ISSN. 1363-6650

SEPTEMBER 1997
Issue 9

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

Comment

We've all heard the stories about the shocking pictures that can be downloaded from the Internet.

The mass-media has conjured up an image of lonely social inadequates who get their kicks peddling in porn using just their PC and a modem.

But for once, the tabloid hype is overshadowed by the reality. Some of the images available would turn even the hardest man's stomach, with pictures of child abuse, scenes of crime and photographs of carnage from accidents and wars across the globe. Most right thinking people can only be repulsed by the extreme nature of some of the material. We have to remember that these are not just mere pixels on a computer screen, but are real people's lives - their trauma and maybe even their death. How do we know that the photo of a child being attacked was taken ten years ago or yesterday?

Many paedophiles or those who collect this sort of illegal material will claim that they have done no harm to anyone else - after all, it's only a computer image they have downloaded in the privacy of their own home.

But while a market exists these pictures will continue to do the rounds and maybe more innocents will be hurt. Everyone involved in sending and receiving images is bound up in the same equation - without demand there would be no supply. It is not just a case of preventing titillating hardcore material, but actively tracking down people who collect it.

That is why it is vital to investigate this sort of crime. Much of the material is available on the Net, albeit in locations that are almost impossible to find unless the Web address is known. But often the worst of the pictures are sent privately through e-mail, making them even harder to track.

Many see the advances in telecommunications as the perfect way to meet others and to swap information. For paedophiles this is even more true - they can find like-minde people in the comfort of their own home withou any of the risks of actual contact. In this way huge informal network has sprung up, wit computer users having access to just about an material they want.

And there is a great danger that paedophile can egg each other on, so that possession an distribution can escalate into something a lo more serious.

Instead of a room piled high with illega pictures or magazines, a paedophile can keep the equivalent of ten times more in his computer hard drive, neatly concealed and quite possibly password protected to keep out prying eyes.

But police forces, with the help of computer investigators, can make a real difference; across the world we are beginning to see a major sea-change in the way such offences of possession and distribution of illegal material is dealt with.

Already in the UK there have been several high profile prosecutions where someone's computer has been found to contain thousands of images, and the threat is at last being taken seriously.

There is much talk of the Internet being a law unto itself and commentators say that it can never be tied down to rules or regulations because no one has either the jurisdiction or the technical might.

But that is not only disingenuous but also largely irrelevant. It is not the concept of the Net that matters, but the people who are using it illegally. And these offenders can be investigated and prosecuted using the same laws most countries already have. Illegal material is still illegal, whether it's online or in a magazine.

Human nature is such that no matter how many successful prosecutions there are the problem will always exist, as it always has. But if police investigations can stop even just one child from being abused, the fight will have been worth it.

News

Indian software piracy

Police in India seized disks and CDs when they raided three addresses in Calcutta during a crackdown on pirated software. The National Association of Software and Service Companies and the Business Software Alliance were also involved in the action.

NASSCOM director Dewang Mehta said: "These raids will send warning signals to software pirates located all over the country and help in reducing software piracy in India.

"Indian copyright law is the toughest. There is no discretion left to the judge as regards jail term and fine. Both are imperative."

In a recent survey software piracy in India was revealed to be up to 60 per cent, with losses estimated at $150 million.

Couple cleared after Internet torture trial

A man and woman who were accused of using the Internet to offer children for torture have been cleared by a German court.

The hearing was told the pair had offered Czech girls as young slaves for sadistic activities and used the nicknames of Sado-Hangman and Leather-Witch online.

The couple allegedly told a journalist posing as a potential client that they would dispose of a child's corpse for $1,580. Bernd Malitzki, 31, and Sabine Pohl-Jovanovic, 37, claimed that any such offer was not made seriously.

Pohl-Jovanovic said in court: "I love children...I just wanted to see what it would be like to lure someone. You realise that there are some weird people about. It is captivating."

Malitzki told the court that he was a practising sado-masochist who gained contacts mainly through the Internet and newspapers. He said: "I am not a paedophile. I am someone who likes to be decent."

Judge Peter Froehlich said that prosecutors had not been able to remove the doubt over whether the couple were serious when they offered the girls up.

Police had found a torture chamber in the couple's home along with indications of sado-masochistic activity, although no evidence of child abuse was found.

Computerised court

Prosecutors in the US want to speed up the trial of the suspected Unabomber using a computer-based litigation system.

The trial of Theodore Kaczynski is expected to take more than three and a half months and will include large amounts of documentary evidence including more than 100 separate exhibits and 1,000 items seized from Kaczynski's home.

And the prosecution team have proposed using a computer with several monitors to display evidence to jurors and the court.

Prosecutors offered to modify the exterior of monitors in response to defence objections that their similarity to televisions might mean jurors believed that the images on screen must be true.

Kaczynki, 55, faces a 10 count indictment in connection with four California bombings, two of which were fatal. He is due to go on trial on November 12 in Sacramento and if convicted he could be given the death penalty.

Japanese Net porn

Police in Tokyo are warning that the amount of obscene material has risen sharply because of the popularity of computers and the Internet.

The National Police Agency said that the number of cases was growing, with only seven violations in 1993 compared to a total of 57 last year. And a report revealed that the number in the first quarter of this year alone was 24.

One of the biggest concerns is that Internet bulletin boards and home pages are being used to sell or advertise pornographic videos. Of the 400,000 home pages set up by Japanese individuals, 14,350 of them post pictures or sell such material.

One company is reported to have made 60 million yen through sales of videos advertised on the Web and the NPA is now considering strengthening restrictions on online pornography.

Illegal software on Net

Software giant Microsoft has filed a lawsuit after its programs were posted on the Internet for free download.

It says its Softimage 3D software, a high-end animation system, was put on the Web by an individual living in Burbank, California, in the US.

And as part of an anti-piracy campaign by the firm, three people in Brazil were charged with copyright infringement after they allegedly sold counterfeit copies of Softimage 3D.

Microsoft corporate attorney Jim Lowe said: "Internet piracy and counterfeit CD ROMs are the dominant piracy problems for Softimage 3D. We are actively surfing the Net and purchasing suspect CD ROMs to target these types of thieves."

A spokesman for the firm said: "We are working hard to warn consumers that pirated software obtained from the Internet may be damaged or contain incomplete programs and could include computer viruses."

The company says anyone with concerns over the legitimacy of Microsoft software should e-mail it at piracy@microsoft.com

Philippines' online commerce

New laws are needed governing business on the Internet, according to the Center for Telecommunication Studies in Manila.

The CTS says that laws addressing tax, trading and jurisdiction should be brought in to help firms and financial institutions work on the Web.

But it warns that most businesses are unaware of the legal pitfalls of online transactions as Philippine laws focus on physical goods or services rather than those conducted over a computer network.

CTS director for special projects Chito Kintanar added that the information superhighway itself remains a poorly defined concept and that progress in providing suitable regulations has remained slow not only in Asia, but also in Europe and the US.

Information age in the US

A study by a technology think-tank group has ranked all 50 states in the US on how they are using computers to improve operations.

The Progress and Freedom Foundation ranked Washington top of the study, saying it had the most up to date approach to law enforcement and the court system.

And the others in the top ten in order were Wisconsin, Florida, Oregon, Maryland, Arizona, Indiana, New Jersey, Missouri and Michigan. Among those ranking bottom were Hawaii, South Dakota, Rhode Island, Ohio and at the bottom of the heap, Connecticut.

PFF president Jeffrey Eisenach said: "Information technology can make government more effective, competitive and user friendly. In fact, digital infrastructure is as much a key to growth in the digital age as railroads and roadways were to the industrial age."

A summary of the results can be seen on the web at www.pff.org

Call to accept e-documents

Electronic documents should have the same legal status in courts as papers ones, according to the society for Computers and Law.

The group in the UK, made up of lawyers, academics and business people, said the digital culture had grown to the point where legal decisions had to be made on computerised documents.

In its report, Digital Information and Requirements of Form, the society says the courts need to prove the validity of such e-documents to make sure they have not been altered or tampered with.

The society's president, Lord Justice Brooke, said: "Electronic commerce is the next big challenge which the law must face. Documents in electronic form need to be treated by the courts as equivalent to traditional paper documents.

"The recommendations of this report would achieve this end. I very much hope that the Government will implement them and that the report will give a lead to any European initiatives."

Sri Lanka to curb computer crime

The Sri Lankan Government hopes to cut down on the growing number of computer misuse cases by bringing in tougher laws.

Under the country's law, the theft of computers is a crime but changing or stealing data on someone else's computer is not covered by the statutes.

Deputy Solicitor General Kolitha Dharmawardena said: "If someone meddles with information served by a computer, reporting to police will be of no avail. There is no law under which police can take action."

A government committee has recommended that new laws, with heavy fines and imprisonment are brought in to deal with those convicted of computer related crimes.

"Hate" web site attacked

A Canadian politician has condemned an Internet site as an insult to both Jews and to those living in Quebec.

Quebec Culture Minister Louise Beaudoin attacked the site, called Quebec, North America's Neo Fascist State, as "stupid and vicious".

The anonymously authored site draws parallels between the region and Nazi Germany and says "Quebec welcomes people as long as they are white and don't speak a word of English".

Beaudoin said: "The Internet isn't on planet Mars. The laws have to apply. We can't pretend that this is a medium above the laws.

"Whether it is a hate propaganda, whether it is our law on commercial advertising, whether it is other laws, they have to apply."

Earlier this year Beaudoin sparked a row when she said Quebec had jurisdiction over the language of Internet sites originating in the province, while Canadian Government officials insisted it was a federal matter.

Police web site

A crime fighting web site has been set up by police in Australia to help spread the message about its work.

Police commissioner Jim O'Sullivan called the Queensland Police Service's site the most comprehensive web home page in Australia.

The site includes information on missing people, the most wanted fugitives and current police investigations. More than 1,500 people visited it during a trial three-week period.

But the page will not act as a conduit for crime tip offs because of fears over Net security.

The site can be found at http:www.police.qld.gov.au

Next generation e-mail

Major software manufacturers are putting the finishing touches to a new e-mail specification that will increase security.

The 5th Generation Messaging Protocol (5GMP) will include facilities such as reply-requested, authenticated and receipted e-mail and will work with most systems and environments, including the Net.

Its makers say that the introduction of 5GMP will mean that it can be proved in a court of law that e-mail has been both sent and received, giving rise to the term "legally admissible messaging".

Novell, Lotus and Microsoft are among the suppliers behind the project and the secure dial-up backup company NetStore is one of the first firms planning to implement the protocol. 5GMP is expected to be launched within a year.

Fight against phone fraud

The State Assembly in California has approved a crackdown on high-tech thieves who use computers and mobile phones to transfer funds.

A bill will give law officers and prosecutors the tools they need to target

offenders and requires the confiscation of cellular phone cloning equipment after a conviction.

The law would attack thefts of telephone calling card numbers, e-mail addresses and cash held in electronically accessible accounts and a state-wide database on high technology crime would be maintained.

Banned web-site to reappear

State officials in Texas, US, say they are powerless to stop an off-shore web-site from including personal information taken from drivers' license records.

The Publiclink site was shut down under state legislature, but is now expected to reopen under a new name this month from the island of Anguilla, in the Lesser Antilles.

