ISSN. 1363-6650

APRIL 1997
Issue 4

International Journal of FORENSIC COMPUTING™

Contents

International Journal of Forensic Computing
Third Floor, Colonnade House
High Street, Worthing, West Sussex
UK BN11 1NZ
Tel: +44 (0) 1903 209226
Fax: +44 (0) 1903 233545
e-mail: ijfc@pavilion.co.uk
http: //www.forensic-computing.com

Negative Reinforcement

Yet again, as highlighted by the recent sentencing of a British couple for offences against children, we witness the destructive effects the Internet can have on the behaviour of certain individuals. This world wide communications network, of such benefit to the majority of users, can serve to reinforce negative behaviour in the minority. Nowhere is this more apparent than with electronic distribution of pornography via the Internet.

The problem arises because the Internet allows users to communicate with ease and relative anonymity. Previously, a person with an interest in paedophilia, wishing to make contact with like-minded individuals, would have to establish contacts within a fairly local geographical area. In the process of doing so there would be a relatively high level of risk of exposure and possible prosecution. Now, via the Internet, paedophiles can communicate with each other on a global scale; exchange information, ideas and, all too often, pornographic material. With speed and ease a group of paedophiles can form, the individual members of which reinforce and extend each others' extreme behaviour. As membership of the group becomes 'safer' and more permanent, the communal views which are expressed and reinforced are perceived as increasingly 'normal' to the group members. The fact that the group members have never met, live in locations which are remote from each other, and have different cultural backgrounds, will serve to further reinforce group belief in the correctness of the communal virtual unreality.

The sad results of the formation of such groups can be seen in cases where paedophiles have been prosecuted for possession and distribution of digital child pornography and, all too often, the sexual assault of children. In the case of the man sentenced last November at Devizes County Court, UK, an interest in children was reinforced and dramatically developed during a nine month 'cyber' relationship with a female paedophile in the USA. Over this period, which saw the development of an embryonic group as others joined in the communications, there was an exchange of information on how to procure young children, how to prevent them from telling parents about assaults, and what sexual practices were most desirable. There were discussions of past experiences and detailed descriptions of fantasies involving extreme child abuse. There was also the exchange of graphic material of an increasingly lurid nature. The result was that a man who would previously have been unlikely to meet other paedophiles and who lacked the skills or 'courage' to approach children to commit offences became more and more detached from reality. He was convinced that his behaviour was reasonable, that young children would welcome and enjoy his excesses (including torture) and was planning to execute his fantasies when arrested. In the opinion of all the investigators involved an apparently mild-mannered man had become a serious threat to the safety of children.

The escalating numbers of active paedophiles communicating world wide via the Internet, and the recognition of the results of such communication as a major problem area requires new policing attitudes and responses. Only when conducted on an international basis will the discussions required result in the development of meaningful solutions. ■

(Microsoft defines this as: the time the file was created. A value of 0,0 indicates that the file system containing the file does not support this time member.)

The last write/modification time may take on many different meanings. For all practical purposes, it means when a program last made any changes to the file. Even though Microsoft defines it as last write time, if you consider this to be the last modification time, all the behaviour of the operating system relative to this time stamp seem to be somewhat correct. Last modification would occur when you re-opened the document, edited it in some way and wrote the result back to the disk. This is the time File Manager and DIR show you. (Microsoft defines this as: the time that the file was last written to. All file systems support this time member.)

Believe it or not, when an original file is copied (using the copy command or File Manager) both NT and 95 keep the original "last write / modification" time on the new file.

So if the file in question was modified (written to) on your government computer in Greenwich last week, that is the time File Manager will display on the suspect disk. Funny, isn't it? The creation time of the file on the suspect disk may be more indicative of the time the file was copied. But the operating system doesn't display it.

The trick to solving our problem may be the third and final type of file time, "last access time". This generally means the last time some action was taken on the file. It can mean when the file was copied, viewed with a viewer (such as Quick View Plus), opened for reading, or printed with a piece of software. (Microsoft defines this as: the time the file was last accessed. A value of 0,0 indicates that the file system containing the file does not support this time member.)

Generally, the NT system resets this "last access time" any time an action is performed on the file. And most activity on a file (except doing a simple DIR) will cause this time to be reset. You must test the operation of each piece of software and determine when and if the last access time is altered. The last access time is what the examiner should look at. But how?

Windows NT and 95 normally do not provide the capability of viewing any time except the last write time. As mentioned earlier, the last write time is the default for File Manager or DIR. The examiner would need custom software to view the last access time. Software exists that will do this, but that's not for this article.

(Note: WIN95 does not appear to completely support the last access time, even though much of the programming documentation written says this time is available. As best as I have been able to determine, WIN95 stores the last access date, but not the time.)

Another interesting titbit concerning floppy disks. Because of long filename capability, if the floppy is being used in an NT or 95 computer, all three date stamps seem to be in effect and follow the WIN95 formats. This means the last access date is maintained (no time) and the creation and write date and time are also maintained. However, that same disk used in a DOS based computer will only update the last write time, as DOS can only handle one file time.

When the examiner finds the last access time of the files, adjusts for time zone and internal computer clock differences, the suspected files are identified and your case is made. This last sentence, although simple, contains a lot of technical problems.

I'm just trying to point out that for some cases, examiners need to be aware of system and file time problems. I guess the moral of the story for NTFS and WIN95 is test the software to see what affect it has on the various file times. And make certain you have software which can accurately depict these times.

Now for the kicker (if you will): towards the beginning of this article I mentioned that the examiner performed all proper image/back-up procedures. Let's say one of these procedures involved either performing some sort of CRC file verification or using a file viewing technique to see what files were on the suspect system. It is possible that the mere actions of the examiner in performing CRC file verification or file viewing has altered the last access time of the suspect files. (If you had a disk write blocker in place, it is conceivable that none of your software would be allowed to run. That's another discussion entirely.) If the guilt or innocence of the defendant depended on the last access time of a file or files the Defence might challenge the examiners' methods. What happens next I'll leave to you to ponder.

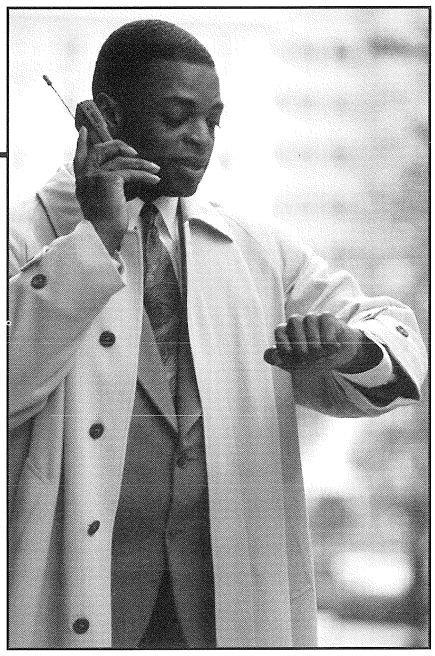
Let me leave you with one thought. What time is it? ■

This article is provided by
Dan Mares
IRS Internal Security, USA.

