Your Computer Forensic Toolkit

Kelly J. (KJ) Kuchta

The last article was Part 1 of the series and was about building a computer forensics laboratory and what it should include. That article briefly discussed forensics tools that you might need. This article takes a more detailed look at the type of tools that are used in computer forensics. In Part 1, forensic software was categorized into seven different categories: (1) imaging, (2) analysis, (3) conversion, (4) viewing, (5) monitoring, (6) security utilities, and (7) over-the-counter software. These categories to define tools will be used in this article.

The forensic software to be reviewed here is probably used by a vast majority of computer forensic professionals, and it is the most common in the field. The latest information on Linux-based forensic tools will be provided. Most businesses use Microsoft Windows products, so the tools that are going to be reviewed will provide good results for this environment. There are also other products which are useful, but will not be reviewed here because of the focus of the article and the space allotted for this topic. The areas covered will be product functionality, limitation, level of expertise required, price, and miscellaneous information needed to use the application.

New forensics software is being introduced on a weekly basis. Consequently, this article should not be considered to contain an all-inclusive list of forensics software products. I write about tools that I am familiar with. The biggest concern in using these tools should be that the user is comfortable with the results and how the product works. The current debate among the forensic community is with "point and click" tools. Purists argue that in order to really know what is going on with tools, users must understand exactly what

KELLY J. KUCHTA is the National Director for the METASeS DefenseONE Computer Forensic and Litigation Support Services, based in Phoenix, Arizona. He is an active member of the High Technology Crime Investigation Association (HTCIA), Association of Certified Fraud Examiners (ACFE), Computer Security Institute (CSI), International Association of Financial Crime Investigators Association (IAFCI), and the American Society of Industrial Security (ASIS). He currently serves as the Chair of the ASIS Standing Council of Information Technology Security.

An individual who works in this area for any amount of time must be prepared to sit down in front of a client, boss, judge, or jury and explain what the tools do.

they are doing. The purists further argue that most users really do not know what is going on when they "point and click" their way around a computer forensic examination. Additionally, the professional is not encouraged to validate the results, instead relying on the output of the application. To their point, what application is bug free? These individuals tend to prefer utilities, DOS applications, or working with applications that require a great deal of understanding about the process.

Neophytes argue that this line of thinking is out of date, pragmatic, and limiting. They argue that using "point and click" tools provides a shorter learning curve and helps bring a greater number of professionals into the field more quickly. There is also the feeling that the old guard is reluctant to change and thereby makes claims of hypocrisy. Whatever the stance, the points that most everyone agrees on are: validate and understand results, be able to explain how the tool works, and never violate the "basic principles" of computer forensics. An individual who works in this area for any amount of time must be prepared to sit down in front of a client, boss, judge, or jury and explain what the tools do.

BASIC PRINCIPLES

Everything that a computer forensics professional does should be grounded in certain principles. They are:

□ Never work on original evidence.
□ Use tools that have been tested and are capable of replicating findings.
□ Take copious notes or have tracking capabilities of all efforts.
□ Strictly follow established procedures for evidence preservation.
□ Maintain chain of custody.
□ Use the highest standards of conduct to obtain results.

This article will focus on two of these principles. The others will be covered in subsequent articles. The principles covered here are the use of tested tools to replicate findings and preserve evidence.

I have yet to find one tool that does everything I need it to do. Some tools have multiple functions and will be mentioned throughout the article. Just as tradesmen have many tools in their toolboxes, so should users anticipate their needs and bring along familiar tools. Let's dig into the toolbox!

IMAGING

An important part of computer forensics is the acquisition and preservation of evidence. To complete this process, an application is needed that makes an exact copy of the data or lack of data in each sector of the targeted hard drive. This must be accomplished without changing any of the data. This process is called "making an image" or producing a "mirror image." The image can then be searched for items of interest or it can be restored to another hard drive or media. Because an exact image of the suspected hard drive has been made, the restored image can be used in place of the original drive and searched without the concern of altering the original data. Some common imaging applications will be described:

SafeBack *www.forensics-intl.com*

SafeBack was originally created in 1990 and marketed by Sydex, Inc. In March 2000, New Technology, Inc. (NTI) purchased the SafeBack product and currently markets it with the rest of their products which will be mentioned here.

Functionality

SafeBack is an MS-DOS-based program which makes an exact bit stream imaging of media like a hard drive without altering the data. As of this article, the latest version available is 2.18. What makes SafeBack so powerful is that it is not file oriented. Therefore it will make an image of just about any hard drive that can be read by a computer, regardless of the target system's operating system.

SafeBack has a robust audit feature that gives the user the ability to compare the original data to the copied data. The application uses both a 16-bit CRC checksum for each block of data and a 32-bit CRC checksum for the file itself to create a hash of the original evidence and the copy. Both hashes are compared to determine that both the original and the copy are exactly the same. The mathematical likelihood of getting a CRC match from different data is astronomical. This information can be saved to a file and used to verify that the data is in fact "authentic." This process can be replicated numerous times to determine the accuracy of the data so long as the information has not been changed. ***Note:*** Data is easily modified. This fact will be addressed in the article on computer forensic methodology.

