ISSN. 1363-6650

AUGUST 1997
Issue 8

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

Computer crime investigation is akin to any other crime investigation, be it murder, blackmail or assault. It's all about finding who did it, attempting to get the offender to admit it, and then collecting enough evidence for a concrete prosecution in court.

The skills, intuition and experience of the detective are the most important link in the chain. But to work properly, law enforcement agencies need the correct tools for the job. There has to be a system, together with the principles and methodology for its use, that can retrieve and collate information simply and effectively.

It doesn't matter who makes such a product - the only important thing is that it actually works and helps put criminals behind bars. At the moment police forces across the world are missing out on valuable evidence when they skip a suspect's computer during a raid, or fail to see the potential of something like a personal organiser or mobile phone found in a suspect's home.

If they realised that a tiny 3.5 inch floppy disk or a wallet-sized Psion computer could contain thousands of names of drug dealers, criminals, contacts or even murder hit-lists, they would certainly think again.

Complexity is the bugbear of progress. Many in law enforcement are unfamiliar with computers so they fight shy of computer investigations. In reality, computers can be made to do the technical side of such work, leaving the officer or detective to do what he or she is best at - investigating. After all, a policeman doesn't need to know how a breathalyser works in order to check whether someone is over the limit. He doesn't need to know how the alcohol molecules are detected or what chemical reaction takes place, he just needs to look if the results are positive or negative - red or green.

The goal for any forensic computing equipment should be to make the work of the police and detectives as efficient and effective as possible.

The article on page 8 in this issue argues that one technology, CD-ROM, presents the world of forensic computing with some tough questions. But we will not know the truth until it is tested in court. The same goes for a myriad of legal issues covering computer investigation and forensic presentation.

Only when these burning issues are resolved will manufacturers and investigators be able to draw up a uniform specification and methodology. And this could take a very long time. ■

We welcome Howard Schmidt to the Journal's editorial board. Howard, who was profiled in last month's issue, is a supervisory special agent and director of the US Air Force Office of Special Investigations Computer Forensic Laboratory. He brings a huge amount of skill, experience and insight to the Journal and you can read his work over the forthcoming months.

We would welcome any comments, suggestions or ideas that readers may have for future issues. And the Journal is always happy to receive technical reports, case studies and papers. You can contact us by phone, fax or e-mail.

News

Japanese study into online porn

The National Police Agency in Japan is conducting a study into pornographic material available on the Internet.

A research panel will look at certain web sites, including so called date-clubs, and will report within a year into how the laws regulating adult entertainment should be changed. Japan currently has no laws specifically covering pornography and has many adult Web pages.

High-tech drug barons

Investigators in South Africa fear that the war against drugs is being hampered by criminals using computers to speed up communications.

The country's Narcotics Bureau says an estimated 136 drug syndicates use Internet link up to control runners, set prices and distribute recipes for drug making and blending. But as the drug problem escalates, police say they are often powerless to act. Bureau director Cobus van Aarde said: "South Africa has emerged as a haven for international narco-traffickers because of the strong defensive measures taken by the industrialised nations. Plus the criminals are exploiting a new and emerging market here."

New German Net law

The lower house of the German parliament has approved a controversial law aimed at controlling commercial online services and Internet content.

Under the legislation, which has yet to be ratified, so called digital signatures will be used to verify business transactions on the Net and controls will be used to block pornography and violent material. And the new law would also make Internet service providers liable for their content. If the services contain banned material, the providers would be held responsible when they know about the content in advance and do nothing to block it. The law faces strong opposition in the German parliament and also from Internet service providers who say they could be forced to relocate in other countries.

Campaign against illegal software

Software piracy watchdog the Business Software Alliance is warning users of copied programs to come clean or risk legal action.

In a summer offensive, the BSA sent 60 letters to companies suspected of breaking software copyright and program audits coupled with court action could follow. BSA's European marketing director Clare O'Brien said: "The breadth of sectors affected show that software piracy is a widespread problem and can affect any company, from the large corporate through to the small start-up business." Penalties for law-breakers include up to two years in prison and unlimited fines.

Privacy protection laws

Computer users in the US would get greater data protection from firms using personal information if a key bill is passed by Congress.

The law would bar companies from disclosing peoples' medical and financial records as well as government information collected online. Although many Internet users are unaware of the practise, web site owners can use technology to track and collect information about their visitors and then sell it on for profit.

The bill is by Rep Billy Tauzin, chairman of the House Commerce Committee's telecommunications subcommittee and is due to be discussed in the autumn.

Net provider not liable for paedophile

A US state judge has ruled that an Internet service provider is not responsible for customers who use the web to peddle pornography.

Judge James Carlisle in Florida, US, said that America Online was not liable after a 14 year old boy was sexually assaulted in 1994 by a man the child had first met on the Internet. The paedophile had pleaded guilty to federal and state charges and is in prison, but a lawsuit had been filed on behalf of the boy saying that AOL had been negligent by not enforcing an anti-pornography policy.

Judge Carlisle ruled that AOL cannot be sued for the statements of others. Lawyers for AOL said it is impossible to monitor all of its chat rooms, where up to 14,000 conversations can take place at once. They said the company has employees who search for paedophiles and that the police had upped their online efforts, often by using officers who pose on the Net as vulnerable children.

Internet wiretapping

Police in Japan could use search warrants to follow Internet communications and telephone conversations under a new law proposed by the government.

The draft bill, to be submitted in the autumn, is aimed at attacking organised crime as well as illegal activities by corporations and religious cults, and would allow investigators to tap data transmissions on the Internet. Critics say that such a law would contravene the privacy and personal security of citizens which are protected under the constitution.

Man denies luring teenager

A 42 year old man in California, US, has pleaded not guilty to charges that he pretended to be a teenager on the Internet to persuade a girl into having sex.

Prosecutors allege that Francis John Kufrovich met the girl in a teen chat room on the Net and carried on the relationship over the telephone and through e-mail. They say the man went to a hotel in Irving, Texas, where the 13-year-old girl and her mother were staying, and invited himself into the girl's room and tried to have sex with her. Prosecutor Christopher Droney said: "At no time prior to meeting Kufrovich in person did the girl know his true name or age."

He added that the case is one of the first to be conducted under the criminal section of the Communications Decency Act of 1996 which makes it a crime to entice a minor to become involved in illegal sexual conduct. The trial is set for September 8 and if convicted of the charges, Kufrovich faces up to 10 years in prison and a $500,000 fine. ▶

Bank shut over Net activity

Federal law enforcement authorities in the US raided and closed down Netware International Bank after it was suspected of improper Internet actions. The bank, in North Carolina, is alleged to have made loans and collected deposits on the Internet. The raid was carried out after the Office of the Comptroller of the Currency and the North Carolina Commissioner of Banks made enquiries about whether the company was legally organised.

FBI clears Army employees of spying

The FBI has announced it has found no evidence to support allegations that staff at a US Army computer lab were engaged in espionage. A former employee of the Army research lab at the Aberdeen Proving Ground in Maryland accused other workers of selling confidential missile data to Iraq at the time of the Gulf War and also to China. The man was fired by lab officials several years ago before he had filed his charges, for reasons not disclosed by the army.

Schoolgirl Net site shut down

An Internet site in California, US, that ranked 152 schoolgirls by looks, personality and sexuality has been scrapped. Boys at the school in Palo Alto, part of the so called silicon valley, are suspected of putting the pages up but so far none have been identified. Police said no law had been broken, but the firm that hosted the site pulled it because of a ban on "hate speech".

Mobile phone fraud

Detectives in Salt Lake City, US, arrested two illegal immigrants who have been accused of cloning cellular phone codes and selling them on the street. Phone operator AirTouch Cellular became suspicious when fraud analysts identified unusually high volumes of call activity on phones registered in Phoenix but being used in Salt Lake City. After months of monitoring and investigating, the firm managed to trace the calls to the suspects.

Cloning phones involves programming stolen cellular phone numbers and electronic serial numbers into other handsets, creating a clone of the original phone that can be used to make unlimited calls. Across the US the fraud costs more than $600 million a year.

Australia's $20 billion fraud

A survey has revealed that nearly half of Australia's companies have fallen victim to fraud at an estimated cost of up to $20 billion a year. The survey said that the known cases were probably just the tip of the iceberg as many organisations were unaware of what was going on or were reluctant to discuss security issues. One in two of the companies questioned admitted they had experienced serious fraud, often by employees or external hackers breaking into computer accounting systems. The average cost per organisation was nearly $500,000 and one company said it had been defrauded by $10 million.

Porn shock for star gazers

Web surfers looking for information on NASA's mission to Mars were surprised to find pornography when they logged onto www.nasa.com. A small New York company had registered the Internet domain name and used it themselves, but the site was shut down after requests from the real NASA and the Federal Trade Communications office.

A 1958 federal law bans the use of the NASA name in conjunction with a product or service in a manner indicating support from the space agency.

CD ROM cuts court time

In what is thought to be a first, a lawyer has done away with bulky paper reports and filed a CD ROM brief with a US Court of Appeal. Charles Gholz, a partner with an intellectual property law firm in Arlington, Virginia, used hypertext markup language, as used in the world wide web, to prepare his brief. Using the file the judge can easily jump to additional text of supporting cases, multimedia depositions or other key exhibits. It is expected that the system will save valuable court time and could mark the beginning of a new era of electronic legal documentation and litigation.

Illegal data from children

Federal regulators in the US warned that marketing firms could be breaking the law by collecting personal information from youngsters online. The Federal Trade Commission said such companies had to tell parents how the data, such as names, addresses and phone numbers, will be used and obtain consent before releasing it to a third party. And the warning has been welcomed by the Center for Media Education, which had said in a report last year that advertisers and marketers were exploiting youngsters by aiming products on the Net in ways that manipulated and violated children.

Legal guide to Net

UK Internet service provider Prestel Online is publishing a free beginner's guide to cyberspace legal issues. The 15-page booklet covers issues such as freedom of expression, electronic commerce, intellectual property, safety and privacy. Prestel Online managing director Michael Holland said: "The majority of Internet users are dangerously unaware of how exactly the law affects them on the Web. With ever greater numbers of people getting online, the Internet is no longer a cyber playground but a medium where users should be aware of legal constraints for their own safety."