AUTHOR'S NOTE: *Neither the procedures nor programs presented in any way reflect the viewpoint of the author's agency, and they are solely the views of the author.*

What Time Is It? Part Two will appear in the next issue of the journal.

What Time Is It?



Most people would not have a problem answering this question. PST, EDT, CST, GMT, ZULU. Do these abbreviations mean anything to you? If you deal with operating systems other than DOS they should. They are time zone designations. Even some DOS programs (such as PGP) make use of these items.

As an investigator dealing with computer evidence how important is the time(clock) setting on the suspect computer? It may not be of much concern, or it may be very important when trying to place a suspect at his computer at a specific time.

Let's look at a hypothetical case. Assume a hacker has penetrated your system and is downloading files to his computer. For arguments sake, lets say you are in Greenwich, England and have monitored this activity on your computer. The time on your computer says 12:00 hours GMT. The next day the suspect's computer is seized and sent for analysis. (The suspect lives in Washington D.C.). It is determined that the suspect is using Windows NT and has the NTFS file system set up.

> ***The only way to convict the suspect is to show that your files showed up on his computer within 5 minutes of the time you were monitoring the activity. Your exact request to the examiner stated "you needed to identify files downloaded at 12:00 hours."***

The examiner performs accepted system handling techniques, including back-up / imaging of a Windows NT system and looks for files with a time of 12:00 hours. None are found. What has happened? What should the examiner be looking for?

One possible item overlooked by the examiner might be the time setting of the seized computer. The time setting of the computer will determine the time stamps that get applied to new or modified files. For this reason, it's important to record the local time setting on that computer. Also you should record how far off the correct local time the computer setting is. Most users are content to have the computer's internal clock set to within a few minutes of local time. (I personally verify my computer clock with an atomic clock at least once a week, but I doubt most people do).

Another setting that may be important is the TZ (time zone) variable. This variable is usually set in DOS via the autoexec.bat file, or under NT in the Control Panel. It will indicate which time zone the suspect computer is using.

Even if the computer clock is determined to be accurately set, any file the suspect may have created during your time period would not reflect 12:00 hours GMT. It would more likely reflect local time of 07:00 or 08:00 hours depending on whether Daylight Savings Time was set and in effect during this period. (Don't forget, Washington D.C. is 4 or 5 hours off GMT). The examiner still can't find any files with a time setting matching your 12:00 hours. Why not?

When you use File Manager or the DIR command to display file times, NT shows you the time the file was last written to. From that point on, NT and 95 may handle file times somewhat differently. (WIN95 is similar to NT in its treatment of timestamps. But not 100% compatible. I will note the differences where appropriate.)

Assume the suspect didn't do any writing to the files. All the suspect did was copy them to his system, and maybe, just maybe, used some program to view them. Depending on the specific "copy" operation the suspect used (i.e. FTP, a simple file "copy", telnet) the operating system may display the original file times recorded on your host system which is not the 12:00 you are looking for. In any case let's assume you still don't have a time match because the timestamp on the files on your system, which have now been transferred to the suspect computer are nowhere near the time in question. The time stamp on your host files reflect when you last changed the file. Where to next?

> ***Well, once your examiner straightens out the differences for suspect's local time setting, the next step might be to check the last access time of the files. "Last access time", what's that?***

With operating systems such as UNIX, LINUX, WIN95, Windows NT and others, file times (and dates) are stored as three separate items. There is the creation time, last write/modification time, and last access time of the file. What does this mean?

The creation time is generally the time the file was created. This means when you first created or wrote the file to your disk. This may be of use, since it should record when the file was first created/written to your disk. ▶

Forensic Accountants ...

... a New Breed of Professionals

The world of accountants is no longer the boring and routine one portrayed in the 1970s by Monty Python, at least not in all spheres of accounting. A new breed of accountants has emerged - specialists in the investigation of fraud and the quantification of losses. These professionals travel the world solving complex problems and presenting them in a manner that can be understood by juries. They have grown up with computer fraud and have learned that computer interrogation is a critical part of their analysis.

Forensic accounting is a profession that has grown exponentially in the past decade, both in terms of the number of people involved and the techniques used.

Rafts of forensic accountants have in the past decade unravelled the complex dealings of Robert Maxwell and the trading activities of Nick Leeson, among others. They have learned their skills through the "Big Six" and other accounting firms, as investigators for the Serious Fraud Office or for regulatory bodies such as the Securities and Futures Authority.

Forensic accounting has grown as an international business with essentially US roots.

The idea of creating and marketing specialist teams of accountants was born in probably the most litigious country in the world, the United States. These accountants have become known as forensic or investigative accountants. Forensic accounting is essentially the preparation of accounting evidence or the performance of accounting analysis as part of actual or threatened criminal or civil proceedings or part of a dispute resolution process.

This type of accounting analysis was once performed by auditors and was seen by them as a novel service; the results were almost immediate and the potential savings or additional actions available to a client armed with well thought out and presented accounting analysis could be significant.

In the UK, forensic accounting grew into a separate branch of the accounting profession as auditors began to be used more and more frequently as experts in accounting, assisting in the analysis and presentation of accounting issues and the resolution of disputes. More and more, accountants would be seen in Court giving evidence in connection with a criminal fraud case or opining on quantum in civil litigation.

At the same time as forensic accounting was becoming an established and distinct part of the accounting profession, computers became more and more widely used. In the early 1980s it would not have been unusual to find a major international UK public company consolidating its world wide financial results from hand written ledgers and schedules. Today almost every accountant prepares accounting information and analysis on a computer. Corporate and government accounting systems are held on and are processed by computers and computers are an essential part of the preparation of the financial statements and results of an enterprise.

As such the majority of frauds are no longer buried in the manual cash book with entries deleted by Tipp-Ex. The series of matching

ledgers filed on a shelf in the cashier's office has been replaced by an off the shelf software package which posts entries across multiple accounts at the touch of a button. Typed memoranda from one office to another have been replaced by electronic mail systems on which notes can be deleted wholesale in a second.

As a result frauds in the 1990s are harder to trace and almost always involve the manipulation of data and programs held on computers.

A recent survey conducted for the Institute of Chartered Accountants showed that the manipulation of programs and data held on computers was the area that worried most companies when it came to detecting and combating fraud.

In this environment of electronically held data the investigation of fraud by forensic accountants is becoming increasingly complex. Computer literacy is essential. The majority of investigations begin with or involve computer forensic techniques. It is imperative at an early stage in the forensic accounting process to take stock of the situation in conjunction with a computer forensic specialist. A typical list of questions at the outset of an investigation may include:

- What computer system is used by the company and what accounting software do they run on in it?
- Is there remote access to the system?
- Who has access? ▶

- Do employees use lap top computers?
- Is the system networked?
- How often, if at all, is the electronic mail system archived?
- Are there back up copies of the accounting system?