Limitations

SafeBack is a non-GUI MS-DOS application.

Level of Expertise Required

While SafeBack is not hard to use, it does require the user to have at the very least a basic understanding of MS-DOS.

Price

At the time of this article, the price for this single product could not be determined. Contact NTI to determine if SafeBack can be purchased separately or if it is included in their other forensics tool suites.

Miscellaneous Information

Sydex stood behind its product and its functionality. If necessary it sent a representative to the court to substantiate the product's functionality. It is unclear whether the new owner NTI will continue this practice. However, NTI's track record of technology support is equally as impressive. SafeBack is an application that is well established and has been battle tested in court. Users should feel reasonable confidence in using this product.

EnCase *www.guidancesoftware.com*

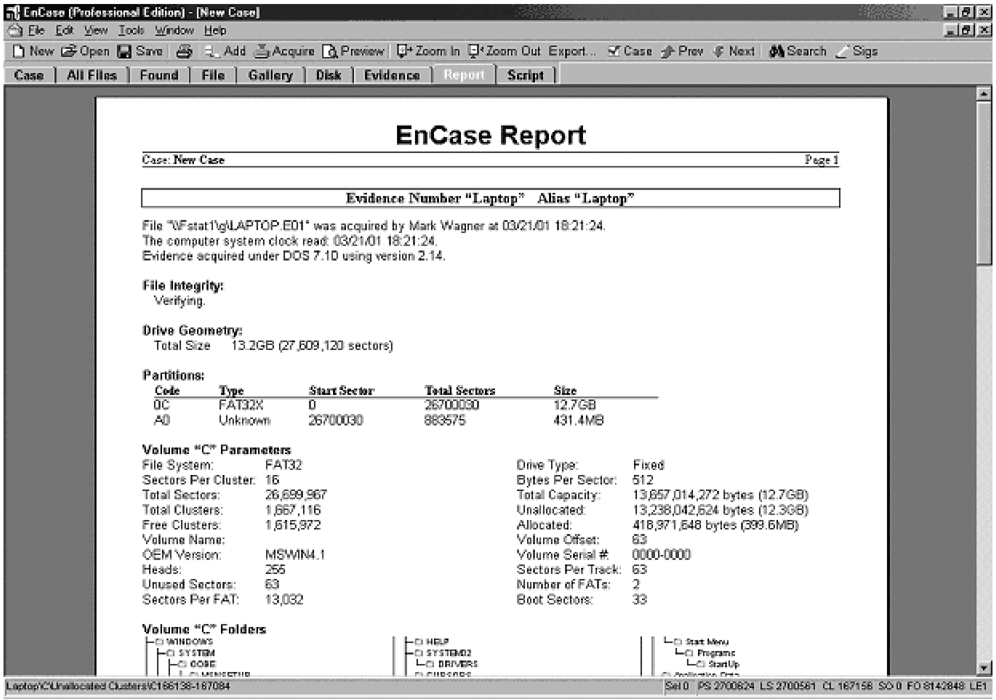
Functionality

EnCase's latest version, 2.16a, has a number of different features that make it useful. It is a Windows-based application with a GUI that gives it a polished look and feel. Forensic professionals should take advantage of its unique evidence acquisition features.

The newest Professional versions can be used to acquire evidence from various operating systems such as FAT12, FAT16, FAT32, NTFS, EXT2, CD-ROM, and Macintosh. While not having the track record of SafeBack, Encase is a solid imaging tool. It provides an audit feature to verify and authenticate evidence. It will automatically record details about the evidence acquisition process and place them into a report format. This type of information might include drive specifics, dates and times, hash values, etc. It allows the forensic professional to create and organize the evidence file to individual preferences. A sample of the report view in EnCase version 2.14 is illustrated in Exhibit 1.

