ISSN. 1363-6650

MAY 1997
Issue 4

International Journal of FORENSIC COMPUTING™

Contents

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

Comment

Computer crime is big business, not just for criminals but for the firms which investigate it and try to protect against it.

It is a burgeoning industry as everyone scrambles to stop the invasion of hackers, viruses, data theft or any other perceived threat from wreacking havoc in the modern fully computerised office.

Indeed the statistics make for frightening reading - in 1994 more than £1.2 billion worth of damage in the UK alone was caused by security breaches of one sort or another. There are hundreds of tales of salesmen walking off with customer databases to use in a new job, or commercial secrets being stolen.

It seems the business world has woken up to the notion with a jolt, with thousands of visitors flocking to the Infosecurity '97, UK, exhibition this month to get a glimpse of the terrifying world of computer misuse. At the various stands and seminars they were told of the horrifying consequences of what the new breed of cyber criminals could do.

Some of the exhibitors rammed the message home with vivid demonstrations of how computer crime would spell disaster, with one firm even featuring a ticking time-bomb and a mock bomb-disposal expert.

Information security is important and firms have to realise that their systems can be at risk from unauthorised access. Obviously computer security companies want to show the consequences of crime as dramatically as possible to sell their products, with the market now worth about $6 billion, rising to an estimated $13 billion by the year 2000.

But the very real threat has to be examined and acted on in a considered and logical way rather than creating a culture of fear and hysteria which will compound the problem.

A similar parallel can be drawn with viruses - when they first hit the computing world there was bedlam as shocked consumers feared complete data meltdown. While a few viruses have caused chaos, the problem as a whole is under control. The same is true for security. There are some who approach the problem from the wrong side with a 'poacher turned gamekeeper' attitude. These people, some of whom have a less than legitimate past, know the loopholes and weak spots and will exploit them for commercial gain.

Fine up to a point, but somewhere along this line the cart starts pulling the horse and we end up in the sad situation where the computer industry is actually making trouble for itself. It is easy to get trapped in ever decreasing circles of security breach and solution, where the ultimate goal is lost.

One security consultant is reported to be touting for business by hacking into firms to show up inadequacies and also trying to get insurance companies to raise the premiums of firms who do not buy his product.

Is this the cyber equivalent of the age-old protection racket or a vital mechanism to ensure firms are always one step ahead of would-be criminals? There is no real answer.

Computers are only tools that help make work easier, so we should make sure they stay working for us rather than getting tangled up in fighting them. ■

Articles are published on the understanding that publication is not taken to imply endorsement of the views therein by the Publisher or Editorial Team or members of the Advisory Board of the Journal. Courses of action described in the Journal in relation to one set of circumstances will not necessarily be appropriate for a different set of circumstances.

Accordingly, readers should take their own independent specialist advice before proceeding on any project or course of action and any failure to do so is at their own risk. No responsibility is assumed by the Publisher or Editorial Team or members of the Advisory Board for any loss or damage to persons or property as a matter of contract, negligence (save in respect of liability for death or personal injury arising out of any negligence) or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Whilst all reasonable care is taken, neither the Publisher, nor the Editorial Team, nor members of the Advisory Board can be held legally responsible for any errors in articles or listings. Upon submission of an article, the author will be requested to transfer copyright of the article to the Publisher.

News

Computers used to forge cheques

Criminals are using high-tech equipment to forge cheques worth millions of dollars in the US.

The US Secret Service and the FBI told members of the House of Congress that their investigators are handling a spiralling number of counterfeit cheque cases.

Forgers use personal computers, a scanner and a quality laser printer to copy and alter cheques and then print out new ones. The FBI estimate that 1.2 million worthless cheques are accepted for payment every day and that the losses to banks, businesses and individuals reached $5 billion in 1993.

Deputy assistant director of the Secret Service Kevin Foley told the House Banking monetary policy subcommittee that the problem involved organised gangs as well as lone computer hackers.

He said: "The motivation behind these schemes is greed. The goal is always money. It's a point and click crime."

Chairman of the subcommittee Michael Castle said: "More alarming than the total amount is the fact that it is growing at a very rapid rate and could threaten the current payment system with unsustainable losses if it is allowed to grow unchecked."

Meanwhile banks in the US have announced plans to combat the problem with measures ranging from educating staff to demanding thumbprints from people cashing cheques who are not customers.

Net surfers warned

Internet users in Britain are being told that they could be prosecuted for storing certain information on their computers.

The Data Protection Act 1985 means that people could be inadvertently breaking the law by processing personal information, even as little as names or addresses, received over the Internet.

Now the UK Government is warning that anyone who thinks they fall into this category should register with the Data Protection Registrar and must follow strict information handling guidelines laid down by the Act.

A spokeswoman for the Registrar said: "The Internet is changing the approach which organisations undertake to certain business activities, such as online shopping and banking.

"With such activities involving interaction with individuals over the Internet, it is highly likely that the processing of personal data will occur.

"Ignorance of the Act is no defence and people operating either as individuals or part of an organisation could be prosecuted and could face an unlimited fine."

The Data Protection Registrar has issued guidelines for anyone who might need to register under the Act as a result of their Internet use. Information is available from the Registrar's Web site at http://www.open.gov.uk/dpr/dprhome.htm

Chaos at the speed of light

Encryption techniques have been developed by French scientists to protect information being carried on fibre-optic cables.

Conventional methods of encryption are too slow to cope with the large amounts of data sent through fibre optic systems, with the risk of unauthorised eavesdropping.

Researchers at France Telecom and the Universite de Besancon have based the new system on chaos theory, which governs non-linear behaviour. They use a laser diode to help encrypt and decrypt an optical signal at high-bit rates.

Law on the Web

An online legal resource facility has been launched on the Internet for anyone interested in UK law.

The easy-to-navigate site is currently free to use and contains a searchable database with thousands of useful contacts, details and addresses.

Included in the listings is information about nearly every UK solicitor, barrister, legal firm, chambers and all of the UK courts.

And 3,000 expert witnesses in more than 1,000 areas of expertise can be searched for either by subject or location, together with a list of most of the UK's legal technology suppliers.

Updated daily, the site also contains more than 2,000 links to other UK law-related Web sites. Online Law can be reached at http://www.online-law.co.uk

New law lets public see e-mail

Electronic mail sent by Government bureaucrats in the US can now be read by anyone after a new law came into effect.

The Electronic Freedom of Information Act means that US citizens should be able to read e-mails, reports or memos sent between staff in federal agencies. The information will be available on CD ROMs, disks or via the Internet.

But critics say that the various agencies do not currently have the technical capability to track and trace all the material and that it could be months or even years before all departments are up to scratch.