The forensic accounting process is one of analysis of data. It relies upon forensic techniques for the retrieval of deleted accounting records or data, on the securing and copying of data recording the fraud held on a personal computer kept in the office or at home, on the securing and copying of floppy disks recording the calculations of and distribution of the proceeds of fraud to the participants, to name but a few examples.

For forensic accounting analysis to be effective, robust and reliable it needs to be supported by carefully performed forensic techniques for the retrieval, securing and manipulation of data.

Forensic accountants have had to learn the principles of integrity of retrieved information the hard way and many have come unstuck in the witness box as a result. It is essential that a forensic accountant involved in the analysis of and the giving of evidence involving data retrieved from a computer is fully conversant with how that data has been recovered, what has been done to it and how the integrity of that data can be maintained.

The end analysis may be worthless in the absence of such an understanding.

Forensic accounting, like computer forensics is a rapidly changing environment. In order to keep up with the perpetrators of fraud the forensic accountant must be technologically aware. Forensic accounting analysis will become more sophisticated, complex and involved. It will rely on computer forensic techniques more and more and on techniques to analyse accounting data. Some will be left behind. ■

This article is provided by **Tim Allen**

Tim Allen is Managing Director of Lee & Allen Consulting Plc, the independent, international firm of forensic accountants.

Lee & Allen has offices in London, New York and Hong Kong and carries out forensic accounting investigations throughout the world, often in conjunction with computer forensic experts.

Tim Allen can be contacted in London by telephone on +44 (0)171 353 5550 or by fax on +44 (0)171 353 5343.

Reader's Response

Angus Marshall of the University of Abertay, Scotland writes:

In your reply to the question "I've been told that if I want to look at the contents of a seized computer I should never just switch it on. Why is this and what should I do?" (*Q&A, Issue 2*), you suggest that the best course of action is to boot the suspect system from a floppy disk.

In a majority of cases, where the suspect machine is known to be running a Microsoft (or compatible) Disk Operating System and the boot disk is MS-Dos, PC-Dos or DR-Dos, your advice is quite correct. However, there are a number of situations where this technique may fail completely, fail to reveal the complete contents of the hard disk(s) installed or even cause severe damage.

Taking some example cases in order :

i) In most modern PCs it is possible to set the CMOS preferences in such a way that the PC will ALWAYS boot directly from the hard disk, only trying to boot from floppy if the hard disk is unavailable. In this case, your comments about rewriting of files during booting still apply and the machine should NOT be booted at all until the CMOS settings have been changed. If the investigating officer is lucky, the built-in CMOS setup program will not be password protected and the boot order can be checked/modified appropriately.

ii) Where the hard disk is larger than MS-Dos' default maximum of around 500 Mb, additional drivers may have been installed on the hard disk to allow access to the extra space. Booting from floppy will not load these drivers, and hence a large proportion of the hard disk may be 'invisible' to the investigating officers.

iii) Where the hard disk is set up to 'multi-boot' into more than one operating system, depending on selections from a start-up menu. Only the MS-Dos compatible portions of the disk will be visible and any partitions set aside for Unix-like operating systems (Linux, FreeBSD, NetBSD, OpenBSD, Minix, Xenix, SCO-Unix, 386BSD etc.) will be invisible under MS-Dos.

iv) Where the whole disk has been set aside for Unix-like operating systems (or any other system not recognised by MS-Dos), MS-Dos will in fact overwrite the ▶

master boot record (MBR) of the disk in an attempt to make it acceptable to MS-Dos partitioning and formatting programs. In my own experience of this situation, it can take several days to recover this MBR information and render the disk readable again. Clearly, in this situation, the integrity of all data on the drive is then questionable.

The last situation is likely to be applicable in cases where abuse of the internet (e.g. Child pornography cases) is involved as the Free Unix systems are seen by many as superior to Microsoft compatible systems for internet activity.

Finally, it should also be noted that not all computers are capable of booting from MS-Dos boot disks. Typical examples of these are all Apple Macintosh series machines, which require their own MacOS boot disks, Commodore & Amiga Technologies systems, which require AmigaDos/Workbench and Atari ST systems which require STOS, or alternative operating systems such as Minix, or one of the many Unix-like operating systems.

In summary, I feel that the advice you should have given was that no machine should ever be switched on again, until an expert has had the opportunity to fully examine it to determine correct operating system boot disk to apply. ■

Angus M. Marshall BSc AMBCS FRSA
School of Informatics, University of Abertay Dundee, Bell Street, Dundee, DD1 1HG, UK.

Vox: (+44) 1382 308600
Fax: (+44) 1382 308877
http://www.tay.ac.uk/mcsweb/staff/amm/

Editorial Reply

Thank you Angus for your comments - however, you appear to have missed the most important point in the final paragraph of the answer:- It is essential that any copying is undertaken with software which is known to prevent information being written to the hard disk and, preferably, which has been specifically written for forensic work.

Taking each of your points in turn:-

i) It is certainly possible to set a sequence in CMOS such that a machine will always boot from the fixed disk first. It is also possible for a machine to boot into the fixed disk for other reasons (bad disks, bad drives, virus activity etc.). Observation during the boot process will normally confirm that this is happening before the system has a chance to write anything to the fixed disk system and appropriate action can be taken. It is also our experience that the incidence of CMOS password protection seems to be significantly higher in Scotland than in the rest of the UK.

ii) There is no "default maximum" disk size in MSDOS because MSDOS deals with logical drives not physical ones. The space for the partition start address under MSDOS parameters is a double word, allowing an absolute sector address of 4,294,967,295. So with a sector size of 512 bytes this would allow up to 2 Terabytes ($2*10^{12}$) of space. However, other limitations reduce this to around 16 million sectors (8 Gigabytes with 512 byte sectors). The physical area of a disk being addressed is governed by the addressing mode (THS, XTHS or LBA) as specified within the controller BIOS. Certainly non-MSDOS partitions may not be directly accessible if a machine is booted from an ordinary MSDOS disk but a forensically sound boot disk would be designed to gain access to the BIOS, not the file systems. Historically, as fixed drive sizes increased past the original BIOS limit of 528Mb, there were some attempts to introduce BIOS modifier programs to allow access to greater space when the drive did not match the controller. In over 200 logged investigations on personal computers we have not seen a single case where the absence of a BIOS modifier caused incomplete disk access. If this situation did exist then preliminary examination of a copy of the system taken with the on-board BIOS will reveal it since any modifier software must be available via the on-board BIOS. If this did happen, expert attention would be required to copy the extra space. Once the copy is completed a number of possibilities are available to gain access to the data.

iii) Your observations on different operating systems may be true but apart from the rare case of a BIOS modifier mentioned above, the content of a fixed disk is irrelevant to a properly designed forensic copying system since the copy is conducted at BIOS level. There are certain conditions which could introduce a controller/drive parameter mismatch but these have little practical significance. Where it is thought that the accused might be technically capable of deliberately introducing such conditions, expert advice should be obtained. However, it is our experience that in such cases expert advice is usually sought much earlier anyway.

iv) Your comments on non-PC type computers are correct. The original answer should have indicated that it referred to only IBM PC compatible machines.

v) Your final suggestion that "no machine should ever be switched on again ..." until expert attention is available is surely not serious? Such a course of action would place an intolerable burden of increased cost and time on the primary investigation authorities. Most criminal investigators are capable of recognising the point at which higher expertise is required and the vast majority of cases can be investigated quite correctly without reaching this point as long as simple, sound and relatively inexpensive equipment is available for them to use. We are reminded of the introduction of breathalyser machines some years ago. Breath testing is now done routinely by traffic policemen but before the breathalyser a doctor or an analytical chemist was needed. ■

Case Studies

There are many occasions when forensic work on computer contents reveals nothing of any evidential value but is almost priceless for the intelligence that it yields. Two such recent cases in the United Kingdom involved a murder and an attempted murder.

