision as to whether or not to use a password is left to the discretion of the analyst.

X The Maximum Desired Evidence File Size should be set to 640 Mb if the image is to be saved to CDs. Larger file sizes may be used if the images file will be written to DVDs.

X In some rare cases, EnCase is unable to create a forensic image of the suspect□s hard drive. In this case, make a forensic image copy of suspect's hard drive onto the target drive using approved imaging software such as SnapBack.

Caution: When using imaging software other than EnCase, care should be used to ensure that the evidence data is not destroyed by copying the target drive

onto the suspect's hard drive.

Hard Drive Imaging Protocol (Continued)

Windows Imaging Procedure

X The Windows imaging procedure may be used to image a hard drive when hardware to write protect the hard drive is used.

Note: The SBI Computer Forensics Unit is equipped with forensic towers purchased from Forensic Computers.com. These computers have a drive bay which is connected to the computer with a read only Firewire connection. Hard drives which are placed in this drive bay are write protected and may be imaged in the Windows environment.

X Place the forensic drive and the Target drive into the computer and boot the computer into Windows.

X Make a forensic image copy of suspect's hard drive onto the target drive using the EnCase forensic program in Windows.

X Image the suspect□s hard drive by choosing the Acquire button on the tool bar. On the Acquire Evidence screen, choose the suspect□s hard drive.

X Enter the case information that the program requests. This information will be used by the program in preparing the EnCase report.

EnCase asks if you would like to compress the file. Compression may be used in the imaging of larger hard drives in order to require less CDs or DVDs to store the image at the completion of the analysis.

Note: Using compression has NO damaging effects on the evidence. The files created are two to three times smaller than uncompressed files. However, creating compressed images may take fives times longer than creating uncompressed images.

X Check the check box for Generate image hash. EnCase uses this hash to verify that the target drive is an exact forensic image of the suspect□s hard drive.

- EnCase offers the ability to password protect the image. The decision as to whether or not to use a password is left to the discretion of the analyst.

Hard Drive Imaging Protocol (Continued)

- The Maximum Desired Evidence File Size should be set to 640 Mb if the image is to be saved to CDs. Larger file sizes may be used if the images file will be written to DVDs.

- In some rare cases, EnCase is unable to create a forensic image of the suspect□s hard drive. In this case, make a forensic image copy of suspect's hard drive onto the target drive using approved imaging software such as SnapBack.

- The target drive can be checked with an approved anti-virus program to ensure that it has not been infected by the suspect□s hard drive.

- After verifying that the copy has been successfully completed, remove the suspect's hard drive from the computer.

Note: There may be some instances when the suspect□s hard drive cannot be successfully imaged. In the event that an image cannot be made of the suspect□s hard drive due to either hardware or software problems, the attempts to image the hard drive should be completely documented before doing any examination on the suspect□s original hard drive.

Cable Acquisition Protocol

EnCase allows the remote acquisition of evidence in DOS through the use of a null-modem parallel (lap-link) cable or a network crossover cable. This procedure can be followed when the hard drive of the evidence computer□s hard drive is difficult or impossible to remove, especially in the case of some laptop computers.

X Always set up the server (suspect computer) first, as follows:

1. Boot the evidence computer in DOS using an EnCase boot floppy.

Caution: Check the suspect computer prior to booting up to ensure the boot order is to the floppy drive first. Also, disable any power saving features in the BIOS.

Note: In order to use a network crossover cable, the suspect computer must be equipped with a network interface card and the forensic boot disk must contain the DOS drivers for that network interface card. Otherwise, the parallel cable must be used.

2. Connect the suspect computer and forensic computer using a network crossover cable between the network interface cards or connect the lap-link cable from the parallel port of the evidence computer to the parallel port of the forensic computer (running through the dongle if a parallel port dongle is used).

3. Once the suspect computer is booted, run EnCase in DOS.

4. The suspect computer will display its hard drive information on the screen and you will note that the suspect drive is locked.

5. Choose □server mode□ from the choices at the bottom of the screen.

6. A window will be displayed showing □Server Mode□ and the message □waiting to connect□.

X Next, set up the client (forensic computer) as follows:

7. After installing the target drive in your forensic computer, run EnCase in DOS and make sure that the screen shows □client mode□ in the title bar.