£6 million in illegal software

Police in Scotland seized £6.2 million in stolen and counterfeit computer hardware, disks and CD ROMs in a one-day blitz. ▶

They swooped on a street market in Glasgow and arrested 41 people. The raid, which involved 130 police officers and about 40 trading standards and customs officers, is part of a crackdown on counterfeit goods which has netted about £20 million worth of items.

Police headhunt experts to crack fraud

Australian police have promised to recruit expert investigators to combat the growing sophistication of fraudsters.

New South Wales Police Commissioner Peter Ryan told a meeting of businessmen in Sydney that he wanted to employ specialists from the private sector who had the skills and experience to identify fraud.

Mr Ryan said: "I want to start recruiting people directly into the service who have financial management skills, who can analyse transactions, who are good at tracing accounts through computers and who I will pay according to the rate for the job. They can be given appropriate powers to do what they have to do, such as search and seize and give evidence in court, but they don't need to be police officers and they only need to work for us for a short period of time."

Fraud is thought to account for up to half the cost of all crime in Australia, with an estimated total of $13 billion a year.

High-tech scrambling to be lifted?

Makers of data encryption products in the US will be able to export across the world if proposals to lift a ban go ahead.

Current legislation stops manufacturers selling or distributing their best systems and programs abroad and software firms and civil liberty campaigners now want the rules relaxed.

Encryption programmes scramble information and render it unreadable without the right software or password, and similar technology is increasingly being used to boost security on the Internet for both communication and trade.

The Security and Freedom through Encryption bill has been signed off by the US House Judiciary Committee and will now be discussed by the House International Relations panel during the next stage.

But the Clinton administration still fears that criminals would use the technology to defeat telephone tapping and data searches by law enforcement agencies, although the bill's backers say criminals already have access to such equipment.

The bill also includes criminal penalties for unlawful use of encryption with sentences of up to 10 years in prison.

Plans for legal judgements on the Net

Court judgements in Britain will be published on the Internet to cut costs and improve access if a new scheme gets the go ahead.

The Court of Appeal has backed the plans to put legal documents on the World Wide Web so judges, lawyers and the public could easily see them.

It is also hoped the move would cut down on the large amount of paperwork and hard copies which have to be distributed after judgements.

The British Government already has a Statute Law database and this is available to subscribers only, although there are calls for this to be put online also.

Man arrested after Gates threatened

A computer enthusiast was charged with extortion after allegedly threatening to kill Microsoft boss Bill Gates. The 21-year-old, from Illinois, US, was arrested by the FBI after blackmail letters were sent to Gates demanding $5 million.

But agents examined a disk the writer had sent to Gates and recovered portions of previous letters sent as well as the names of the suspect's parents.

Court documents said: "The writer cautioned Gates not to notify law enforcement and that if Gates did so, the writer could kill him with 'one bullet from my rifle at a quarter of a mile away."

Danger of Internet paedophiles

Interpol child-protection co-ordinator Ann-Kristin Olsen told a meeting of international police chiefs that the fight to stop perverts had to be stepped up.

Olsen was speaking at a top-level law enforcement conference in Norway and she said that the threat of paedophiles using the Internet had to be taken seriously.

She said: "Instead of hanging around playgrounds looking for a lonely child, potential abusers can now just log onto the Net. We need a babysitter for the Internet who can expose paedophiles operating in cyberspace."

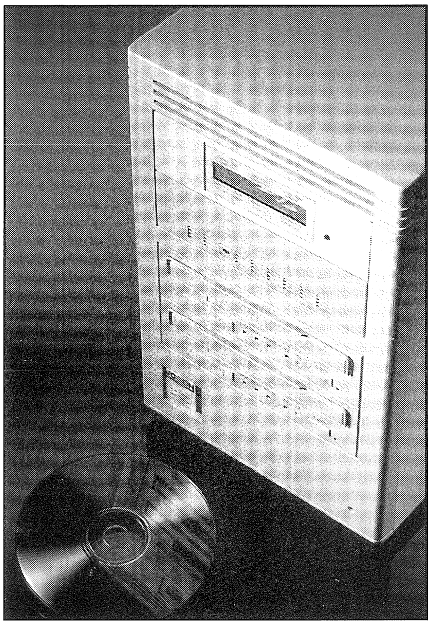
Olsen, who is herself police chief of Norway's arctic Svalbard Archipelago, said monitoring could be done centrally, possibly at Interpol's headquarters in Lyon, France.

College's crime tip offs on the Internet

A US college hopes to cut campus crime by encouraging students to give anonymous information using a special site on the Web.

The University of Richmond in Virginia hopes the system will act as a deterrent and so far three students have been indicted on drug charges and up to 40 others could also face action by the college or campus police. ■

Product News



Data capture system unveiled

Vogon has launched a system for imaging information onto CD-ROMs for use in investigating computer crimes.

Its makers say the Imager system is faster than any other product on the market and is the only one if its kind that can make both a master copy and a working copy of the data simultaneously.

A spokeswoman for Vogon said: "Our system not only makes imaging faster and more efficient, it also speeds up the data searching operation.

"Once the image has been taken, you can search the data on up to 18 CDs at a time. Our high-speed software searches the text for relevant names or phrases, and the extracted data can be analysed and sorted using any database or spreadsheet package."

Vogon claims the captured data is fully reliable and can be used as evidence in court.

Vogon International has offices in Germany and in England and can be contacted in the UK on +44 (0)118 989 0042 or e-mail on sales@vogon-int.demon.co.uk

Security on the Internet

Data transmission over any unsecured network stands the risk of being seen by prying eyes but one firm thinks it has the answer.

Portcullis Computer Security is launching a new system called F-Secure Virtual Private Network, which is a 128-bit encryption device that allows users to channel private communications across the Net.

Its makers say that unlike traditional firewall based systems, F-Secure is simple to configure and update. *For more information contact Portcullis Computer Security on (UK) 0181 868 0098 or e-mail on portcul@dircon.co.uk*

New computer evidence service

Data recovery firm Ontrack has launched a new service to find and analyse information on its clients computers for use in investigations.

The service is aimed at the legal and corporate community, particularly in the areas of trade secrets theft, harassment by e-mail and malicious destruction of data by disgruntled employees.

Ontrack says it can make exact copies of data within hours, with one copy kept with a third party for preservation purposes and a working copy made so investigators can search for relevant files.

Michael Rogers, chief executive officer of Ontrack, said: "Two years ago our customers began asking us to assist them in recovering data that was to be used as evidence in criminal investigations and civil discovery.

"By modifying the proprietary techniques, tools and procedures we had used to successfully perform tens of thousands of data recoveries, we now were able to support a new type of customer with a new set of needs.

"Since those initial calls two years ago, we have worked with hundreds of civil and corporate lawyers, who believed that electronic documents were critical to the outcome of their cases."

Ontrack says more than two-thirds of those in the legal community have not used such services because they feel uncomfortable with the procedures and technology involved.