Murder

One Sunday morning, a young girl's body was found on waste ground not far from a local nightclub. The police were called and their preliminary enquiries established first that she had been murdered and also that she had last been seen at the nightclub the previous evening.

The police interviewed the staff at the nightclub and discovered that a computerised membership system was in use that enabled the owner to provide them with a list of everyone who had attended the club on the Saturday evening. The system used a membership card with a magnetic strip and on entry, every member had to swipe their card through an electronic reader. This collected the data from the card and stored it, together with the date and time of entry, into a database. The card reader was connected to a dedicated desktop computer and every twenty four hours the computer software interrogated the card reader and downloaded the database. The card reader memory was then wiped in preparation for the net night's clientele. The computer software then searched the database and as each record was examined, the details of the member and date of attendance were transferred to the master database which kept an on-going record of every member's attendance at the club. It was this master database that had been used to generate a list of attendees on the night in question and it gave the police valuable information to assist their investigation.

Unfortunately, as the software transferred information from the downloaded card reader database to the master database the time of entry was discarded. Since the card reader database was deleted after the records had been transferred, this important information had been lost - or so the owner thought!

Enquiries of the suppliers of both the hardware and software used in the system suggested that they thought the transient database was not recoverable. Since 344 people had attended the club on the Saturday evening, the police were faced with the huge (and expensive) task of locating them at addresses dotted all over the Home Counties. Almost as a last resort the computer was taken for forensic examination in spite of the club owner insisting that he could not be without the machine for a single night.

The investigation was conducted on the Tuesday after the murder, and the machine had been in continuous use since the previous Saturday. Thus the download-interrogate-wipe cycle had completed a further twice in that time, making it less likely that any useful information would be found.

A forensic copy of the computer was made and liaison with the software suppliers provided details of the format and content of the transient database. Armed with this, a search was conducted of the copy image and the complete contents of the transient database for Saturday were recovered. The recovered file contained only membership numbers but cross reference to the master database (also on the copy) enabled a full printout to be completed of the whole file with every member's name and address, together with the vital time data. This was cross-checked to ensure that it corresponded with that provided by the club owner and interestingly (although of no evidential significance) it indicated that four people had entered the club twice during that night. Copying, searching and printing took less than three hours and the club owner was relieved to get his computer back into action without losing any time.

Using the new printout the police were able to begin their interviewing with those people who had entered at around the same time as the girl. They also had the extra information about the time of entry to help verify the answers they were receiving to their questions.

A considerable amount of time and money were saved on the investigation because the police were able to target their initial enquiries. A man later confessed to the murder and was subsequently tried and found guilty. ■

Attempted Murder

Late one evening a telephone call was received from the police asking for forensic assistance on a desktop computer found switched on and operating at the scene of a particularly brutal attempted murder. The victim was not expected to survive and a full-scale murder inquiry had been launched. Upon receipt of the call, the investigator immediately advised the police to leave the machine on and then drove over 200 miles to the crime scene to assist.

When he arrived he found the place swarming with police and civilian investigators and reported to the Scenes of Crime Officer. He was issued with the standard "clean suit" and overshoes to prevent any contamination and then taken to the computer.

With due regard to the possibility of fingerprint evidence he donned gloves and started his examination. Comprehensive photographs of the area around the computer had already been taken so a note was made of any external features - manufacturers' labels, ▶

serial numbers, peripherals, and so on. Once this was done work was started on the computer itself. The displayed program was Microsoft Word and there was a blank document template loaded. Switching to the task manager the investigator determined that no other tasks were running and then switched the machine off prior to making a forensic copy of it.

Once the copy was completed the S.O.C.O. was advised and the machine was bagged and sealed for further investigation. The copy was taken to the incident room and a preliminary examination was begun. Nothing unusual was found but there were a number of documents which indicated the recent activities of the victim and a suggestion of possible conflict in her business and domestic affairs. The relevant documents were printed there and then and the copy was then taken for a fuller examination back to the laboratory. A full report provided the police with a wealth of information and several promising lines of enquiry. The case is proceeding.

As far as I am aware, none of the material recovered in these cases was or is intended to be used in evidence. However, the intelligence value of the material may well prove incalculable. ■

The above case studies are provided by **Jim Bates**, *BSc(Eng), FIAP (Cmpn), President of the Institution of Analysts and Programmers, UK.*

Discovery ...

...and the Use of Computer-based Information in Litigation

INTRODUCTION

Personal computers and electronic information have become ubiquitous in the information age. The most common form of electronic information - E-mail - is becoming widespread.[1] It has been estimated that 35% of corporate communications never reach paper. Electronic information is contained in many forms and formats including internal computer files, disks and diskettes, magnetic tapes and various transaction reports including those from fax machines and telephone systems.[2] It is routinely retained on diskette or tape as a back-up for the inadvertent loss of data through computer malfunction or other casualty, for archive purposes, and in many instances because of laziness[3] or lack of understanding by the computer owner or operator.[4]

Computer-based files are an often over-looked subject of discovery and source of helpful information in litigation. Knowledge about the methods of storing and using computer-based information can give a litigator a tactical advantage over opposing counsel. Similarly, counsel should advise clients of the potential dangers and burdens of uncontrolled retention of computer-based information.

An understanding of certain technical details is critical to the effective discovery of computer files. A computer file is not physically erased from a disk when it is deleted. Rather, the computer operating system changes the first character of the file name in the disk directory to indicate that the space occupied by the file is not in use and may be re-used. Therefore, it is a relatively straightforward process to recover "deleted" files, as long as new information has not been written over them. Similarly, when a magnetic tape is re-used, the information that is written over will be lost, but old files may exist and survive beyond the end of the new information.

Finally, an attorney seeking to discover electronic information from an opposing party should be aware of the chaos of disks and back-up. The disks and tape cartridges used for back-up are generally of a relatively small size, often are not catalogued and are rarely needed. In some organisations, back-up materials are stored at an off-site location.

DISCOVERY TECHNIQUES

The basis for discovery of electronic information is Rule 34[5], which permits a party to serve on the other party a request:

(1) to inspect and copy documents (including writings, drawings, graphs, charts, photographs, photo-records, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form), or

(2) to inspect and copy, test or sample any tangible things which constitute or contain matters within the scope of Rule 26(b)...[emphasis supplied.]