The guide is available via e-mail by contacting legalguidenetsales.prestel.co.uk and Prestel hopes to put the publication on its website for downloading at http://www.prestel.co.uk ▶

New security group

The National Computer Security Association in the US has announced that it has formed a new group to monitor the Net and keep it crime free. Called the Internet Service Provider Security Consortium, the body hopes to protect the Net from attack, detect malicious activity and to quickly fix any cyberspace problems using the expertise of its members. CompuServe, IBM Global Internet and UUNET are among those involved. A spokesman for the group said: "This will increase our understanding of each others problems. All of this will contribute positively towards increasing security on the Internet."

The next meeting of the consortium will be on August 20 1997 in San Francisco. For more information contact Scott Markle by e-mail at smarkle@ncsa.com

Move to ban online gambling

Internet betting sites in the US could be shut down if a law making them illegal is passed by Congress. The bill would make web gaming a federal offence, punishable by a maximum fine of $20,000 and two years in prison. Under the terms, operators of similar sites in other countries who beam their services into the US would be targeted as well. And local and state law enforcement groups would be able to demand that telephone companies and Internet service providers pull the plug on the gambling pages.

Senator Jon Kyl, who is sponsoring the bill, said: "Society has always prohibited most forms of gambling because it can have a devastating effect on people and families and it leads to other crime and corruption if not strictly regulated."

Echoing this, senator Richard Bryan said: "The greatest danger posed by Internet gambling is that there is no way to control it and no way to regulate it. It is physically impossible for any state to regulate gambling on the Internet, and the only responsible choice Congress can make is simply to prohibit it."

Worry over web site

The US Department of Defense is keeping close tabs on who visits its Internet site in an attempt to stop hackers from getting access. In an announcement, the DoD said users of DefenseLINK, the official web site, were monitored and information gathered about their systems. A DoD spokesman said: "Computer vandalism has become an ever increasing problem over the past few years. Such attacks can lead to alteration of information used and trusted by millions of people. The Department is employing hardware and software programs to monitor network traffic. Such efforts will help to identify unauthorised attempts to upload or change information or otherwise cause damage."

Internet freedom in Hong Kong

The new Hong Kong government and Net service providers have pledged that the area will continue to enjoy electronic freedom of information.

In China such sites as Playboy and The New York Times are blocked, but officials from the Special Administrative Region government, which has taken over from the British, said that the current climate will not change. Hong Kong secretary for broadcasting, culture and sport Chau Tak-hay said: "Our position on political material carried on the Internet is based on the idea that there must be freedom of expression and speech. There will be a continuation of pre-existing policies."

President of the Hong Kong Internet Service Providers Association Daniel Ng said that most Net firms would err on the side of caution in order to preserve themselves. He said: "The problem lies more in self-censorship, because people don't want to do anything wrong. It seems like some people are more conservative than the Chinese officials."

The government had considered issuing personal identification numbers to adult users of pornographic Web sites, but in April this year the idea was dropped and the industry was allowed to regulate itself.

Emily Lau, whose Web page is critical of both Chinese and SAR politicians, said: "There is always this lurking concern that it will come, because the Chinese are very intolerant of freedom of expression. If it does come to pass, I don't think very many people will be surprised."

Junk e-mail targeted

Lawmakers in the US want to bring in tough controls to restrict the amount of unsolicited e-mail sent to computer users.

The US Congress is currently discussing two bills on how to control unwanted e-mails, with strict penalties and punishments for offenders being suggested. One law would give anyone receiving junk mail the right to $500 damages for each violation, and the other law would mean that all junk e-mail would have to be tagged as an advert so the user could filter it out if required.

The Federal Trade Commission says that junk e-mail not only causes extreme irritation to computer users but also can slow up the whole cyberspace system. And firms using false e-mail addresses are immune from any repercussions as they are effectively invisible. FTC commissioner Christine Varney said: "We will try to go after them and prosecute some fraud."

David Sorkin, professor at the John Marshall Law School in Chicago, said: "Unsolicited bulk e-mail is likely to become a much greater problem without effective regulatory or technical solutions. Governmental regulation that stops short of a complete ban would serve merely to legitimise unsolicited e-mail and is likely to make the problem worse.

"A legislative ban on unsolicited e-mail could be an effective means of addressing the problem, but only if the legislation is adopted in a similar or identical form in every relevant jurisdiction."

Clinton wants a clean Net for kids

President Clinton has called on the Internet industry to regulate itself by creating ▶

a system to stop youngsters getting access to undesirable material.

The move comes after the Communications Decency Act in the US was recently struck down as being unconstitutional, reducing legal control over the World Wide Web's content.

Now the White House wants a labelling system introduced which would restrict access to minors and alert parents and teachers of any adult content.

President Clinton said: "The Internet community must work to make these labels as common as food safety labels are today. We simply must not allow pornographers and paedophiles to exploit a wonderful medium to abuse our children."

Chairman of Internet service provider America Online Steve Case said: "We, and by that I mean all the people in the Internet industry, accept those challenges. We are right now delivering tools that empower families, neighbours and educators to limit and filter what can be seen by and sent to our children."

In a statement released by the White House, the US Government said that all steps were being taken to make sure that any illegal Web content was investigated and removed and those responsible taken to court.

It said: "The administration remains committed to the vigorous enforcement of federal prohibitions against the transmission of child pornography and obscenity over the Internet and other media, and the use of the Internet by paedophiles to entice children to engage in sexual activity."

The White House said that in response to concerns, the FBI has now increased by 50 per cent the number of staff investigating computer-related exploitation of children and has established a task force that specialises in computer child pornography and solicitation cases.

And it added that the US Customs Service has used the Internet to crack down on child pornography, with an increase in convictions from 35 in 1995 to 90 last year.

More information on software Net filters is available at www.netparents.org

Lawsuit over alleged scam

Telephone firm AT&T in the US is suing three companies for an alleged Internet scam that it reckons cost millions of dollars. The $7 million lawsuit against Connect America, parent company ICB Telecommunications, OneSource Communications and a number of individuals, charges the group with wire-fraud racketeering, civil conspiracy and violations of the Communications Decency Act. AT&T allege that it was defrauded when the fictitious accounts were set up for toll-free services and then sold on for profit to Internet service providers.

The firm says that when it restricted these accounts for non-payment or suspicious calling patterns, the group then established extra fraudulent accounts, substituting the restricted toll-free numbers with replacements.

AT&T said it uncovered the scam through a combination of improved telecommunications systems monitoring and solid investigative work. Vice president of law for AT&T's Business Markets Division Dan Stark said: "AT&T vigorously combats telecommunications fraud. We take swift and decisive action against all those involved, evidenced by this lawsuit."

Lawyers get into cyberspace

New technology will create whole new legal issues in the next few years according to experts and lawyers are being urged to start tackling them now.

The stark message came out of the American Bar Association's convention in San Francisco, where a host of topics were discussed.

Important legal questions included copyright on the Internet, patents on cyber-technology inventions, freedom of speech and computer crime.

John Gage, director of Sun Microsystems' science office, said the Internet era is in the same stage of development as the car industry early this century when there were no traffic restrictions or laws.

He said: "We've got to build the same legal environment for the Internet in the next few years that we did for cars over 70 years."

He added that as well as the infrastructure, phone companies' legal departments would have to look at the fact that the Internet can carry conversations and faxes at a much lower cost than traditional calls. "Don't think that what's expensive today will be expensive tomorrow," he said.

Roberta Katz, general counsel lawyer for Netscape Communications, said that the legal world would move slowly, but that lawyers had to be able to deal with issues raised by new technology.

She said: "This is a really scary time for us lawyers. Don't fear the technology changes or fear them if you must, but recognise that they're going to happen anyway. Here's to the future and here's to the lawyers who will help bring it about."

Internet Society's talk

The hottest topic at the moment is online censorship, according to the Internet Society which held a recent convention in Kuala Lumpur in Malaysia. One speaker said he had scanned more than 300,000 e-mails or discussion documents about the subject and reckoned that feelings in Asia were running high among the Net community.

In China Internet users were initially required to register with the police and about 100 Web sites were blocked, including those belonging to US media organisations.

Singapore filters the Net to get rid of pornography and other undesirable material, and in South Korea an Internet service provider can be ordered to delete and restrict material while Vietnam requires users to get a permit. Peng Hwa Ang, of Singapore Nanyang Technical University told the convention that governments in the area were beginning to loosen their restrictions. He said: "In every case I've seen, there's been a retrenchment from a previous position."

Larry Landweber, from the US, said at the conference: "If we try to control access at the government level, countries will not have full participation." ■

New security group

The National Computer Security Association in the US has announced that it has formed a new group to monitor the Net and keep it crime free. Called the Internet Service Provider Security Consortium, the body hopes to protect the Net from attack, detect malicious activity and to quickly fix any cyberspace problems using the expertise of its members. CompuServe, IBM Global Internet and UUNET are among those involved. A spokesman for the group said: "This will increase our understanding of each others problems. All of this will contribute positively towards increasing security on the Internet."

The next meeting of the consortium will be on August 20 1997 in San Francisco. For more information contact Scott Markle by e-mail at smarkle@ncsa.com

Move to ban online gambling

Internet betting sites in the US could be shut down if a law making them illegal is passed by Congress. The bill would make web gaming a federal offence, punishable by a maximum fine of $20,000 and two years in prison. Under the terms, operators of similar sites in other countries who beam their services into the US would be targeted as well. And local and state law enforcement groups would be able to demand that telephone companies and Internet service providers pull the plug on the gambling pages.

Senator Jon Kyl, who is sponsoring the bill, said: "Society has always prohibited most forms of gambling because it can have a devastating effect on people and families and it leads to other crime and corruption if not strictly regulated."

Echoing this, senator Richard Bryan said: "The greatest danger posed by Internet gambling is that there is no way to control it and no way to regulate it. It is physically impossible for any state to regulate gambling on the Internet, and the only responsible choice Congress can make is simply to prohibit it."

Worry over web site

The US Department of Defense is keeping close tabs on who visits its Internet site in an attempt to stop hackers from getting access. In an announcement, the DoD said users of DefenseLINK, the official web site, were monitored and information gathered about their systems. A DoD spokesman said: "Computer vandalism has become an ever increasing problem over the past few years. Such attacks can lead to alteration of information used and trusted by millions of people. The Department is employing hardware and software programs to monitor network traffic. Such efforts will help to identify unauthorised attempts to upload or change information or otherwise cause damage."

Internet freedom in Hong Kong

The new Hong Kong government and Net service providers have pledged that the area will continue to enjoy electronic freedom of information.