8. The information that you now see on the screen will be from the suspect

computer.

Cable Acquisition Protocol (continued)

9. You may now acquire the evidence following the steps in the normal manner.

10. When acquisition has started, the server (suspect) computer window will show that a connection has been established and the data being transferred.

Note: This is a very slow method of data acquisition. Using a network crossover cable is a faster method of imaging a hard drive than using a parallel cable. A large hard drive (>20 gigs) may take several days to acquire using a parallel cable.

Removable Media Imaging Protocol

For the purposes of this section, removable media includes floppy disks, CDs, Zip disks, Jazz disks, LS120 disks, flash memory cards, and any other type of portable digital storage media. This also includes digital cameras and PDAs.

X If possible write protect any removable media.

X The evidence can be copied to a blank copy of the same media type. The original media should be labeled as the original, and the copies should be used for examination.

Note: If working with a suspect's CD-R or CD-RW disks, reading them in read only CD drives is preferred. This will prevent changes from being made to the evidence. The Sony CD-R/DVD-R drive on the computer forensic units have been validated to ensure that changes will not be made to suspect media.

X If using EnCase for the examination, the removable media can be added to the case and copied to the image drive.

Note: Hard drives must only be imaged in DOS if write protection hardware is not in use. Likewise, removable media which can be write protected, can be imaged in the Windows based EnCase program.

X High density and double density floppy disks should be batch imaged separately.

Note: When batch imaging floppy disks, EnCase chooses the disk capacity of the first floppy imaged as the capacity of all floppies in the batch. If a double density disk is imaged first, EnCase will not see all of the data on any high density disks which are imaged later in the batch.

X When using EnCase to image CD-RW disks, care must be used to ensure that EnCase can read the data on the disk.

Note: EnCase has problems reading the format used by some computers to write to CR-RW disks. If a CD-RW is imaged or previewed in EnCase and shows no data on the disk, the disk should be examined in Windows Explorer. If there is data on the disk and EnCase doesn't recognize it, Windows Explorer will read it. If a disk is found that contains data but is not recognized by EnCase, the data on the disk should be copied to a CD-R disk and this copy used in EnCase. It should be noted that this method will

only capture the Logical files on the CD-RW, and not the deleted files or slack space.

Removable Media Imaging Protocol
(continued)

X Zip disks cannot be write protected and should be imaged in DOS **only**.

Note: Zip disks can be imaged using the DOS version of EnCase, The forensic towers see the Zip drive as a floppy drive and assign the drive a drive letter of B. EnCase treats the Zip disks the same as floppy drives and images them in a batch process. EnCase write blocks the Zip drives by default.

X If media can be write protected and keyword searches are not needed on the media, it is permissible to preview the original media without making a copy first.

X For PDA examination, a docking cradle made for the particular make and model of PDA is required. When the PDA is attached to the forensic tower using the cradle, EnCase see the PDA as a piece of removable media. The data contained on the PDA can then be acquired by EnCase in the same method as with any other type of removable media.

Caution: When a case is submitted to the laboratory which contains a PDA, great care should be taken to ensure that the batteries do not go dead. The volatile memory in a PDA can be lost when the batteries are totally discharged. PDAs which use AA or AAA batteries should have new batteries placed into the PDA. PDAs with rechargeable batteries should charged if the charger is submitted. If these things cannot be done to ensure the safety of the evidence on the PDA, the evidence should be imaged and then worked at the appropriate time.

X For examination of digital cameras, the flash memory cards should be removed from the camera. A flash media card reader is then attached to the computer and the media inserted. EnCase sees the flash media as a piece of removable media. The data contained on the flash media card can then be acquired by EnCase in the same method as with any other type of removable media.

Evidence Search Protocol

X Install the system hard drive and the target hard drive in the computer workstation.

X Insure that the system hard drive is installed as the primary master and the target drive is installed as either the primary slave, secondary master, or secondary slave.

Caution: If the system drive is not installed as the primary master, the computer may boot from the target drive. This may destroy evidence.

X Boot computer workstation from the system hard drive.