Although the term "document" is defined in Rule 34, a request for production which seeks electronic information should be expressed so that there can be no misunderstanding. In particular, the requesting party should specify the form of storage (tapes, disks and memory), the condition (including back-up and deleted files) and location (on-site or off-site). It is also important to specify that drafts are to be considered additional documents. Unless ones' client or computer expert has very good information about the other party's computer systems, a request to inspect should be phrased broadly to avoid limiting the ▶

expert's search. One approach is to serve interrogatories on the other party to develop the information which counsel and the computer expert can use to determine whether to make a request to inspect. In particular, one would seek identification of computer systems and equipment in use, the persons responsible for operation and maintenance of the system, any written back-up policies and procedures, and any record retention and destruction policies.[6]

DUTY TO PRESERVE INFORMATION

An important issue in many of the reported discovery cases is the duty to preserve information during litigation. While it is generally accepted that a litigant is under no duty to keep or retain every document in its possession, one has a duty to preserve what he knows or reasonably should know (i) is relevant to the action, (ii) is reasonably calculated to lead to the discovery of admissible evidence, (iii) is reasonably likely to be requested during discovery, and/or (iv) is the subject of a pending discovery request.

However, there is disagreement as to when this duty arises. In Skeete v. McKinsey & Company, Inc., No. 9099 (S.D.N.Y. 1993) (LEXIS), the court stated the duty arises "once a complaint is filed." In contrast, several courts have held that the duty arises when one is on notice that documents are relevant to either pending or potential litigation. Wm. T. Thompson Co. v. General Nutrition Corp., Inc., 593 F. Supp. 1443, 1455 (C.D. Cal. 1984); Capellupo v. FMC Corp., 126 F.R.D. 545, 551 (D. Minn. 1989). In any case, it is clear that a party ignores the obligation to preserve information at his own peril:

> The obligation to retain discoverable materials is an affirmative one: it requires that the agency or the corporate officers having notice of discovery obligations communicate those obligations to employees in possession of discoverable materials.

National Ass'n of Radiation Survivors v. Turnage, 115 F.R.D. 543, 557 (N.D. Cal. 1987).

Given the duty to preserve information and the danger and ease of destroying electronic information, one should consider sending a letter to a prospective defendant or his counsel requesting preservation of computer-based files and records prior to the commencement of litigation.

SANCTIONS FOR DESTRUCTION OF EVIDENCE

Both state and federal courts have considerable authority to impose sanctions on parties who destroy requested documents under Rule 11, Rule 37, 28 U.S.C. §1927 and the "inherent power [of the court] to regulate litigation, preserve and protect the integrity of the proceedings before it, and sanction parties for abusive practices." Capellupo, supra, 126 F.R.D. at 551.

The sanctions for bad faith include rulings that affect the proof or defence of a party's case, monetary sanctions and the imposition of special procedures to prevent future violations. The courts often preclude the introduction of evidence as to a contested issue if a party has destroyed relevant evidence. See Allstate Insurance Co. v. Creative Environment Corp., No. 13307 (D.R.I. 1994) (LEXIS); Fashion House, Inc. v. K MART Corp. 892 F.2d 1076, 1080 (1st Cir. 1989); but see Skeete, supra, where the court declined to impose sanctions because the plaintiff in a Title VII case who had lost tapes and documents was unsophisticated and did not act in bad faith. In particularly egregious cases, the courts may also terminate the litigation. Thompson was an antitrust suit in which the plaintiff alleged that the defendant had used bait-and-switch advertising practices. The plaintiff proved that the defendant had destroyed extensive records of inventory and sales. The court found that the records were irreplaceable and that the defendant "deliberately and purposefully undertook a program to impede and obstruct the litigation process." Thompson, 593 F. Supp. at 1456. Finding the bad faith, it held that any sanction less severe than default would reward the defendant for its misconduct. Consequently, it entered default against the defendant. The Rhode Island Supreme Court has held that the remedy of termination under Rule 37(b)(2) is not available without the development of a record on the reasons for the unavailability of the evidence. Sampson v. Marshall Brass Co., 661 A.2d 971 (R.I. 1995).

An extreme example of discovery abuse by defendants occurred in Turnage. In that case, veterans who had been exposed to ionizing radiation during military service were challenging the constitutionality of the claims procedure adopted by the Veterans Administration. The effect of the challenged claims procedure was to deny the claimants the right to counsel. Because of the obstruction of the discovery process by the VA, the court imposed additional discovery obligations on the VA. It ordered that all future responses to discovery requests be signed by an attorney designated by the VA and by general counsel of the VA. The court also required the VA to develop and present to the court a plan for compliance with future discovery. The VA was directed to circulate notices to all of its employees advising them of (i) the action and (ii) their obligation to preserve evidence and to co-operate in the proceedings. Finally, the court appointed a special master to oversee future discovery and impose monetary sanctions.

In Turnage, the court imposed a counsel fee of $105,000 against the defendant, while in Thompson, the court awarded a counsel fee of $457,000 for the plaintiff's efforts in discovery.

HOW TO PROTECT AGAINST DISCLOSURE

After litigation has been commenced or threatened, it is too late to consider measures to avoid disclosure of documents. However, a thoughtful record retention policy and control of the use of e-mail by corporate employees ▶

can reduce the discovery burden if one becomes a party to litigation.

There are several dangers associated with the adoption of a record retention policy. The first is uneven application or implementation of the policy. Thus, in Lewy v. Remington Arms Co., 836 F.2d 1104, 1112, (8th Cir. 1988), the court held that the trial court should determine "whether the record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents." There is also the risk of the inadvertent destruction of records after the commencement or receipt of notice of litigation - " [A] corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy." Id.

A record retention policy must promote a business purpose (e.g., control of the volume of records and files that must be stored), and be adopted in good faith. The policy must provide for a reasonable retention period by category of documents and, as noted above, be implemented and enforced evenly. The policy itself should specify what files must be saved and provide a retention period for each class of files. It should specify storage location, storage media, and destruction processes. Finally, it should contain an explicit process to secure documents and files in case of litigation to avoid the inadvertent destruction of records.

E-MAIL

Corporate e-mail has been characterised as a "plaintiff's dream and a defendant's nightmare". Anyone who has used e-mail will likely recognise the following characteristics:

- E-mail is immediate - messages and replies are often stream of consciousness; unlike a letter or even voice mail, one often replies to e-mail immediately.
- E-mail is rarely thoughtful (most of us would not send a letter with the typos that we tolerate in e-mail).
- E-mail messages proliferate with mailing lists, copies and replies.