Software to trap a thief

New technology is being brought in to fight fraudsters who are costing telephone companies millions of pounds.

Criminals manage to get free airtime using stolen credit cards, corporate networks and by hacking into the exchanges.

Now software detection packages are being used to identify and catch culprits by checking on any usual or costly activity and then alerting operators to potential fraud.

Industry supplier Applied IT has produced a package called Fraud Management System which it says speeds up detection rates by up to 50 per cent. The system can also store data if a file of use is needed for an investigation.

Irish mobile operator Eircell, which takes the threat very seriously and prosecuted several people last year, has just installed the system in a bid to further curb crime.

Ray Haughey, network security manager for the firm, said: "Time is money and lapsed time detecting fraud can be a lot of money."

NTI buys security software

US firm New Technologies Inc. hopes to help victims of computer theft after it bought all rights to special security software. NTI purchased the MICRO-ID software and the matching law-enforcement security programme COP-ONLY and together the products help police and companies identify the owners of stolen computers.

▶

President of NTI Michael Anderson said: "Computer theft, particularly the theft of laptop computers, has been an international epidemic.

"MICRO-ID offers both individual, corporate and government users a low cost way to mark their personal computers and maximise the possibility of recovery and return.

"Without it, all computers look the same to the police. With MICRO-ID, there is no doubt as to the original computer owner and little difficulty in obtaining the prompt return of the equipment."

The system operates by marking the hard drive of the computer in multiple locations with encrypted information about the owner, plus make, model and serial number.

Thieves have no idea that the hardware has been electronically tagged and the information can only be read by the COP-ONLY programme which has been given to bona fide law enforcement agencies free of charge.

The system means police can immediately test recovered or suspected stolen computers for ownership information and the software can also be used to check for stolen equipment in shops and markets offering second-hand computers.

NTI, which is based in Gresham, Oregon, and is a supplier of computer forensic software and training, hopes to bundle the programme as part of its suite of security products.

For more information contact NTI on (US) 503-661-6912 or e-mail annette@secure-data.com and the Web site is at http://www.secure-data.com/ ■

Information on new products or industry-related news can be sent to the Journal for inclusion in future issues.

Internet

The Internet has been hailed as a bastion of free-speech, with a world-wide platform for anyone who has something to say and has the correct equipment to go online. But this could now change dramatically, with huge implications for computer crime, after German prosecutors charged Compuserve with distributing illegal material. Paul Johnson looks at the case and what it holds for the future of the Web.

The global Internet community could begin to buckle after calls for greater regulation and the threat of prosecution.

Compuserve, the world's second largest on-line information service, is likely to re-examine its services world-wide after German police investigated it for carrying illegal pornography and neo-Nazi symbols.

The case is the first of its kind and will send shockwaves through the entire industry, with the likelihood that many other service providers will curb their excesses rather than risk legal action.

Compuserve's head of German operation, Felix Somm, was indicted on charges of aiding the exchange of pornography and extremist propaganda.

Prosecutors said subscribers to the service had access to news groups containing child pornography, pictures of violent sexual acts and bestiality, as well as computer games containing images of Hitler and Nazi swastika symbols.

Under German law such obscene pictures and Nazi material are explicitly banned and investigators in Munich spent nearly two years trawling through the Internet in a bid to find violations of publishing laws.

In 1995 Compuserve was in the news after it blocked access to more than 200 newsgroups throughout its service worldwide, and after complaints of censorship, it opened most of these up again but offered customers special software to stop online pornography.

Now Compuserve is strenuously denying the latest charges, calling them entirely groundless, and has vowed to fight the case all the way.

It says it cannot control the content of news groups, which are used by thousands of people to post messages and data, and that the sheer number means the information cannot be properly monitored or filtered.

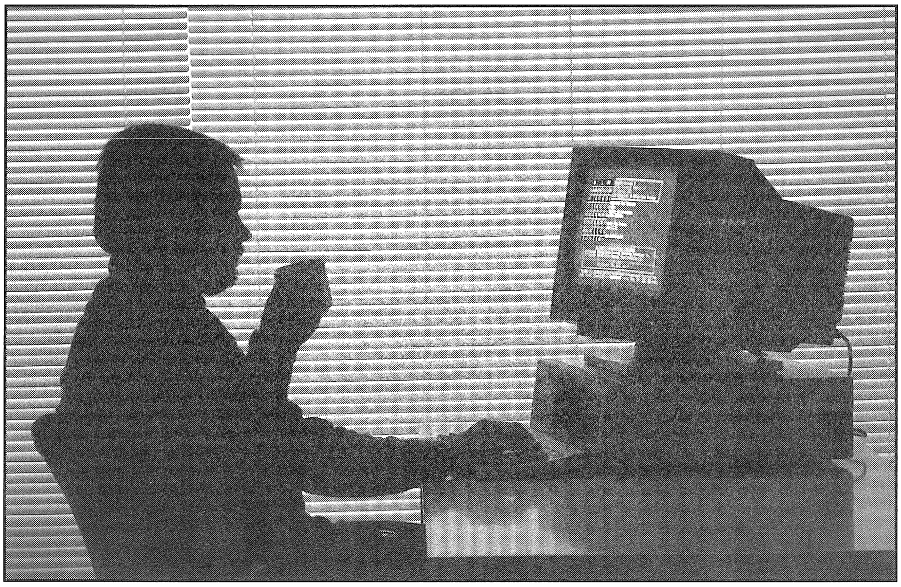
But the technology exists that will let individual countries or service providers police and censor the Internet's contents at will. Already China is using these "firewalls" to limit its Internet users, and many critics fear that this could eventually affect the global position as well.

The concept that the toughest laws in any given country will act as the lowest common denominator across the world breaks through the notion of the Web as having no political or geographical borders.

Both the Supreme Court in the US and the European Parliament are looking closely at possible legislation to restrict indecent material sent electronically, although the practical hurdles are still considerable.

The German Government announced proposed laws in the Information and Communications Services Bill to make Internet service providers criminally liable for material uploaded through their systems.

German technology minister Juergen Ruettgers, said: "The Internet must not become a legal vacuum. This country is not ▶



prepared to tolerate certain things that appear there."

The European Parliament is likely to adopt a similar policy and request that its member states adopt guidelines and take a pro-active legal standpoint.

A group of European MPs have set up a working party to look at some of the technical and legal issues of the Internet. Ideas discussed include service providers barring access to persistent offenders and locking out users who type in certain banned keywords when searching the Web.

But those who say freedom of speech should be protected at all costs are outraged, and say the Compuserve case could create a precedent which will destroy the Internet community.

An international coalition from a dozen countries is urging German Chancellor Helmut Kohl to intervene in the prosecution of the service provider, calling the case a violation of "international norms for the protection of speech".

The Global Internet Liberty Campaign, with 24 members including the American Civil Liberties Union, has written to Kohl warning him of possible repercussions.