Driving license information includes a person's name, weight, birth date and sex and while such data is open to the public, there are fears that any online access will be misused by stalkers and criminals.

The Texas Department of Public Safety says that a new law will make the information less attractive in the future with a form that will allow Texans to delete their own data.

Couple in Net pornography charges

A Swiss couple have been charged with transporting child pornography to the US and selling the material on the Internet.

John Grabenstetter, 52, and his wife Buntham Grabenstetter, 26, from Basel in Switzerland, were arrested in Buffalo. They are alleged to have sold wholesale quantities of child pornography on the Net as well as carrying thousands of illegal files from their Swiss home.

Officials said that the pair agreed to sell 250 CD-ROMs to US investigators for $10,000, and that one CD-ROM contained 7,000 images.

If convicted, the couple face up to 15 years in prison and a fine of up to $250,000. The charges were brought after an investigation by the US Customs Service and the office of New York State Attorney General, Dennis Vacco.

US Customs Service special agent Jeremiah Sullivan said: "The alleged conduct in this case demonstrates the potential misuse of computer technology to violate and abuse our children.

"With the assistance and support of federal and state prosecutors, we are aggressively pursuing these violations."

Credit card hacker

A computer hacker in the US accused of taking 100,000 credit card numbers off the Internet has pleaded guilty.

Carlos Salgado Jr, 36, from San Francisco, now faces up to 30 years in prison and a $1 million fine when he is sentenced on November 25. He was indicted in May on charges that he gathered credit data from a dozen companies selling products over the Internet.

Salgado was arrested after an FBI sting in which he tried to sell the card numbers for $260,000.

He admitted to four counts, including unauthorised access of a computer, trafficking in stolen credit card numbers and possessing more than 15 stolen card numbers with intent to defraud.

Crackdown on Net paedophiles

A Royal Commission report in Australia has called for an aggressive attack on child sex offenders who use the Internet.

Justice Wood said in the report that encouraging children to engage in sexual activities and using online services to peddle pornography should become indictable offences.

And he called for a hotline to be set up so that members of the public could alert police if they spotted illegal material on the Net.

The report said that Internet service providers should be required to disclose information about users if asked by law enforcement agencies and that the police should have enough resources and technology to tackle the problem properly.

Call to catch Nazis

Internet users who find illegal neo-Nazi material should report the site to police, said German research and technology minister Juergen Ruettgers.

The campaign comes after Nazis used the Web to help organise a march marking the 10th anniversary of the death of Hitler's aid, Rudolph Hess.

Federal officials think about 150 neo-Nazis keep in contact with each other through the far right Thule Netz bulletin board network, which has inner areas accessible only to select people.

Under Germany's new multi-media law, which took effect recently, anyone spreading neo-Nazi material on the Net can be sentenced to five years in prison.

Virus industry in legal squabble

Two rival firms which make anti-virus software are taking their fight with each other to the law courts over allegations of stealing trade secrets.

McAfee Associates Inc is suing Symantec Corp for defamation and is seeking $1 billion in damages in the latest war of words between the companies.

The argument centres on two batches of software code that appear in two McAfee products. Symantec sued McAfee earlier this year, accusing the latter of taking those codes and McAfee deny the allegations.

Symantec says that their rivals stole portions of Symantec Crashguard and used it in McAfee PC Medic 1997 and also that McAfee took another 100 lines of code and used it in McAfee VirusScan.

McAfee responded by saying it had conducted an internal investigation and had found 100 lines of code in VirusScan that were downloaded from the Internet, although it said these lines did not have any function and had now been deleted.

General manager of McAfee's Network Security Division Peter Watkins said: "Not only is the code in question not significant, it is not used at all. These facts are apparent to ▶

anyone examining the code, and the matter could have been resolved with a simple phone call."

Symantec's vice president and chief technical officer Enrique Salem said: "It's clear to us they've misappropriated the code. They say it's available on the Web, but they can't tell us where it is.

"It seems to us they're very desperate here. We're going to push aggressively for a jury trial. The great thing is, it's all going to come out in the trial."

Increased trade needs tighter controls

The Japanese Government said it will boost the protection of Internet users by strengthening rules governing online businesses.

New legislation cracking down on unscrupulous operators could be passed next year, according to the International Trade and Industry Ministry.

The ministry plans to review the law on door to door sales so that online businesses will be required to display the name of a representative and a telephone number on any adverts.

A ministry official said: "We have decided that immediate action is necessary because electronic commerce is expected to explode in the near future."

Net security would boost trade

Proper enforcement of existing laws would boost confidence in buying goods online, according to the Consumers Association in the UK. The independent consumer watchdog, the publisher of Which? magazine, says electronic commerce would grow rapidly if fears over contract law, privacy and security were addressed.

Among the key recommendations by the CA to improve Internet trade are a single UK communications regulator, voluntary codes of practise to cover the legal problems and greater powers for the Advertising Standards Authority to act on misleading ads.

Editor of Which? Online Alan Stevens said: "Security is always likely to be a risk on the Internet. But that risk need not be any greater than with other remote ways of paying for goods and services, such as over the telephone.

"Issues surrounding payment systems, contracts, privacy and regulation all need to be examined if consumers are to feel comfortable buying goods and services on the Net.

"Self regulation would appear to be the best option for solving potential problems, and those who stand to gain commercially from the development of Net transactions should bear the responsibility of ensuring consumers are educated and informed."

A summary of the report can be seen online at:

http:www.which.net/nonsub/cacampaigns/currcampaigns/intemet.html

Fraudsters online

Internet service provider America Online is warning customers to be on their guard after a credit card scam was discovered.

Someone pretending to be AOL chairman Steve Case sent e-mails to users asking them for credit-card information, with a hyperlink to a Web page where the information was to be entered.

The site was shut down on August 12, and Federal authorities are now investigating, but it is not known how many people received the messages or were taken in by the scam.

AOL vice president of integrity assurance Tatiana Gau said: "Sometimes I worry that our messages reminding members that we never ask for billing information sort of fade into the background, but in this case members forwarded the information to us right away. People are beginning to realise that the same kind of scams that occur in real life do occur online. So in the same way you would never dream of giving out your PIN number to your ATM card, you shouldn't be doing it online either."

The firm said that in the event of such fraud, it could not be held legally responsible but added that most credit card companies would foot the bill.

Hoax spamming

Electronics firm Samsung is taking action after millions of forged e-mails were sent out in Japan under its name.

The false messages threatened recipients and accused them of being behind attacks to the company. They worried many of those receiving them, and angered others. Samsung was inundated with replies and had e-mail messages, telephone calls and faxes criticising it.

A statement by the company said: "An unknown party has distributed a number of fraudulent e-mail messages under the names of Samsung Electronics America, Sailahead and an individual purported to be Samsung's legal counsel.

"These e-mails were neither written nor condoned by Samsung. As policy, Samsung does not conduct mass e-mailings, known as spams. We respect the integrity of the Internet and the rights of users.

"Samsung is working with Federal authorities to identify the individuals responsible for this hoax and intends to take legal action against the perpetrators."

Online fraud warning

The Federal Trade Commission in the US has sent warnings to 31 advertisers who could be selling get rich quick schemes over the Net.

It said that the electronic mail messages may break the law by making exaggerated or unsupported claims.

The FTC trawled the Internet for such adverts, particularly those selling coupon booklet sales and work at home coupon clipping services.

It says the action was part of a broader campaign clamping down on online fraud and that more than 24 cases had been brought so far.

Jodie Bernstein, director of the FTC's bureau of consumer protection, said: "While fraud artists might try and take advantage of the Internet to perpetrate a fraud very quickly, the Internet also makes them susceptible to very quick and sure detection."■

Product News

New Ontrack software

Data recovery firm Ontrack has announced the release of software which lets users improve the performance of hard disks.

Disk Manager for Windows 3.1 and 95 uses a graphical interface and provides users with a collection of program utilities to install new drives, copy files and remap CD-ROM driver letters.

The software also includes a utility that overcomes BIOS limitations by replacing restricted or unsupported drive parameters.

President of Ontrack John Pence said: "We are very excited to provide Windows users with a seamless, easy to operate hard drive installation utility. The release of Disk Manager for Windows is testimony not only to this installation utility's continued ability to adapt, but also to its continued ability to meet the demands of users and equipment manufacturers alike."

The software has a RRP of $99.95 or current Disk Manager owners can upgrade for $39.95. *Contact Ontrack online at http://www.ontrack.com*

Online insurance

An insurance policy has been launched which offers protection from the legal risks of operating on the Internet. US company Chubb Corp already has customers for its new policy, aimed at software developers and Net service providers who are worried about copyright or defamation issues.

Chubb says the risks are uncertain, but estimates that the cover will bring in $21 million by the end of next year. Manager of the electronics industries group at Chubb Thomas Cornwall said: "There are no actuarial tables for this."

Data mining

Two computer companies in the US have joined forces to offer a data mining service to combat both public and commercial fraud.

Sequent Computer Systems, which supplies high-end open systems, and systems integrator specialist SRA International are using the best of both firms hardware, software and consulting services.

Potential applications for the system include fraud detection for insurance, government agencies, health care, credit groups and cellular phones.

Sequent Computer Systems can be contacted on +1 212 750 9300, or e-mail mikefaysequent.com

SRA can be contacted at its web site on http:knowledgediscovery.com

GPS puts police on the spot

Law enforcement and emergency response teams know exactly where an incident has taken place thanks to a panic button system.

The OnGuard response system uses global positioning satellites and cellular communications to provide immediate assistance when necessary. Made by ATX Technologies in the US, the tracker allows 24-hour vehicle monitoring, roadside assistance and in emergencies enables police, fire and paramedic personnel to be directed to a person's exact location.

ATX say the system helped save one man's life recently after he had been stabbed during a dispute. He pushed the panic button on his mobile phone and was put through to trained staff who gave medical advice while calling and guiding in emergency agencies.

For more information contact ATX on +1 210 979 4999

Fingerprinting firm needs cash

Electronic fingerprint specialist Finger Matrix Inc says it has run out of operating funds and is temporarily stopping its activities until it gets a cash injection. Company president Thomas Harding made the announcement in August and said that the US firm was in discussions with investors to get both short and long term financing.

He said: "We have fulfilled all our current orders and are continuing to pursue additional orders and contracts from more prospects than we've ever had. We're confident ongoing funds will soon become available."

The company makes the ten-print system called Chek/Ten, which was recently certified by the FBI and is being sold across the world.

Recovering stolen computers

A new service has been launched which hooks users up to the Internet to help locate and recover lost or stolen PCs. Canadian company CompuTrace, which specialises in computer tracking systems, has announced its online monitoring service which uses a secure Net website so that customers can check on the location of their computers at any time.

When CompuTrace is installed in computers, it silently calls in to a monitoring centre on a regular basis. If a system is stolen, it can be traced the moment it next calls in.

Its makers, Absolute Software, based in Vancouver, work directly with law enforcement agencies to help recover items.

The software sells for US $29.95, with an annual monitoring fee of US $60 and the programs works with Windows 3.1, 95 or DOS 5 or greater.

Absolute Software can be contacted on +1 800 220 0733 or via the Net at www.computrace.com.

Automated risk assessment

Trident Data Systems has a new system to help IT managers calculate the possible risks their networks face.