The potential danger of e-mail to a corporate defendant was demonstrated in Strauss v. Microsoft Corp., No. 7433 (LEXIS), 68 Fair Employment Practice Cases 1576 (S.D.N.Y. 1995), where the plaintiff, an assistant editor at the Microsoft Systems Journal, filed suit against Microsoft alleging sex discrimination in its failure to promote her to the position of technical editor. Microsoft sought to preclude the use of sexually explicit e-mail and comments, arguing that they were irrelevant, unfairly prejudicial, and would confuse and mislead the jury. Not surprisingly Microsoft's efforts were rebuffed.[7]

The risk of e-mail to a client can be reduced by adopting and enforcing a company e-mail policy or protocol. This should at a minimum include the following provisions:

- The e-mail system is owned by the employer.
- E-mail is to be used for business purposes only (no solicitation or distribution).
- E-mail messages are to be kept confidential by the employee.
- The employee acknowledges that e-mail may be monitored and disclosed by the employer.[8]
- Humour and sarcasm are often misinterpreted and should not be used in e-mail.
- Do not use the system for personal matters or comments about others.
- Do not send an e-mail message if you are angry.
- All messages will be deleted 30 days after they are sent unless archived by the recipient.
- Employees should archive only important or critical messages.
- Employees should organise archived messages by subject and delete groups when they are no longer needed.
- Archived messages will be subject to review and production in litigation (see the "Providence Journal" rule above.)

CONCLUSION

The proliferation of e-mail and other computer-based files presents fertile opportunity for discovery by creative counsel in litigation. It also presents a danger to counsel who does not understand the measures one must take to preserve electronic evidence. Finally, it offers a challenge for corporate counsel in developing policies to control and minimise the risk and burden of responding to discovery. ■

This article is adapted from a presentation by **Peter V Lacouture** *of Peabody & Brown (placouture@peabody.com) and* **Thomas R Galligan** *of Electronic Evidence Recovery Inc. (tgalligan@cyberdetective.com).* *It is printed with kind permission of the Rhode Island Bar Association.*

APPENDIX

Sample definition for request for production (RCP 34)

"Document means any writing, drawing, graphic material or data compilations, including, without limiting the generality of the foregoing, agreements, contracts, notes, work papers, memoranda,... [insert additional descriptive phrases as preferred], whether stored in tangible, electronic, mechanical or electric form or representation of any kind (including (i) materials on or in computer tapes, disks and memory and (ii) back-up copies and "deleted" files on a computer or computer storage device or media) whether located on-site or off-site. All drafts, copies or preliminary material which are different in any way from the executed or final document shall be considered to be additional documents as that term is used herein."

Sample interrogatories

1. Describe the computer system(s) used by [plaintiff/defendant] currently and at any time within the past [5] years, including, but not limited to, for each such system, the brand and model of the computer, the amount of memory and size of the hard disk, the version of the operating system, the type and version of network software, if any, the brand and model of all peripheral devices including tape drives, external disk drives, other storage devices and modems; the brand and version of major software in use on the ▶

system(s) during such period, and the name of all on-line (electronic) services that have been accessed with the system(s) during such period.

2. Provide the name, employer, title, business and home addresses and telephone numbers for each person with operational or maintenance responsibility for the computer system(s) described above [during time period], including, but not limited to, the person(s) who maintain the hardware described in (1) above, the person(s) responsible for installing new and upgraded software on the system(s), the person(s) responsible for the day-to-day operation of the system(s), and the person(s) responsible for making back-ups or archiving files and date on the system(s).
3. Describe policies and procedures followed by [plaintiff/defendant] for backing-up files and data on the computer system(s) described in (1) above, including, but not limited to, the frequency of back-ups, the type of back-up (full, differential or incremental), the software used during [period], the number of sets of tapes or other media and the rotation of such media, and whether such policies are in writing.
4. Describe all record retention and destruction policies and procedures followed by [plaintiff/defendant] during [period] including, but not limited to, the date the policy was adopted, the types of documents covered and the respective retention periods, the frequency of document destruction, whether any record is kept of what documents are destroyed, the manner the policy is communicated to [plaintiff's/defendant's] employees, and the identity of all employees with responsibility for implementing and executing the policy.

Sample request to inspect (RCP 34)

Plaintiff requests that defendant permit plaintiff to enter defendant's premises at [address] and to inspect, test, sample and copy the data, records and files (including e-mail sent or received by defendant and files located on remote computer systems that may be accessed by defendant's computer system(s) on the hard drive(s), other storage devices, back-up tapes and in memory of the following computer system(s) and any other computer systems located on said premises: [List computer systems.]

Footnotes

[1]It has been reported that Kodak employees send 2 million e-mail messages per day over their systems.

[2]A typical 3½ inch diskette which is used in a personal computer can hold 1,000 pages of double-spaced, type-written material; a CD can hold up to a half million pages; and there are tape cartridges on the market which can hold 2½ million pages of information.

[3]It is easier and probably cheaper to buy more hardware to store more data than to review an old index of documents to delete outdated, obsolete documents.

[4]Many on-line services retain copies of e-mail messages that are sent or received by a subscriber on the service's central computer system. Therefore, deleting the message from the user's own computer will not delete the message stored on the service's computer.

[5]The Federal and Rhode Island Rules are identical except for the time periods for responses provided in Rule 34(b).

[6]A definition of "document," sample request for production, request to inspect and interrogatories are contained in the appendix to this article.

[7]The court quoted other courts as follows: "the Federal Rules favour placing even the nastier side of human nature before the jury if to do so would aid its search for the truth" and "what is prejudicial to the defendant is beneficial to the plaintiff." It failed to note the irony of Microsoft's attempt to exclude e-mail from the record.

[8]The first four items can be summarised in the "Providence Journal" rule - do not write anything in e-mail that you do not want to see on the front page of the Providence Journal.

Searching

A large proportion of the work of an investigator into computer material involves searching for recognised information. When this concerns active files, the process is relatively simple and there are many software tools capable of completing the task satisfactorily. However, there are more subtle searches which can be very fruitful but care needs to be exercised and the investigator needs to be aware of the limitations.

The major problem is the huge quantity of information which needs to be searched in most cases. The original format of printed text was 66 lines per page, 80 characters per line. This gave a maximum capacity of 5,280 characters per page (without indentation and general formatting). If a sheet of paper is assumed to be around .004 inches thick, the contents of a 1 gigabyte (1,073,741,824 bytes) disk printed at such a density would produce a stack of paper around 68 feet high! Fortunately the nature of the information allows us to use the power of a computer to search it, but even then we need to be aware of the significance of how and where information is stored. Active file space, slack space, unallocated space, orphaned space and even unconfigured space all need to be considered when examining the results of a search.

Methods of Searching

There are a number of tried and tested search systems but only the very specialised ones will search all the areas which may interest a forensic investigator. Norton Utilities have a simple search capability but will generally be an exact match (case insensitive) of a single item. For the reasons outlined below, an effective search will need to be simultaneously through active chains of clusters (however fragmented they may be), on a simple sequential sector basis (for non-organised areas of a disk) and on a simple sequential cluster basis for the whole of the organised data area. Ideally the search process should handle multiple targets and provide some degree of flexibility (e.g. fuzzy matching) for instances where abbreviations or misspellings have occurred. One system uses a single pass to build an index of the occurrences of all groups of ASCII characters. This is slow and requires huge resources for the index but under certain circumstances it can be quite effective. A major limitation of such indexing techniques is that only textual characters are considered and often the location of the item (which may contain vital information in its own right) is obscured or not reported.