In the letter the group says: "The action will have a harmful impact on Internet users around the world. The charges against Compuserve will establish a harmful precedent, and may encourage other governments to censor speech, limit political debate, control artistic expression and otherwise deny the opportunity for individuals to be fully informed."

The coalition added: "A service provider cannot easily stop the incoming flow of material. No one can monitor the enormous quantity of network traffic which pass through in dozens of text and binary formats, some of them readable only by particular proprietary tools. A second technical problem is that a provider cannot selectively disable transmission to particular users. Compuserve cannot provide material in one country while blocking it in another. Such a distinction would require an enormous new infrastructure on top of the current network.

"Some networking technologies, such as newsgroups, may allow individual operators to select some groups or items and block others, but the World Wide Web does not support such selectivity."

One Internet provider in Germany, XS4ALL, was recently blocked by the German authorities in a separate matter and its administrator, Felipe Rodriquez, says imposing restrictions is futile.

He said: "It's not possible for a provider to censor the Internet according to the local law, custom or tradition. The Net is too international and too dynamic for that to be possible. Censoring has in most cases proved to be counterproductive."

Andy Oram, a member of the Computer Professionals for Social Responsibility group in the US thinks the move made by the German authorities was impractical.

He said: "Even if an Internet provider is notified that illegal material is coming from a certain site and cuts off all access to that site, the publisher of the material can easily find another site from which to send it."

Last summer the Canadian Government commissioned a study by a team of legal experts on liability for content posted or transmitted on the Net and the findings, called The Cyberspace Is Not a No Law Land, have just been released.

The team's brief was to examine how current laws affect the content of the Internet, including obscenity and pornography, hate propaganda, copyright and trademark law and civil liability such as invasion of privacy and libel.

But the conclusions expose a murky minefield for Internet users, law makers, lawyers and service providers alike, and argue that there are large grey areas in issues such as liability and definitions of what is and is not acceptable.

The report said: "If amendments to existing laws are needed, they should only be made in a de minimis way and in a way as technologically neutral as possible under the circumstances.

"Legislators should also be mindful of the need to balance the interests of the users, publishers and disseminators on the one ▶

hand, and those of the authors on the other, while preserving freedom of expression and only imposing limits on such freedom as necessary in a free and democratic society."

It seems the only thing commentators can agree on is that one man's free speech is another's propaganda and perversity. But it is all too easy to forget that the politicians, libertarians and technocrats are arguing over real people.

Chief Superintendent Karlheinz Moewes is the head of Munich police department's special unit for the investigation of the Internet and has seen pictures which would sicken most people.

He led a five strong team which handled the initial investigation of the German division of Compuserve and is absolutely convinced there are very real ethical reasons to curb the Internet. Mr Moewes sums up the mood for many when he says: "Behind every one of these pictures is an abused child. How can free speech be carried out on the backs of abused children?"

The German situation has crystallised the central dilemma faced by the Internet community, and forced some hard questions to be asked. One thing we can be sure of is that the problem will not go away, so governments across the world now have a duty to examine what laws are currently in place and what new ones need to be introduced.

At the very least this will make the job of police forces and computer investigators a lot easier as they will be able to work within clearly defined parameters, avoiding some of the confusion currently experienced.

However, the sheer mass of illegal material on the Internet, and the practical difficulties in identifying and locating the people who put it there, will mean an even higher workload on law enforcement agencies. A comprehensive solution will only be reached with compromise and co-operation from all. ■

Is encryption the key?

The Compuserve debate has sparked a row over the police's right to break encrypted data in Germany. There are calls for manufacturers of security devices to provide the police with 'keys' to their products which would allow the code to be cracked on some of the information sent over the Internet.

Interior minister Manfred Kanther said at a conference of the Federal Agency for Information Technology Security in Bonn that police work should not be hampered. He said: "The criminals are hiding in the anonymity of the networks, wiping their electronic tracks. Investigating agencies and police are faced with completely new challenges.

"The technical and organisational competence of agencies charged with fighting computer crime must be strengthened. The artificial world is in the end a lot like the real world. Where there is light there is shadow. We will confront the dark sides and fight them decisively."

But others in the Government are less enthralled by the prospect of letting law enforcement officials tap into encrypted phone calls and computer data. German economics minister Guenter Rexrodt said he was against limiting the use of encryption products and that his ministry had prevented such a law.

Legal jurisdiction of the Internet is brought into question - individual states have their own laws, but there is no comprehensive policy internationally.

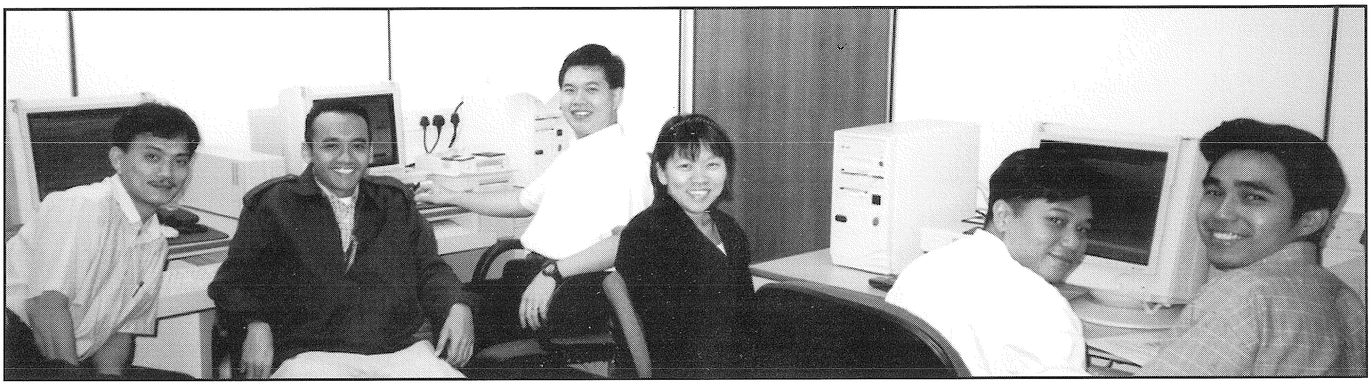
The Web of hate

The Internet is often dismissed by the ill-informed as a plaything for the technically minded, with little impact in the real world. But Germany has a very real reason to be worried about the capabilities and potential the Web gives some minority groups to grow and spread their propaganda. Recent figures show that right-wing hate crimes surged in 1992 to 2,639 cases, but fell to 781 last year following several laws and bans on extremist groups.

However, the Internet has given a new platform to the estimated 6,000 militant right-wingers and their 35,000 sympathisers, offering those behind the groups the security of being able to distribute propaganda and recruit new members from the comfort of their own home. Vice president of the German Government's Federal Office for the Protection of the Constitution, Klaus-Dieter Fritsche, said: "A particular concern above all is that in foreign countries the neo-Nazi or revisionary propaganda that is punishable by law in Germany is available on the Internet and accessible to every Internet surfer."