In China such sites as Playboy and The New York Times are blocked, but officials from the Special Administrative Region government, which has taken over from the British, said that the current climate will not change. Hong Kong secretary for broadcasting, culture and sport Chau Tak-hay said: "Our position on political material carried on the Internet is based on the idea that there must be freedom of expression and speech. There will be a continuation of pre-existing policies."

President of the Hong Kong Internet Service Providers Association Daniel Ng said that most Net firms would err on the side of caution in order to preserve themselves. He said: "The problem lies more in self-censorship, because people don't want to do anything wrong. It seems like some people are more conservative than the Chinese officials."

The government had considered issuing personal identification numbers to adult users of pornographic Web sites, but in April this year the idea was dropped and the industry was allowed to regulate itself.

Emily Lau, whose Web page is critical of both Chinese and SAR politicians, said: "There is always this lurking concern that it will come, because the Chinese are very intolerant of freedom of expression. If it does come to pass, I don't think very many people will be surprised."

Junk e-mail targeted

Lawmakers in the US want to bring in tough controls to restrict the amount of unsolicited e-mail sent to computer users.

The US Congress is currently discussing two bills on how to control unwanted e-mails, with strict penalties and punishments for offenders being suggested. One law would give anyone receiving junk mail the right to $500 damages for each violation, and the other law would mean that all junk e-mail would have to be tagged as an advert so the user could filter it out if required.

The Federal Trade Commission says that junk e-mail not only causes extreme irritation to computer users but also can slow up the whole cyberspace system. And firms using false e-mail addresses are immune from any repercussions as they are effectively invisible. FTC commissioner Christine Varney said: "We will try to go after them and prosecute some fraud."

David Sorkin, professor at the John Marshall Law School in Chicago, said: "Unsolicited bulk e-mail is likely to become a much greater problem without effective regulatory or technical solutions. Governmental regulation that stops short of a complete ban would serve merely to legitimise unsolicited e-mail and is likely to make the problem worse.

"A legislative ban on unsolicited e-mail could be an effective means of addressing the problem, but only if the legislation is adopted in a similar or identical form in every relevant jurisdiction."

Clinton wants a clean Net for kids

President Clinton has called on the Internet industry to regulate itself by creating ▶

a system to stop youngsters getting access to undesirable material.

The move comes after the Communications Decency Act in the US was recently struck down as being unconstitutional, reducing legal control over the World Wide Web's content.

Now the White House wants a labelling system introduced which would restrict access to minors and alert parents and teachers of any adult content.

President Clinton said: "The Internet community must work to make these labels as common as food safety labels are today. We simply must not allow pornographers and paedophiles to exploit a wonderful medium to abuse our children."

Chairman of Internet service provider America Online Steve Case said: "We, and by that I mean all the people in the Internet industry, accept those challenges. We are right now delivering tools that empower families, neighbours and educators to limit and filter what can be seen by and sent to our children."

In a statement released by the White House, the US Government said that all steps were being taken to make sure that any illegal Web content was investigated and removed and those responsible taken to court.

It said: "The administration remains committed to the vigorous enforcement of federal prohibitions against the transmission of child pornography and obscenity over the Internet and other media, and the use of the Internet by paedophiles to entice children to engage in sexual activity."

The White House said that in response to concerns, the FBI has now increased by 50 per cent the number of staff investigating computer-related exploitation of children and has established a task force that specialises in computer child pornography and solicitation cases.

And it added that the US Customs Service has used the Internet to crack down on child pornography, with an increase in convictions from 35 in 1995 to 90 last year.

More information on software Net filters is available at www.netparents.org

Lawsuit over alleged scam

Telephone firm AT&T in the US is suing three companies for an alleged Internet scam that it reckons cost millions of dollars. The $7 million lawsuit against Connect America, parent company ICB Telecommunications, OneSource Communications and a number of individuals, charges the group with wire-fraud racketeering, civil conspiracy and violations of the Communications Decency Act. AT&T allege that it was defrauded when the fictitious accounts were set up for toll-free services and then sold on for profit to Internet service providers.

The firm says that when it restricted these accounts for non-payment or suspicious calling patterns, the group then established extra fraudulent accounts, substituting the restricted toll-free numbers with replacements.

AT&T said it uncovered the scam through a combination of improved telecommunications systems monitoring and solid investigative work. Vice president of law for AT&T's Business Markets Division Dan Stark said: "AT&T vigorously combats telecommunications fraud. We take swift and decisive action against all those involved, evidenced by this lawsuit."

Lawyers get into cyberspace

New technology will create whole new legal issues in the next few years according to experts and lawyers are being urged to start tackling them now.

The stark message came out of the American Bar Association's convention in San Francisco, where a host of topics were discussed.

Important legal questions included copyright on the Internet, patents on cyber-technology inventions, freedom of speech and computer crime.

John Gage, director of Sun Microsystems' science office, said the Internet era is in the same stage of development as the car industry early this century when there were no traffic restrictions or laws.

He said: "We've got to build the same legal environment for the Internet in the next few years that we did for cars over 70 years."

He added that as well as the infrastructure, phone companies' legal departments would have to look at the fact that the Internet can carry conversations and faxes at a much lower cost than traditional calls. "Don't think that what's expensive today will be expensive tomorrow," he said.

Roberta Katz, general counsel lawyer for Netscape Communications, said that the legal world would move slowly, but that lawyers had to be able to deal with issues raised by new technology.

She said: "This is a really scary time for us lawyers. Don't fear the technology changes or fear them if you must, but recognise that they're going to happen anyway. Here's to the future and here's to the lawyers who will help bring it about."

Internet Society's talk

The hottest topic at the moment is online censorship, according to the Internet Society which held a recent convention in Kuala Lumpur in Malaysia. One speaker said he had scanned more than 300,000 e-mails or discussion documents about the subject and reckoned that feelings in Asia were running high among the Net community.

In China Internet users were initially required to register with the police and about 100 Web sites were blocked, including those belonging to US media organisations.

Singapore filters the Net to get rid of pornography and other undesirable material, and in South Korea an Internet service provider can be ordered to delete and restrict material while Vietnam requires users to get a permit. Peng Hwa Ang, of Singapore Nanyang Technical University told the convention that governments in the area were beginning to loosen their restrictions. He said: "In every case I've seen, there's been a retrenchment from a previous position."

Larry Landweber, from the US, said at the conference: "If we try to control access at the government level, countries will not have full participation." ■

Product News

Tracking and auditing program

Attest Systems, a developer of asset management software, has launched a new version of its tracking and auditing package. The program, called GASP 4.0, runs on PCs using Windows 3.1x, 95, NT or IBM OS/2 and uses a graphical interface to look at owned licenses, software profiles and year 2000 compliance. It can also uncover unwanted graphics and other files downloaded from the Internet and its makers say that companies can see cost savings by eliminating fees paid for software that is either no longer installed or already licensed.

President of US firm Attest Systems Herbert Gottlieb said: "With this new version, it is easier than ever to protect a business from the problem of unwanted and potentially costly software, graphics, fonts and other files within their computer environment. GASP can detect any attempt employees may make to disguise the programs on their computers in hopes of circumventing the process of inventory software.

"This high degree of accuracy gives companies the confidence that they can find illegal software, including the possible legal problem of employee downloaded pornographic files, when they audit their PCs."

GASP is also available for Apple Macintosh computers and is used by the Business Software Alliance and Microsoft for detecting software piracy.

Attest Systems can be contacted at (US) 800 471-4277, by e-mail at info@gasp.com, or at the firm's web site at http://www.gasp.com

Forensic investigation programs

Computer Forensics in the UK has launched a suite of new programs designed to help investigators retrieve important evidence. The firm, which supplies the DIBS® imaging system to law enforcement and commercial investigators, now has an extended software range with tools to find and extract data.

Included in the Computer Forensic Laboratory is a floppy disk investigator, a search engine, a slack space viewer and a cluster analyser which can draw a cluster "map" of a hard drive.

Managing director of Computer Forensics Peter Verreck said: "This software is a major tool for anyone investigating computer crime. It greatly speeds up and simplifies the process of analysing and investigating suspect data.

"Designed for investigators, the programs are easy and intuitive to use and have been developed in response to the unique requirements of computer forensic investigations. Often computer data is hidden or not easy to find, and information retrieved using these special programs can make all the difference in an investigation and prosecution."

The CFL starter kit, containing all four programs, costs £450 plus VAT.

Computer Forensics can be contacted on (UK) 01903 823181, e-mail at info@computer-forensics.com or the firm's web site at http://www.computer.forensics.com

Security video

Pattern recognition firm Neurodynamics has launched a video image recording and playback technology aimed at helping security surveillance. The system, called Witness, uses digital recording on DAT and its makers say it provides high-quality pictures that are ideal for detecting fraud and robbery involving bank cashpoints. Data from cameras can be transmitted over normal phone lines and Neurodynmanics says Witness can record for up to six days before tape changes.

Neurodynamics can be contacted on (US) 201 364 0010 or e-mail at pjr@neurodynamics.com

AOL reins in Trojan Horses

Internet service provider America Online is fighting the threat of computer hackers by introducing an automatic warning program for e-mail users.

The Download Sentry system is designed to counter illegal programs, called Trojan Horses, which can capture passwords on a user's machine and e-mail them back to hackers, giving access to private accounts or files.

AOL said that some of these programs can also damage the victim's hard disk and could also contain undesirable files and pictures.

An AOL spokesman said: "The Download Sentry will pop up when a subscriber attempts to download an e-mail with one of the types of file attachments associated with Trojan Horse programs."

Singapore Internet Security firm

A new company has been set up in Singapore aimed at making sure commercial transactions on the Net are secure. The government's National Computer Board, together with Network for Electronic Transfers Pte Ltd, has set up Netrust to provide so called digital signatures that verify sender and receiver identities and keep communications private.

CompuServe limits child access

Internet service provider CompuServe has announced it will put adult material into special online areas that need passwords to stop children getting access.

The firm, which has 5.4 million customers worldwide, does not carry pornography, but does provide adult-orientated chat rooms, games and other material that might be considered risque. Users will now need a password to enter certain areas and the service provider will use its own records to try to confirm ages.

CompuServe spokesman Steve Conway said: "This isn't foolproof, but it's a start. All online services are trying to put controls and safeguards on adult-orientated material."

Meanwhile service provider Prodigy has cut access to child pornography newsgroups ▶

which allowed paedophiles to talk with each other and swap illegal material.

