Global Information Assurance Certification Paper

SANS/GIAC Practical Assignment
For GSEC Certification
Written by Rejean Lavoie
Version 1.4b

Abstract

In this paper I will discuss computer evidence. The law enforcement agencies are at the cross road of the new technology. These days, some crimes are committed by using computer and often the offender is located miles away from the victim. That kind of crime (fraud, threat, DoS and other) is very hard to resolve. Investigators have to perform searches on computer. To make sure that the searches are the perfect copy of the seize computer, they have to create forensic computer evidence.

Computer evidence is relied upon more and more in criminal and civil litigation actions. It was computer evidence that helped identify the now infamous 'Blue Dress' in the Clinton impeachment hearings [1]. In this paper I shall give a brief explanation of the forensic acquiring and analyzing in general to provide a good over view of the responsibility of the peace officer to bring digital evidence to be acceptable for the court.

Forensic acquiring and analysis

Introduction

Criminals have always been the first to take advantage of new technologies in the commission of their crimes. To say that the introduction of the personal computer (PC) in 1981 changed our lives would be a huge understatement. How could we function today without them? They have changed the way we do almost everything. Not only have they impacted the average law abiding citizen's life, they have been a facilitator for the common criminal. Traditional crimes were made easier to commit with the computer. Legislation even had to be changed to reflect the new technological crimes the criminal element could now commit.

Today, computers are used in every facet of life to create messages, compute profits, transfer funds, and access bank accounts and to browse the Internet for good and evil purposes. Notebook computers provide computer users with the benefits of portability as well as remote access to computer networks. *Computer users today have the benefits of super computer speeds and fast Internet communications on a worldwide basis. Computers have increased productivity in*

business but they also increase the likelihood of company policy abuses, government security breaches and criminal activity [2].

In the past, documentary evidence was primarily a paper-based document we could touch with our bare hands. Copies were made with carbon paper or through the use of a photocopy machine. Most documentation today is saved on computer hard drives, floppy diskettes, Zip™ disks and other types of removable computer storage media. Potential computer evidence may now reside on these mediums and it is up to the forensics investigator to find it using computer forensics tools and computer evidence processing methodologies. The best evidence now is not always the traditional paper document.

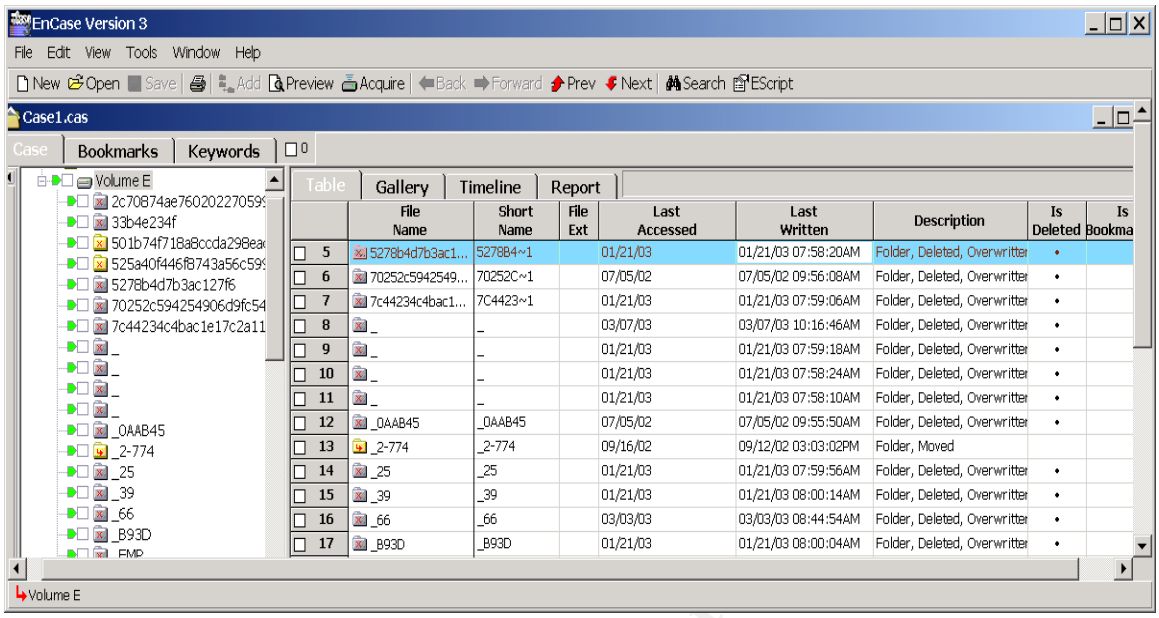
In criminal proceedings, the forensic analysis of a computer and the way the data is acquired is normally the responsibility of police officer. On occasion, some police agencies have civilian personnel trained to acquire digital evidence. Law enforcement personnel must be involved in the forensic acquisition and analysis due to evidentiary constraints inherent to the judicial process. Any and all actions prior to the acquisition, during the acquisition and analysis afterwards must be correctly noted for presentation to the criminal courts. The rules regarding the presentation of evidence must be respected if the information found is to be accepted by the Court.