Fanatics and militia groups in the US are also thought to be using the Internet to communicate and spread their message. Through the various newsgroups and Web sites they offer tips on armed combat, survival techniques and weapons and equipment for sale. The Southern Poverty Law Centre in the US, which tracks right wing groups, said in a report: "The computer is the most vital piece of equipment in the patriot movement's arsenal." It added that the number of armed groups has risen by at least six per cent since 1995 to about 440 in the 50 states.

The Singapore Police Force



Computer Crime Branch

A comprehensive approach to providing solutions to the problems posed by computer related crime is seen in the response of the Singapore Police Force. For the first time in SE Asia a full computer forensic laboratory facility and computer crime response team has been set up at police headquarters in Eu Tong Sen Street in Singapore. The Computer Crime Branch will provide dedicated computer forensic services.

Recognition of the need for a computer crime unit can be traced back to the passing into law of the Singapore Computer Misuse Act in August 1993. This delineated four main offences as prosecutable under the act:

- Unauthorised access to computer systems in order to read or remove data i.e. copying of a database without permission.

- Unauthorised access to computer systems with intent to commit fraud i.e. hacking into a bank's computer system in order to fraudulently transfer funds by electronic means.

- Unauthorised modification of data i.e. addition of false information to a database.

- Unauthorised interception of computer data during transmission i.e. intercepting transmission of data across a network in order to illegally gain information.

The Computer Crime Branch has responsibility for full investigation of all aspect of crimes committed within the terms of the act. This includes not only the conventional investigative process but also computer forensic examination comprising copying of suspect machines, examination and analysis of content, and presentation of findings to defence and courts of law.

The Branch will also provide a computer forensic service to the rest of the Singapore police force. In this role they will not be responsible for the investigation but will supply specialist support for any case where a computer is either found at the scene of a crime or believed to contain information, which may or may not be evidential, pertinent to the solution of a crime. In this role the Computer Crime Branch officers will work closely with the investigators to provide any necessary technical support.

The team comprises a mixture of skills. Some members are highly skilled investigators with limited computer knowledge. Others have advanced technical skills but limited hands on experience of actual investigations. It is anticipated that this mix will produce a strong team capable of responding to any anticipated situation. It is expected to result in the establishment of a new breed of 'computer detective'.

The Computer Crime Branch is part of the Commercial Crime Division of the Criminal Investigation Department (CID). It is headed up by Mr Tan Swee Wan, a respected detective with a wealth of experience gained in the investigation of commercial fraud.

Mr Tan is in charge of two teams of investigators, each team under the control of an Officer-in-Charge, supported by one Senior Investigation Officer, two Investigation Officers and two Assistant Investigation Officers. The teams will alternate with each other to provide permanent cover.

The Computer Crime Branch is currently located in temporary accommodation within the Singapore Police Force CID Headquarters compound. It is housed in a purpose built, air conditioned, humidity controlled, two storey office block.

On the upper floor there is office accommodation for all team members with full support services. On the lower floor there is a conference/lecture room with advanced electronic presentation equipment, a copying room, an analysis room, an evidential storage area and office accommodation for the Branch head, Mr Tan Swee Wan.

▶

The equipment used for each area is:

Copying Room: Two DIBS® Portable Evidence Recovery Units for image copying

Analysis Room: Three PC based Forensic Workstations each with fast Pentium processors, 32MB of RAM, two removable hard disk drives, one CD ROM reader/writer and an optical disk reader/writer. On one of the removable hard disks forensic software is installed. This includes files listers, sorters and viewers, dedicated forensic search engines, graphic file viewers and printers, floppy disk imaging tools, hard disk analysers etc. The Branch has invested in the most comprehensive and up-to-date software available.

Also in use in the analysis room is a Power Mac complete with CD ROM reader and writer. Although of limited use at the current time it is anticipated that more Mac based work will be undertaken in the future as additional equipment becomes available for this system.

Storage Area: Two types of material have to be stored. Firstly there are the computer systems under examination. These are placed in sealed polythene bags on purpose built shelves. Secondly there are items such as floppy disks and image copies of computer hard disks. These are stored either within temperature and humidity controlled cabinets or, if of an evidential nature, within a fire proof safe.

The Computer Crime Branch has recently completed training and is now fully operational. The Branch will remain in the current accommodation for the next two years while the new police headquarters building is completed.

The Branch will then move into much larger, purpose built accommodation and the current team will form the nucleus for the development of an expanded computer forensic facility designed to meet the demands of the next millennium. ■

Personnel Problem

The bizarre behaviour of a marketing executive had started to cause embarrassment to senior management. The individual had told a series of fantastic and probably untrue stories to colleagues and business associates. Whilst this person was on holiday, a laptop computer was copied and its image examined. A number of fabricated letters, written by the executive, were discovered which made claims that were false and detrimental to his employer. Further fictitious letters purported to come from an outside organisation which even sported its genuine company logo on the letterhead template.

Technical notes

The logo was discovered as a bitmap graphic (.BMP) and had been scanned in using a graphic scanner which had been borrowed from the IT department. There are numerous files available at various Internet sites which offer full colour corporate logos for the Fortune 500 and Times 1000. There are obvious fraudulent applications to which these graphics may be put. Many of the letters were discovered by the simple expedient of running Norton Unerase against a DIBS® image. In the author's experience, it is extremely rare for evidence to be found this way; of approximately 400 inspections undertaken so far, only two have revealed evidence using Unerase. As an observation, most residual data is found in slack space which Unerase cannot access. The dates and time stamps of the letters were compared with the company's fax logs which revealed a likelihood that some of them had been faxed to commercially sensitive third parties. A fax header template was found but without any recipient details. When interviewed, the suspect admitted writing and sending the letters to unauthorised third parties.

Misguided investigations have often resulted in Norton being used systematically to unerase files which are found to contain no evidence; the investigator concluding, wrongly, that no evidence resides on disk. It is important, therefore, that anyone examining computers understands DOS allocation units and the phenomenon of slack space. Allocation units on modern operating systems such as Windows 95 are typically 32 kilobytes in length which gives rise to a huge potential for residual data to remain on disk.

Erased files should not be revived on a DIBS® image itself as this will change the contents of the FATs (File Allocation Tables) and the root directory. In any event, evidential DIBS® images should remain write-protected at all times which effectively pre-empts the incorrect use of Norton or other disk utilities. Instead, unerased material should be copied to a non-evidential disk using the Unerase "Save as" facility. Alternatively, erased data may be copied out to a non-evidential drive at sector level using a disk editor.