Limitations

EXHIBIT 1 Report View in EnCase v2.14


EnCase (Professional Edition) - [New Case]
File Edit View Tools Window Help
New Open Save Add Acquire Preview Zoom In Zoom Out Export... Case Prev Next Search Sigs
Case All Files Found File Gallery Disk Evidence Report Script
WINDOWS
SYSTEM
OOBE
HELP
SYSTEM32
DRIVERS
Start Menu
Programs
StartUp
Laptop\C\Unallocated Clusters\C166138-167084
Sel 0 PS 2700824 LS 2700581 CL 167156 SO 0 FO 8142848 LE1

```
                         EnCase Report
Case: New Case                                                    Page 1

             Evidence Number "Laptop"   Alias "Laptop"

File "\\Fstat1\g\LAPTOP.E01" was acquired by Mark Wagner at 03/21/01 18:21:24.
The computer system clock read: 03/21/01 18:21:24.
Evidence acquired under DOS 7.10 using version 2.14.

File Integrity:
  Verifying.

Drive Geometry:
  Total Size    13.2GB (27,609,120 sectors)

Partitions:
  Code    Type       Start Sector    Total Sectors    Size
  0C      FAT32X     0               26700030         12.7GB
  A0      Unknown    26700030        883575           431.4MB

Volume "C" Parameters
File System:          FAT32              Drive Type:         Fixed
Sectors Per Cluster:  16                 Bytes Per Sector:   512
Total Sectors:        26,699,967         Total Capacity:     13,657,014,272 bytes (12.7GB)
Total Clusters:       1,667,116          Unallocated:        13,238,042,624 bytes (12.3GB)
Free Clusters:        1,615,972          Allocated:          418,971,648 bytes (399.6MB)
Volume Name:                             Volume Offset:      63
OEM Version:          MSWIN4.1           Volume Serial #:    0000-0000
Heads:                255                Sectors Per Track:  63
Unused Sectors:       63                 Number of FATs:     2
Sectors Per FAT:      13,032             Boot Sectors:       33

Volume "C" Folders
```

It has been reported that EnCase has some difficulty in imaging large evidence files. This limitation can be overcome by using certain techniques and the newest version is thought to address this issue.

Level of Expertise Required

EnCase does not take a great deal of training to master the basic functionality. Persons who attend a training class and can use their newfound skills on a regular basis can quickly contribute to your practice. Guidance Software also provides a better than average user manual.

Price

EnCase has two versions: Standard and Professional. A single-user license for Standard is $995 and the Professional version is $1,650.

Miscellaneous Information

Guidance Software provides both technical support and an EnCase user group to answer questions. Guidance was scheduled to release a new version of EnCase, 3.0, sometime in the second quarter of 2001.

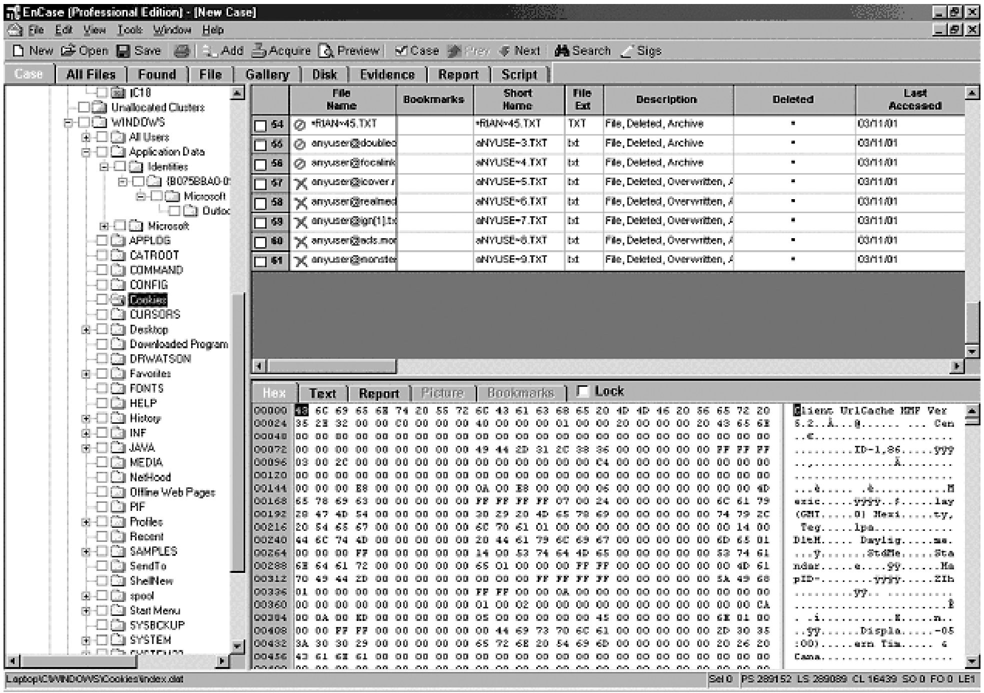
ForensiX *http://all.net*

For Linux gurus, the "dd" command makes a forensics-quality image of the media to be copied. I know of only one Linux forensic utility. It's developed and sold by Fred Cohen & Associates.

Functionality

The preferred operating system for ForensiX version 1.0 is RedHat Linux, although other versions of UNIX will partially support it. It is capable of imaging Mac, DOS, Windows, UNIX, and other disks and files. It can also image PCMCIA cards, IDE, SCSI, parallel, serial, etc. Other important features are that it automatically produces chain-of-evidence information, does not modify the original evidence, accommodates large amounts of data (reported to be 16 terabytes), and will replay the analysis with automatic analysis integrity verification.