Prodigy spokesman Mike Darcy said: "We have no intent on monitoring all of the Internet newsgroups for child pornography, but if a newsgroup in question was created specifically to spread child pornography, we will not store it on our servers because it is against the law to distribute it."

Lawyers on e-mail

An Internet information service for the legal profession has launched a new service linking up thousands of lawyers by e-mail.

The Martindale-Hubbell Lawyer Locator web page, which gets more than 10,000 "hits" a day, now allows direct communication with law firms and individuals as well as providing other resources. Publisher and chief operating officer of Martindale-Hubbell Louis Andreozzi said: "The activated e-mail links for more than 125,000 lawyers, with more than 16,000 outside the US, instantly creates the largest e-mail directory of attorneys in the world."

The website can be viewed at http://www.martindale.com

Off-site data protection

A new service has been launched for small businesses to store valuable data automatically without the hassle of tapes or monitoring.

US firm @Backup sets up systems so it can encrypt and transfer data over a modem to a separate location each night. The firm says lost files can be retrieved in minutes and with a total data loss, information can usually be restored within a day. The service costs $19.95 a month. Options offered range from nightly virus detection to a twice yearly CD ROM containing all a firm's data.

Chief executive officer of @Backup Gary Sutton said: "20 million small offices rely on personal computers. About eight per cent have a secured backup procedure. And 80 per cent of all tape backups fail when needed, often with catastrophic results to the business."

@Backup can be contacted on (US) 800 538 2000 or by its web site at www.atbackup.com

New data capture system

UniRom Technologies has launched a document imaging machine that combines both digital and microfilming techniques to reduce paper filing.

The AIM 4300 system, which costs $40,000, is a scanner capable of a 60 page per minute rate while simultaneously producing a microfilm backup for long term storage. It is designed at cutting a firm's need for mass storage and can process documents ranging in size from cheques to legal sized papers.

Contact (US) 888 226 0020 or e-mail unirom@aim-inc.com

Information service for lawyers

Information providing service Lexis-Nexis has launched a web-based interactive resource for the legal profession. The Xchange service provides a single Internet location that can be used to securely send documents, get the latest legal and general news and access a legal database that has more than one billion documents.

Ira Siegel, president of Lexis-Nexis, said: "This will provide legal professionals with a single site on the world wide web where they can find the information to answer essentially any practice related question, a location each legal professional can tailor to their individual information needs."

More information about the service can be found at the web site at www.lexis-nexis.com

Search for missing children

Internet service provider America Online has launched a program designed to locate abducted or missing children. The idea, called Kid Patrol, works like a digital milk carton according to AOL and posts emergency alerts with photos and information about missing youngsters during the first 36 hours after a disappearance.

AOL chairman Steve Case said: "We're taking the millions of eyes that scan our services daily and are trying to make the faces of missing children familiar to them. The 36 hours after a report is made are the most critical in the search for missing children. We're tapping the immediacy of this interactive medium to enable our members to help these kids get back home."

Network security checkup

US firm Navigist has launched a security review service for businesses to cut down on the risks from unauthorised entry. The Network Security Review includes a look at existing procedures, equipment and potential flaws and ends with a mock hacking attack by Navigist's experts to test the level of penetration defence. Costing $4,000, the full service is aimed at preventing rather than curing hackers, who can cost companies millions in fraud or lost revenue.

Navigist can be contacted on (US) 408 437 3190 or by e-mail at info@navigist.com

Backup data on mobile phones

Users of "smart" mobile phones in Finland will be able to backup information remotely over the airwaves.

Telecom Finland Ltd and phone software firm Geoworks have teamed up to offer the service for GSM phones, including the Nokia 9000 Communicator. Virtually any data can now be stored on some phones, and police across the world have found evidence retrieved from them useful in investigations.

President of US firm Geoworks Gordon Mayer said: "This collaboration will create a valuable offering for users of GSM smart phones who want to safeguard important personal information such as their e-mail, faxes, appointment calendars and address books." ■

CD-ROM v. Optical Disks

A recent question to the Journal asked about the relative merits of collecting potentially evidential material onto CD-ROM or rewritable optical media.

We thought that on the face of it there seemed no question that CD-ROM was better - it was both cheaper to use and its read only capabilities provided obvious protection against deliberate or accidental alteration.

However, commercial copying devices offering both methods are available in the UK and it appears that systems using rewritable media are much more widespread than their CD-ROM counterparts within the various UK Police Forces, which, after all, require the most stringent adherence to forensic principles and have the tightest budgetary controls. We decided that this needed deeper investigation so we spoke to a number of people with professional expertise in both CD-ROM and optical disk technology and discovered some quite surprising things.

The Technologies

CD-ROM technology was originally developed for sound recording as a better quality alternative to the long playing vinyl records, and the current standard CD will contain about 74 minutes of digitally recorded audio material. The recording process is like a long playing record in that a spiral track consisting of a sequence of microscopic "pits" and "lands" actually contains the data.

Audio CDs are produced by pressing a master onto a metal foil coated disk and then covering the result with a protective coating of hard, transparent plastic lacquer. The recording is played back by focusing a low power laser beam onto the spiral track such that disk rotation causes the pits and lands to produce a variation in the reflection of the beam. It is this reflection that is sensed and electronically converted into the high quality sound that we are familiar with.

The disks themselves are more robust than the old vinyl disks because there is no physical contact with the surface during playback and much better quality because there is no physical vibration like the stylus pickup. The electronic arrangements are also more convenient because individual track selection is achieved electronically rather than by manually repositioning a pickup head. So far, so good.

However, CDs are nothing like as robust as the various vendors would have us believe. Fingermarks and minute scratches on the plastic surface can cause degradation and corruption of the audio signal. Such defects would usually cause little interference to our enjoyment of the sound because of their transient nature and the fact that the digital signal is grown into an analogue one for audio purposes. Larger defects will obviously cause more noticeable effects but still the digital to analogue conversion, both electronic and aural will smooth most of them out.

As computer technology progressed, some enterprising soul decided that the CD presented an excellent mass storage medium - the 74 minutes of audio translates into around 600MB of digital information - so the CD-ROM was born. Once again, the advantages were obvious - the disks were cheap to produce and could hold the huge amounts of data that advanced programs required. However, the potential for surface defects could no longer be considered a negligible problem.

Quite obviously the manufacturers and distributors of CD-ROM disks play down this negative view of their products because it is contrary to their own marketing interest. What is apparent is that the commercial CD-ROM disk is a very fragile animal. Its useful life is seriously dependent upon the handling that it receives, even sliding it gently in and out of a plush holder can cause micro-scratches that may produce digital errors when the disks are read by a computer.

The ubiquitous CD cases are designed to store the disks with minimum contact to the recorded surface. Even so, the potential for error is still small and there is no doubt that CD-ROMs are here to stay. Unfortunately however, the next step in CD-ROM development introduced a far greater potential for error. This was the introduction of the CD-R media - which were recordable CDs that could be written to by CD-ROM "burner" drives. In this case the digital information could be recorded by a higher power laser which burned appropriate pits into the blank spiral track.

This means that CD-R disks are not pressed like their mass produced CD-ROM cousins as both the substrate and the protective coating are substantially different (and more fragile). So any micro-defects on the surface of CD-R media may cause errors both during the burn phase and when being digitally read.

Those who regularly burn in CD-R disks indicated practical failure rates ranging from 5 per cent to 12 per cent. For normal archival use this level of failure is not a serious problem, if a disk fails to verify after burning, it is relatively trivial to throw it away and burn a new one. However this has important consequences when considering the forensic requirements as mentioned later.

Another interesting aspect of CD-R disks is that the continuous spiral nature of the technology means that information has to be burned in a continuous stream rather than in the discrete addressable blocks used on magnetic disks. So it is up to the processing program to ensure that the data buffer of the CD-R burner is kept full during the burn. This is fine if data access to the source is both fast and error free but it may cause problems if the data cannot be retrieved fast enough to ▶

keep the burner buffer full.

CD-R burner software usually anticipates this problem by providing a drive profiling facility whereby the source drive (usually a magnetic fixed disk) is read and checked for data transfer rate and possible errors before a burn is attempted. It should also be noted that the need for a continuous burn precludes any possibility of verifying data as it is written; verification must take place after the burn has been completed.

This need to maintain a continuous stream of data is obviously a considerable drawback so a more recent development introduced the multi session CD. This refers to a system whereby information can be recorded in several interrupted actions (sessions) if required, even on different drives.

Each session can contain information according to one of the CD standards (ISO, XA, DA, etc.) and the data in different sessions can be linked, ie a newer session can refer to data in an older session. A true Multi Session CD-ROM reader will automatically go to the last session and present all linked sessions as one; the user will not be aware of the number of sessions on the disk.

A variation on this principle produces a multi volume disk. This has an important difference: each session or volume on the disk has no reference to another volume and each volume is seen as a separate CD; similar in some ways to the partitioning of magnetic disks. At the moment, multi session and multi volume disks introduce an overhead of around 15 megabytes per session so the drawbacks still exist.

A still newer development which is not yet available, will be known as incremental write. This involves dividing each track into data packets such that each packet can be written separately to the disk. The ISO 9660 standard for CD-R disks (introduced in 1988) does not support incremental writes and so a new (European) standard, ECMA 168, has been introduced which is an extension of ISO 9660 and contains descriptions of the enhancements needed to support incremental write. The overhead in this case will depend upon the packet size - for example a 64Kb packet will have an overhead of around 10Kb (around 15 per cent). Most CD-ROM readers currently available can not read an incrementally written disk and Incremental Writing is not yet supported by CD-R Recorders.

We also learned that CD-ROM disks are not unalterable. The burning process mentioned above is controlled by the relevant software and this will not attempt to re-burn a used part of the disk. However, there is no technical reason to prevent the burner from re-burning an area containing data although the effect would be to add new pits rather than to rewrite the overall pattern. Nevertheless, the potential exists for data to be deliberately corrupted and this has obvious forensic implications.

Rewritable optical media (known as OPT-R)

OPT-R disks were developed right from the start for use by digital computers and the early technology made use of a material which was like tiny magnets embedded in plastic. The direction in which these magnets pointed could be changed if the plastic was softened, so a system was developed which softened the plastic with a medium power laser beam and then flipped the magnets with a series of pulses through a magnetic write head similar to that used in magnetic disk drives. Unfortunately, unless all the magnets had already been aligned in a specific direction, the reliability of the flipping process was questionable. This was overcome by providing a two pass approach - as the disk rotated, the first pass aligned all the magnets in one direction and then the second pass flipped some of them to record the digital pattern of information. This became known as magneto-optical technology and although it was quite reliable, it was relatively slow because of the need for two passes.