Digital evidence is very different than any other evidence that is reported to court. The reason is that it's very easy for any person without professional conscience to modify the digital evidence with a few keystrokes. Physical evidence can be tampered with but it is usually much harder to do and leaves discernable marks. Imagine trying to alter serial numbers on a weapon. Now imagine modifying the contents of a paragraph in MS-Word™.

Another unique aspect of computer evidence is the potential for unauthorized copies to be made of important computer files without leaving behind a trace that the copy was made. This situation creates problems concerning the investigation of the theft of trade secrets [2]. To be considered forensically sound, digital evidence must be collected in a manner where any copies made must be exactly the same bit for bit. A checksum of the original media and the forensic image on the target media must be exactly the same.

Data acquisition

To analyze digital evidence, it is imperative the investigator starts with a bitstream image of the media that he wants to investigate. The reason for this procedure is that you do not want to modify the data on the seized media. By creating an image file, the investigator will keep the suspect media as it was when it was seized. A simple cold boot of a computer is enough to significantly alter the data contained on the suspect hard drive. Last access dates on many of the system files would be altered by such an intervention.



The acquisition of the digital evidence file is the most important step for the investigator. This image file has to be the exact replication of the original media. The investigator will search the entire image file for any evidence. Obviously he will search the existing active file system and the unused portion of the original media. This unallocated space can be divided into two (2) categories; file slack or disk slack.

A hard drive is divided up into sectors. For addressing reasons, a predefined multiple of sectors make up a cluster. The cluster is the smallest addressable unit in the file system. *Rarely do file sizes exactly match the size of one or multiple clusters perfectly. The data storage space that exists from the end of the file to the end of the last cluster assigned to the file is called "file slack" [3].* A criminal might want to hide evidence from being discovered. A skilled criminal that had incriminating information to hide could exploit file slack space. As an example, if a hard drive was partitioned in FAT32, it would have four (4) sectors of 512 bytes per cluster. In this cluster it will be potentially possible to store any file of two kilobytes. To further the example, we will take a file of 2049 bytes. This file will use the space of two clusters on the disk but the second cluster will use only one (1) byte of the cluster. The file system tables must indicate both the 1st and 2nd clusters as being in use. The second cluster has 2047 bytes of space that are reserved yet not being used by the file in our example.

This means, if we use a low level tool such as Norton™ Disk Editor, it would be possible to edit the disk of a computer and store almost two pages of typical plain text data in the 2nd cluster of our previous example. As long as the “secret” data was written after the 1st byte of the 2nd cluster, the average user would notice

nothing unusual. A normal user of the computer would open the original 2049 byte file and see their document as they left it. The file system would protect this "secret" data as long as no one adds anything to the original file.

Example of a 8193 bytes file save on a disk

cluster #223				cluster #224			
512	512	512	512	512	512	512	512
cluster #225				cluster #226			
512	512	512	512	512	512	512	512
cluster #227				cluster #228			
1	511	512	512	512	512	512	512	512

Used sectors
Bytes left unused which can be use to hide data
Free cluster

On today's modern systems we rarely see the FAT16 file system anymore. With it's maximum limitation of 65536 clusters per partition; you can imagine the large cluster size. A two (2) gigabyte partition would require a cluster to be 32768 bytes in size (64 sectors of 512 bytes). Files slack of this size makes it possible to store very large amounts of data that can potentially elude detection.