EXHIBIT 2 Typical View with EnCase



	File Name	Bookmarks	Short Name	File Ext	Description	Deleted	Last Accessed
□ 54	*RIAN~45.TXT		*RIAN~45.TXT	TXT	File, Deleted, Archive	•	03/11/01
□ 55	anyuser@doubleo		aNYUSE~3.TXT	txt	File, Deleted, Archive	•	03/11/01
□ 56	anyuser@focalink		aNYUSE~4.TXT	txt	File, Deleted, Archive	•	03/11/01
□ 57	anyuser@icover.r		aNYUSE~5.TXT	txt	File, Deleted, Overwritten, A	•	03/11/01
□ 58	anyuser@realmed		aNYUSE~6.TXT	txt	File, Deleted, Overwritten, A	•	03/11/01
□ 59	anyuser@ign[1].tx		aNYUSE~7.TXT	txt	File, Deleted, Overwritten, A	•	03/11/01
□ 60	anyuser@ads.mor		aNYUSE~8.TXT	txt	File, Deleted, Overwritten, A	•	03/11/01
□ 61	anyuser@monster		aNYUSE~9.TXT	txt	File, Deleted, Overwritten, A	•	03/11/01

```
00000 43 6C 69 65 6E 74 20 55 72 6C 43 61 63 68 65 20 4D 4D 46 20 56 65 72 20  Client UrlCache MMF Ver 
00024 35 2E 32 00 00 C0 00 00 00 40 00 00 00 01 00 00 20 00 00 00 20 43 65 6E  5.2..À...@...... ... Cen
00048 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..€.....................
00072 00 00 00 00 00 00 00 00 00 49 44 2D 31 2C 38 36 00 00 00 00 00 FF FF FF  .........ID-1,86.....ÿÿÿ
00096 03 00 2C 00 00 00 00 00 00 00 00 00 00 00 00 C4 00 00 00 00 00 00 00 00  ..,............Ä........
00120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
00144 00 00 00 E8 00 00 00 00 00 0A 00 E8 00 00 00 06 00 00 00 00 00 00 00 4D  ...è.......è...........M
00168 65 78 69 63 00 00 00 00 00 FF FF FF FF 07 00 24 00 00 00 00 00 6C 61 79  exic.....ÿÿÿÿ..$.....lay
00192 28 47 4D 54 00 00 00 00 00 30 29 20 4D 65 78 69 00 00 00 00 00 74 79 2C  (GMT.....0) Mexi.....ty,
00216 20 54 65 67 00 00 00 00 00 6C 70 61 01 00 00 00 00 00 00 00 00 00 14 00   Teg.....lpa............
00240 44 6C 74 4D 00 00 00 00 00 20 44 61 79 6C 69 67 00 00 00 00 00 6D 65 01  DltM..... Daylig.....me.
00264 00 00 00 FF 00 00 00 00 00 14 00 53 74 64 4D 65 00 00 00 00 00 53 74 61  ...ÿ.......StdMe.....Sta
00288 6E 64 61 72 00 00 00 00 00 65 01 00 00 00 FF FF 00 00 00 00 00 00 4D 61  ndar.....e....ÿÿ......Ma
00312 70 49 44 2D 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 5A 49 68  pID-........ÿÿÿÿ.....ZIh
00336 01 00 00 00 00 00 00 00 00 FF FF 00 00 0A 00 00 00 00 00 00 00 00 00 00  .........ÿÿ.............
00360 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 CA  .......................Ê
00384 00 0A 00 ED 00 00 00 00 00 05 00 00 00 00 00 45 00 00 00 00 00 6E 01 00  ...í...........E.....n..
00408 00 00 FF FF 00 00 00 00 00 00 44 69 73 70 6C 61 00 00 00 00 00 2D 30 35  ..ÿÿ......Displa.....-05
00432 3A 30 30 29 00 00 00 00 00 65 72 6E 20 54 69 6D 00 00 00 00 00 20 26 20  :00).....ern Tim..... & 
00456 43 61 6E 61 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  Cana....................
```

Laptop\C\WINDOWS\Cookies\index.dat

Sel 0 PS 289152 LS 289089 CL 16439 SO 0 FO 0 LE1

Limitations

None noted.

Level of Expertise Required

It is strongly suggested that users be familiar with RedHat Linux because many of the features require the use of UNIX like code to execute certain commands.

Price

At the time this article was written a single copy of ForensiX was offered for $899.

Miscellaneous Information

Dr. Fred Cohen is very well respected in the computer forensic area and has an excellent reputation of being accurate and knowledgeable. From all accounts, this tool is a good one.

There are other imaging tools that I have not mentioned such as Snapback, Drive Image Pro, Byte Back, and, of course, Linux. Snapback and Byte Back are utilities that are favored by the law enforcement community; however, they are only offered to the law enforcement community.

ANALYSIS

In Part 1, “analysis” tools were defined as: “conducting document, application or word searches, file comparisons, matching data from a known document to an unknown document, reviewing deleted data or comparing source code.” I will outline a few of the more popular tools below and mention several that may warrant further research.