X Run software to undelete any deleted files and recover files or file fragments from unallocated space.

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

X If the evidence drive used a FAT file system, the forensic image of the evidence drive should be examined for the presence of any deleted folders on the hard drive. Any deleted folders should be recovered.

X A signature analysis should be run on all of the 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 misidentified with an incorrect file extension.

Cases involving photos or images:

X Computer search software or graphics thumbnail software can be used to view images on an image drive.

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

Note: In EnCase, .art, 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 should be searched for and viewed with external viewers.

Evidence Search Protocol
(Continued)

EnCase does not display images inside of .zip files in the gallery view. The examiner should search for .zip files. These files should be opened manually or with the Zip opener EnScript in EnCase and any images found inside examined. This can be done by the examiner or recovered for examination by the submitting officer.

EnCase does not display images that are attached to e-mail files (i.e. Outlook Express and AOL e-mail files). If images may be important in a case, the e-mail files should 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. This examination can be done by the examiner or recovered for examination by the submitting officer.

X Examine files found for data useful to the investigation.

X Make note of any files found with valuable information.

Data searches:

X Use forensic search software or the Windows search program to perform keyword searches on the image drive.

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

X Examine files found for data useful to the investigation.

X Make note of any files found with valuable information.

Note: Due to the size of modern hard drives, it is not possible to read all of the data recovered in a case. Every effort should be made to search by relevant dates or file types and search by relevant keywords in order to find information pertinent to the case.

X At times, it will be necessary to view the subject□s computer just as they would have viewed it at the time it was in use. To do this, 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 subject□s computer.

Results

X Make a copy of the files which were found to be of evidentiary value onto a CD or DVD. Any CD or DVD that has pornographic images of children copied on it as part of the examination will be labeled to reflect the following:

> ◘*This media may contain contraband and is intended for use by law enforcement in an official criminal investigation. Dissemination of this material may result in a criminal violation.*◘

X If desired, print a hard copy of files which were found during the examination and were found to be of evidentiary value. Be sure to note on the printout the location on the hard drive where the file can be found. These printouts can be placed into the analyst◘s notes and/or returned to the investigating officer.

X If desired, print the EnCase report that is prepared by EnCase.

X Make a copy of the forensic image onto a set of CDs or DVDs. These CDs or DVDs will be returned to the submitting agency. If any further analysis needs to be done, the set of CDs or DVDs can be returned to the lab. The target hard drive used to make the image may be wiped and reused in further casework examinations.

Note: In cases where the forensic image is exceptionally large (image files that are many Gigabytes in size) it may not be practical to copy the image to CDs or DVDs. In these cases the analyst may elect, at his discretion, to eliminate this procedure. If so, the report must clearly state that no copy of the forensic image was prepared and that if additional searches of the computer are anticipated, it should be held as evidence rather than being returned to the owner. In these instances the original computer must be re-submitted to the lab in order for any additional analysis to be conducted.

Caution: Only CD-R, DVD-R or DVD+R disks may be used to copy recovered files and the forensic image. CD-RW or DVD-RW disks should never be used because the data on the disk may be altered.

Note: When creating a CD or DVD, the session should be finalized. This will help prevent accidental damage to the CD.

Results
(continued)

X Evidence determined to have pornographic images of children on it will be labeled:

> ◘*This media may contain contraband and is intended for use by law enforcement in an official criminal investigation. Dissemination of this material may result in a criminal violation.*◘

Approved Software for Forensic Computer Examinations

Note: EnCase is a very powerful forensic software package which is used by the NC SBI Crime Laboratory Computer Forensics Unit. The standard protocols used by the NC SBI Computer Forensics unit are written for investigations using EnCase. Other approved forensic software may be used as necessary, at the analyst□s discretion. This is a list of the software which is owned by and approved for use in the NC SBI Crime Laboratory Computer Forensics Unit.