A different method uses a database of selected targets and uses it to generate a list of hits together with their location, owning file (if any) and condition (slack, orphaned etc.). A supplementary function then allows the operator to examine the context of each of the hits to see if they are of any evidential value. This too takes time and any change in the target requirements will necessitate a re-run of the search process. However, it does have some distinct advantages in that non-ASCII characters can be searched for and it is even possible to set an offset within a cluster where the target is considered valid (see the section on Headers below).

Cluster Boundaries

Active files may display some degree of fragmentation and it is therefore possible that the information being searched for runs across a cluster boundary. For example, a search for the phrase "paedophile organisation" would be most likely to locate it completely within a single cluster. However, since the phrase contains 23 characters there could be 22 possible positions where the phrase runs into the next allocated cluster. Thus the result of the search might locate the phrase in two different - possibly widely spaced - clusters. Within active space this ▶

should not be a problem since the operating system is aware of cluster linkages and naturally appends them in the correct order. But what if the file has been deleted and you are looking at the remnants? It is obviously important to know that this situation can exist and the investigator should be aware of it. A simple calculation will show the odds - if the cluster size is 8Kbytes (8192 bytes) and the target phrase is 23 characters long (as in the example above) then the odds are 8192.22 or around 373.1 against the phrase running beyond the end of the cluster.

The general equation is C/(P-1) where C is the cluster size in bytes and P is the number of characters in the target phrase. Obviously the odds can be improved if the length of the target phrase is kept small and the cluster size is large. It should be possible to design search software which will reduce these odds even further by listing partial hits at the beginning and end of clusters but care would need to be exercised since this would increase the risk of false positive hits.

Similar reasoning can be applied to the possibility of false positive search hits resulting from a target being found which runs across the boundary between used and unused space (slack space) in the final cluster of a file. It is difficult to calculate the likelihood of this happening but it is thought to be extremely small.

Headers

The remnants of organised information which may be found in unallocated areas of a disk can be particularly interesting in certain cases. Many types of file precede their content with a recognisable and reasonably constant header section. This provides an excellent method for the potential identification of traces of such files. Some examples developed while working on actual cases will illustrate the method...

Subdirectories: Within MSDOS, each subdirectory will always begin with what are known as the subparent and parent entries (also known as dot and dot-dot). The subparent (dot) comes first and always at offset) within the cluster. When decoded this entry contains its own cluster number as well as the date and time the subdirectory was created. At offset 31 of the same cluster will be the parent entry (dot-dot) and this will contain the cluster number of the parent directory which points to this one. Thus a search for a full stop followed by 10 spaces at offset 0 of each cluster may identify redundant subdirectory entries even if other traces have disappeared. Inconsistent cluster numbers may show evidence of defragmentation and subsequent decoding of the entries may reveal details of a previous directory structure. In a case where a partitioned disk had been reformatted and reused, such a technique yielded a lot of information about a previous directory structure but contained cluster numbers which were beyond the range of the current partition size. Further investigation revealed the presence on another partition of a utility designed to allow re-partitioning without loss of data and tests indicated that use of this produced exactly such anomalies on certain areas of the disk. The utility had been downloaded via the internet and was accompanied by a message that proved to be extremely valuable evidence. Extending the principle and using a character range search within a fixed range of offsets may enable the investigator to identify other clusters previously used as subdirectory entries.

File Headers: A refinement of the same technique has proven invaluable in a number of other cases where wholesale file deletion had taken place over a period of time. Many of the original file directory entries had been overwritten by later activity although much of the file contents remained intact. ZIP files provide perhaps the best example, each ZIP file will begin with the letters PK followed by characters 3 and 4 (Hex - 50 4B 03 04) so a search for this pattern at offset 0 within a cluster will identify the probable starting point of a ZIP file. Extraction of the first and intermediate sequential clusters as a file may produce enough of the file to unzip and reveal the contents.

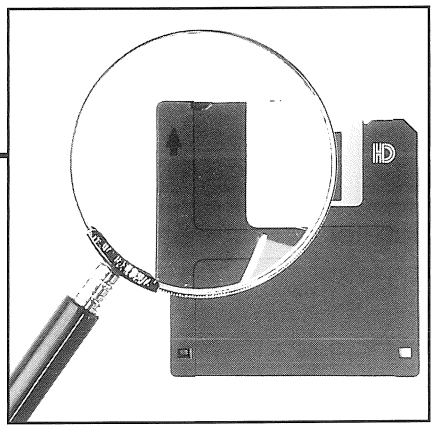
Similar header consistency can be found on a number of file types: JPG image files will often contain "JFIF" at offset 6, GIF image files will often begin with "GIF" (offset 0), BMP graphic files may begin with "BM" (offset 0), CorelDraw graphics files may begin with "RIFF" (at offset 0), some Word Perfect files may contain "WPC" at offset 1, EXE files will usually begin with "MZ" or "ZM" and so on. An interesting point here is that in several cases, known file headers were discovered amongst the active file structure in spite of them being renamed. This immensely powerful technique has also been useful in identifying encrypted files since the encrypting program will often prepend a recognisable header to a file after encryption.

Of course it must be noted that this method only identifies the first cluster and it may only confirm what is already known from an examination of the active file list.

Another fascinating technique which is still in the research stage was used successfully in a case in the U.K. last year. This involves counting the occurrence of each byte value within a file or cluster and building a byte frequency profile. When this is done, the profile is displayed graphically and inspection can reveal distinct similarities between files of varying types. Profiles of files containing a lot of text, compressed files and encrypted files all display features that can be recognised with practice. Other types are more difficult but still may show unique patterns that can provide a rapid indication of file type without the need for individual examination.

It should be obvious that file material which has been recovered with no reference to its original name, date, time or position within the data structure must be treated with more care when producing reports and analyses. However, on occasions where it has been successful, the production of otherwise untraceable material has appeared quite magical to the uninitiated. ■

Forensic Q&A



Q *A suspect company has a UNIX system. Is there any easy way in which this can be copied?*

A There are many variations of the basic UNIX operating system which may be running on hardware as small as a single PC or as large as a mainframe. With such a wide variety of potential hardware and software combinations it is impossible to have one single easy procedure that will work in every situation. If the system is of a similar size to a PC, with either a SCSI or IDE interface, and commonly found buses, the copying procedure should be straightforward once clean access has been obtained to the system. Normally this can be achieved via the floppy drive and a copy made of the hard disk contents using one of the proprietary image copying systems. However, the investigator should be aware that when booting a system with a UNIX operating system a check is made of all system components. If discrepancies are found the system may not boot. To overcome this problem a second disk may be used containing the necessary system files for the boot process. If a mainframe is encountered specialist advice will be required. The accepted practice for handling such a system is to supply the most recent back-up tapes to a data recovery company, who are then able to generate a list of all the active files stored on the tapes. Using this method, information contained within file slack space, unallocated space or orphaned clusters will not be available. This creates two major drawbacks:

- there may be information in these areas which could further the investigation and/or prove to be vital evidence
- the integrity of any evidence found and presented in court may be challenged by the defence on the grounds of being an incomplete record of hard disk activity.