The next development was based upon a different material which had the property of existing in two different physical states (or phases). This stuff could either be crystalline or amorphous - when crystalline it was extremely reflective, when amorphous it was dull and non-reflective. The phase of the material could be changed by heating it to pre-specified temperatures. If heated to near liquidity and then allowed to cool it became crystalline, if heated only to a semi-solid state, it cooled into the amorphous phase.

This was coated onto the surface of a disk and the heating process was controlled by a tri-power laser beam. Thus during a write process, the laser would alternate between high power (to switch to the crytalline phase) and medium power (to switch to the amorphous phase). The third - low - power level of the laser was used to read the recorded information by responding to the reflectivity without changing the existing phase. This system became known as phase-change technology and it could overwrite existing information without the need for two passes.

A more recent development in the magneto-optical field has produced a slightly different media (known as Direct OverWrite or DOW) which does not need the two pass approach. As with CD-R disks (although less so), the surface of both types of optical disk is sensitive to grease and scratches which can cause errors during both the read and write processes. However, probably because they were developed for accurate digital use in the first place, both magneto-optical and phase-change optical disks are supplied in protective cases with auto-activating shutters that protect the surfaces against mishandling. As discussed below, any errors are handled on an individual basis and no one that we spoke to could remember any errors on optical disks in normal use nor any disks being rejected as unusable.

Accessing the Data

As mentioned above, CD-R technology records the information in a continuous stream onto a spiral track. In keeping with the original audio idea, locating any particular section on a disk is done by timing. For example, if the spiral track on a 74 minute CD had 74 loops, then each loop would represent one minute's worth of recording. If the laser head was positioned, say 30/74ths of the radius in to the disk, reading would begin some 30 minutes into the recording. This is quite accurate enough for audio recording but ▶

may cause noticeable delay when accessing digital information.

Obviously this situation will change when the incrementally written disks come into service. Both types of optical disk use a completely different physical layout where the information is recorded in a series of concentric circles. Each circle is divided into a number of sectors and each sector contains a pre-specified number of bytes. So with these disks, information can be accessed by providing a track and sector number exactly as is done with magnetic disks. The rate at which data can be recovered from disks is also an important consideration. Optical drives typically offer around 3 Mb/s (megabytes per second) and CDs were originally designed to produce a data transfer rate of 153KB/s (kilobytes per second). This huge difference has been offset somewhat by the introduction of drives capable of spinning the disk faster. Thus drives running at twice, four times and even twelve times faster are now available, although a little simple arithmetic shows that these are still considerably slower than optical drives. Similarly the speed at which CD-Rs can be written has been improved up to four times although the faster speed may increase the incidence of error and modified media is now available to offset this problem.

Writing the Data

The electromagnetic environment in which most of us live is extremely cluttered and it will give rise to occasional surges. Even with the best screening and protection, such surges are a fact of life and modern computers are designed to detect and correct any errors which may appear as a result. It is relatively simple to arrange that information being stored onto magnetic media is checked for errors as it is written. Any errors can then be corrected by rewriting as and when required. Optical drives operate in a similar way and each block written can be verified before proceeding and rewritten in the event of an error. Any defects on the media are handled by relocating the data to a reserved area of the disk and noting the fact in a relocation table. This is totally transparent to the user who is not aware that a particular block may have been relocated. Current CD-R technology cannot do this; data can only be verified after the burn phase has been completed and any errors mean that the disk is effectively useless and should be discarded.

Forensic Implications

The major problem when copying potentially evidential computers is that their capabilities are initially unknown. Internally the disk drive may be slow and there may be errors that will slow down the rate at which data can be recovered. In addition the investigator will not know the speed of an available interface (usually the parallel port is used with an appropriate translation adaptor). Optical drives will accept data up to several megabytes a minute but as noted above, the minimum speed requirements of CD-R burners make it impossible to guarantee a direct copy process.

This problem has apparently been overcome in at least one UK copying device by providing an intermediate magnetic drive on which to collect the data before it is streamed out to the CD-R disk. Although at first sight this seems technically acceptable, a number of informed police officers have expressed reservations about this process from a legal point of view. They feel that some enterprising defence barrister may suggest that the intermediate disk should be considered as unused material which would mean that it must be available for legal disclosure.

They are also concerned that if the intermediate drive is not positively wiped of all information between copies, defence counsel may suggest the possibility of contamination between machines. These are both legal questions and only time and actual cases will decide the issues.

The actual speed of copying will depend almost solely upon the throughput capability of the interface. While it is possible to write two CD-R disks virtually simultaneously (from the same buffer full of information) this gain in speed will be more than offset by the need to verify each CD separately. It seems that the verification required by CDs is the major difficulty. As noted above, the verification of a CD can only be achieved after the burn has been completed. Thus to verify the data, the fixed disk will need to be read again and compared with the content of the CD. The verification between the suspect drive and an intermediate drive will probably be completed on the fly, as it is when writing to ordinary optical media. The data paths within each copying process can therefore be summarised as follows:

Optical media

Suspect drive - Interface - Optical Media: read optical media for verification with existing information from suspect drive.

CD-R Media

Suspect drive - Interface - Intermediate Drive - CD-ROM: read CD-ROM and intermediate drive for verification.

What About the Costs?

Costs will obviously vary considerably between countries so we present here only approximate known costs in the UK There are two costs to be considered - the capital cost of the drives, interfaces and controlling software, and the ongoing media costs. Let's look at CD first .

A 4X write and 4X read CD-ROM drive currently costs around £500 and the disks are available in varying qualities from around £4.50 to £5.50 each. At a usable 600 Mb, this represents between 75 and 91 pence per 100 megabytes.

A magneto-optical drive will cost around £1000 and the disks cost between £35 and £60 each. At a usable 2.6Gb, this represents between £1.34 and £2.30 per 100 megabytes.

Phase-change optical drives cost around £1500 and the 1.5Gb disks cost around £80 or so - equivalent to about £5.33 per 100 megabytes.

Conclusions

The practical requirements dictated by forensic considerations are so fundamental that current CD-ROM technology cannot be considered as a serious option for the primary collection of data.

The initial costs are comparable since a CD system capable of writing two copies at virtually the same time will require two drives. ▶

The convenience of the CD system is undeniable since most machines now come equipped with CD drives as standard. However, the possibility of errors, the sensitivity of the media to handling and the added complexity of the copying process with an intermediate drive does not justify the saving in cost or the marginal advantages of convenience.

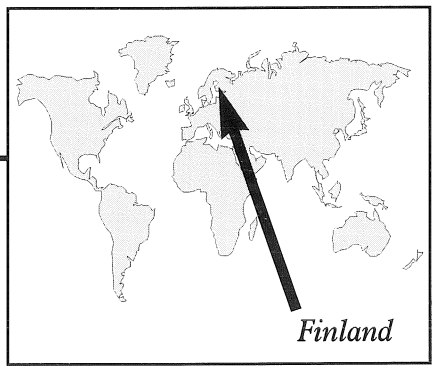
CD costs have remained fairly static for some years now whilst the costs of both drives and media in optical disk technology are steadily reducing. The difference in media cost has reduced dramatically within the last year and look set to fall further. It must also be remembered that rewritable media is re-usable whereas CDs are not.

On the other important consideration - time taken to complete a forensically sound copy - there seems little difference. Although the longer verify cycle on CD-ROM will increase the copy time, both processes are limited by the throughput capabilities of the interface and even at its best this does not approach the maximum write speed of either CD-R or Optical drives. CD-R may gain slightly if multiple copies are required because of its ability to create two CDs from a single read of the suspect drive. However, the advantage is almost completely lost by the need for separate verification of each CD after the event and the effects of a disk error rate between five per cent and 10 per cent.

The introduction of internal integrity verification makes two copies unnecessary. If this is applied to CD-R devices it makes the initial cost less but applied to optical devices it produces a reduction in copying time to well below that of CDs. CD-ROM devices certainly have their place as part of an archival system and are valuable when used in a controlled environment that will limit the effects of errors.

This makes them ideal for the second stage copying of evidential material for disclosure and/or archive purposes. For preliminary copying with security and speed and with ongoing costs now comparable to CD-R, there is no doubt that optical technology is the way forward. ■

Finland



Finland has one of the most technically advanced societies in Europe and computers for most people are as much a part of everyday life as the television. The potential for computer crime is huge, so unsurprisingly the Finnish police are at the forefront of investigation. Paul Johnson went to Helsinki to see how the computer crime unit is set up.

From the moment you step off the plane, it is obvious that the Fins take their technology very seriously indeed. Nearly everyone has a phone pressed against their ear so it is unsurprising to find out that the country has the world's highest ownership and use of mobile telephones.

Finland covers a huge geographical area but has only a relatively small population at just five million, with about 900,000 living in the Helsinki metropolitan area. About a quarter of the country is above the arctic circle and some of the towns and villages are extremely remote, making communication and travel difficult.

While the rest of Europe slowly comes to terms with computers, Finland has already fully embraced the microchip. An estimated one in three homes already have PCs, and nearly all Fins are adept at using computers for work or leisure.

And the Fins also lead the world in the number of Internet connections per person, with a recent survey showing that out of every 1,000 people in Finland, 75.83 are connected to the Net, a figure higher than in any other country and twice as high as in the US.

But this level of technology also brings with it an increased potential for criminals to use computers both directly and indirectly. The Finnish police are at the forefront of investigation into technology crime and are constantly developing new techniques and equipment to further increase their ability.

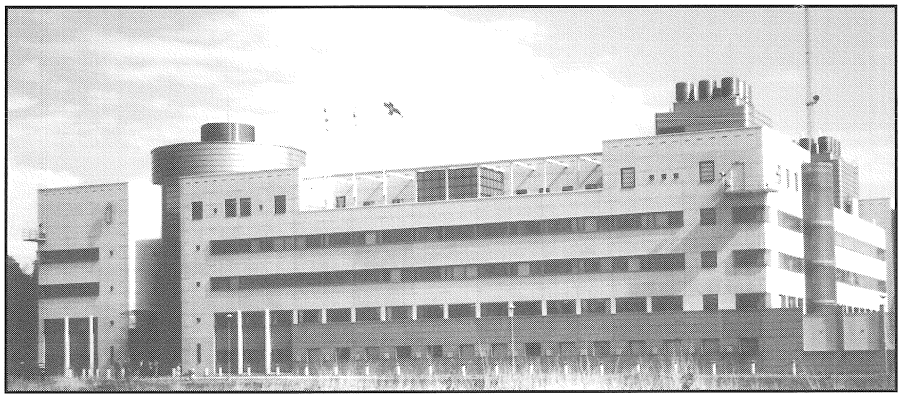
Currently the computer crime unit is centralised at the National Bureau of Investigation's imposing headquarters in Vantaa, a suburb of Helsinki. The huge fortress-like building houses the various Bureau departments and has such tightly controlled security that no one without the correct authorisation or smart card can either get in or pass through the various interior doors.