The NetRISK tool is aimed at the legal community and helps to locate problems and draw up safeguards to protect valuable data.

Brian Kelly, vice president of information protection systems at Trident, said: "Like many other businesses, law firms and court houses have streamlined operations by tapping today's technology, housing incredibly confidential material on computers. These computers include modems and internet access which magnifies the risk and requires increased protections."

US company Trident can be contacted on +1 310 556 4443.

Fax manager legal firms

Most law firms make extensive use of fax machines to send documents and one firm has announced a network solution to ease possible bottlenecks.

TRS Technologies in the US has launched LegalFax 97 which replaces earlier versions and users get real-time warnings of the status of outgoing faxes as well as knowing when an incoming fax arrives.

Using the system, it is possible to receive, view, annotate and send faxes without having to print them out or manually feed in a document.

The makers say that LegalFax 97 now has full integration with the DOCS Open network document storage and retrieval system, and is easier to use with more features.

President of TRS Technologies Jeff Gretz said: "The opportunity for cost savings and productivity enhancement provided by LegalFax 97 is exciting news for law firms looking for a LAN fax solution designed specifically for their industry.

"TRS will continue to build specialised systems that manage document transmission efficiently for document-centric industries with unique requirements."

LegalFax starts at $1,995 for the client and server software, plus a per-seat license fee. *Free demo software can be downloaded from the Net at http://www.trstech.com/faxguest.htm*

TRS can be contacted on +1 503 626 7841 and the web page is http:www.trstech.com

Computer dispatch system

Emergency services can use a computer aided control system to monitor and communicate with mobile personnel.

Designed for communities with populations of 15,000 or more, LifeLine CAD NT enables crucial data to be sent instantly over the radiowaves or through digital cellular systems.

Its makers, Unisys Corporation Information Services Group, says that the system can save valuable seconds which could make the difference between life and death, or catching a criminal.

Michigan State Police in the US has installed LifeLine and says that already response times are quicker.

Chief assistant division director of the force Tom Evens said: "Our officers now respond to emergency situations faster, with more complete information.

"We also provide for better officer safety because we are able to provide them with more accurate and relevant information."

For more information contact Unisys at +1 215 986 3507 or access the Web page on http://www.unisys.com

Police fleet connected

Laptop computers using mobile communication link ups will be installed in 460 police cars in a US force to improve efficiency. Officers in Charlotte-Mecklenburg, North Carolina, will be able to keep in touch with their base instantly and transmit and receive vital information.

The system uses the Bell Atlantic Nynex Mobile AirBridge service and is the second largest installation of its type in the US.

Data available to police in the field includes access to local, state and national law enforcement databases to retrieve complete motor vehicle records, criminal warrants, police reports and other information.

Messages are encrypted in both directions to improve security and is transmitted on the existing cellular network, which its makers say is much better than traditional two-way radios.

Charlotte-Mecklenburg police chief Dennis Nowicki said: "We believe in the value of technology in police work. When officers graduate from the police academy, they should be given a badge, a gun, a radio and a laptop.

"This new technology will directly benefit local residents as well by enabling our officers to spend less time doing paperwork and more time in the community."

For more information contact Bell Atlantic Nynex on +1 617 520 7069

Network improves efficiency

A local area network installed at a major law firm in Canada has cut overheads dramatically, with large savings to clients.

Newbridge Networks announced that it has put in a VIVID switched routing system at Borden and Elliot in Toronto.

The law firm uses the system to provide 250 lawyers and paralegals and 350 support staff with litigation support packages, high speed Internet access and video conferencing tools.

Chief operating officer at the company, Norman Williams, said: "We've created an incredibly rich technology culture, which allows us to practice law smarter, quicker and more cost-effectively.

"We figure that on balance, the communication network we have in place has helped reduce the cost of litigation for clients by about 20 per cent, simply because lawyers spend less time performing the same functions they used to."

Newbridge Networks can be contacted on the Net at www.vivid.newbridge.com

Wireless scrambling

Pager messages can be encrypted using a special system to ensure privacy for businesses and government agencies.

The V-One corporation in the US has launched Air SmartGate, which embeds scrambling technology into paging systems so messages cannot be spied on by anyone else.

Recently three men were charged with illegally intercepting highly sensitive pager messages between senior New York City officials.

Senior vice president of V-One Charles Griffis said: "Pagers using Air SmartGate will be as easy to use as today's pagers but with ironclad security.

"Both customers and network administrators can do secure paging with Air SmartGate in the exact same way as they do unsecured paging today."

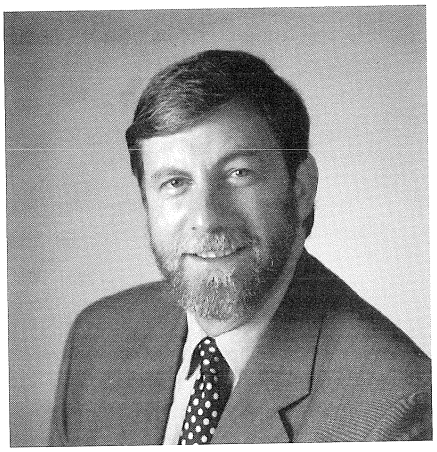
V-One can be contacted on +1 301 515 5200 or on the Net at http://www.v-one.com ■

Case Study

Vindictive eMail

by **Peter Verreck,** *Computer Forensic Investigations Ltd*

This case study is concerned with an investigation into a breach of security on an internal network in which a vindictive e-mail message was transmitted. The investigation focused on the probability of retrieving and tracking the e-mail. In the course of the investigation serious breaches of system security were uncovered.



Background

On a Wednesday morning an employee accessed his internal e-mail. He downloaded a number of messages one of which appeared to have been sent by an executive within the company.

It contained strong criticisms of the employee's work, vindictive personal statements and a demand that the employee should no longer speak to the executive, with whom he had previously enjoyed an excellent working relationship.

The employee was severely shocked and upset by the contents of the e-mail and immediately deleted it from the system. The executive was out of the office until the following Monday and in the intervening period the employee mentioned the matter to no-one.

Normally the employee would have gone to the office of the executive to discuss any problems, however, on the Monday, he attempted to speak to the executive in the open plan general office.

After uttering a few words the employee, having brooded on the content of the e-mail for some days, and being under considerable personal strain, broke down and was unable to continue. He was taken to a quiet area and medical assistance was sought. During this period he outlined what had happened. The employee was placed on sick leave and an investigation launched.

The computer forensic brief

The internal investigator sought the help of a computer forensic analyst.

The brief to the analyst was:

- To copy the network server.
- To locate and retrieve the e-mail message.
- To establish the origin of the e-mail message.

Initial enquiries consisted of interviews with relevant members of the staff including the senior executive. These established a number of facts.

Elimination of executive as suspect

The message was not sent by the executive. She was not at the office during the period when the e-mail was transmitted and to have done so was completely out of character. Indeed, she was extremely upset by the pain caused to a valued employee and close, respected colleague.

Staff held grudges

It was established that certain members of staff held grudges against both the executive and the employee.

- **Against the executive**

The executive had joined the corporation within the last year and was charged with changing the ethos of the department concerned. It had a non-productive orientation and needed to change within an increasingly competitive environment. Some of the staff who were long time employees begrudged the changes and blamed the executive. They also resented the close working relationship she maintained with the maligned employee.

- **Against the employee**

The employee had responsibility for ensuring that certain new work policies were adhered to. He was diligent in his work. Some staff members deliberately tried to thwart his efforts, regarding the frustration caused as a source of amusement. Furthermore they resented the good relationship the employee maintained with the executive.

Examination of the Computer System

- **External network**

The external network was for communication between geographically remote sections of the company. If the e-mail was sent from an external source a record would initially have been placed within a transaction log controlled by a mail manager system. The mail manager system automatically purges the log on a regular basis and removes old entries. The transaction log would contain only a record of the origination, destination and dates of the transmission but not the content.

- **Internal network**

Server and Configuration

The internal network consisted of a 20 gigabyte server running Novell 3.12. There were 64 Megabytes of RAM. The server was 95 per cent full and, for some time there had been discussions about the need to upgrade to a larger hard disk.

Attached to the server there were 120 workstations, each of which had up to 500 megabytes of local hard disk space. This was used only to contain the swap file. ▶

E-mail system

The internal e-mail system was run on a commercially available program. Messages were stored on the central server. The transaction files were located on Drive G:. In order to save space on the server all transactions were normally truncated to zero and deleted from the server on receipt. Messages were saved within the user's private sub-directory on the server, unless deleted by the user.

Passwords

There were three levels of password access.

Level 1 - system access

To access the network the user was required to log-on with a unique password assigned by the network administrator. Recently the log-on password system had been changed in order to make it simpler to use. The password was now the number assigned to each employee by the company.

Level 2 - directory access

To log-in to the user's private server directory a user defined password was required.

Level 3 - e-mail access

To log-in to e-mail a user defined password was required.

Result of the analysis

- **Internal/external origin**

Due to the reported content of the e-mail, it was unlikely to have been sent via the external network. The perpetrator was in possession of information, contained within the e-mail, that would only have been available to an employee. The enquiry therefore concentrated on the internal system.

Potential recovery of e-mail

The vindictive e-mail had only been seen by the employee and the unknown sender. It had not been printed. If the e-mail was recovered it might be possible to identify the sender through content or transaction logs. However, due to the configuration of the system and the lack of password security (see below) the probability of recovery was considered to be too low to justify the time and cost involved. The reasons for the decision were:

- **Searches**

In order to locate the missing, deleted document the normal procedure would have been to copy the server and conduct searches of the data using search criteria taken from the original message. In this case there was no copy of the message and therefore no accurate search criteria were available.

- **Server Over-Use**

The hard disk on the server was over-used and there was very little unoccupied space. Therefore the probability was high that the space occupied by any deleted data would quickly be re-used and the previous information overwritten and lost.

- **Encryption of e-mail**

The e-mail system transmitted and stored data in a proprietary encrypted form. Searches would have needed to be conducted in the encrypted form. If this led to recovery of fragments of the deleted e-mail these would need to be de-crypted in order to be read. The decryption method used was not known and was not freely available.

- **Logging of e-mail origin and identification of sender**

The e-mail transaction log deleted entries automatically. If the deleted log entries were recovered they would identify the origin of the e-mail by the log-in entry and not by the workstation from which it had been sent. The log-in entry was based on the access password. This would not identify either the sender or the sender location on the network.

Password Breaches

- **Log-on password level**

The log-on password was not secure. Details of employee codes were freely available. The server identified the unique user by the log-on password. Any employee, knowing any other employee's code, could log onto the system from any workstation and be identified by the system according to the entered password.

- **Log-in password level**

The log-in password was assigned by the user. There was no control over what type of password was used nor was any advice given to the staff about password security. Most passwords were obvious. For example the executive used the name of her only child, of whom she spoke frequently. This was known to at least three other employees. In another instance, a number of employees had discussed possible passwords and had decided to use their car registration numbers.

However, at this level there was a much more serious security breach. During the course of the enquiry it was found that if, when prompted for the password, a particular three key sequence was entered, the password was circumvented and access given. At some time in the past this key sequence had been disclosed to some members of staff, by a previous system administrator, in order to reduce the number of calls due to forgotten passwords. It was now known to the majority of staff.