Hard Drive Imaging

X EnCase

X SnapBack

Anti-Virus Software

X Norton Anti-Virus

Deleted File Recovery

X EnCase

X Norton Unerase

Slack and Unallocated Space Recovery

X EnCase

X Norton Diskedit

Text String Searches

X EnCase

X Windows 98 Find function

Approved Software for Forensic Computer Examinations (Continued)

Text Viewers

X EnCase

X Quick View Plus

X Microsoft Word

X Wordpad

X Notepad

X Outlook Express

X Adobe Acrobat Reader

X AOL

Graphics Viewers

X EnCase

X Thumbs Plus

X Quick View Plus

X Outlook Express

X AOL

X IrfanView

X XnView

Password Recovery

X Access Data

Glossary

BIOS	Basic Input Output System. A number of machine code routines that are stored in ROM and available for execution at boot time.
Browser	Browser is short for Web Browser. A browser is a computer program that locates and displays pages from the Internet.
Cache	A computer□s cache is an area where the computer can temporarily store frequently used data that would otherwise have to be loaded from a slower source. The computer□s cache speeds up the operation of the computer.
CDFS	The standard used to describe the file structure on a CD.
Cluster bitmaps	Used by NTFS to keep track of free clusters by using a bitmap. This file contains one bit for every cluster on the volume.
Clusters	A group of sectors in a logical volume that is used to store files and folders.
Compressed file	A file that has been reduced in size via one or more compression techniques.
Compression	A method of storing files resulting in great savings in disk storage space. Compressed blocks are checked for validity in the same way as uncompressed one.
Cookie	A cookie is a short piece of data that Web servers place on your computer to help identify Web users. Cookies can be used by Web servers to track your Internet browsing habits.
Cylinder	The set of tracks on the drive platters that are at the same head position.
Disk	An actual piece of hardware that you can hold in your hand. It could be a floppy disk, hard disk, ZIP disk, etc.

Glossary
(Continued)

DOS	Disk Operating System - usually refers to MS-DOS. Operating system which was developed by Microsoft for IBM compatible PCs. Still used today to help control operation on computers, operating beneath the Windows environment.
Drive Geometry	The number and position of the bytes, sectors, tracks located on the physical drive.
EXT2	The primary file system used on the Linux operating system.
Fdisk	DOS program that provides information about and editing of the partitions on a hard drive.
File entries	Each folder contains starting cluster and can be expanded or contracted as files are added or removed from the folder. Each file in the folder is represented by a 32 byte entry in the table. The content of a folder ◘file◘ is an array of records containing information about the files in the folder. Each entry in the folder can be either a file or another folder. In this way a ◘tree◘ structure can be built.
File slack	The space between the logical end and the physical end of a file.
File signature	A few bytes at the beginning of some files (such as graphic or document files) that constitute a unique signature of the file type, regardless of the file extension used.
File allocation table (FAT)	An array of numbers that sits near the beginning of a DOS volume. The length of the numbers is determined by the size of the volume. Each entry in the FAT corresponds directly to one cluster and there is always one FAT entry for every cluster.
Format	DOS command used to prepare a storage medium (hard drive, floppy disk) for reading and writing. Format does not erase data on the disk. It checks for bad sectors and resets the internal address tables (FAT).
Head	A device that ride very close to the surface of the platter and allows information to be read from and written to the platter.

Glossary
(Continued)

Hyperlink	A hyperlink is a text phrase (which often is a different color than the surrounding text) or a graphic that conceals the address of a Web Site. Clicking on the hyperlink takes you to the Web Site.
Image drive	Same as the target drive.
Internet	The Internet is a world wide network with more than 100 million computer users that are linked for the exchange of data, news, conversation and commerce. The Internet is a decentralized network that no one person, organization or country controls.
ISDN Line	Integrated Services Digital Network - A phone line that connects two computers to transmit a digital signal between them, as opposed to the analog signal transmitted over normal phone lines. This allows data to be transferred more than twice as fast as with an analog phone line with a 56kbps modem.
Logical file size	The exact size of a file in bytes and is the number represented in the properties for a file. This is different than physical file size.
Logical drive	A drive named by a DOS drive specifier, such as C: or D:. A single physical drive can act as several logical drives, each with its own specifier.
Master boot record	The very first sector of a physical disk (sector zero) is referred to as the MBR It contains machine code that allows the computer to find the partition table and the operating system.
MD5 hash	A 128 bit number that uniquely describes the contents of a file. This is the standard hash code used in forensics.
NTFS	NT File System. The file descriptors for for every file on an NTFS volume are stored in the Master File Table.
Partition table	Describes the first four partitions, their location on the disk, and which partition is bootable.
PGP	Pretty Good Privacy - Program used to encrypt data on a computer, such as messages on the Internet.