The Bureau investigates crimes in which computers are used both directly and indirectly, either to commit the actual offence or store evidence about it, and these investigations are split into two departments.

There are three officers in the dedicated direct computer crime group and eight in the other unit, although they share many of the ideas, techniques and equipment used in finding and presenting evidence.

Detective sergeant Jukka Makynen, together with a detective constable, unravels the data trail from the cases he is working in a small room on the second floor. Only the high-tech Pentium 200 system and large 21-inch monitor give any indication that this is anything other than a normal office. Once suspect data has been successfully copied, Jukka transfers it to his own computer for proper investigation and analysis.

His workstation is also connected to a police network which can handle an incredible number of law enforcement related tasks. It hooks up to the central police computers and databases and among its functions it can give instant information on known criminals, vehicle registration plates, inter-office communications and also has an online law reference facility. And using the system every one of the 9000 policemen in Finland is connected up by e-mail, greatly speeding up communications and ▶



Headquarters of the National Bureau of Investigation, Helsinki, Finland.

investigations.

But while many police forces elsewhere in the world would be envious of the Finnish set up, Jukka says there is still not enough investment made in tackling computer crime.

He said: "At the end of the day it comes down to money. It seems that just about every police force in the world has the same sort of problems. We want to do as much as we can, but our job is made extremely hard because of budget limits. There is not enough money to buy the right equipment or to have enough people working on computer crime investigations.

"We have all kinds of cases. With such a high level of computer use in this country we have a relatively high workload. It depends on the case, but you never know what you're going to find.

"While we mostly investigate PCs and Macintosh computers, we also look at personal organisers such as the Psion, which can often contain important data in a case. And a suspect's mobile phone can also be vital in an investigation as these often hold large address books full of phone numbers."

Because of the geography of Finland, Jukka and his team often have to work hundreds of kilometres away from base.

"At the moment we are involved in work right across the country. This can be quite hard because of the great distances involved," he said. "Many of the areas are very rural and inaccessible. It can be extremely frustrating if we travel to examine a suspect's computer but then discover that we need additional equipment and have to come back to Helsinki to get it.

"To solve this we're hoping to set up regional centres for computer investigation, although the hardest and most serious crimes will still be investigated from the headquarters here.

At the time Jukka was working on more than half a dozen cases, most of them involving alleged hacking into other computers.

He warned about the need to get the police force fully trained and aware of computer investigations.

He said: "Most police in Finland don't fully understand computers so when they go into a suspect's home and see a computer they will just switch it on. This can be extremely dangerous as it means important data can be lost, especially if the suspect has set a trap which wipes information.

"It's very important to educate law enforcement groups, even those who aren't going to be working much with computers. They all use computers but they need to know a lot more about the role of computers and crime."

But Jukka said that Finland's laws on computer related crime and evidence fare better than some other countries which have not specifically addressed the issue.

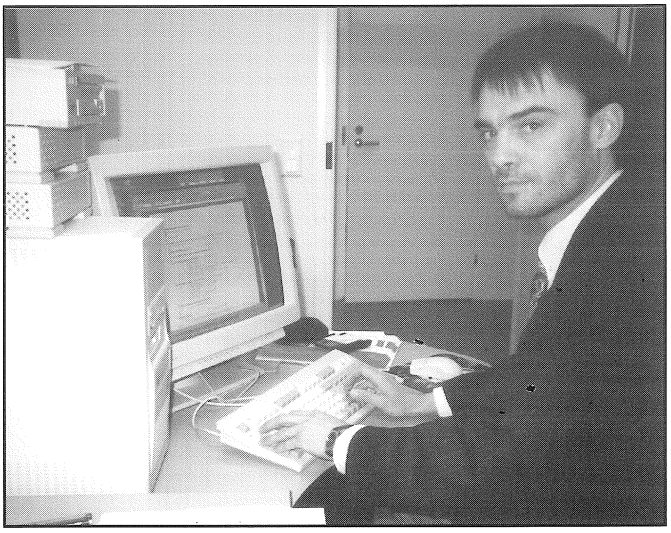
"The main law which covers this was made in 1889. But due to recent changes, the law now takes the modern situation into account quite well.

"While it's important that all the evidence from a computer is retrieved and presented as effectively as possible, it doesn't seem as important or full of problems as in other countries. Here, if you do something wrong it doesn't mean the case will be thrown out. You may get into trouble but the evidence is still the evidence."

Jukka has been on the force for 11 years and over this time he has been involved in five different jobs, with his current one starting in July last year. Unlike many police forces in many other countries, Finland does not operate a tenure system.

Jukka said: "I may well do something different at some point, but at least I can concentrate on computer crime at the moment knowing I won't have to move on unless I want to. This has the advantage that I can build up my knowledge and experience of computers rather than have someone new start from scratch.

"Lack of time is our biggest problem. There's only 24 hours in a day and we're constantly working on several things at once. Computer crime is growing all the time. Everyone has to be aware of it, especially the police." ■



Det. Sgt. Jukka Makynen at his desk.

Cyberlaundering :

Anonymous Digital Cash and Money Laundering *By* Mark Bortner

Part I Humble Beginnings

In the beginning, laundering money was a physical effort. The art of concealing the existence, the illegal source, or illegal application of income, and then disguising that income to make it appear legitimate required the launderer to have the means to physically transport the hard cash. The trick was, and still is, to avoid attracting unwanted attention, thus alerting the Internal Revenue Service (IRS) and other government agencies.

In this "lo-tech" world of money laundering, the process of cleaning "dirty money" was limited by the creative ability to manipulate the physical world. Other than flying cash out of one country and depositing it in a foreign bank with less stringent banking laws, bribing a bank teller, or discretely purchasing real or personal property, the classic approach was for a "smurf" to deposit cash at a bank.

Essentially, platoons of couriers assaulted the lobbies of banks throughout the US with deposits under the $10,000 reporting limit as required under the Bank Secrecy Act. The result was the formation of a serious loophole under the Bank Secrecy Act, allowing couriers almost limitless variables in depositing dirty money such as the number of banks, the number of branch offices, the number of teller stations at one branch office, the number of instruments purchased, the number of accounts at each bank, and the number of persons depositing the money.

In 1986, the Money Laundering Control Act attempted to close the loophole. In criminalising the structuring of transactions to avoid reporting requirements, Congress attempted to "hit criminals right where they bruise: in the pocketbook." Under the Act, the filing of a currency transaction report (CTR) is required even if a bank employee "has knowledge" of any attempted structuring. Thus, it appeared as if the ability to launder the profits from illegal activity would be severely hampered.

As the physical world of money laundering began to erode, the tendency to use electronic transfers to avoid detection increased. These wire transfer systems allow criminal organisations, as well as legitimate businesses and individual banking customers, to enjoy a swift and nearly risk free conduit for moving money between countries. Considering that an estimated 700,000 wire transfers occur daily in the United States, moving well over $2 trillion, illicit wire transfers are easily hidden. Federal agencies estimate that as much as $300 billion is laundered annually, worldwide. As the mountain of stored, computerised information regarding these transfers reaches for the virtual stars above, the ability to successfully launder increases as the workload of investigators increases.

Although wire transfers currently provide only limited information regarding the parties involved, the growing trend is for greater detail to be recorded. If the privacy of wire transfers is compromised, due to burdensomely detailed record keeping regulations, electronic surveillance of transfers, or other potentially invasionary tactics, then the leap from the physical to the virtual world will be nearly complete. If laundering is to survive it must expand its approach, entering the world of cyberspace.

As the above mentioned race through laundering history demonstrates, creativity, and not necessarily greed, has been the launderer's salvation. The recent explosion of Internet access, may be the new type of detergent which allows for cleaner laundry.

Part II Enter, Anonymous Ecash

In the virtual universe of cyberspace the demand for efficient consumer transactions has lead to the establishment of electronic cash. This digital money is an electronic replacement for cash and has been defined as a series of numbers that have an intrinsic value in some form of currency. Using digital cash, actual assets are transferred through digital communications in the form of individually identified representations of bills and coins - similar to serial numbers on hard currency. While the ultimate goal of each vendor is to facilitate transactional efficiency, bolster purchasing power on the Internet, and, of course, earn substantial profit in a new area of commerce, each vendor plays by slightly different rules. Although the intricacies of individual vendors are quite fascinating, for the purpose of this article, it is fair to say that all but one vendor have one trait in common: lack of anonymity.

The exception to the general rule of lack of anonymity is DigiCash. Digicash is an Amsterdam-based company created by David Chaum, a well respected cryptologist. DigiCash's contribution to Internet commerce is an online payment product called "ecash." According to DigiCash, this "combines computerised convenience with security and privacy that improve on paper cash." Ecash is designed for secure payments from any personal computer to any other workstation, over e-mail or Internet. In providing security and privacy for its customers, DigiCash uses public key digital blind signature techniques.

Ecash, unlike even paper cash, is unconditionally untraceable. The "blinding" carried out by the user's own device makes it impossible for anyone to link payment to payer. But users can prove unequivocally that they did or did not make a particular payment, without revealing anything more. While ecash's security technology may be among the best in the business, the focus of this article is upon one aspect of DigiCash that is of particular interest to money launderers and law enforcement: Anonymity.

Part III The Money Laundering Control Act and Anonymous Laundering

This section examines how the Amendments to the Bank Secrecy Act of 1970, commonly referred to as the Money Laundering Control Act of 1986, apply to ▶

cyberspace and cyberlaundering. Without delving into the actual techniques involved in using public keys, blind signatures or any other encryption or decryption device, the best way to explain how anonymous digital cash could benefit money launderers' is by example. The following example will be used to demonstrate the law's application.