- **E-mail password level**

The e-mail password was assigned by the user and the same comments apply as for the log-in password, except that this password could not be circumvented.

Conclusions

The enquiry had commenced as a conventional computer forensic investigation involving the copying of a network server, the location and recovery of deleted material and the identification of the source of an e-mail.

Due to the detailed survey and analysis of the network system at the commencement of the enquiry the analyst was able to establish that full forensic examination would not achieve the result required. Even if the vindictive e-mail was recovered, an unlikely event, the serious breaches of password security, in conjunction with the lack of logs, meant that it would not be possible to identify the sender.

The analysis was significant for the client and highlighted the following major problems:

- The hard disk on the network server was too small. This had two implications. Firstly, measures had been instituted to save space. These included the routine deletion of security transaction logs. If these had been available it might have been possible to trace the movement of

the e-mail. Secondly, deleted material would quickly be overwritten.

- There were serious breaches of system security which enabled any employee to access files in any other employee's server sub-directory.
- Passwords were not controlled and were not secure. It would have been a simple matter for any employee to send an e-mail from any of 120 workstations posing as any other employee.
- There was no means by which the server could accurately identify any individual workstation. Identity was established by user entered password only.
- To commit a major crime involving any computer based material, including agreements, company records, employee details, financial accounts and banking transactions would have been simple for an employee with minimal information.

The client instituted a major review of all aspects of both internal and external computer and communication systems. Suitable security measures were implemented and are now tested and reviewed on a regular basis.

For the forensic investigator the case serves to illustrate the importance of good preparation and survey in any computer forensic enquiry. The investigator was able to assess the probability that full forensic analysis would not produce the required result. In the event the analyst provided the client with advice which prevented inappropriate work being carried out and avoided unnecessary expense. ■

Software Warning

A firm specialising in computer crime and investigation has issued a warning that using certain software could create problems if a case goes to court.Computer Forensics Ltd in the UK says that using a disk called Pure Magic could jeopardise the forensic process because it could change data while a system is under investigation. The company issued the following warning to the users of its DIBS© imaging system and says that the use of Pure Magic on a system may cause any subsequent evidence recovered to be regarded as inadmissable.

"We have been at pains to continually stress the special nature of computer based material which may be required as evidence in a court of law. Let us point out once again that computer material can be altered without trace.

"This simple fact makes it absolutely vital that the Court should be convinced that the evidence has not been altered. This is not as easy as it may sound. Without intimate knowledge of the investigative software which has been used, it is not possible (even for an expert) to be certain that nothing has been written to the disk under investigation.

"These days, even the simple process of switching a machine on and allowing it to start under the control of its own software may write information to the fixed disk. It would then be perfectly legitimate for a defence counsel to argue that since some information had been written to the disk after its seizure, the reliability of all of the information was now questionable.

"A similar argument could apply whenever a machine was investigated directly without independent supervision. The simple way around this difficult problem is to concentrate investigations on a copy of the material in question and to ensure that the copying process is forensically sound and has been specifically designed to avoid altering the source material. The copy should ideally be completed in the presence of the owner of the computer or his legal representative and it could then be proven to a Court that at no time was the material at risk of being altered even by inexpert operation.

"The copying process may be time consuming but investigators should avoid the temptation to examine a potentially evidential machine directly unless they are absolutely certain both of their own capabilities and the behaviour of their investigative software. Even then, bearing in mind the observations above, the evidential integrity may be weakened.

"Considering all this, our concern can be imagined when a number of users asked us about a disk they had been given called "Pure Magic", which was apparently configured for police officers in the UK to use in direct examination of evidential computers. We have obtained a copy of this disk and the results of our examination have prompted us to issue a warning concerning its contents.

"We understand that the disk was issued as an aid to computer forensic investigators but the executable programs on the disk are all commercially available programs which were not written with forensic requirements in mind.

"Since they are commercial, if permission has not been granted for their distribution, their use on this disk appears to be illegal. Quite apart from this, the content and configuration of the disk mean that if it was used it could be in breach of major forensic principles. The system on the disk is DOS 6.22 which is known to have a serious flaw in that software on the first fixed drive may be executed during the floppy boot cycle.

"Symantec programs UNERASE, UNFORMAT and DISKEDIT are all designed to write to the disk under examination.

"DOS programs CHKDSK and FDISK are both capable of writing to the disk under examination.

"The unidentified program IDEINFO is specific to IDE fixed drives and will not report details of any other types.

"A DOS shell application called Path Manager exists in a directory on the floppy together with an installation batch file which will place the relevant files onto the first fixed disk.

"There is no doubt that if this disk was used to examine an evidential machine directly there would be a strong case for suggesting that any evidence gained thereby should be declared inadmissible."

A spokesman for Computer Forensics Ltd said: "It's vital that investigators follow the correct principles and procedures to maintain the integrity of any evidence.

"If any data is written on to a suspect's machine, it would be in serious breach of the guidelines unless the process was correctly documented. This could be jumped upon by an alert defence lawyer.

"It would be awful if a case was lost and a criminal walked free because the wrong investigative tools were used or the correct procedures were not followed.

"Forensic computing is a science in which it's hugely important to follow the exact letter of

Developments in Forensic Computing Science

Searching for the digital truth

by **Dr Hans Henseler,** *Forensic Science Laboratory*
Netherlands Ministry of Justice

Abstract

Today, crime investigations are increasingly faced with evidence in computers, storage media, telecommunications and data communications. Reason and deduction from traces of evidence are traditionally based on forensic science. Searching and finding evidence in digital information requires the specialist science of computer forensics. Developments in this field can be divided into three main categories - embedded systems, open systems and communication systems.

This article presents an overview of these categories together with the most recent developments that have influenced or will influence the nature of forensic computer science.

Finally, the article shortly discusses the implication of cryptography and it's use for securing digital evidence.

Introduction

The days of Sherlock Holmes are over. Many things have changed in the world around us. An ever increasing flow of information is sent through computers, fax or mobile phone communications.

Computer systems and electronic organisers are replacing paper administrations and diaries and criminals operating in world-wide organisations are using this kind of modern equipment. Figures show that the number of computers and digital storage media that are seized by police is continually increasing.

Intercepting data communication in wiretaps used to be restricted to fax messages. Today, a wiretap on a high-speed modem connected to an Internet provider will give a large variety of message formats.

Analysing this kind of evidence requires a fundamental change of methods, which has resulted in a fast development of forensic computer science. We must emphasise that forensic computer science is applied in a very broad range of crime sorts, i.e. organised crime, drug trafficking, violent crimes, fraud and also computer crime.

Although computer crime is an emerging challenge for law enforcement[1] it is not the driving force behind the development of forensic computer science. This article presents an update on the developments in forensic computer science in the past three years. A short introduction into the fundamentals of computer forensics is also presented[2].

Major categories

Computer forensics can be subdivided into three major categories:

1 Embedded computer systems
2 Open computer systems
3 Communication systems

This subdivision largely reflects the nature of the items that are seized or intercepted and that are submitted for further forensic investigation. Typically, consumer electronics belong to the first category, for example an electronic organiser or a mobile phone.

Accessing information in embedded computer systems requires analysis of the hardware using special equipment. The open systems refer to items such as computers and storage media that adhere to open standards and that are accessible via software rather than hardware, for example MS-DOS, Wintel computers or plain standard storage media such as IDE hard drives, computer tapes and disks.

Not only data but also software in open systems may contain interesting traces of evidence and should be investigated. Traces of evidence are found in both embedded systems and open systems by investigating physical items, e.g. electronic organisers, PCs, discs, tapes etc. In contrast, items found in communication systems are not physical but are found in, for example, digital transmissions.

- **Embedded Systems**

Embedded systems are found in the field of consumer electronics. This is a field that has experienced a tremendous amount of new developments over the past three years. Especially the explosive growth of the digital telecommunications, e.g. mobile GSM, the large scale introduction of smart card applications and the revival of the electronic organiser, all of which have greatly influenced the development of new forensic techniques.

Electronics have become more user friendly and are able to store information which may be interesting when searching for traces of evidence. Hardware investigations are further complicated by the continuing miniaturisation in combination with increased functionality, e.g. organiser, phone, fax and e-mail.

Investigating evidence traces in electronics requires a hardware approach. Skilled technicians with a broad knowledge of computer architectures are essential to analyse pieces of hardware when looking for memory locations. Sometimes, even removing the back panel of an electronics device and putting it back together requires special equipment and experience.

This is even truer for encapsulated integrated circuits (ICs), for example in the case of a smart card. The introduction of multi-functional smart card applications (i.e. for payment, insurance, and phone) simply begs for new forensic methods.

And this will become more interesting once biometrics (e.g. fingerprint) are used so that digital traces have larger potential to deliver important evidence. Hardware investigation of smart cards and ICs require either chemical solvents or strong acids that leave the electronics undamaged but remove surrounding epoxy in a fast and clean way.

Moreover, investigating microelectronics requires miniature equipment, and a microscope is needed to analyse the internals

of an IC. Measured signals can subsequently be analysed using standard methods or with special-purpose software.

Manual analysis is not feasible owing to the high clock speeds yielding millions of samples per second. However, analysis is still essential. Sometimes it suffices to examine data only and look for particular information. In other cases it may be necessary to analyse the firmware (software in the embedded hardware) before a good interpretation or recovery of the information is possible.

Since embedded hardware mostly operates with special-purpose processors using an unknown machine instruction set, forensic analysis becomes a difficult and laborious task.

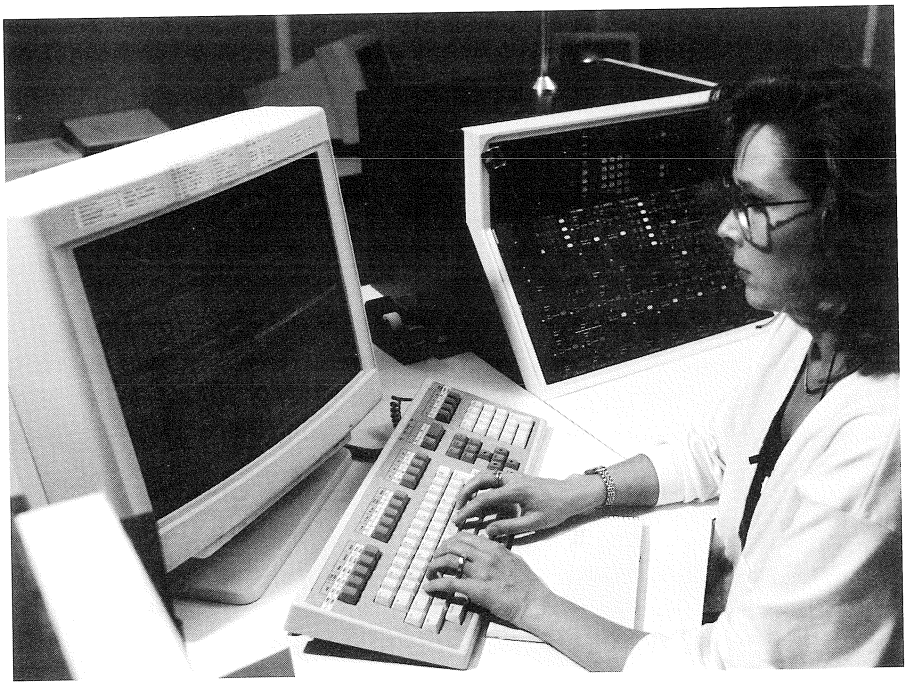
One might ask what is the use of analysing an embedded system in such hardware detail. It is tempting to think that a good manual will yield all information that is stored in the equipment. For example, both mobile phones as well as electronic organisers can be accessed using the keypad.