This case, like many others, required the use of experienced interviewers. The single most important point about confronting a suspect in interview is that this must only be done by an experienced interviewer who has a thorough understanding of the investigation and the technical issues involved. The experienced interviewer will be conversant with the rules of libel, privilege, the Police & Criminal Evidence Act, self-incrimination, when and how to formally caution a suspect, the laws governing entrapment and the procedural methods necessary to disprove subsequent accusations about intimidation, coercion, sexual molestation or harassment which can arise, even when a verifiable confession has been made. Generally speaking, Personnel Departments and Human Resources staff do not have the experience or knowledge to conduct such an interview. ■

The above case study is provided by **Edward Wilding**, *Senior Consultant at Network Security Management Ltd, who may be contacted at the following addresses: edward@nsml.com, Compuserve 101377,2675.*

What Time Is It? *part 2*

Time recording may seem a trivial part of the work of the computer crime investigator, but it can carry heavy implications for the success of a case. The time signatures can record when certain activities took place and can forensically link individuals with their actions. Unfortunately it is not quite as simple as reading the time from the computer screen, and in last month's Journal Dan Mares looked at some of the problems dealing with file times on Windows NT and WIN95 file systems. Here he presents a short list of programmes, available on the Internet, that can keep your system clock synchronised to various "time servers" around the world, and also gives an overview of software he has written which helps investigators when dealing with file times.

With Windows NT and 95 there are actually three file times available: file creation time, last modification time, and last access time. Last month's article provided in-depth information about these three times. (Please note: when mentioning file dates or times, I use the term date to mean the combined file date and time for simplicity.)

First let me list some programs I have found on the Internet which I use to set the correct time on my computer. Simply search the web for keywords in the filenames to locate the programs.

These packages are designed to work under NT or WIN95, although I have found that most authors also have versions for other operating systems. Most of them will not work through a firewall, and one is designed to work through a modem under MS-DOS. Some are free, some provide demo versions, and some are for sale.

You can also look at:

http://www.eecis.udel.edu/~ntp/software.html or http://tycho.usno.navy.mil/ctime.html for additional software. Most of the servers I have found are located in the US, however, there are many other servers located across the world. Here is a short software list:

4DTIME40.ZIP, ATOMCLK.EXE, NBSCOM.EXE, NETDATE.EXE, SNTP.EXE, YATS32.EXE.

In doing forensic analysis on hard drives it is good practice to always work on an imaged copy, and have a write blocker installed.

Let's assume that at a minimum you will be using a file viewer to view suspect files. File viewing and most file operations will attempt to alter the access date of a file. If a write blocker is installed, it may not allow this operation and this poses a problem. You can turn off the write blocker when viewing files and performing other operations, or live with the inconvenience that it presents. (At this point, I'm going to assume the write blocker is inactive so you can use your viewer and you are working on a copy of the evidence.)

For the remainder of this article, I will present a procedure and some file cataloguing or inventory programs that will provide you with a strong defensible position when facing challenges about file dates. I will generally assume the investigator is using Windows NT. However, most of the techniques (except those dealing with last access time) will also work on WIN95 file systems.

Here is the procedure: As soon as possible during the analysis the investigator should create some sort of inventory of all the files on the system. Most methods use software that lists the last modified date of a file. (The simplest command might be DIR/AHS.) This is because the last modified date is the one which File Manager and DOS present.

For some investigations this file date may not be the best, or you might want to record one or both of the other file dates. Since this discussion focuses on file dates, I will describe only those aspects of the programs dealing with date processing. In order to get a complete feeling for the operation the user needs to try the program(s) and become very comfortable with its use.

One program I have created is called HASH.EXE. This program will produce a list (similar terms might be "catalogue", or "inventory") of every file on the disk, providing you with the necessary "inventory" of all the files. The output record produced includes the file name, file size, MD5 hash value of the file and one of the three file dates (whichever one the user selected).

Even though this discussion is about file dates, I feel it is important to take a slight detour and touch on the MD5 hash value and its value in ensuring file integrity. In the US we feel that one of the most important aspects of forensic analysis is being able to show that your examination did not alter any part of the original file or evidence.

A way to do this is calculate a CRC, Checksum, or Hash/Signature value of the file. These calculations are all basically the same in that they perform some sort of mathematical calculation using every bit of the file. The final value is the CRC, Checksum, Hash or Signature of the file. Depending on the algorithm used the chances are from roughly one in 64,000, to one in two times 10^{34} (that's 10 with 34 zeros) that two dissimilar files will produce the same value. ▶

When two dissimilar files produce the same value that is usually referred to as a "collision". If a strong algorithm is used to calculate the initial value of a file, then at a later time if that value hasn't changed, you can be pretty certain the contents of the file hasn't changed. MD5 is the algorithm where the chances of two dissimilar files having the same value is two times 10^{34}. That's pretty good odds in anyone's book.

Searching the Internet on MD5 will produce many documents describing the operation and reliability of this algorithm. MD5 is a strong enough algorithm to satisfy even the most sceptical.

Back to the HASH.exe program. HASH can be used initially to produce a list of every file with its last access date. (Remember WIN95 doesn't use last access time, just the date. On WIN95 systems the last access time is 00:00). After the initial run to record the last access date, you might run the program again to list the last modification date, and a third time to record the creation date. Running the program as soon as possible will provide the investigator with a "checkpoint" of the status of the files before virtually any forensic analysis was done. At a later time, if a program was used that altered the last access date the investigator would have an arguable defence and be able to show what the original access date was. This may be a very important file date.

This simple procedure of creating an inventory of every file on the system, including its various file dates, is one of the most important forensic steps you will do.

Using software to produce output which is meaningful and manageable will help you in your analysis. It is not unusual with today's large systems to find over 10,000 files on a stand alone computer, and networks compound the number of files which need to be catalogued.

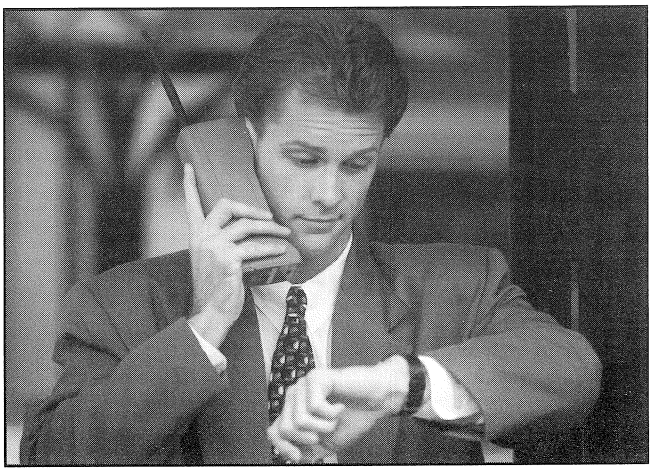
The next two programs I will talk about are also capable of producing file listings. They just operate in slightly different ways, and the investigator may choose to use any or all in the forensic analysis.