EnCase *www.guidancesoftware.com*

Functionality

EnCase provides the ability to search for the text in GREP, Case Sensitive, and Unicode. It also provides the examiner with the ability to view thumbnails of graphic files. It can bookmark files of interest into the case folder for future reference and place them into reports. It allows for multiple views of files in Hex, Text, or a report summary. It also allows information to be exported to other formats or files. Exhibit 2 illustrates the typical view seen with EnCase.

Limitations

EnCase appears to have difficulty in viewing Linux file structures and is not as powerful on Linux as it is on Windows products.

Level of Expertise Required

EnCase does not require a great deal of training to master the basic functionality. Persons who attend a training class and can use their newfound skills on a regular basis can quickly contribute to your practice. Most of the analysis functionality is fairly intuitive. Guidance Software also provides a better-than-average user manual.

Price

EnCase has two versions: Standard and Professional. A single-user license for Standard is $995 and the Professional version is $ 1,650.

Miscellaneous Information

EnCase is probably one of the most popular forensic analysis tools used in the computer forensics community, providing the user with a good support group of other professionals who are familiar with the product.

NTI Forensic Utilities

www.forensics-intl.com

Functionality

NTI has been in the business of providing forensic tools since 1996 and is the owner of "SafeBack." NTI's tools are actually a collection of utilities designed to do specific tasks such as capturing file slack, deleted files, or chaining fragmented files. The utilities are designed to accommodate DOS, FAT, and NTFS file structures of Windows operating systems. NTI has a robust suite of tools for just about every forensic need.

Limitations

A user looking for a fully integrated GUI product to shorten the learning curve, is looking in the wrong place. Plan on allowing *plenty* of time to master these tools and the results will be pleasing.

Level of Expertise Required

The user must be comfortable and familiar with MS-DOS and DOS-based products such Disk Edit and System Commander. If a user cannot master a majority of the DOS commands it will be difficult to use this tool to its fullest potential. The required time to master these tools can be much longer, but once accomplished the examiner will generally know the ins and outs of computer forensic examinations.

Price

These utilities can be purchased in a package or "Suite" or they may be purchased individually. Contact NTI for price information.

Miscellaneous Information

The price for NTI tools includes a training class on how to use them. Each utility is licensed to the user to help establish ownership of the tools and validate their use. Most NTI tools cannot be purchased without attending their training classes.

Access Data's Forensic Toolkit or "FTK" *www.accessdata.com*

Functionality

FTK provides full text indexing, advanced searching, known file filtering, graphical file viewing, hash verification, and interoperability with Access Data's password recovering kit (sold separately). It can accommodate all FAT operating systems, NTFS, EXT2, and CDFS.

Limitations

None.

Level of Expertise Required

As with most forensics tools, some training is suggested to maximize effective use. Access Data provides training with the purchase of their software, although the product may be purchased separately.

Price

A single licensed copy is $995.

Miscellaneous Information

A new version of FTK was scheduled for release in the second quarter of 2001.

ForensiX *http://all.net*

Most have heard a commentary about how powerful and flexible Linux can be. ForensiX provides these features and more.

Functionality

Its biggest virtues are that ForensiX can quickly search through large volumes of data, examine deleted files, swap space, and other key areas of interest. It has the ability to view graphics files from disks at the rate of one every second and provides programmable and customizable analysis capabilities along with a Web-based user manual and audio training built into the application.

Limitations

None noted.

Level of Expertise Required

It is strongly suggested that users be familiar with RedHat Linux because many of the features require the use of UNIX-like code to execute certain commands.

Price

At the time this article was written a single copy of ForensiX was offered for $899.

Miscellaneous Information

Nothing noted.

Other tools that are often used in the forensic community are ILook and Drive Spy. ILook is only offered to the law enforcement community so unless you are a law enforcement officer, you are out of luck — especially since it is free.

CONVERSION

To get data into a format that can be viewed, searched, or even recognized, conversion tools are sometimes necessary. Today more tools allow for both importing and exporting of data from and to other applications. Most text files can be converted to similar applications, therefore, I will not belabor the point. However, e-mail presents a much different issue. For e-mail, I strongly suggest using UniAccess.

UniAccess *www.comaxis.com*

Functionality

UniAccess supports the conversion of e-mail between the following e-mail applications: Exchange, Outlook, Notes, GroupWise, Netscape, Eudora, IMAP4, Pegasus Mail, ExpressIT, cc:Mail, daVinci, Notework, CompuServe, Calypso, and HTML. It is also powerful if users need to view a large number of e-mails on an e-mail application that is unfamiliar: e-mail can be exported to a familiar application.

Limitations

None noted.

Level of Expertise Required

Because UniAccess is not a mainstream product, a good dose of patience is needed. As with most data conversion processes, things do not always work as planned. Do not put a junior person on this process until a process or methodology has been developed.