Glossary
(Continued)

Physical drive	A single disk drive. A single physical drive may be divided into multiple logical drive.
Physical file size	The amount of space that a file occupies on a disk. A file or folder always occupies a whole number of clusters even if it does not completely fill that space.
Plug-Ins	A piece of computer hardware or software that adds a specific feature or service to a larger system.
RAM slack	The space from the end of the file to the end of the containing sector. Before a sector is written to disk, it is stored in a buffer somewhere in RAM.
RAM	Random Access Memory. Volatile read/write memory whose contents are lost when the power is turned off.
ROM	Read Only Memory. Chips that contain a permanent program that is burned on the chip at the factory and maintained when the power is turned off. The information on these chips can be read but not written to.
Root folder	Stored in a known location, this is a tree structure that supports files and folders within folders to an arbitrary depth.
Sector	A group of bytes within a track and is the smallest group of bytes that can be addressed on a drive. The number of bytes in a sector can vary, but is almost always 512.
Spam	Unsolicited □ junk □ e-mail which is sent to persons who did not request it. It is usually commercial e-mail.
Suspect drive	The drive (or drives) that are removed from a suspect□s computer or in the possession of the suspect that will be imaged for later analysis. This drive is never analyzed; rather is copied so the analysis can be conducted on the image.
System drive	The forensic hard drive used to boot the forensic tower. This is the drive which contains the forensic search tools.
Target drive	The drive that information from the suspect drive is being written to.
Track	Each platter on a disk is divided into thin concentric bands

Glossary
(Continued)

	called tracks. Tracks are established when the disk is low level formatted.
Upload	To send or transmit data from your computer to another computer or network.
URL	Universal Resource Locator - An address at which documents or other resources can be found on the Web.
Volume	A mounted partition. There may be only one volume on a floppy or ZIP disk, or there may be several on a hard disk.
World Wide Web	A group of Internet servers that support HTML formatting. The World Wide Web is one part of the Internet.

References

X How Computers Work, Millennium Edition: Ron White: Que, A Division of Macmillan Computer Publishing, USA: 1999: ISBN 0-7897-2112-0

X Upgrading and Repairing PCs, 12th Edition: Scott Mueller: Que, A Division of Macmillan Computer Publishing, USA: 2000: ISBN 0-7897-2303-4

X Using Microsoft Windows 95, Fourth Edition: Kathy Ivens: Que, A Division of Macmillan Computer Publishing, USA: 1998: ISBN 0-7897-1573-2

X EnCase Version 2, User Manual: Guidance Software, Inc.: Revision 2.0: Copyright 1998 - 2000

X DOS for Dummies

X Microsoft MS-DOS, User□s Guide and Reference Version 5.0: Microsoft Corporation: Document No. SY07661/20885-0391

X Cybershock, Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption: Winn Schwartau: Thunder□s Mouth press, New York: 2000: ISBN 1-56025-246-4

X I-Way Robbery, Crime on the Internet: William C. Boni and Dr. Gerald L. Kovacich: Butterworth-Heinemann: 1999: ISBN 0-7506-7029-0

X Digital Evidence and Computer Crime ; Forensic Science, Computers and the Internet: Eoghan Casey: Academic Press: 2000: ISBN 0-12-162885-X

X High Technology Crime Investigators Handbook, Working in the Global Information Environment: Dr. Gerald L. Kovacich, William C. Boni: Butterworth-Heinemann: 2000: ISBN 0-7506-7086-X

X EnCase Version 3.0, User Manual: Richard Keightley : Guidance Software, Inc.: Revision 3.18

X EnCase Intermediate Analysis and Reporting: Guidance Software, Inc. : Intermediate Revision 3.05 : Copyright 2002

X EnCase Intermediate Analysis and Reporting: Guidance Software, Inc. : Intermediate Revision 4.01 : Copyright 2002