The second program, called DISKCAT.exe, also has the capability of recording all three dates. The name DISKCAT is short for "disk catalogue". As you might expect, this program will produce a catalogue of every file on a disk. As part of its operation in addition to the normal filename, date, and size, it can list any of the file dates, generate a 32 bit CRC, and show what type of program generated the file. It does all this in a fixed length record for easy importation into a data base for future analysis.

This program only changes the last access file time when the CRC is requested. All other modes of operation do not alter any file times.

The third program is one called CRCKIT. This program will calculate the 32 bit CRC of a file. It also has the capability of listing any of the three file dates chosen. Like HASH, CRCKIT attempts to reset the file dates so no significant alteration is produced. It does not have all the capabilities of HASH and is mainly used for single directory listings. However, for a file by file validation, it is excellent.

The last program is called MDIR.exe. The MDIR program is designed to be an intelligent replacement for the DIR command. MDIR produces an output listing with the look and feel of the DIR command, but provides much more capability. As one of its enhancements, MDIR will show any one of the three file dates based on the users choice. MDIR is a "quick and dirty" method of doing an intelligent DIR of a directory. It can also be used to display any one of the three file dates of a file(s).



HASH, DISKCAT and CRCKIT when requested to calculate the MD5 or 32 bit CRC of a file will open and read the file in order to compute the values. Because they open the file for reading, the operating system resets the last access date of the file. There is absolutely no way around this.

However, the programs are designed to restore the date on all files to the original value. This restoration of original date does make changes to the disk, but produces no significant alterations.

With advanced operating systems in use today, it becomes almost impossible to run a system without the operating system itself changing items on the disk. If you are prepared to testify why you turned on the system, and that the operating system altered the disk, you should have no problem explaining this operation.

If changing the date back to its original value poses an evidentiary problem, the user should use the HASH or DISKCAT program and not request the MD5 or CRC calculation. This operation without any calculations will not open any file and will produce only a catalogue of the disk. In this mode, no file opening takes place, and the operating system doesn't alter file dates. But all you get is a file listing, and no numeric validation as to the integrity of the file. You must choose which you prefer, but don't forget that you are still working on your copy. ▶

At the time of writing HASH, DISKCAT, and CRCKIT cannot reset the date of read-only files, but by the time you read this that problem should be solved.

In summary:

- During a forensic examination, the investigator should make certain the forensic computer has the correct time set. To do this obtain appropriate software to synchronise the computer's clock with a standard. Record the time on the suspect's machine to determine the difference of computer times.

- When dealing with advanced operating systems like Windows NT and WIN95 be aware that the system maintains three file dates and that almost any operation will alter the last access date.

- Create a listing, catalogue of every file on the suspect system with its appropriate date and time. If necessary take appropriate precautions when dealing with last access date on the computers. ■

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

Dan Mares is a special investigator for the Internal Revenue Service in the US working in Atlanta, Georgia.

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

Remember that you must always do your forensic analysis in a way that follows acceptable evidentiary procedures. Each country and each agency within that country may have specific regulations concerning processing of evidence. Nothing I present here is intended to alter or circumvent those requirements.

Book Review

High-Technology Crime

Investigating Cases Involving Computers

by Kenneth S. Rosenblatt
KSK Publications, PO Box 934, San Jose, California 95108-0934, USA.
603pp. ISBN: 0-9648171-0-1.
US$69.95 (plus postage).

Computer crime is a relatively new phenomenon presenting a whole new set of challenges. The pitfalls for the unwary are numerous, with potentially huge legal and practical problems arising from the collection, analysis and presentation of data.

Kenneth Rosenblatt's book High-Technology Crime aims to give the newcomer to the field a much-needed grounding, taking the reader from basic definitions right through to step-by-step investigations. He looks at a wide range of computer-related crime, including the damage done by hackers, the theft of information and data stored on computers, and how to search, seize and study evidence. Embezzlement, computer viruses and software piracy are not covered, but are large enough areas for books in their own right.

Rosenblatt himself is a deputy district attorney in California's Silicon Valley, and he has headed that office's high technology unit for four years. He has given advice and provided testimony on computer crime to the US Congress, the Department of Justice and the California Legislature and has an in-depth first hand knowledge of his subject.

The book has been written for a wide audience, including police and law enforcement agencies, corporate and private investigators and lawyers. The author steers clear of the jargon trap and the material is covered in a straightforward and easy to understand way. No previous experience is assumed, and a full introduction to the basics of computer hardware and software is given.

The book advises how to tackle a case in both the public and corporate sectors, guiding the investigator on the protocols to observe and decisions to be made, as well as the major mistakes to be avoided. One chapter deals exclusively with the physical theft of computer components and the methods used to find the suspects and recover the parts. Computer intrusion, or hacking, is also looked at thoroughly and the methods of tracing and tracking the culprits are outlined, although the sub-chapter on the Internet gives only brief details on this ever expanding area.

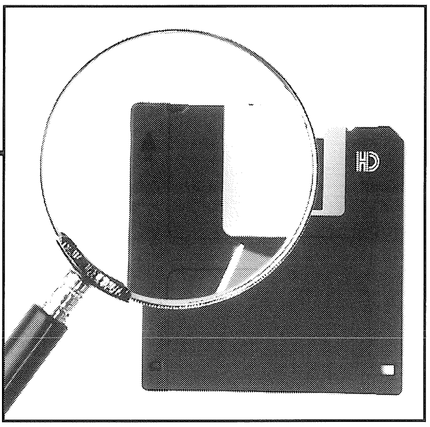
Rosenblatt's chapter on searching, seizing and analysing evidence gives a rough idea on how to tackle investigations, with the caveat that this is a subject for experts only, who know exactly what they are doing. Therefore the information cannot constitute a do it yourself guide, but is more a basic grounding for those starting in the field. The book is written more or less exclusively from a US-perspective, with detailed chapters on computer crime and its relation to the legal system, including details on the Fourth Amendment, Federal privacy laws and drafting search warrants.

This is great for US-based investigators, but of much less consequence for those elsewhere in the world whose countries have vastly different laws and constitutions. However, many of the principles and ideas mentioned still stand and investigators can only benefit from a greater understanding of forensic techniques, although they will have to take expert help on the legal details.

Overall, this is a useful and stimulating book for anyone involved in computer crime investigation. While it is ideal for those approaching the subject for the first time, it is still a great help for the more experienced who can use it as a reference work, dipping in whenever necessary. Well-written and concise, High-Technology Crime is a good start to forensic computing and what the book lacks in absolute details it makes up with the breadth of material covered. ■

Reviewed by Paul Johnson

Forensic Q&A



Q *During an investigation of a hard disk I have found a number of files containing colour graphics. I need to present these as a part of my evidence in court. What is the best way of doing this?*

A There are three methods you might consider using, depending on the equipment and budget available. The most impressive presentation, and the most expensive, can be made electronically in court using appropriately placed display monitors and/or a screen projection system (this may be a transparent LCD panel and overhead projector or a dedicated screen projector). The material to be displayed can first be organised onto a CD ROM that can be run on a standard PC. This system will provide a high quality presentation and the option to display from a wide range of material depending on the direction of the proceedings.