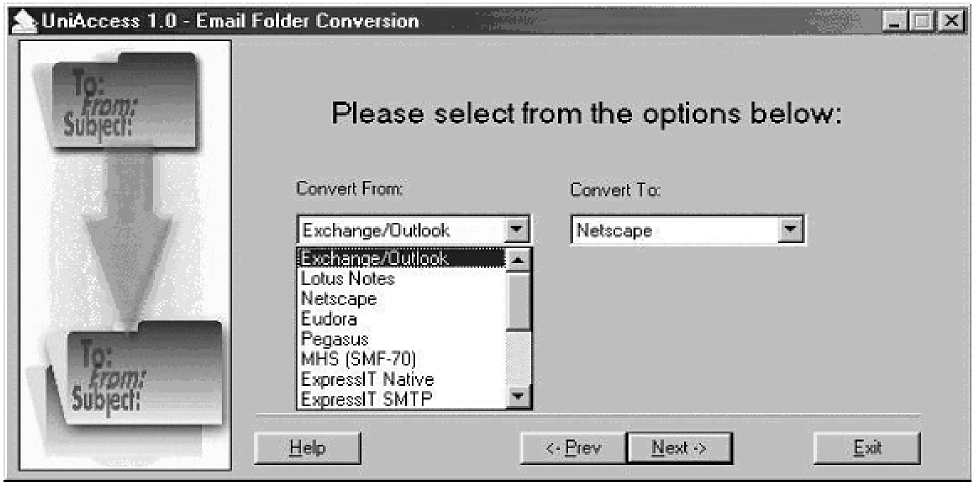
Price

UniAccess is $295 and allows up to 50 licensed users.

Miscellaneous Information

UniAccess cannot be purchased directly from Com/Axis Technology. However, their Web site provides authorized dealers by area. Exhibit 3

EXHIBIT 3 Step 1 of Conversion Using UniAccess


UniAccess 1.0 - Email Folder Conversion

Please select from the options below:

Convert From: Exchange/Outlook

Convert To: Netscape

illustrates the initial step of the conversion process with UniAccess.

VIEWING

Many times a forensic professional will be asked to find certain graphics files or to determine their contents. The law enforcement community deals with this issue frequently in the area of child pornography. Some of technologically savvy individuals with illegal, immoral, and unethical intent attempt to hide the presence of contraband in these files by changing the file header to disguise its contents. To really know what is in the files, they must be viewed. A viewing application is instrumental to view not only graphics files, but also other types of files. Viewing applications present the forensic examiner with a thumbnail picture of the file contents or an image of the document.

EnCase and FTK have built-in file viewers, which allow the forensic examiner to view several pages of thumbnail pictures at one time and then concentrate on a particular file to determine key information about the file such as creation date, size, etc. An example of the thumbnail view in EnCase is illustrated in Exhibit 4.

There are a number of stand-alone viewers to consider. Specifics about each of them follows.

Quickview Plus v 6.0

http://www.jasc.com

Functionality

Quickview Plus has the ability to view over 200 different file formats. This makes it a good all around product to view many different files without having to purchase and open the different types of applications encountered. It supports Win 95, Win 98, WinNT, and Windows 2000.

Limitations

None noted.

Level of Expertise Required

Quickview is very easy to use and requires only a basic amount of knowledge to use the application properly.

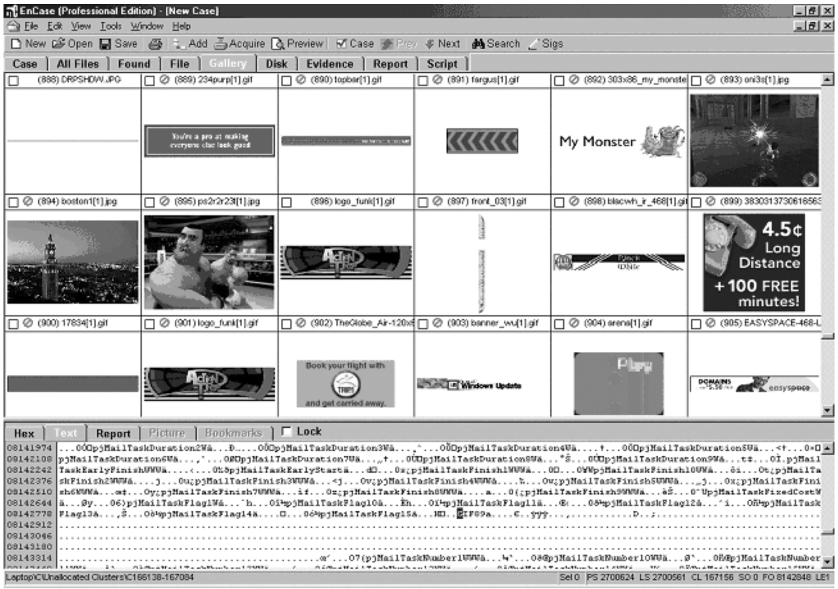
Price

The price for Quickview Plus varies from the low $40 range to as high as $59.

Miscellaneous Information

None noted.