Unallocated file space potentially contains intact files, remnants of files and subdirectories and temporary files, which were transparently created and deleted by computer applications and also the operating system. All of such files and data fragments can be sources of computer evidence and also security leakage of sensitive data and information [4]. Deletion or erasure of a file on a file system does not mean it is truly unrecoverable. The data of a deleted file remains on the disk in the unallocated space. Most modern file systems simply indicate the cluster or clusters are available for reuse. This is a performance issue. If the operating system has to "zero" the clusters that were is use, the performance of the file system would be greatly degraded. If a user has a requirement to permanently remove a file or data from a disk they must use specialized "wiping" software. Access data has fairly good wiping software. Wipedrive is used by law enforcement agencies in North America.

There are many software utilities available that can produce a bit stream copy of magnetic media such as a hard drive, Zip™ drive, Jazz™ drive, diskette, flash media card and so on. Some of the more popular software packages in use by law enforcement are SafeBack™, Encase™. There is also Norton ghost that can

make image file, which I will talk about, but it is not use by law enforcement agencies.

An excellent tool, which is very common, is the Image Master Solo Forensics Hard Drive Duplicator™. Intelligent Computer Solutions produces the Master Solo and it is very helpful in the creation of an image of a hard drive including the Master Boot Record, the unallocated space and all the files contain on the hard drive. It is very fast as there is no operating system or software. It is a modified hard disk controller with a simple menu screen from which the investigator can enter commands. This device is small, easy to use and you can copy multiple suspect hard drives on a single target media. The target media must be large enough to hold the aggregate of suspect data acquisitions. A drawback to this hardware copy, is the data is written "raw" to the target media therefore no target image file is created. A subsequent image file acquirement will have to be performed on the target media in lab environment at a later date.

The acquisition phase must not alter the suspect data during the acquisition. The bit stream copy or image file can be created using the previously mentioned software imaging tools. They need traditional operating systems like DOS™ or Windows™ to function. It is crucial the suspect system be booted using an external "safe" copy of the operating system more commonly known as a boot disk. Forensic boot media system files must be altered as well to ensure there are no references to suspect media. This will ensure the media is not accessed in any fashion during the booting sequence. Some of these tools "lock" the suspect media by intercepting IO interrupt, again ensuring no write access possible to the suspect media. Once safely booted, the image file can be written via parallel port, network cable, SCSI cable or FireWire (IEEE1394).

Utility comparison

Norton Ghost

Norton Ghost is a software package that creates image files. Those image files contain all the information necessary to recreate the hard drive or logical partition. Norton Ghost verifies possible data error by doing cyclic redundancy checking (CRC32). But as an investigation tool, this software will not be very helpful or forensically sound because some version of the Norton Ghost image contains only the active files on a hard drive. It does not contain the unallocated space, which is potentially the most important part. The majority of the evidence found on hard drive is in the unallocated space.

Symantec's website indicates the following information regarding Ghost; *Symantec Ghost makes complete, reliable backups of PC drives, including applications and critical data. Administrators can choose to deploy entire operating systems, application packages, user "personalities," network configuration settings, or incremental backups.* [5]. The tool was never designed

with forensics in mind. It is supposed to help administrators with deployment of multiple workstations. Ghost filters out what it considers unused space making it forensically unsound.

Safeback

SafeBack has been the industry standard in making evidence grade bit stream backups since 1990 when Sytex Inc. developed the first version of the software. SafeBack was designed for military and law enforcement use and the original design incorporated two important levels of mathematical hashing to guarantee accuracy. [6]. Safeback is a software that is capable of making bit stream backup, which meets the exactness and precision required by law enforcement agencies. The precision of the safeback back up is guaranteed by the mathematical cyclic redundancy checking (CRC).

One of the most important aspects of forensic analysis is being able to show that your examination did not alter any part of the original file or evidence. A way to do this is to calculate a checksum. These calculations perform a mathematical calculation using every bit of the file. The final value is the CRC of the file. Depending on the algorithm used the chances are from roughly one in 64,000, to one in two times 10^{34} that two dissimilar files will produce the same value.[6]

The CRC process validates the comparison of the data on the hard disk, which has been copied to the restored data. For the investigator, the accuracy of the digital evidence is the primary concern, because he has to validate in a courtroom that the image that he has is the exact integral copy of the original.

An advantage of the image files created by this particular software is that it can be write to many different media such as magnetic tape, hard drive, CD-ROM and DVD. Safeback also copies all the data from the source hard drive including the file and disk slack.

The best way to create an image file with Safeback is to insert the suspected hard drive in a forensic system, which contains the system disk, and a sanitized disk to send the image files to. Safeback will create an audit file, which will contain all the software operations during the imaging process, including date and time of the acquisition and the hash value (SHA256).