In most cases there will not be the time or the money available to use electronic presentation. Where this applies there are two perfectly adequate methods that have been used successfully in court. One is to print the material using a bubble jet or laser colour printer onto special high quality paper. This will give good quality output perfectly suitable for use in most cases. The other option is to have the material photographed as displayed on a standard screen. This will give the court a clear impression of the appearance of the material and it may also be the most cost effective solution. In recent cases this method has been used with notable success.

Q *I have copied the hard disk of a suspect computer and am now looking to examine it. Several thousand files were found on the hard disk and I really don't know where to start. Are there any guidelines on this?*

A An average hard disk will contain between 5,000 and 8,000 files and a high volume hard disk will have 20,000 to 30,000 files. The most difficult problem facing the computer forensic investigator will be how to examine this volume of information as quickly and efficiently as possible. To achieve this, it will be necessary to remain focused and to work in an ordered, structured and methodical manner.

The first action is to sit down and think about what has to be done. Consider carefully the nature of the case being examined. This may sound obvious, but all too often the new forensic analyst will rush off and start looking all over the copied data for 'evidence' without having thought about what such 'evidence' may actually comprise. For example, if it is a fraud case, then what type of fraud involving what type of digital information? If forged agreements are involved then the most likely way they will have been produced is with a word-processor. What word-processor is present and what type of documents does it produce? Are there any of these on the machine? If so, where? This type of approach, which is called structured investigation, will enable you to look in the most obvious places first and only move on to other areas if nothing is found at the previous location.

The background of the suspect or computer operator in question should also be closely considered. This information will help you to decide exactly how far to proceed in the analysis and should be obtained prior to commencing the examination.

For example, if you know that the suspect is highly computer literate then it is possible that information could be deliberately hidden. If, on the other hand, the level of computer knowledge is minimal, then hidden information is unlikely and a detailed deep level search of contents is unlikely to prove fruitful. Information concerning the suspect's knowledge that an investigation is underway can be used in a similar manner.

Armed with such background information, the first task that should be undertaken is a full listing of all the files on the hard disk, including those that have been deleted. A printed copy can then be studied while the hard disk contents are viewed in a suitable display such as Windows 3.11 file manager. Used in conjunction with the background information already considered, this will enable the most obvious areas to be examined first. If the information required is found in this area there may be no need to look any further. If not, then more detailed examination will be required of other more obscure areas of the disk. However, before moving on to such further time consuming examination, do consider carefully the likelihood of finding the required information based on your background knowledge of the suspect.

(Editor's Note - we shall be running a series of articles on the techniques of structured investigation, starting in the August edition)■

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

INFOPOL 97

27-29 May, Hallen Kortrijk, Belgium
Tel: +32(0)56/24 11 11
Fax: +32(0)56/21 79 30

International Police & Security Expo 97

1-3 July, Cardiff International Arena
Contact: Labelex Exhibitions
Tel: +44(0)181 313 3535
Fax: +44(0)181 468 7472

WebSec '97

29-31 July, Cumberland Hotel, London
Optional Workshops: 28 July & 1 August
Conference on Web, Intranet and Internet Security

The agenda includes keynote address from Tom Mulhall, BT Security, on Computer Related Crime: Beyond the Hacker Headlines; The Internet and Criminal Law; Using Cryptography to Secure the Web; The Latest Hacker Tools and How to Combat Them; Information Warfare; How to Handle Computer Crime Incidents. Optional workshops allow the exploration of topics in-depth.

Contact: MIS Training Institute
Tel: +44(0)171 779 8944
Fax: +44(0)171 779 8293

Security Workshop

6-8 September, Hamburg, Germany

The European Institute for Computer Anti-Virus Research plans to hold a three day security workshop at the University of the German Federal Armed Forces in Hamburg. The event is being supported by the German Ministry of Defense, the NATO C3 agency and NCSA, US. The workshop aims to cover aspects of IT security ranging from threat and risk assessment, through to the implementation and configuration of technical security measures and on to the secure operation and lifetime management of IT systems. Other issues to be covered include viruses, network attacks and the recovery from hacker attacks, post-attack investigations, law enforcement and computer forensics. The event also aims to cover legal, ethical, and social aspects of IT and the Internet.

Further details: http://www.eicar.com

COPEX (Police & Security Exhibition)

30 September-2 October, Farnborough, UK
Contact: Defence Manufacturers Assn.
Tel: +44(0)1428 607788
Fax: +44(0)1428 604567

Computer Security Institute's 24th Annual Computer Security Conference and Exhibition

17-19 November, Washington DC, US

CSI's annual conference will feature over 120 sessions on topics including Internet & WWW, Intranet, Network Security, Electronic Commerce, Computer Crime and the Law, Telecommunications, Audit and Risk, Encryption.

Contact: CSI
Tel: +415 905 2626
Fax: +415 905 2218

MILIPOL PARIS '97

24-28 November, Le Bourget, France

10th MILIPOL PARIS international police and public security exhibition.

Contact: IMEXPO
Tel: +46 27 82 00
Fax: +46 27 91 63

International Conference on Forensic Computing

3-5 December, The Grand Hotel, Brighton, UK

A unique three day conference to be addressed by speakers from across the world, covering computer crime, investigation and forensic evidence.

Experts from a wide range of forensic computing fields will be attending, as well as exhibitors from firms involved in this fascinating area.

Places on the conference, which is being held in one of the best hotels in the seaside resort of Brighton, are limited and anyone interested should get in touch as soon as possible.

Contact: International Journal of Forensic Computing
Tel: +44(0)1903 209226
Fax +44(0)1903 233545
e-mail: ijfc@pavilion.co.uk

TRAINING

Training in Computer Forensics

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

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

Reader's Response

Marian Svetlik, a computer crime investigator based in Prague, has written in with advice following a piece on seizing Mac computers featured in the Journal Forensic Q&A section in Issue 3.

Because the Mac operating system writes some system information on attached disks, we have tested one little trick to avoid this. We make a physical image of the seized disk using Norton Diskedit and then restore it on a magneto-opticalcartridge, and set the write-protect switch on it. Mac then correctly attaches this disk as the second disk (in external drive, connected to the computer using SCSI cable) and does not write anything to it.

Marian Svetlik, Computer Crime Unit,
Institute of Criminalistics, Prague.

International Journal of
FORENSIC COMPUTING TM

Published by
Computer Forensic Services Ltd.