EXHIBIT 4 Thumbnail View in EnCase


EnCase (Professional Edition) - [New Case]
File Edit View Tools Window Help
New Open Save Add Acquire Preview Case Prev Next Search Sigs
Case All Files Found File Gallery Disk Evidence Report Script
(888) DRPSHDW.JPG
(889) 234purp[1].gif
(890) topbar[1].gif
(891) fergus[1].gif
(892) 303x86_my_monste
(893) oni3s[1].jpg
You're a pro at making everyone else look good
My Monster
(894) boston1[1].jpg
(895) ps2r2r23[1].jpg
(896) logo_funk[1].gif
(897) front_03[1].gif
(898) blacwh_ir_468[1].gif
(899) 383031373061656
4.5¢ Long Distance +100 FREE minutes!
(900) 17834[1].gif
(901) logo_funk[1].gif
(902) TheGlobe_Air-120x
(903) banner_wu[1].gif
(904) arena[1].gif
(905) EASYSPACE-468-L
Book your flight with TRIPS and get carried away.
Windows Update
DOMAINS
easyspace
Hex Text Report Picture Bookmarks □ Lock

```
08141974 ...OÓ□pjMailTaskDuration2Wà...Ð.....OÓ□pjMailTaskDuration3Wà...‚ˆ...OÓ□pjMailTaskDuration4Wà....†...OÓ□pjMailTaskDuration5Wà...<†...O×□
08142108 pjMailTaskDuration6Wà...‚ˆ...OØ□pjMailTaskDuration7Wà...„†...OÙ□pjMailTaskDuration8Wà...ˆŠ...OÚ□pjMailTaskDuration9Wà...t‡...OÌ.pjMail
08142242 TaskEarlyFinishUWà....‹...O%ðpjMailTaskEarlyStartà...d□...O±¿pjMailTaskFinish1WWà...O□...OŴpjMailTaskFinish10UWà...ðì...O±¿pjMailTa
08142376 skFinish2WWà....j...Ou¿pjMailTaskFinish3WUWà...<j...Ov¿pjMailTaskFinish4WWà....‰...Ow¿pjMailTaskFinish5UWWà...„j...Ox¿pjMailTaskFini
08142510 sh6WWà...æ‡...Oy¿pjMailTaskFinish7UWWà...if...Oz¿pjMailTaskFinish8UWà....a...O{¿pjMailTaskFinish9WWà...èŠ...O^UpjMailTaskFixedCostW
08142644 à...Øy...O6)pjMailTaskFlag1Wà...¨h...OÍ¼pjMailTaskFlag10à...Èh...OÍ¼pjMailTaskFlag11à...Œ...Oš¼pjMailTaskFlag12à...´i...OÑ¼pjMailTask
08142778 Flag13à...‚Š...Oò¼pjMailTaskFlag14à....□...Oó¼pjMailTaskFlag15à...H□..□IF89a....€..ÿÿÿ...‚...........D..;.......................
08142912 ..................................................................................................................................
08143046 ..................................................................................................................................
08143180 ..................................................................................................................................
08143314 .................................................æ´...O7(pjMailTaskNumber1UWWà...¼ˆ...O8@pjMailTaskNumber10WUà...Øˆ...OÑ@pjMailTaskNumber
```

Laptop\C\Unallocated Clusters\C166138-167084 Sel 0 PS 2700624 LS 2700561 CL 167156 SO 0 FO 8142848 LE1

Thumbs Plus v 4.10
http://www.cerious.com

Functionality

Thumbs Plus provides a full page of thumbnail graphic files allowing a quick visual review of the contents to look for things of interest. It is compatible with Win 95, Win 98, WinNT, and 2000. It allows the user the ability to adjust the image quality of the picture and preview movie clips (including the audio portion) and offers a conversion feature for converting multiple files.

Limitations

None noted.

Level of Expertise Required

This application is very easy to use and requires only a basic amount of knowledge to use the application properly.

Price

New users of Thumbs Plus should expect to spend $79.95 for a licensed copy.

Miscellaneous Information

This is a robust application that Cerious Software, Inc. has made a commitment to improve. A number of enhancements are planned between now and 2009. I have heard nothing but good things about technical support issues.

Monitoring

In Part 1, I mentioned that occasionally the events that the user is trying to investigate are ongoing. After the electronic evidence is preserved, the event may be monitored in a near- or real-time basis. There are plenty of different types of applications available. However, for this article, I will focus on two; *keystroke capture programs* and *sniffers*.

Keystroke capture programs can be instrumental in obtaining a confession from the instigator — especially when it is in their own words as captured on the keyboard. The premise is that all of the activity on the keyboard is recorded and preserved. Two programs that might warrant attention are Investigator and Silent Watch.

Just remember that the bad guys can also use software against you. So be careful.

Investigator
www.winwhatwhere.com

Functionality

This application has many interesting features that make it appealing in investigating IT events. The company Web site describes it as follows: "WinWhatWhere Investigator provides a highly detailed audit trail of all computer activity. This includes date, time, elapsed time, window titles, URLs, and keystrokes — providing an accurate picture of usage on the monitored computer."