Encase

Encase is the industry standard as a forensic tools for investigators. This software is user friendly and makes the peace officer's duties easier. With Encase, it is possible for a person to go through the whole process of the computer investigation. What I mean by this is that with Encase, an investigator will create the image file of the suspect media (hard drive, Zip™ and Jazz™

drive, floppy, CD, DVD, flash card). After the creation of the image file, he will be able to analyze it. In the process of analyzing it is possible to export any suspect files or documents from the image file. Encase produces a complete report as well. The report includes the disk geometry, hash set (to confirm the exactitude of the image file), will display the file structure tree and will list all the incriminating files that you found in the course of your investigation.

The hard drive acquisition can be securely made with the IDE Fastbloc™. Offering an unmatched combination of convenience and speed, FastBloc™ IDE is the most advanced hardware write-blocking tool available today. FastBloc™ IDE is an IDE-IDE write-blocked architecture allowing IDE media to be acquired safely in Windows. [7].

In fact, by using the Fastbloc™ to write block the suspected hard drive you protect your evidence of being altered at the beginning of your investigation. This tool ensures integrity during the acquisition phase of your analysis.

Another appreciated aspect of Encase is that the software gives you the opportunity to preview the media that you investigate before imaging. For example, sometime there are judiciary constraints imposed on the investigator. A judge of justice of the peace may ask you to make sure that the evidence is on the hard drive before you seize it or image it. The best way of previewing the media is by using the Fastbloc™ because it will be possible to write block the disk.

Another way of previewing is by booting the suspect computer with an Encase boot disk and preview the hard drive through parallel port or network cable. The program offers you the possibility of setting the suspected computer as a server and your machine as client. Encase is able to read and image any MAC OS, Windows, Linux, Solaris, HP UX.

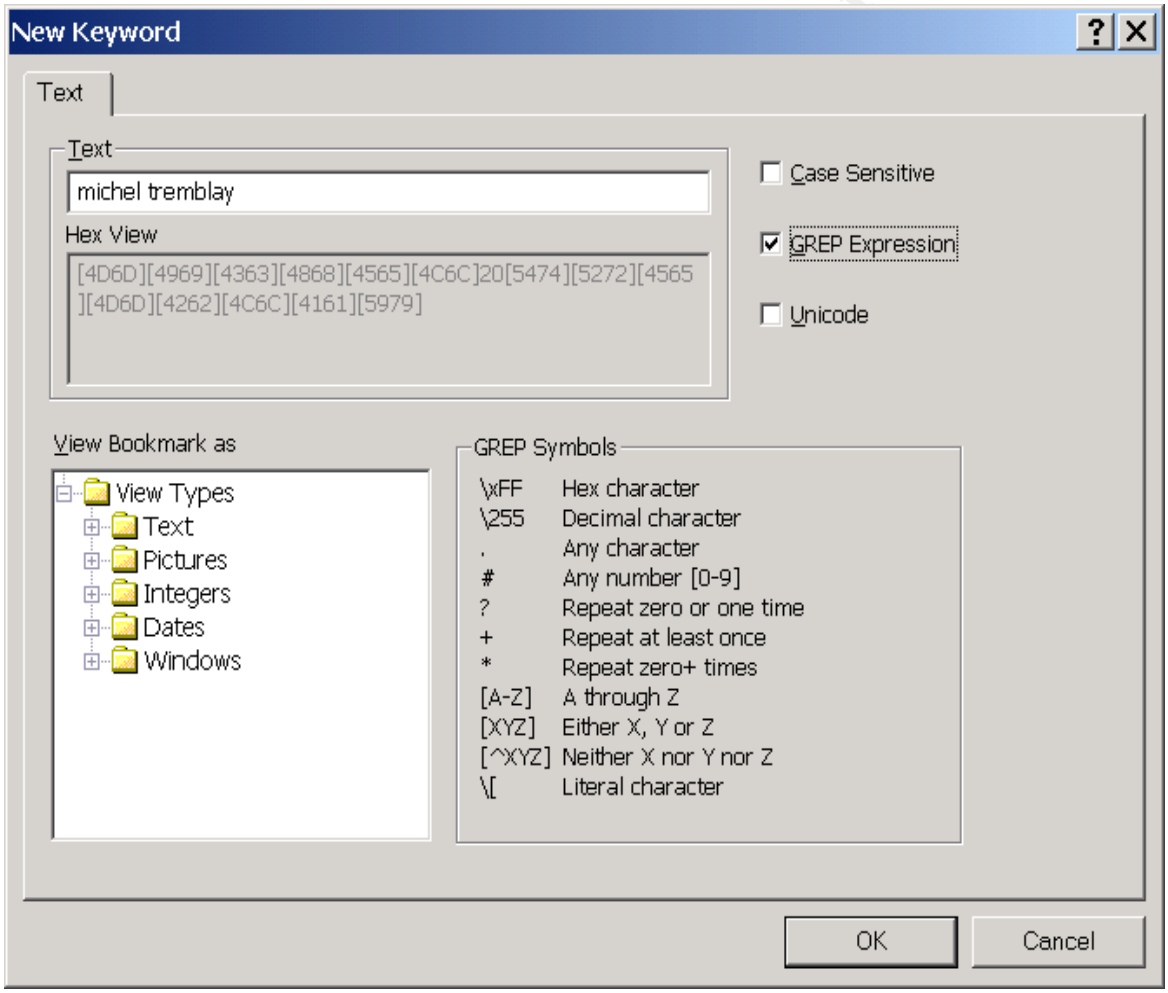
Once the suspected computer is booted with the Encase Boot Diskette you have safe access to the data, Encase offers you the two possibilities. The first one is that you have access to all the active files on the disk. The investigator has the possibility to select the View All Files button and sort them by name, by file extension, by creation date and by last access date. This way, it is possible to have quick overview of the file system.