However, things are not what they seem to be. Firstly, making a memory dump is more reliable and faster than manually copying all information. Secondly, memory may contain traces of information that has been erased by the user and which is not accessible normally. Removing information from an index does not always imply that the information has been erased in memory. In case of broken equipment, making a memory dump may be a final resort to recover any information at all.

Finally, as it turns out in many cases, the computer will keep more information in records that the user can access. For instance, it may be possible to discover in which chronological order information was entered into the system.

- **Open systems**

The major changes in the forensic investigations of open systems are caused by the fast development of the personal computer (PC). A well-known PC type is the IBM compatible PC with the MS-DOS operating system. In the 1980s, Unix was the main operating system on minicomputers and workstations in computer networks. PCs were



used mainly as stand-alone systems. In the late 1980s and in the beginning of the 1990s, the Novell network enabled PCs to connect them to a server in a network.

Even three years ago the MS-DOS operating system played a central role in the forensic investigation of storage media and operating systems. With the arrival of first Windows for Workgroups 3.11 and later Windows 95 and Windows NT 3.51 a new trend was set that greatly influenced the forensic investigation of open systems.

Operating systems are with no exception graphical, new file systems are being used (FAT-32 and NTFS) and operating systems are object oriented. A thorough analysis of a PC requires new methods, new software and a new approach. The shift from stand-alone to network PCs further complicates the analysis of stored information.

In contrast to digital electronics in embedded systems, PCs and storage media in open systems are not opened with screwdrivers or probed with logical analysers. Instead they are probed and processed with software. Software to copy and search information and software to write special programs that access information that would otherwise remain inaccessible. Most investigations have to deal with MS-DOS and increasingly with Windows computers as well as removable storage media, e.g. computer tapes and disks that may contain gigabytes of information.

Knowing how to approach the open system is essential. Removable media can not only have different physical formats (i.e. 5.25 inch versus a 3.5 inch disk) but they can also have different logical formats. Beware of the 3.5 inch disk that turns out to be used on a machine writer rather then on a PC. (See [3] and [4] for a discussion on the forensic analysis of floppy disks).

Computer centres at large companies and universities have experience of dealing with a large variety of different digital media. The equipment that has been developed for them is expensive but can speed up the forensic investigation considerably.

Accessing zeros and ones is the first step. Next step is accessing the actual information that is represented by the zeros and ones. Envision a relational database with 100 data tables. Accessing the information in one table may not be sufficient. Accessing the entire relational database could be essential to find the required evidence.

In cases where relations are hard-coded in software this will probably imply that not only the data but also the original software and ▶

perhaps the operating system must be restored.

So far we have only discussed the analysis of storage media. The name "open system" may give the impression that open systems are not or can not be secured. In reality, open systems support a large variety of security mechanisms because they are open.

Open Standards, for example the Wintel standard, enable many different hardware and software manufacturers to incorporate their own security module. PC security software restricts file access and encrypts information before it is stored.

In order to analyse traces of information it is necessary to analyse these security modules and to study their effect on the information. In some cases the operation of programs has to be analysed in detail, disassembling every single instruction, in order to bypass the activated security mechanisms.

This is better known as reverse engineering. Reverse engineering can also be quite useful in case a fast implementation of an encryption program is needed to launch a brute-force attack on a security mechanism.

Speed is not always essential. In some pin-code systems only ten thousand trials are necessary to try every possible key combination. With a machine that does two tries per minute, it will take one week on average to break the code. Obviously, such an attack will not succeed for security systems that restrict the number of trials.

Both analysis of information storage and software require knowledge of the underlying operating system. Analysis of complex operating systems, e.g. Unix, Windows NT and even Windows 95, is essential to computer forensics. The term "Unix Forensics"[5] is introduced to emphasise the complexity of the forensics required to capture data in computers running Unix. These systems will register actions of identified users in various ways. Advanced Windows programmers know that information concerning the use of the system is stored in the system registry and countless configuration files on the hard drive.

Moreover, systems running multi-tasking operating systems function as nodes in a network and may contain information residue of communications from the network. Forensic investigation of computer networks is essential to isolate traces of computer hackers that have penetrated the network security and have entered a computer system.

With the current explosion of Internet connectivity, computer hacking is once again a growing item that requires investigation.

- **Communication systems**

In a relatively short time the fax has become a very popular means of communication. It has been and perhaps still is the most important form of data communication encountered in criminal investigations. In the early days, fax messages have been a subject for forensic computer science research.

However, the highly standardised communication protocols for fax transmissions soon led several commercial companies to develop turn-key solutions for intercepting fax messages. These solutions have been integrated in modern wire tapping equipment.

Fax communication was no longer a priority in forensic computer science and fax interceptions that were recorded without proper equipment were considered to be an acceptable loss.

With the introduction of high-speed modems the need for analysing data communication once again has gained top priority. Until some years ago, forensic analysis of modem communication was restricted to rare cases of computer hacking or software piracy in which suspects used modems to connect to Bulletin Board Systems (BBS) and dial-up computers.

As the Internet and World Wide Web (WWW) have experienced an exponential growth and because high-speed computer modems have enabled serious on-line applications, modem communication plays a central role in the communication of information and it influences the development of forensic computer science.

In contrast with fax communication, Internet communication follows "open standards" that change every week. Internet can deliver multi-media content and potentially provides much more bandwidth than fax to communicate information in an organisation.

Internet and WWW protocols have become more complex and may require an effort that sometimes even out ranges reverse engineering of software. The OSI-layer model varies from physical transport layer to application layer.

Every layer adds its own information by assembling new packets of information that have to be routed over the physical infrastructure. Well-known protocol keywords, e.g. TCP/IP, ATM, PPP, POP, HTTP, HTML, SSL etc., give a new dimension to forensic computer science.

Analysing layer after layer can be a laborious task even when the used protocols are known. Sometimes, analysis may yield interesting information about the sender and receiver. Also, information may be lost.

In case compression techniques were used, a detailed analysis of the partial data is required when attempting to recover as much information as possible. This requires advanced knowledge of network protocols and information encoding techniques in combination with good programming skills to convert raw data into readable (or visible or audible) information.

Currently, new techniques age quickly. In the upper layers of the OSI model (application oriented) new protocols or message formats are being introduced at high speed. This has become possible through the introduction of plug-in technology that allows WWW-browsers to plug-in new software to deal with new data formats.

Developments such as Java, COM (for Common Object Model) and the distributed version DCOM allow an almost instant spreading and online installation of Java applets and Active-X software components in computer systems.

Today, the already enormous flow of information is increased even further by so-called push technology that delivers information automatically to the user. The stand alone application of today is the network application of tomorrow. Perhaps ▶

new standards such as DCOM will have the greatest impact on forensic analysis when data objects are virtually distributed over an entire computer network still enabling a single point of access.

Being able to preserve all information stored in a distributed compound document will make analysing clusters in a fragmented FAT-16 file system[6] look like child's play.

Knowledge of data communication and information encoding is not sufficient. To be able to intercept messages, knowledge of the telecommunication infrastructure is essential. This is true for both the fixed and the mobile infrastructure.

Service providers will compete by offering different kinds of services to their customers. In mobile telephony, both the handset as well as the infrastructure may contain information that can prove to be essential evidence, for instance, pre-set numbers, voice-mail and dialled numbers.

Cryptography

In the past few years cryptography has become of increasing importance to forensic computer science. Firstly, the increased speed of personal computers has enabled the use of cryptography in virtually any security application.

Secondly, there is more privacy awareness and users are becoming more and more security minded when dealing with computer networks and e-mail. In such applications, cryptography can be a serious obstacle for a forensic investigation.

It can be safely assumed that this problem will further emerge once stronger encryption becomes commercially available. From the point of view of prevention this can be considered good. Too often electronic information can be easily read by others and privacy of customers is not always that well protected.

More encryption wouldn't hurt and should perhaps be made obligatory from a privacy point of view. At the same time, however, one should realise that cryptography in the hands of a criminal organisation is a dangerous weapon that can be a serious threat to society. Either key-recovery schemes or key-escrow schemes in combination with a Trusted Third Party (TTP) system will hopefully present a solution for this dilemma. The main condition will have to be that only a judge can order the decryption of encrypted information.

Cryptography also plays another part in forensic computer science. Many results of forensic investigations will be attached to the report in digital format, for example on a computer disc. To guarantee the authenticity of the digital results, a cryptographic hash function is used. A hash function is a mapping from a binary string of arbitrary length to a binary string of some fixed length, called a hash value. The hash value is mentioned in the report. This hash value represents a numerical message digest that is uniquely related to the contents of the message by a cryptographic algorithm.

This hash value represents a numerical message digest that is uniquely related to the contents of the message by a cryptographic algorithm. For example, the Secure Hash Algorithm (SHA-1) is one of the state-of-the-art algorithms that has been developed by NIST and can be found on the Internet as standard FIPS 180-1.

The Forensic Computer Science department of the Netherlands Forensic Science Laboratory has implemented the SHA-1 algorithm that has been certified by NIST (http://csrc.ncsl.nist.gov/cryptval/dss/dssval.htm). This implementation is used to secure digital evidence that is distributed with the report of the forensic investigation. In[7] it is reported that even CD-ROMs can be altered which underlines the need of securing digital evidence by cryptographic means.

We can expect to see similar applications of cryptography for authentication in the near future, and those in computer forensics could have to answer questions regarding the strength of such digital signatures. ■

About the author

Dr J Henseler is head of the Department of Forensic Computer Science of the Netherlands Forensic Science Laboratory of the Ministry of Justice. Currently the department has 21 researchers who specialise in the analysis of storage media, operating systems, software, smart cards, telecommunications equipment, electronic organisers, data communication, information encoding, telecommunication infrastructure, Internet and computer networks in general.

As a forensic laboratory of the Ministry of Justice, the Forensic Science Laboratory has three core activities. Firstly, it produces independent expert-witness reports in criminal investigations. Secondly, the laboratory performs research and development to explore the application of new technological advances to forensic investigations. Thirdly, the laboratory is a centre of expertise on new technology and may be consulted by other government agencies.

References

[1] D.L. Carter and A.J. Katz, Computer Crime An Emerging Challenge for Law Enforcement, FBI Law Enforcement Bulletin, December 1996, Volume 65, no 12.

[2] J. Bates, The Fundamentals of Computer Forensics, International Journal of Forensic Computing, January 1997, Issue 1.

[3] Floppy Disks - not a problem, International Journal of Forensic Computing, March 1997, Issue 3.

[4] Investigating Floppy Disks, International Journal of Forensic Computing, March 1997, Issue 3.

[5] Unix Introduction, International Journal of Forensic Computing, June 1997, Issue 6.

[6] Cluster Analysis, International Journal of Forensic Computing, January 1997, Issue 6.

[7] CD-ROM vs. Optical Disks, International Journal of Forensic Computing, August 1997, Issue 8.