A forensic professional must have access to the target computer's hard drive. Investigator allows the application to be loaded onto the target computer, making it invisible to the user. The forensic professional chooses where the application is placed in the target computer's directory. Then the program is only visible by using a certain combination of keystrokes which is how the forensic professional will need to access the application in the future. The data must then be retrieved through direct access to the computer or through its "Stealth Email" feature. This feature will allow the forensic professional to compress the captured data and e-mail it to an account of their choice, unknown to the user. The frequency and time of the e-mails are customizable to permit updates as often as necessary.

Limitations

None noted.

Level of Expertise Required

Investigator is fairly easy to use, but I highly recommend testing and using the product first before using it in the field. If not set up correctly, your efforts can be compromised.

Price

A single copy of WinWhatWhere Investigator may be purchased for $99.

Miscellaneous Information

As with all of the monitoring software I discussed, there are privacy issues that must be addressed. Please understand which issues that are pertinent to the situation before deploying these tools or any other tools of this nature.

Silent Watch *www.adavi.com*

Functionality

The company Web site describes Silent Watch as follows: "ADAVI Silent Watch allows you to control misuse of your computers and restrict objectionable content that may harm or distract others on your computer network. ADAVI Silent Watch will also track computer idle time, record keystrokes, URL logs, monitor incoming and outgoing e-mail and monitor an unlimited number of computers on your network." The single user or "at home" application is call "Silent Guard."

Limitations

None noted.

Level of Expertise Required

Silent Watch has evolved into a network-based product. Because of the complexity of network issues, it requires the forensic professional to have network skills. It is highly advisable to test and use the product prior to using it in the field. Silent Guard, its stand-alone product, is much more user friendly.

Price

A single copy of Silent Watch including four seats may be purchased for $199.95. Additional seats can be purchased in incremental blocks. A single license of Silent Guard is $49.95.

Miscellaneous Information

Many in the news media prominently mention Silent Watch and WinWhatWhere Investigator. The news media seems to indicate that these products are being used by a fair number of individuals. Most of the examples given by these accounts were of private citizens monitoring children, spouses, or significant others. However, it is also mentioned that businesses use the products with some success. Just remember that the bad guys can also use software against you. So be careful.

Sniffers come in many shapes and sizes. Use the one that provides the highest level of comfort and confidence for its purpose. One consideration is that sniffers can collect huge amounts of data. When zeroing in on a target, it is essential to have the ability to control the device's collection activity. These logs must be preserved for future reference.

The diversity of sniffers that are available to forensics professionals is not covered in this article; however, there are two that I would like to mention. I have had very good experiences with Session Wall 3 and Network Flight Recorder.

SECURITY UTILITIES

If given a chance, look at an experienced, computer forensics professional's toolkit. It will contain a potpourri of utilities that have been collected over the years. The list will likely include

□ 1. Password crackers — Cain, L0pht Crack, John the Ripper, etc.
□ 2. Encryption software — PGP
□ 3. Erase utilities — Wipe Info, Secure Clean, etc.
□ 4. Comparison utilities — Araxis Merge 2001 Professional
□ 5. Hash utilities — MD5, etc.
□ 6. DOS utilities and operating systems — Disk Edit, etc.
□ 7. Search and indexing utilities — DT Search, etc.
□ 8.Back-up software — Backup Exec, ARCserve, etc.

The type of work the computer forensics professional is involved with determines the software tools they carry.

The type of work the computer forensics professional is involved with determines the software tools they carry. If their skill sets are used primarily in an incident response mode, the toolkit may be more heavily weighed to password cracking, encryption, and the hash utilities. Computer forensics professionals who spend much of their time in the litigation support area will likely consider a search or indexing software such as "DT Search" to be their best friend. The software must index the data and then allow the user to search by keywords, finding every instance of the keyword. The most time-consuming part is the indexing piece; however, after the indexing is completed, search time is minuscule.

OVER-THE-COUNTER SOFTWARE AND HARDWARE

At this time, things are changing frequently and without warning. I strongly recommend that organizations save at least one copy of every version of operating systems they have used as well as e-mail applications and proprietary software. The best way to accomplish this is by approaching the person in the IT group who is in charge of the "Bone Yard." Every organization has a "Bone Yard." Its the place where old and used equipment and software go to after their purpose has been served. Before any item is tossed, ask this IT person to contact you to determine your interest. You can start a nice little library of old software. Who knows, one day it might be worth something. Better yet it will make the job much easier when you are trying to recreate data from the “age of Noah.”

The same can be said for hardware. Ask for the same privileges as for software. Reconstructing records and data from 5 or even 10 years ago may be accomplished only by having access to old equipment. Think of the old “8-track” tapes or “vinyl” records. Their use is very limited without the right hardware.

WRAP UP

Now that you have had some exposure to some of the tools that a forensic professional might use, you need to get some training. The next article in this series will cover what kind of training programs are available, what to look for in the curriculum, the number of hands-on exercises that you should receive, where to find these training courses, and finally some pitfalls to avoid. ■