The second possibility is that the software offers you a search tool that will allow you to search the entire disk including the file slack, the unallocated space and the active files. You can search by keyword, date and specific expression. You can search normal expression or GREP expression. *GREP is a Unix tools with a powerful a flexible syntax. You can use GREP syntax to describe a search term when you want to be very careful about the nature of the text that produces a*

match. You can also use GREP to avoid having to specify many redundant instances of search terms. Here a GREP expression example: [8]

(*### [) \ -] *### [\ -] *####

This expression matches a Canadian phone number in one of several formats. The (* expression means that the open parentheses '(' character can be present or not. The [ ) \ -] expression means that either a space or a close parentheses or a dash can be present or not. Here a picture of a keyword tool in Encase.



At that point, if you find any word or document that incriminates the suspect, you can start to acquire the disk or seize the whole computer and bring it in lab for the forensic analysis.

Encase is the most complete forensic analysis software available on the market presently. The software offers you the possibility to acquire the image file,

analyze it and make different keyword search which save the investigator precious time. To present your evidence to the criminal courts, Encase creates a complete report of the actions you took during this analysis and a copy of the incriminating file.

There are more forensics tools on the market but which one is the best one to use. Different agencies use different criteria to evaluate the use of one software package over another. The criteria are often created as a result of local laws and other regional judicial constraints. Bearing these differences in mind, I feel it is impossible to dictate which one is best for any given agency.

Analysis of acquired data

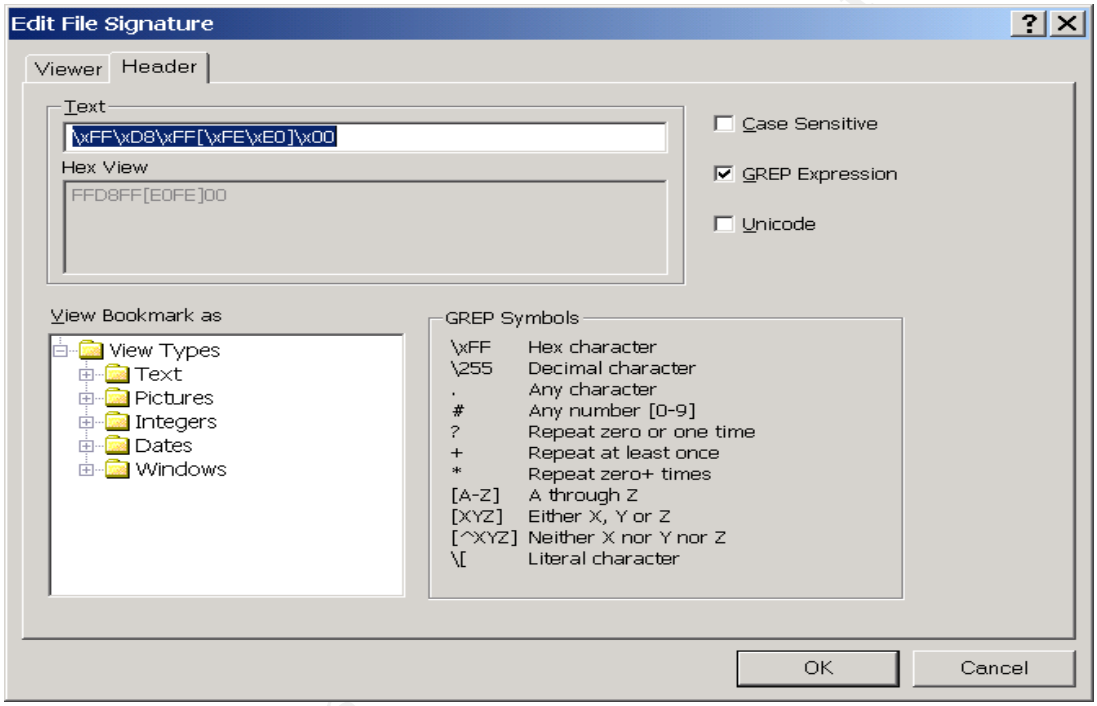
When a forensic analyst has to search evidence to bring a suspect to court, he has a large responsibility and he should perform this duty as professionally as possible. The investigator should be very methodological when working on evidence files:

1. Make sure that the image file is copied to a storage area network (SAN) or on another backup device.
2. Never work on the original file. The reason for this is if you accidentally corrupt the file you are able to make another copy.
3. Create a folder to place all the data that you will accumulate while analyzing the evidence such as case folder, export folder and evidence folder.
4. With the Encase software, let the software verify the integrity (MD5 hash algorithm) of the entire disk image before you start working on the analysis.
5. *Run the signature analysis by Encase. Most common graphics and document files contain a well-defined signature at the beginning. This allows file viewer to recognize the type of file regardless of the file extension. Encase utilizes this convention to look for files that have been renamed to hide their true contents. [8].*
6. Add all file viewers that it is possible that you will need to use Encase. Such as an HTML viewer (IE), Word, Excel, movie player and graphics viewer.
7. Prepare a keyword list with the lead investigator of the operational file to refine searches of the evidence.

When the forensic analyst proceeds with the analysis, he should be aware of what is looking for. For example, if the analyst is looking for a .doc file, he has the possibility to order all files per file extension and verify the entire .doc file. But this

process could be long and depending on how many files he has to look into. But if he knows exactly which file is looking for, that process is the fastest.

But if you are looking for any kind of document/part of document and/or file, Encase software offers you the possibility to make keyword searches, which will look into all files that you have on the disk including all the deleted files and in the file slack space. *Sometimes you might need to search not for text, but for hex. This could be to find hex headers for files to find partition information, or what you have. [9].* If you're looking for .jpeg header, you can get the JPEG hex header in the Encase software from **tools…file signatures** dialog box. Here an example.



The software also has the possibility to recreate a document or part of document to reconstitute evidence that will permit the law enforcement agency to charge the criminal offender. It is also possible to have a quick view of all pictures contain on the image file just by using the gallery view. The investigator has a thumbnail view of the picture and can expand the suspected one.

Conclusion

In conclusion, I will say that it is very easy for any person to hide data on hard disk or any media available on the market. It is important for the forensic investigator to receive the proper training for the type of duty they have to accomplish. But they have the responsibility to guarantee that all the incriminating digital evidence that is presented before the criminal courts is

identical to the one that was contained on the original media seized during their investigation. For that reason, some software companies specialize themselves in the creation of forensic software, which will be helpful to all law enforcement agencies around the world. The responsibility of the peace officer doing forensic system analysis is very important because in some case it could be the difference between a guilty verdict and a non-guilty verdict against a charged individual.

Reference:

[1] New technology Computer Evidence Defined.
http://www.forensics-intl.com/def3.html

[2] New technology
http://www.forensics-intl.com/def3.html

[3] New technology. File Slack Defined.
http://www.forensics-intl.com/def6.html

[4] New technology. Computer Evidence Defined.
http://www.forensics-intl.com/def8.html

[5] Symantec Ghost enterprise.
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=3

[6] SafeBack - Evidence Grade Backup Software.
http://www.forensics-intl.com/safeback.html

[7] Guidance software. encase software.
http://www.guidancesoftware.com/products/hardware/fastbloc/index.shtm

[8] Guidance software, Encase version 3
Document/manual: User Manual

[9] Guidance software, Encase version 3
Document/manual: User Manual