Doug Drug Dealer is the CEO of an ongoing narcotics corporation. Doug has rooms filled with hard currency which is the profit from his illegal enterprise. This currency needs to enter into the legitimate, mainstream economy so that Doug can either purchase needed supplies and employees, purchase real or personal property or even draw interest on these ill-gotten gains.

Of course, this could be accomplished without a bank account, but efficiency demands legality. Anyhow, Doug employs Linda Launderer to wash this dirty money. Linda hires couriers ("smurfs") to deposit funds under different names in amounts between $7,500 and $8,500 at branches of every bank in certain cities. This operation is repeated twice a week for as long as is required. In the meantime, Linda Launderer has been transferring these same funds from each branch, making withdrawals only once a week, and depositing the money with Internet banks that accept ecash. To be safe, Linda has these transfers limited to a maximum of $8,200 each. Once the hard currency has been converted into digital ecash, the illegally earned money has become virtually untraceable; anonymous. Doug Drug Dealer now has access to legitimate electronic cash.

Doug Drug Dealer is, of course, likely to be found guilty of more than just participating in a money laundering scheme. However, how the law applies to Linda Launderer and the Internet banks is more confusing. The purpose of the 1986 Act was to specifically criminalise the structuring of transactions so as to avoid the reporting requirements. Linda and her army of couriers are almost certainly violating structuring regulations by depositing small amounts in regular bank accounts. The problem is how to apply current money laundering law to cyberlaundering.

In the scenario above, Linda Launderer transfers sums of money less than $10,000 from non-Internet bank accounts to Internet-based ecash accounts. If the Internet bank is FDIC insured then federal depository regulations may apply. However, the cyberbank will not automatically be required to file a CTR regarding these transactions as all are under the $10,000 filing requirement. Nevertheless, if any employee of the Internet bank has even a suspicion of structuring, a CTR may be filed. As in the tangible banking world, the information contained on a CTR is only as insightful as the information presented by the bank conducting the prior transaction. In essence, each record in the chain of transfers is only as strong as the previous recordation.

The catch is that Linda Launderer's transfer was deposited into an ecash account. According to one cyberbank which currently accepts ecash, ecash accounts are not FDIC insured. A lack of federal insurance protection is understandable for the reason that digital money is currently created by private vendors, rather than the Federal Reserve. Thus, digital cash does not enter into the marketplace of hard currency thereby affecting monetary supply or policy, yet.

Since Linda Launderer's transfer was deposited into a non-FDIC insured, and thus, presumably non-federally regulated account, there should be no mandatory compliance with the filing regulations contained within the Money Laundering Control Act of 1986. If these assumptions prove correct, whether digital money is anonymous or not will be of less relevance to money launderers and law enforcement.

If certain cyberbanks, or even specific non-FDIC currency accounts within a cyberbank are able to operate outside the reach of current federal regulations, laundering on the Web may become one of the most rapidly expanding growth industries. It should be remembered that a criminal organisation desires to clean its dirty money, not necessarily protect their deposits from institutional banking failures.

Once the ecash account has been established, digital funds can be accessed from any computer that is properly connected to the Internet. A truly creative, if not paranoid, launderer could access funds via telnet. Telnet is a basic command that involves the protocol for connecting to another computer on the Internet. Thus, Linda Launderer could transfer illegally earned funds from her laptop on the Pacific Island of Vanuatu, telneting to her account leased from any unknowing Internet Service Provider in the United States and have her leased Internet account actually call the bank to transfer the funds, thus concealing her true identity. This would, of course, leave an even longer trail for law enforcement to follow.

Anyhow, ecash, being completely anonymous, allows the account holder total privacy to make Internet transactions. Thus, the bank holding the digital cash, as well as any seller which accepts ecash, has virtually no means of identifying the purchaser. Therefore, the combination of anonymous ecash and the availability of telnet may give a launderer enough of a head start to evade law enforcement, for the moment.

In the world of earth and soil, money can be laundered by the purchase of real and personal property. However, any cash ▶

transaction over $10,000 is subject to a transaction filing requirement.

On the Internet, anonymous ecash would allow for anonymous purchases of real and personal property. This fact yields at least two separate, but interrelated problems. First, the launderer will be able to discretely use illegally obtained profits to legitimately purchase property. Second, the temptation for automobile and real property dealers to become players in the game for anonymous ecash seems overwhelming. If a seller or dealer understands that it can not possibly trace who spent ecash at its establishment, the fear of becoming involved with dirty money is drastically reduced.

Under current law, a seller of property must file a CTR for any cash transaction over $10,000. If the purchaser's identity is anonymous, and even the bank can not trace the spent ecash, the force of the Money Laundering Control Act of 1986 is withered into mere words on a page. Of course, Congress could attempt to legislate in this new area of commerce.

Obviously, transferring hard currency to ecash and then spending the ecash is an appealing opportunity to potential launderers. What if the ecash is then transferred back to a regular hard currency account? This may seem a foolish act as the entire purpose is to reap the benefits of anonymous ecash. However, presently, there are no opportunities to purchase automobiles or real property by the exclusive use of anonymous ecash. Thus, the desire to convert private and untraceable ecash into a more functional means of purchasing is understandable.

Whether a regular, non-Internet currency account already exists or must be created to deposit the transferred ecash into may be irrelevant. Filing a CTR would be a legal necessity if the transfer amount is over the $10,000 reporting limit, as the transfer will deposit hard currency in a tangible, institutionalised, and regulated bank account. A transfer from completely anonymous ecash to hard currency might alert law enforcement as to the existence of the ecash account. While this alone would not track down laundered money, it might put a suspicious agent on notice.

In summary, Linda Launderer has knowingly structured financial transactions so as to avoid reporting requirements. Under current law she is in violation of The Money Laundering Control Act of 1986. However, if the cyberbanks in which she has ecash deposits are outside the reach of current banking regulations, these banks have no duty to file any currency transaction reports. Nevertheless, assuming that cyberbanks which accept anonymous ecash are somehow subject to the same laws and regulations which financial institutions in the tangible world are, Linda must first be caught before she can be found guilty. This is where anonymous ecash may save Linda from fines and jail time.

Even if cyberbanks are required to file transactional reports pertaining to ecash, the reports will be virtually useless, as the banks have no knowledge as to which funds are Linda's. Thus, Linda, our overly creative launderer, and Doug, our devious drug dealer, may enjoy the benefits of completely anonymous money laundering. That is, unless Congress decides to attempt legislation in the area of digital money and virtual banking, or FinCen is somehow granted the constitutional authority to secretly monitor all cyberbanking transactions, despite its lack of accountability to the general population.

Part IV The Struggle For Privacy

The battle that emerges is between the right to privacy by means of anonymous digital cash verses the desire of law enforcement to ferret out crime. The fact of complete anonymity guarantees that some money laundering will be easier to pull off.

On the other hand, the lack of anonymity means that every move made on the Internet will be traceable. Thus, whether money laundering becomes rampant under the guise of anonymous ecash may be one of the first tests of the practical aspects of DigiCash's future.

In California Bankers Association v. Schultz, the Court held that bank record keeping requirements do not violate the Fourth Amendment right to privacy and do not amount to an illegal search and seizure. In United States v. Miller, the Court held that a criminal defendant had no Fourth Amendment right to protection of his bank records, and did not have a legitimate expectation of privacy regarding these papers.

Concluding over two centuries of Constitutional erosion, it is apparent that an individual's right to financial privacy is limited. The issue involving cyberspace is whether financial privacy rights are so limited that the federal government could monitor a digital cash user's financial transactions in a detailed fashion. In effect, rendering completely anonymous digital cash completely pointless.

While the Supreme Court has sliced financial privacy rights on several, previously mentioned, occasions, Congress has attempted to restore financial and informational privacy rights to the individual. The Privacy Act of 1974, The Right to Financial Privacy Act of 1982, and The Electronic Communications Privacy Act of 1986 are currently the three best hopes for individual financial privacy.

The Privacy Act of 1974 regulates the practices of federal agencies regarding personal information. With certain exceptions, no federal agency may disclose ▶

any record contained in its system to any other person or agency without the written request or consent of the individual.

Next, The Right to Financial Privacy Act of 1982 ("RFPA") attempted to further protect financial records. Under RFPA, in order to obtain a customer's financial records from a financial institution, the federal government must serve a subpoena on the customer before or concurrently with service on the bank. The government must show that the records are related to a "legitimate law enforcement inquiry," and notify the customer that it can take steps to block the bank's disclosure of the records.

Finally, The Electronic Communications Privacy Act of 1986 ("ECPA") attempts to protect the individual against the unauthorised interception of electronic communications. Title I focuses on the interception of wire, oral and electronic communications. Title II prohibits an electronic communications service provider from knowingly divulging the contents of a communication while in electronic storage.

Applying current law to the Internet, the result is inadequate protection of individual financial privacy. The combination of The Privacy Act and RFPA prevent the government from groundless searches of individual financial records. However, the standard required for a search is only that there exist some evidence that the records are related to a "legitimate law enforcement inquiry." Due to this relaxed standard, individual financial privacy may be violated without any probable cause. A "legitimate law enforcement inquiry" is clearly an easier requirement to meet than a Fourth Amendment probable cause standard.

Expanding into cyberspace, if the Internet falls under the protection of the ECPA, as it is an electronic communication, then individual financial privacy in cyberspace is afforded as little protection as financial privacy in the tangible world. Essentially, the government need only claim that it requires access to financial records due to a "legitimate law enforcement inquiry."

Taking one step further, the application of current financial privacy laws to DigiCash's Ecash may be the eulogy for completely anonymous digital cash. If the government believes that ecash is overflowing with money launderers, a "legitimate law enforcement inquiry" into the situation would likely allow access to ecash account records. Since even the bank can not trace ecash to a user, pressure would be placed on various agencies to solve the problem.

First, the Federal Reserve would likely announce that all cyberbanks accepting anonymous ecash conform with FDIC regulations. Thus, these banks would be subject to federal scrutiny and pressured into insuring anonymous ecash deposits. Since insuring anonymous ecash might prove unprofitable, it is probable that many timid cyberbanks will succumb to federal intimidation and abandon anonymous ecash altogether.

Second, cyberbanks could be convinced to implement special "investigatory software" into their computer systems so as to flag suspicious ecash accounts. While the technical aspects of such a system are beyond the scope of this article, it is fair to say that if such programming is both possible and practical, then no ecash account would be safe from the "legitimate law enforcement inquiring" software.