The author can be reached at the Forensic Science Laboratory, Volmerlaan 17, 2288 GD, Rijswijk, The Netherlands. Telephone + 31 70 4135410, Fax + 31 70 4135454, or e-mail henseler@holmes.nl.

Down loading

Downloading: Using Computer Software as an Investigative Tool

By Arthur L Bowker, MA and Leonard N Drinkard

Downloading can help to eliminate complicated and time-consuming computer crime-solving procedures, such as seizing bulky computer equipment and wading through volumes of paperwork.

Consider the following scenario. At 9am one Monday morning, the owner of a local business makes a frantic call to your agency's fraud unit. She reports that she arrived at work early that morning and was surprised to find the office manager, a five-year employee, already busy at the computer. He appeared extremely nervous, and as the owner approached the computer, she discovered that he had gained unauthorised access to the company's payroll files.

When asked why, the office manager nervously responded that he thought the system had miscalculated the withholdings on his last paycheck, and he was only "checking it out." Suspicious of this response, the owner checked the computer's access log for the payroll system, something she had not done for some time.

Her inquiry revealed that the office manager had accessed the system before and after each pay day for the past year.

Investigating further, the owner made a startling discovery. The company that prepares her firm's checks had been issuing 60 paycheques every pay period, even though she employs only 55 people.

Confronted with the discrepancy, the office manager admitted to "borrowing" some funds. Heavy drinking had dulled his memory of exactly how much money he had "borrowed." He refused to answer any more questions and tendered his letter of resignation.

When the police responded, the owner promised to co-operate with the investigation. Yet, she also informed the officers that she could not afford to have her business disrupted in any way.

This unfortunate business owner had fallen victim to a computer manipulation crime, an offence that involves changing data or creating records in a computer system to commit another crime, in this scenario, embezzlement.

Although the law enforcement community has recognised the seriousness of these crimes for more than a decade, investigations typically have been complicated, time-consuming, and disruptive to the victim's business operations. However, using a technique known as downloading, law enforcement agencies now can use their computer software as an investigative tool to solve computer manipulation crimes quickly and easily.

Not for computer experts only

Downloading is the process of transferring a computer program, file, or other electronic information from a remote database or other computer to a user's own computer. When investigating computer manipulation crimes, law enforcement officers can download the victim's computerised financial records to a disk, return to their office, and use their agency's software to reorganise the data into a format that enables them to detect falsifications.

Specifically, downloading enables investigators to sort, select, and organise entries in whatever manner the investigation demands. This method makes analysing the data much easier than manually examining journals, ledgers, or check registers in whatever manner the entries might be organised, such as by date or check number.

Investigators can examine only those entries that may be evidence of a crime - such as checks with false payees, fictitious voided checks, or checks for large amounts - without searching every computer entry and every cancelled check by hand. By reducing the number of computer entries investigators need to compare to hard-copy evidence (for example, cancelled checks, vouchers, or invoices), downloading permits easy detection of any discrepancy and/or falsification the embezzler used to conceal the crime.

In short, downloading allows law enforcement agencies to use commercially available software to analyse volumes of data without seizing computer equipment, disrupting the victim's business, and manually searching every piece of evidence.

Downloading possesses clear advantages over the methods traditionally used to investigate computer manipulation crimes.

Traditional investigative methods

Some investigators note that investigations into computer manipulation crimes comprise 90 per cent detective work and 10 per cent computer work. This division between detective and computer work also is reflected in the two types of software law enforcement officers traditionally have used to solve these crimes: investigative and application software.

Investigative software

Investigative software allows users to search computer systems, particularly the computer's hard drive, for hidden files or data that subjects sometimes conceal in a deliberate attempt to thwart law enforcement. For instance, drug traffickers might hide information about their foreign bank accounts on a hard drive.

Investigative software packages typically prove most useful in cases involving unco-operative subjects whose business is crime.

In such cases, investigators must serve a search warrant and seize all of the components of the computer system, a cumbersome, time-consuming, and disruptive process.

In computer manipulation cases, however, subjects most often commit their crimes against their employer, who operates a legitimate business. Furthermore, these subjects usually have limited computer expertise; rather, they have a general understanding of how the victim's computer system works and where its weaknesses lie. This limited knowledge allows them to manipulate the system, but not to hide files. For this reason, traditional investigative software is inappropriate in these types of crimes.

Application software

Investigators primarily use application software - which includes programs for word processing, spreadsheet, and database functions - to document and later to present their findings to the proper authorities. By doing so, they do not use the software to its fullest potential. Because of increased compatibility among computer systems, many of today's application software packages permit the easy downloading of data created in other software packages. As a result, white-collar crime investigators can use today's application ▶ software to do more than write reports and

present evidence.

With the ability to download, investigators can use application software as an investigative tool.

Guidelines for downloading evidence

Preparation

Investigators first should try downloading on a small scale, such as in a case where an embezzler only had access to the computer for a short time or where the organisation's receipts or disbursements are small. By starting out with smaller cases, investigators will gain the experience and confidence they need to solve those cases involving greater amounts of data. As with any new investigative technique, before downloading, investigators must become thoroughly familiar with the functions and limitations of their agency's application software. In particular, they should know what data files it can translate into a readable format.

Procedures

First and foremost, investigators must secure the victim's system. This ensures that the subject no longer can access the system to change or destroy data, or worse, to steal additional funds.

Methods to secure the victim's system vary, but generally they consist of changing the passwords for all users and from all points of entry, including computers in the office and telephone lines that allow users to access the system from remote locations. The subject also must be prevented from entering the premises after the passwords have been changed, which may mean placing the subject on administrative leave and notifying co-workers that this person no longer has clearance to enter the workplace.

After securing the system, investigators should determine what software the company uses to maintain its financial data. Some small companies contract with computer firms for customised financial software packages, and as a result, may not know what format they use.

Fortunately, these computer firms often customise a product by making only minor modifications in a standard software program.

In such cases, investigators can determine

which program the victim uses by viewing a directory of its financial files and checking the three-symbol extension after each file name. For example, WKS and WK1 represent two types of Lotus software.

If the victim and the agency use the same file format, the downloading process entails merely copying the necessary files to a disk. If not, the company's system or the agency's software may be able to convert the data into a compatible format.

Specifically, if the victim's or agency's software can save the file in the American Standard Character Information Interchange (ASCII), a standard data information format, then any spreadsheet or database program can read the file.

Although not all software packages can convert data to ASCII, they can transmit data to a printer and produce a hard copy of the file. By the same token, with a slight variation in print commands, users can send data to a file instead of to the printer. Once created, this print file can be copied to a disk. Special software, called a print file reader, can read the data and convert it to a format that the agency's application software will understand.

Downloading's investigative counterparts

In addition to downloading, investigators can use the password-based security controls built into many computer systems to discover who made the fraudulent entries and when. In many cases, computer access logs reveal that suspects enter the system after-hours and on weekends, when they have no legitimate reason to do so. In such cases, suspects will be hard-pressed to deny the evidence, as well as to explain why they needed to access the computer system at times when no one could witness their actions.

Legal considerations

Although law enforcement officers traditionally have seized entire computer systems to investigate white-collar crimes, victims of computer manipulation cases usually cannot afford to have their businesses disrupted in this manner. Downloading allows investigators to access computerised records without removing the computer itself. Still, search warrants may be required, and investigators should consult their department's legal advisor or the local prosecutor for guidance.

Another important area of consideration involves the admissibility of computerised records in court. In general, computerised records are subject to the hearsay rule, the best evidence rule, and the authentication requirement. Investigators should seek legal advice in these areas as well.

Furthermore, as with any piece of

evidence, establishing a proper chain of custody helps to ensure the admissibility of computerised records in court. To accomplish this, investigators must document fully the procedures they used to obtain and store the downloaded data, including where, by whom, and under what circumstances they gained access to the victim's system, and which specific files they downloaded. These files must be maintained on a write-protected disk, which prevents data from being altered. To provide additional protection against data loss, investigators should use copies of the downloaded files to sort, select, and organise the data during the investigative process and should remember to back up the files periodically.

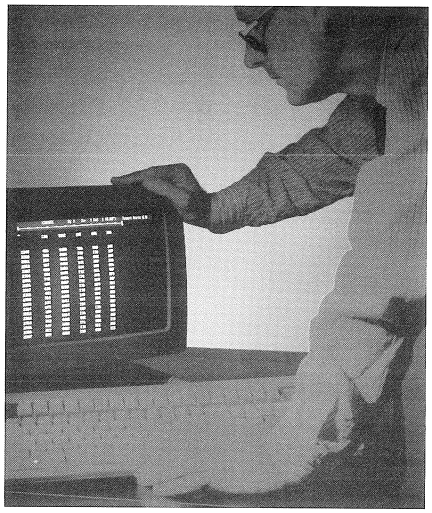
Helping businesses prevent computer embezzlement

White-collar crime investigators should encourage businesses to institute security procedures to combat computer manipulation crimes. First, companies should institute computer access controls. Specifically, employees authorised to access the computer should have access codes or passwords.

Computer systems should recognise authorised users, as well as their level of authority, and admit them accordingly. For example, the payroll clerk might be permitted to sign on to the system only every pay-day, while an office assistant might be denied access entirely. Computer systems also should change access codes periodically.

In addition, companies should establish and maintain internal accounting controls. These include separating financial duties so that the person who keeps the records is not the same person who prints the checks; periodically rotating duties; developing and documenting financial policies and procedures, such as defining authorisation limits for checks; and conducting periodic internal audits and surprise inspections.

Third, the computer system should log every unusual occurrence automatically. For example, a system might search for checks that are out of sequence; transactions that are out of the ordinary-too high, too low, too many, too often; or an employee who repeatedly attempts



to gain access improperly. To be effective tools, however, these reports must be inspected periodically. The business owner in the opening scenario who fell prey to computer embezzlement failed to check her computer's access log on a regular basis.

Finally, employers should pay attention to their workers. The behaviour of employees who deviate from the firm's standard operating procedures or merely from their own past performance levels may signal that something is amiss.

Conclusion

In the past, businesses locked up their books and records to prevent destruction, falsifications, and losses. Unfortunately, today's technology enables embezzlers to manipulate data and falsify records, even at their leisure from their own homes. Law enforcement agencies must accept the fact that financial records, once falsified by pen and pencil, now can be altered by computer.

Fortunately, investigators can fight back by using their agency's own computers to detect false entries quickly and accurately, establish criminal intent, and successfully prosecute embezzlers. By using downloading as an investigative tool, white-collar crime investigators can take a "byte" out of computer crime.

The authors are investigators with the Office of Labor Management Standards, US Department of Labor, Cleveland,

The benefits of downloading

Downloading allows investigators to:

- Use a familiar software package to examine, analyse, and organise volumes of data
- Reduce considerably the time required to investigate and document a case
- Limit greatly the intrusion into the victim's business by avoiding the need to seize hardware and software to investigate the crime
- Authenticate work papers and schedules that document a loss and can be used in court because they represent an exact copy of the original data
- Eliminate errors that might occur if investigators needed to enter data into the computer from hard copies of ledgers, journals, check registers, cancelled checks, etc.