A further consideration in dealing with a UNIX system is the second stage of the forensic examination i.e. analysing the copied data. This may prove to be far more problematic than the copying. In some instances it will be possible to view data using DOS utilities, in others a dedicated UNIX system and utilities will be required. Dealing with a UNIX system is not a job to be undertaken lightly. In general, the less experienced investigator should seek assistance from a suitably qualified specialist.

Editors Note: *It is clear from the above answer that dealing with UNIX systems is far from simple. Few forensic techniques have been developed to date. In future issues we will be running a series of features looking at UNIX from a computer forensic viewpoint. We would welcome contributions from any investigators or analysts with knowledge of this area.*

Q *I have been trying to look at some accounts which are contained on a copy of a hard disk. If I look at the individual data files they are incomprehensible. I have tried to get the accounts program to run but it needs to write back to the copy, which is write protected. Should I remove the write protection?*

A Do not remove the write protection. If you do the accounts program will make changes to the material you are examining. You will not necessarily know what these changes are and during any subsequent examination you may make a wrong assumption based on the altered material rather than the original. Of even more concern is the possible damage you may cause to non-active information such as deleted files. As the program writes files to the copy it may use space containing deleted material which will be overwritten and lost. And, of course, the integrity of any subsequently recovered evidence will be compromised. When faced with this type of problem first of all try to obtain a copy of the accounts program and install it on an investigative computer. Then copy the data files to this computer and view them by running the accounts program. If, as is frequently the case, it is not possible to obtain the original program try copying the directory structure, together with files, from the examination copy to an investigative machine. This is simple and quick to do if you are using a standard forensic workstation with a second working hard disk configured as Drive D: to which the copy is made. This copy can then be run. Sometimes you will need to change initialisation files for this to be successful. Which files these are will vary according to the program. 'Trial and error' to be the best way of solving initialisation problems. Change only copies of files. Then, if you completely 'mess things up' you can always delete your mistakes, take another copy and try again. An advantage of computer forensic analysis is that use of the correct techniques and procedures allows the use of copies with which to experiment and to learn. Finally, if you are still unable to view the accounts seek the advice of forensic accountants. They will probably be aware of the accounts package you are trying to access and will be able to offer advice. They may well have the package installed on an investigative machine and be able to quickly produce the information you require. ■

Please e-mail your questions and / or comments to ijfc@pavilion.co.uk

Although every effort is made to ensure the accuracy of these answers, they are presented for general information and may not apply in rare specific cases. Readers are advised to seek confirmation from an independent specialist in forensic computing when dealing with evidentially valuable material.

Notice Board

EVENTS

Audit Managers & Directors Symposium

(13)14-16 May, Hilton Head

A high level information exchange on creating and maintaining a blue-ribbon audit department.

Contact: MIS Training Institute
Tel: (508) 872 1153

Challenges to Governments and Industry in the Information Age. Revolution in Military Affairs?

21&22 May, London

Contact: Sharon Moore, The Conference Unit, The Royal Institute of International Affairs
Tel: +44(0)171 957 5754
Fax: +44(0)171 957 5710

Audit Director's Guide to Information Systems Technology

21-22 May, New York

Information security technology in realistic audit scenarios and how technological change is affecting audit departments.

Contact: MIS Training Institute
Tel: (508) 872 1153

FIN/SEC: The Conference on Information Security for Financial Services

(23)24-26(27)June, New York
(17)18-20, London

Valuable strategies and tools for protecting highly sensitive data at risk in the unique financial services environment.

Contact: MIS Training Institute
Tel: (508) 872 1153

Auditing Fraud: *Warning Signs and Prevention, Detection, and Control Techniques*

4-6 August, Chicago

Internal auditors are relied upon more and more to recognise the characteristics of potentially fraudulent activities, and to be knowledgeable about where fraud is most likely to occur in the organisation. This intensive, three-day seminar includes Fraud in the Organisation: Assessing/Controlling Risks and Threats; Keeping Fraud Risks Low: The Importance of Internal Controls; Audit Strategies for Detecting Fraud; Responsibilities for Minimising Fraud; Auditor's Role in Achieving Prosecution.

Contact: MIS Training Institute, US
Tel: (508) 872 1153

The Fundamentals of Investigating Fraud

11-13 August, New York
10-12 November, Chicago

A three-day seminar which offers the ins and outs of fraud investigation - what to look for as indicators of fraud and how to conduct a successful investigation, from developing allegations to interrogating the suspect. Learn the steps required to collect evidence, build a case, and preparation needed should the case go to court. Throughout the session case examples will be used to illustrate covered concepts and techniques.

Contact: MIS Training Institute, US
Tel: (508) 879 7999

TRAINING

Training in Computer Forensics

Four modules comprising:
Fundamental Computer Forensics
Applied Computer Forensics
Advanced Computer Forensics
Legal and Procedural Computer Forensics
Courses held monthly in West Sussex.

Contact: Computer Forensics Ltd
Tel: +44(0)1903 823181
Fax: +44(0)1903 233545

NEWS

Mobile Phone Fraud

A powerful blow against Britain's mobile phone crime figure has been claimed by the UK industry's representative trade body - the Federation of Communication Services - following the successful passage of the Telecommunications (Fraud) Bill. The Bill, which became law on 28 February, comes into effect at the end of this month (April). The Telecommunications (Fraud) Bill, which proposes to jail for up to five years people found in possession of equipment used to defraud eg cloned phones, tampered SIM cards, reprogrammed GSM handsets, will protect the mobile phone industry and its customers from telecoms fraud by giving police the powers to act against phone cloning and fraudulently accessing airtime. The Federation of Communication Services has been fighting actively on behalf of its industry members and in the interests of Britain's 7 million mobile phone subscribers in seeking Government and Parliamentary support to crackdown on the use of any equipment which has facilitated airtime fraud. FCS has recently produced a video-based training package on mobile phone crime for police forces.

Contact: Anton Matthews
Tel: +44(0)181 778 5656
Fax: +44(0)181 778 8402

Software Piracy

Company directors face a prison sentence if it is proved that their company is using illegal or unlicensed software. As reported this month, the managing director of the Vogue Computer Company was, on 7 March, sentenced to two-and-a-half years' imprisonment following a two-year investigation by Hertfordshire Constabulary Fraud Squad.

Business Software Alliance Europe has announced that it is launching a broad-based campaign of education and enforcement to reduce piracy on a Pan-European basis; it is to enlist other industries in a wider campaign against the economic plague of counterfeiting.

Contact: Nikki March
Tel: +44(0)171 379 3404

Computer Forensics Ltd have appointed John Whelan as Finance Director.

We will be pleased to receive contributions to this page. Please mark all correspondence 'Notice Board'. We reserve the right to edit if required.

Published by
Computer Forensic Services Ltd.