Finally, if ecash accounts become subject to greater scrutiny, the IRS and FinCen will capitalise on the additional information being unearthed. Since there is no requirement of probable cause to search an individual's financial account, the IRS and FinCen could use the preliminary information obtained from the "legitimate law enforcement inquiry" so as to have sufficient facts to establish probable cause, enabling a full scale search and seizure of an individual's financial records.

Part V Conclusion.

Technology has created the means and ability to launder money by use of completely untraceable digital currency. While current money laundering laws apply to the fledgling art of cyberlaundering, the actual effect of these laws may be limited.

Structuring of transactions so as to avoid currency reporting requirements becomes less risky if the funds used to structure are virtually untraceable. In addition, the filing of currency transaction reports may be pointless if the money can not be traced into a specific account. However, the actual requirement that a transaction report be filed may be non-existent if cyberbanks which accept ecash deposit accounts do not fall under current federal or state regulation of financial institutions.

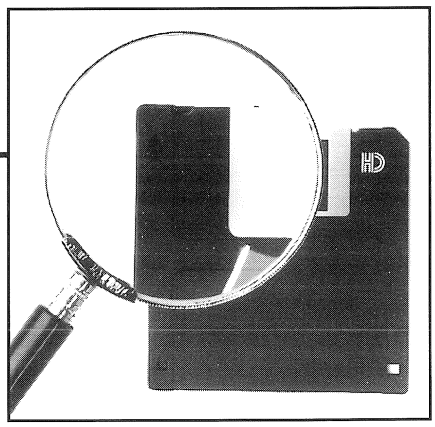
The end result may be a compromise between federal agencies that wish to have access to all financial records and the individual desire for some reasonable level of financial privacy. Since it has been determined that there is no legitimate expectation of complete privacy in financial records held at a financial institution, and that the production of such records is not self-incriminating in violation of the Fifth Amendment, then allowing for anonymous digital cash transactions is not as threatening as once believed.

In effect, it may be more difficult to trace criminal activity which uses anonymous currency. However, if sufficient cause exists, the government clearly has the right to compel an individual and his or her banking establishment to produce all relevant financial records upon court order.

In essence, forcing the ecash account holder to disclose its identity by revealing its "blinding" factors. The result being that the privileged right to privacy regarding digital currency carries a price: responsibility. If such liberty is misused, then it should be taken away from that specific violator, rather than confiscated prior to its misuse.

Therefore, prohibiting or secretly monitoring ecash transactions on the grounds that such transactions are more difficult to trace is not sufficient justification for invasionary tactics aimed at further limiting financial privacy. Fear of the unknown is not an adequate reason to quash a potential privacy restoring means of conducting financial transactions. ■

Forensic Q&A



Q *When using MS Undelete in Windows File Manager is the list of deleted files all of the files deleted since the disk was last reformatted?*

A No. In MSDOS the normal deletion process just changes the first character of the file name to a special indicator and releases the disk space that the file used so that it is available for re-allocation. To appreciate just why this works it is essential to understand the directory structure that MSDOS uses. A directory (or sub-directory) is a list of entries stored on a disk in a very specific form with 32 bytes for each entry. The first eight bytes are the file name and the next three bytes are the extension. Other information about the file (like where it begins on the disk, what its attributes are, how long it is and the date and time stamp) are stored in the remainder of the entry. When MSDOS searches for a particular file it begins at the top of the specific directory list and searches downwards. Any file names marked with the special delete character are ignored but the search continues. Once an entry beginning with zero is encountered the search stops. Otherwise the details from the found file entry are read and the file can be opened for access. When MSDOS creates a new file, once again it begins at the top of the specific directory list and searches downwards. In this case however, it will stop when it finds an entry beginning either with the delete character or a zero and write the new file details into that entry. MS Undelete is a program designed to locate and display any entries beginning with the delete character and present them for your selection. Some of these may have been overwritten by new file names as described above so quite obviously the original names will have been overwritten and lost even if the actual content of the original file still exists on the disk. The main problem with undeleting files is that the undelete program can only recover the first cluster that the file occupied from the directory entry. The File Allocation Table (FAT) can be checked to see if this cluster is currently in use but the undelete program cannot determine whether that cluster has been overwritten since the file was deleted. It is also impossible to reliably rebuild a cluster chain for the longer deleted files, although by making several assumptions an undelete program may be able to make a series of "intelligent guesses" about deleted chains. While generally MS Undelete does a reasonable job in recovering deleted files it is not considered absolutely reliable for forensic use and any results should be checked. Note that the more time (and therefore the more machine activity) that elapses between deletion and attempted undeletion the less chance there is of success.

Q *Is there any way a deleted file can be hidden from appearing in MS Undelete?*

A Yes, there are a number of ways that file undeletion can be prevented. There are some utility programs which will remove deleted entries automatically. The process of defragmenting a drive will usually remove deleted entries and entries can be cleared out by using a disk editor. The simplest way is to delete the directory where the file was located. This requires that there are no active files within the directory and it may be necessary to temporarily move any active files to another directory, delete the directory, recreate it and then move the files back. Since creating a directory effectively sets all the entries to zero this will remove any remnants of old filenames. Note also that MS Undelete cannot undelete directories.

Q *During an investigation I have found a number of WordPerfect files which are encrypted. How can I look at them?*

A Most of the encryption methods used in the standard word-processing packages are relatively simple and can be broken using dedicated software which is available from commercial organisations. If you need details of suppliers, or if you are a supplier, please contact the Journal and we will be happy to pass them on.

Q *When running a search engine the results have shown hits in unallocated clusters. What are these and why do they contain data?*

A The space on a hard disk is divided up by the disk operating system (DOS) into separate physical storage areas. Each of these is called a sector. When space is required to store data on the hard disk it is assigned in sets of sectors referred to as allocation units or clusters. On hard disks clusters are normally 8, 16, 32 or 64 sectors in size, depending on the physical characteristics of the drive defined during manufacture. When a cluster or group of clusters is in use by a file it is referred to as being allocated. When the file is no longer required the clusters it occupied are marked as being available for use by another file and are referred to as being unallocated. The information that was recorded in the clusters from the previous owning file remains and it is within this that your hits are occurring. ■

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

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

Notice Board

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

OSS '97 - International Conference and Exhibit on 'Global Security and Global Competitiveness: Open Source Solutions'

3-5 September, Crystal Gateway Marriott, Crystal City, Washington, DC.

The conference and exhibit include a half-day pre-conference orientation on open sources and methods of collecting intelligence, and three days of government lessons learned, business intelligence lessons useful to government, and academic and private sector vendor contributions to the 'virtual intelligence community'. Topics will include scientific and technical intelligence collection, commercial imagery applications for government and business, economic and financial espionage, proliferation, terrorism and transnational criminal intelligence, cyberlaw and cybertheft workshop, commercial technologies for open source intelligence collection and processing.

Contact: OSS'97
Tel: +1 703 242 1700
Fax: +1 703 242 1711

Proving Computer Crime: Admissibility, Experts and Presentation

26 September, London School of Economics, London

A one-day Master Seminar organised by the Computer Security Research Centre, LSE and the Computer Related Crime Research Centre of Queen Mary and Westfield College, University of London. Following an introduction by Mr Justice Jacob, the day's proceedings will include The Role and Instruction of Experts, Types of Evidence, Practical Issues of Collection, Provenance and Formal Procedures, Admissibility of Evidence, Court Presentation, and Matters for Officers of the Court. This seminar qualifies for five (5) hours of Law Society Continuing Professional Development

Contact: Robert S Jones, Queen Mary and Westfield College
Tel: +44 (0) 171 975 5326
Fax: +44 (0) 181 980 2001

InfoWarCon '97

10-12 September, Sheraton Premiere, Tysons Corner, Virginia, US

The NCSA and Interpact Inc. have announced that Major General Michael V Hayden will speak at this conference. Major General Hayden is the commander of the Air Intelligence Agency and Director of the Joint Command and Control Warfare (C2W) Center, Texas. An Air Force Field Operating Agency, AIA's mission is to exploit and defend the information domain. Information Warfare, originally a military term, now fully pervades the civilian community. Information Warfare is being used to interrupt both personal and corporate activities, to destroy assets and to steal private information. Dr Mich Kabay, NCSA, will provide a summary of computer crime cases.

Contact: NCSA
Tel: +1 717 241 3233
Fax: +1 717 243 8642

Onshore-Offshore World 1997

6-7 October, Lugano
Contact: D&D Comunication, Milan
Tel: +39 2 58 30 61 65
Fax: +39 2 58 31 56 55

Internet Security and Firewalls

15-16 October, Maidenhead, UK

This course highlights the potential risks and identifies common sense approaches and methods to minimise risk and enable safe and beneficial business use of the Internet. Additionally, the course promotes a detailed understanding of TCP/IP Firewall technologies. Aimed at anyone responsible for planning, implementing or managing their company's interface to the Internet, or tasked with ensuring it is used in a safe and secure manner. The course covers a wide spectrum of business and technical skills.

Contact: Zergo Limited
Tel: +44 (0) 1256 818800
Fax: +44 (0) 1256 812901

Computer Law Conference

16 & 17 October, The Cafe Royal, London

Intended to become an annual event, this conference will bring together leading UK figures in IT law. The event is aimed at IT directors and managers, company secretaries, accountants, purchasers, in-house lawyers and IT lawyers. Day one will tackle system problems and contract issues, looking specifically at technology and its impact on IT law, data protection, the Year 2000 and EMU legal issues, suppliers liability, outsourcing and software maintenance and support. Day two will concentrate on the Internet, and discuss issues including data security, legal implications, encryption and trusted third parties, tax issues, and liability stemming from use of the Internet.

Contact: National Computing Centre
Tel: +44(0)161 242 2117
e-mail: diane.finnncc.co.uk

HTCIA National Training Conference 1997

27, 28, 29 October, Embassy Suites Hotel, Lake Tahoe, California

For further details see the National Conference Page of the Northern California Chapter. Go to: HTCIA 1997 National Training Conference

Financial Services on the Internet

6-7 November, Milan
Contact: D&D Comunication, Milan
Tel: +39 2 58 30 61 65
Fax: +39 2 58 31 56 55

Strategic Solutions '97

9-12 November, Rancho Mirage, California

The conference will feature sessions on software, electronic commerce, IT services, finance, legal and public policy.

Contact: Bob Cohen, ITAA
Tel: +1 703 284 5333

International Conference on Forensic Computing

3-5 December, The Grand Hotel, 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
Fax: +44 (0) 1903 233545

Published by
Computer Forensic Services Ltd.