Guidelines for downloading

Investigators should:

- Try downloading on a small scale to gain confidence
- Become familiar with the functions and limitations of your agency's application software
- Secure the victim's system to prevent unauthorised access
- Determine the victim's software package (If the package is the same as your own, copy the data onto a disk, if it is not the same:
  a) convert to an ASCII file and use spreadsheet or database software to read;
  or b) create print file, copy onto disk, and use print file reader software to convert data)

Preventing computer manipulation crime

Business owners should institute computer access controls, establish and maintain internal accounting controls, programme computers to record unusual occurrences, regularly review security logs, note employees who deviate from acceptable procedures or performance levels.

Ohio.

EPIC Analysis of New Justice Department Draft Guidelines on Searching and Seizing Computers. By Dave Banisar, Electronic Privacy Information Center

The Electronic Privacy Information Center (EPIC) has obtained the Department of Justice's recently issued draft "Federal Guidelines for Searching and Seizing Computers." EPIC obtained the document under the Freedom of Information Act. The guidelines provide an overview of the law surrounding searches, seizures and uses of computer systems and electronic information in criminal and civil cases. They discuss current law and suggest how it may apply to situations involving computers. The draft guidelines were developed by the Justice Department's Computer Crime Division and an informal group of federal agencies known as the Computer Search and Seizure Working Group.

Seizing Computers

A major portion of the document deals with the seizure of computers. The draft recommends the use of the "independent component doctrine" to determine if a reason can be articulated to seize each separate piece of hardware. Prosecutors are urged to "seize only those pieces of equipment necessary for basic input/output so that the government can successfully execute the warrant."

The guidelines reject the theory that because a device is connected to a target computer, it should be seized, stating that "in an era of increased networking, this kind of approach can lead to absurd results." However, the guidelines also note that computers and accessories are frequently incompatible or booby trapped, thus recommending that equipment generally should be seized to ensure that it will work. They recommend that irrelevant material should be returned quickly. "Once the analyst has examined the computer system and data and decided that some items or information need not be kept, the government should return this property as soon as possible." The guidelines suggest that it may be possible to make exact copies of the information on the storage devices and return the computers and data to the suspects if they sign waivers stating that the copy is an exact replica of the original data.

On the issue of warrantless seizure and "no-knock warrants," the guidelines note the ease of destroying data. If a suspect is observed destroying data, a warrantless seizure may occur, provided that a warrant is obtained before an actual search can proceed. For "no-knock" warrants, the guidelines caution that more than the mere fact that the evidence can be easily destroyed is required before such a warrant can be issued.

"These problems . . . are not, standing alone, sufficient to justify dispensing with the knock-and-announce rule."

Searching Computers

Generally, warrants are required for searches of computers unless there is a recognised exception to the warrant requirement. The guidelines recommend that law enforcement agents use utility programs to conduct limited searches for specific information, both because the law prefers warrants that are narrowly tailored and for reasons of economy. "The power of the computer allows analysts to design a limited search in other ways as well . . . by specific name, words, places. . . ."

For computer systems used by more than one person, the guidelines state that the consent of one user is enough to authorise a search of the entire system, even if each user has a different directory. However, if users have taken "special steps" to protect their privacy, such as using passwords or encryption, a search warrant is necessary. The guidelines suggest that users do not have an expectation of privacy on commercial services and large mainframe systems because users should know that system operators have the technical ability to read all files on such systems. They recommend that the most prudent course is to obtain a warrant, but suggest that in the absence of a warrant prosecutors should argue that "reasonable users will also expect system administrators to be able to access all data on the system." Employees may also have an expectation of privacy in their computers that would prohibit employers from consenting to police searches. Public employees are protected by the Fourth Amendment and searches of their computers are prohibited except for ""non-investigatory, work related intrusions" and "investigatory searches for evidence of suspected work-related employee misfeasance."

The guidelines discuss the Privacy Protection Act of 1980, which was successfully used in the Steve Jackson Games case against federal agents. They recommend that "before searching any BBS, agents must carefully consider the restrictions of the PPA."

Citing the Jackson case, they leave open the question of whether BBS's by themselves are subject to the PPA and state that "the scope of the PPA has been greatly expanded as a practical consequence of the revolution in information technology — a result which was probably not envisioned by the Act's drafters."

Under several DOJ memos issued in 1993, all applications for warrants under the Privacy Protection Act must be approved by a Deputy Assistant Attorney General of the Criminal Division or the supervising DOJ attorney.

For computers that contain private electronic mail protected by the Electronic Communications Privacy Act of 1986, prosecutors are advised to inform the judge that private e-mail may be present and avoid reading communications not covered in the warrant. Under the ECPA, a warrant is required for e-mail on a public system that is stored for less than 180 days. If the mail is stored for more than 180 days, law enforcement agents can obtain it either by using a subpoena (if they inform the target beforehand) or by using a warrant without notice.

For computers that contain confidential information, the guidelines recommend that forensic experts minimise their examination of irrelevant files. It may also be possible to appoint a special master to search systems containing privileged information.

One important section deals with issues relating to encryption and the Fifth Amendment's protection against self-incrimination.

The guidelines caution that a grant of limited immunity may be necessary before investigators can compel disclosure of an

encryption key from a suspect. This suggestion is significant given recent debates over the Clipper Chip and the possibility of mandatory key escrow.

Computer Evidence

The draft guidelines also address issues relating to the use of computerised information as evidence. The guidelines note that "this area may become a new battleground for technical experts." They recognise the unique problems of electronic evidence: "it can be created, altered, stored, copied, and moved with unprecedented ease, which creates both problems and opportunities for advocates." The guidelines discuss scenarios where digital photographs can be easily altered without a trace and the potential use of digital signatures to create electronic seals. They also raise questions about the use of computer generated evidence, such as the results of a search failing to locate an electronic tax return in a computer system. An evaluation of the technical processes used will be necessary: "proponents must be prepared to show that the process is reliable."

Experts

The DOJ guidelines recommend that experts be used in all computer seizures and searches — "when in doubt, rely on experts." They provide a list of experts from within government agencies, such as the Electronic Crimes Special Agent program in the Secret Service (with 12 agents at the time of the writing of the guidelines), the Computer Analysis and Response Team of the FBI, and the seized recovery specialists (SERC) in the IRS. The guidelines reveal that "many companies such as IBM and Data General employ some experts solely to assist various law enforcement agencies on search warrants." Other potential experts include local universities and the victims of crimes themselves, although the guidelines caution that there may be potential problems of bias when victims act as experts.

About EPIC

The Electronic Privacy Information Center is a public interest research centre in Washington, DC. e-mail info@epic.org. Telephone +1 202 544 9240.

SPECIAL MACINTOSH SCSI CONSIDERATIONS

Howard A. Schmidt looks at the Apple Mac small computer systems interface (SCSI) and considers the special problems it can pose for investigators.

For those of us that have the pleasure of doing Mac cases we all know first hand what "VOODOO SCSI" is all about. This document should help those of you who are still waiting to get zapped. As complex (or easy depending on your perspective) SCSI becomes there are always those little distractions that make dealing with them more challenging.

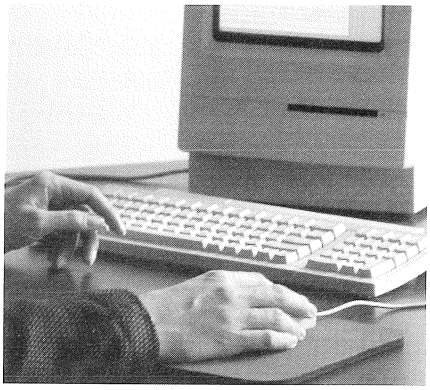
Some of the Macs require special attention, some Classics, Quadras and PowerBooks can cause problems. The IIfx, above all, causes some unique problems so we will start with that one.

IIfx

The terminator for the IIfx is black and physically looks different from the standard gray terminator. The IIfx terminator should cost about $20 from third party vendors. If the IIfx has a third party (non-Apple) hard drive installed internally, there are some special issues to deal with.

Normally these drives come with a resistor pack that provides termination. Even with this built in termination you still need a special filter for proper termination. To achieve this you must plug the SCSI cable directly to the logic board in the IIfx and place an internal SCSI filter (Apple P/N 590-4516) between the cable connector and the hard drive. If for some reason you remove the internal drive (or someone else has), you should install both the Internal SCSI filter AND an Internal SCSI termination Block (Apple P/N 590-4515).

If you are out on a site and find yourself without the internal termination block you can insert a regular passthrough terminator at the beginning of your SCSI chain and make sure there is a black terminator at the end.



Quadra 700 & Mac Classic

If you have either one of these systems you should install an internal device (Apple P/N 630-0408) Like the fx terminator it plugs into the logic board.

Quadra 900 & 950

The 950 comes with two SCSI controllers, internal and external. The internal terminates at the logic board and at the end of the ribbon cable. Because of this ANY internal drive must have their internal SCSI resistor termination removed as the termination takes place with the cable. For cases where you are not sure whether or not the hard drive comes with termination or are not sure of the resistor packs location contact the hard drive manufacturer for technical support. (There is a freeware file on the schmidt.org FTP site called TEKSUP.ZIP that has various tech support numbers.)

Powerbook & Duo

These popular notebooks have a very sensitive SCSI bus. To minimize problems keep any cable lengths as short as possible.

Don't forget the powerbooks require the HDI-30 SCSI adapter so if you don't have one, grab one now.

I hope this helps with some of the SCSI problems we face every time we run into a Mac system. If there are any questions feel free to contact me.

Howard Schmidt is a supervisory special agent and director of the US Air Force Office of Special Investigations Computer Forensic Laboratory. He can be e-mailed at schmidt@mci.net ▶

Book reviews

Entry, Search and Seizure: A guide to civil and criminal powers of entry

By Richard Stone
3rd edition. Sweet and Maxwell, London
pp 386. Price: £58.00

The rights of entry can present a minefield to the police officer or investigator seeking to seize a suspect's computer and trawl through it for data.

There are a series of strict conditions and guidelines, which if not met, could invalidate the admissibility of evidence and jeopardise possible legal action.

Stone's book takes the reader across the whole range of rights, powers and pitfalls, covering the basics of legal definitions and going right through to specific acts and cases.

While the computer crime investigator may not see the book as directly relevant, the information in it will clarify the position of gaining entry to premises and removing evidence. Computer data is, at the end of the day, evidence in the same way a bloodied knife or a set of fingerprints might be.

Stone takes a comprehensive look at the UK's scope and limitations of search and seizure, including specific police powers, personal searches, taxation, customs and excise, local and central government as well as the gamut of civil procedures.

Since the last edition of the book, the laws have changed considerably, with the introduction of the Criminal Justice and Public Order Act 1994, which has added to police powers, and other legislation such as the Drug Trafficking Act 1994 and the Proceeds of Crime Act 1995.

There are several sub chapters in the book which are specific to data evidence and computer crime, although they are relatively scant and serve to give a general overview rather than attempting to fully explore the ramifications of the various laws.

In addition, Stone spends some time explaining the Anton Piller order - the High Court's power to authorise entry and seizure of possible evidence in a civil case. This "civil search warrant" is hugely important and it is vital that the civil investigator is familiar with the process from start to finish, as well as the potential for the suspect to challenge the order.

Stone, who is professor of law at Nottingham Law School, Nottingham Trent University in the UK, is obviously very familiar with the subject matter and covers the material with great authority.

However, the language used is deeply embedded in legal jargon and phraseology, making the text difficult at first for the non-lawyer. All the information is there, but the reader has to make an effort to unravel it and put it into a practical perspective.

A comprehensive table of cases is included as is a full table of statutes and statutory instruments, all of which are indexed to the relevant areas in the book. While this book is highly specific to the UK, investigators in other parts of the world may be able to draw on some of the principles and concepts mentioned.

Overall, Entry, Search and Seizure is extremely useful for any investigator working in the field, where the powers and limitations of the law could make or break a case. As a reference work, to be dipped into as required, it could prove invaluable.

Crime, Deviance and the Computer

By Richard C Hollinger
Dartmouth Publishing Company Limited, Aldershot, Hants, UK
pp 573. Price £99.50.

This large tome takes the reader on a journey of computer crime, from the emergence of computers in 1946 through to their current pre-eminence in modern society.

Hollinger, who is at the Department of Sociology at the University of Florida, has gathered together a series of articles and perspectives from some of the most well-known technology commentators.

As a sociologist, he is fascinated by the incredible growth and evolution of computers and their impact on everyday life, especially the growth and potential for machines to be used as tools of crime.

And as he points out, criminals usually discover this long before law enforcement agencies do: "Those who are intent upon taking advantage of others through deception usually discover the weaknesses and vulnerabilities of these new technologies long before the agents of social control and law enforcement."

The book is divided into four parts, The Discovery of Computer Abuse (1946 to 76), The Criminalization of Computer Crime (1977 to 87), The Demonization of Hackers (1982 to 92) and The Censorship Period (1993 to present). This takes the reader on a chain reaction of computer abuse and misuse and the subsequent reaction by the authorities in an attempt to stop it.

A huge range of subjects is covered, spanning the changes in technology, law and society, including types of crimes, their frequency, the hacker culture, paedophiles and computer pornography and the issue of censorship and control of the Internet.

The overall message that the book conveys is that technology crime is here to stay and that we all have to realise it and react accordingly. Hollinger takes a considered approach to the subject and lets his contributors speak for themselves. This broad range of views gives the book a refreshing and broad-minded perspective and lets the reader gather together the various strands and work out the larger picture for him or herself.

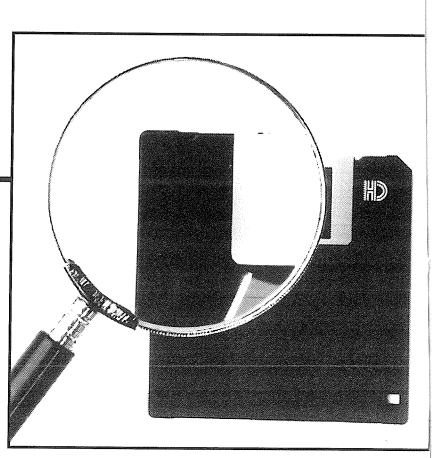
While Crime, Deviance and the Computer is not a practical reference book for investigators, and it certainly never tries to be, it is still an interesting read that everyone in the field of forensic computing could learn something from.

Hollinger has underlined the fact that society and technology are inseparably bound up, and that changes in one have huge implications in the other.

However, many would find this serves to further emphasise the eclectic and varied nature of the work, and add to its interest.

Overall, the book is a comprehensive look at computer misuse, taking a historical glance but underlining the fact that we can learn from our mistakes for the future. It can be dipped in and out of at will, and has some fascinating insights.

Forensic Q&A



Q *I have been given the results of a search which show hits by cluster numbers. What do the numbers refer to and how do I examine these areas?*

A Space on a hard disk is assigned or allocated to a file in units referred to as clusters (a cluster consisting of a defined number of sectors). Each cluster on a hard disk is assigned a number which refers to a physical location. For example a typical 1.0GB hard disk with 64 sectors (each sector being 512Bytes) comprising each cluster will have a total of 33,006 clusters or allocation units. These will be numbered consecutively by the operating system starting with 2 and ending with 33,007 (the area prior to 2 is reserved by the system). The cluster references in your hit list refer to these locations.

In order to examine the contents of a given cluster you need to use either a dedicated cluster viewer or a general DOS based program such as Norton Version 4.5. A dedicated viewer will normally work in Windows and will enable cluster contents to be rapidly displayed, examined and printed. A DOS based viewer will be much slower to use and will be unlikely to have the capability to rapidly print cluster contents in a form that will be suitable for use in a court of law.

Q *I have seized a computer which I believe to have been stolen from a solicitors office. There are no external, physical characteristics by which it can be identified. I know the hard disk has recently been reformatted. Is there any way in which I can trace the original owner?*

A It may be possible to check if the original owner was the solicitor by examining the unallocated areas of the hard disk. Success will depend on:

- The type of hard disk - SCSI or IDE and the way in which the hard disk was reformatted
- The difference between the amount of data on the hard disk prior to and after reformatting
- Details about the hard disk contents prior to reformatting that can be used as unique search criteria.

Taking each of these points in turn.

If the hard disk was of the SCSI (small computer systems interface) type then when it was reformatted all the physical surface of the platters will have been written over. This will have permanently destroyed any information that was contained on the disk. In this instance identification of the computer from the hard disk will not be possible. If the hard disk was of the IDE (integrated device electronics) type then there are two types of reformatting that can be carried out: high level and low level. The normal formatting is high level and this only writes over the sectors containing system information. The sectors containing the data are not written over and can still be accessed using appropriate software. If, however, the reformatting was carried out at a low level then all the physical area of the platters will have been written over and the data destroyed. As with the SCSI drive, identification of the computer from the hard disk will not be possible.

Let us assume that the hard disk was of the IDE type and had been high level reformatted. The data area of the disk will still exist although the 'index' (known as the file allocation table or FAT) will have been destroyed. Let us further assume that the disk has a total capacity of 1.2GB of which 560MB was occupied by files. After reformatting, the operating system and programs will have been reinstalled on the hard disk. Work will then have been completed which will have created further new files on the hard disk. If, when the hard disk is subsequently examined, the total amount of files re-installed is less than 560MB then it is quite possible to retrieve previous information. The probability of successful retrieval will increase the lower the volume of reinstalled files. If, however, the total volume of reinstalled files exceeds 560MB then the probability of retrieval will decrease significantly, though not completely since the reinstalled material may not lie in the same physical location as the original.

If information is available about the original owner of the computer then this can be entered into a suitable search program. The type of information should be unique such as details of a client's address which is known only to the potential original owner. For example, in one case it was suspected that a computer had been stolen from a building society. The name of the building society and unique customer account number details were entered into a search engine. The subsequent examination of the hard disk revealed several hits for the account number and hundreds of hits for the name, positive proof that the computer had been stolen.

(Editors Note: In order to efficiently identify stolen computers the use of a dedicated search program is recommended. The Journal has such a program which is used by professional computer forensic investigators specifically for this purpose. The program, known as Mycroft, is available free of charge to subscribers. To obtain a copy send us a fax or e-mail with your delivery address.) ■

If you have any tips, advice or cautionary tales you would like to share with readers, please contact the Journal.
e-mail your questions and comments to ijfc@pavilion.co.uk

Notice Board

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

EVENTS

The International Conference on Privacy

23-26 September, Montreal

How to protect personal information and respect privacy are growing concerns all over the world. Informatics and privacy - are they necessarily incompatible? And will the Internet necessarily resist all controls over the circulation of information? These and many other questions will be on the agenda at this conference. Speakers from around the world include: Phillip J Swinburne, New Scotland Yard's Computer Crime Unit, Herbert Burkert, German National Research Centre for Computer Science, Michel Carlos, Economic Crimes Unit, Surete de Quebec.

Contact: Hydro-Quebec
Tel: +1 514 289 2289

Criminal Justice Expo & Conference

30 September-1 October,
Hynes Convention Center, Boston, US

Seminar topics include: Advances in Forensic Science, Police Education, Policing Research Challenges Facing Private Security, War Against Crime.

Contact: RDP Group Trade Show Prod.
Tel: +1 800 243 9774
Email: rdpsteven@aol.com

Cruising the Internet Securely

20-21 October, London

A two day guide for security and audit practitioners.

Contact: MIS Training Institute
Tel: +44 (0) 171 779 8944

Preventing European Payment Card Fraud

21-22 October, Amsterdam

How big a threat is the growth of card fraud? Who are the target institutions and markets for organised payment card crime? What can be done to combat 'card not present' fraud? How do you establish an effective fraud prevention strategy? What needs to be done at the legislative level? Is competition frustrating the fight against fraud? How secure are smart cards? What will Interpol's working group on counterfeit payment cards be able to achieve?

Contact: Lesley Ferdinand,
International Conference Group Limited
Tel: +44 (0) 181 743 8787

Emerging Trends in Financial Crime

5-6 November, London

Topics include: What are the new issues and new crimes which will confront the financial sector as it approaches the next millenium? Are financial crimes a policing priority any more, and, if not, who will investigate them? Have tax evasion and fiscal flight taken on a higher priority than commercial crime?

Contact: International Conference Group Limited
Tel: +44 (0) 181 743 8787
Fax: +44 (0) 1903 233545

Fourth International Law Enforcement Conference on Computer Evidence, the IOCE '97

10-12 November, The Hague

This three day conference is hosted by the Dutch National Criminal Intelligence Division and the Forensic Science Laboratory, both part of the Netherlands Ministry of Justice. The conference will accommodate technical, legal and procedural issues. Participants will visit the forensic science laboratory where a number of state of the art forensic methods for analysing computer evidence will be demonstrated. IOCE working group meetings will be scheduled on the final conference day and some time will be reserved to hold new elections for the IOCE board.

Conference fee is US$200.

Contact: Dr J Henseler
Tel: +31 70 4135410
Fax: +31 70 4135454
Email: ioce@holmes.nl

Internet Gambling Law and Management First International Symposium

11-13 November, J W Marriott, Washington, DC

Industry analysts foresee a 10 billion Internet Gambling Industry by the year 2000. This international symposium, bringing together legal, business and technical leaders in the field, will address the specific opportunities in Internet Gambling, the integration of new technologies, and the legal and regulatory considerations that must be resolved in a global environment.

Due to the high visibility of the event in this field, corporate sponsorships are being made available. The conference is being sponsored by Gaming Law Review and BioConferences International.

Contact: Esther Bicovny or Mary Ann Liebert
Tel: +1 914 834 3100

Business Crime and Risk

18-19 November, London

This conference will look at the likely future developments in such areas as: business intelligence/industrial espionage, kidnapping and extortion, IT security, terrorist threats, organised crime.

Contact: International Conference Group Limited
Tel: +44 (0) 181 743 8787

Money Laundering in Banking and Financial Systems

26-28 November, Rome
Contact: D&D Comunication
Tel: +39 2 58 30 61 65

The First International Conference on Forensic Documents

20-22 January 1998, Bangalore, India
Contact: Dr R K Tewari, Bureau of Police Research and Development
Tel: +91 11 436 2676
Fax: +91 11 436 2425

International Conference on Forensic Computing

3-5 December, Brighton, UK

Three day conference to be addressed by speakers from across the world.

Contact: International Journal of Forensic Computing
Tel: +44 (0) 1903 209226
Email: ijfc@pavilion.co.uk

International Journal of FORENSIC COMPUTING™

Published by
Computer Forensic Services Ltd.