IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

JOURNAL
volume 14 number 4 autumn 2004 ISSN 1741-4229

Programme for members' meetings 2004 – 2005

Tuesday 7 September 2004 Late afternoon	**Computer Audit Basics 2: Auditing the Infrastructure and Operations**	16:00 for 16:30 KPMG
Thursday 7 October 2004 Full day	**Regulatory issues affecting IT in the Financial Industry**	10:00 to 16:00 Old Sessions House
Tuesday 16 November 2004 Full day	**Networks Attacks – quantifying and dealing with future threats**	10:00 to 16:00 Chartered Accountants Hall
Tuesday 18 January 2005 Late afternoon	**Database Security**	16:00 for 16:30 KPMG
Tuesday 15 March 2005 Full day	**IT Governance**	10:00 to 16:00 BCS – The Davidson Building, 5 Southampton Street, London WC2 7HA
Tuesday 17 May 2005 Late afternoon AGM precedes the meeting	**Computer Audit Basics 3: CAATS** ***Preceded by IRMA AGM***	16:00 for 16:30 KPMG

Please note that these are provisional details and are subject to change.

The late afternoon meetings are free of charge to members.

For full day briefings a modest, very competitive charge is made to cover both lunch and a full printed delegate's pack.

For venue maps see back cover.

Contents of the Journal

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

Refereed articles are academic in nature and reflect the Group's links with the BCS, which is a learned institute governed by the rules of the Privy Council. Articles of this nature will be reviewed by our academic editor prior to publication and may undergo several iterations before publication. Lengthy dissertations may be serialised.

Technical articles on any IS audit, security, or control issue are welcome. Articles of this nature will be reviewed by the editor and will usually receive minimal suggestions for change prior to publication. News and comment articles, dealing with areas of topical interest, will generally be accepted as provided, with the proviso of being edited for brevity. Book and product reviews should be discussed with the appropriate member of the editorial panel prior to submission. All submissions should be by e-mail and in Microsoft Word, Word-Pro, or ASCII format. Electronic submission is preferred.

Submissions should be accompanied by a short biography of the author(s) and a good quality electronic digital image.

Submission Deadlines

Spring Edition	7th February	Autumn Edition	7th August
Summer Edition	7th May	Winter Edition	7th November

The ***Journal*** is the official publication of the Information Risk Management & Audit Specialist Group of the British Computer Society. It is published quarterly and is free to members.

Letters to the editor are welcome as are any other contributions. Please contact the appropriate person on the editorial panel.

Editorial address:
47 Grangewood,
Potters Bar
Herts, EN6 1SL
Email: john@lhscontrol.com

Designed and set by Carliam Artwork, Potters Bar, Herts
Printed in Great Britain by PostScript, Tring, Herts.

Editorial

In my last column I reported on my woes as a result of BT Yahoo changing the IP addresses of their Domain Name Servers without telling their customers. At that time I had only received a holding response from them in relation to my letter of complaint to Sir Christopher Bland, the BT Chairman. Since then I have had some interesting conversations and correspondence with someone designated as an 'Open World Complaints Review Executive'. A fancy title for someone who apparently does nothing else but review complaints. Nothing in the job title about resolving them you notice and that's a good job too as this guy was totally useless in not only explaining what had gone wrong, but also in not giving me any satisfaction that such a thing will not happen again in the future. Indeed, so useless was he that he provided me with incorrect information regarding the change that had caused the problem so I then had to correct him, not once but twice. I was so incensed by this lack of professionalism in a company that is both ISO 9000 and ISO 17799 accredited that I wrote again to Sir Christopher expressing my displeasure at the way my complaint had been handled. But Bland by name is bland by nature and all I received this time was a reply from yet another assistant thanking me for my views! Still I have been given three months free access, which is what I demanded when I first complained, but I only got that after querying why they were offering me only two months! To add insult to injury BT have since reduced their monthly charge by three pounds. Why is this an insult? Well, they are going to impose a usage restriction based on data transfer over the web. To someone who listens to web radio whilst they do their work as I do this will mean a reduction to my service. Hey ho, another letter to Sir Christopher perhaps?

The postal voting debacle in the recent local authority and European elections and the subsequent claims of electoral fraud will be as nothing if the Government go head with their proposals for the extension of electronic voting. I have been looking into this issue on behalf of the BCS and am greatly concerned with the various proposals being put forward by the Office of the Deputy Prime Minister. I have been liaising with a number of other computer societies on this issue and there is universal concern that security will just not be good enough to prevent massive electoral fraud. There is always going to be a conflict between ease of access and security, as we control professionals know, but it is important to balance the two. To my mind the Government proposals are putting too much emphasis on ease of access and not enough on the prevention and detection of electoral fraud. The use of computers invariably means that a few powerful people (in some instances perhaps only one) can manipulate the result. With the postal voting fiasco the Government ignored the advice of the Electoral Commission so I am not too hopeful that it will take any notice of the BCS, but we can try.

On to the content of this issue. Greg Krehel continues with his tips on how to conduct an investigation by examining the concepts of case analysis. This ties in nicely with the first of a sequence of articles dealing with computer forensics by Celeste Rush, our very own membership secretary, who did her MSc dissertation on the subject. Bob Ashton our correspondent from the antipodes updates us on risk and computer crime in Australia, which brings me to the unrelated area of the IRMA accounts which you can examine at your leisure. Priscilla Emery reminds us of the importance of paper in our business continuity planning and Colin Thompson, the BCS Deputy Chief Executive, does his usual excellent job of keeping us current on what is happening in our parent body.

The summer is now over and for some of you this may be the last edition of the Journal that you receive. Unless of course you have renewed your subscription!

John Mitchell

Chairman's Corner

Email addresses

You will have noticed a change in the format of the subscription renewal forms this year. This is part of a drive to improve the communications within IRMA. The key aspect of this is that we are able to use your email address to alert you to forthcoming IRMA events and other events of interest to members.

To do this in accordance with data protection legislation and the like, we do need your permission. A short message outlining that your are happy for IRMA to contact you about matters of interest to the membership is enough. If you have not supplied your email address yet, please can I ask you to do so.

We will not be selling or marketing the email addresses for any other organisation to use, so your permission will not result in an avalanche of spam.

You will need to quote your IRMA number so we can track your record down. The email address to use is at the bottom of this column.

Spyware/Adware

At the time of writing, it's the silly season, when news is thin, and not much is going on... at least that's how it's supposed to be. This year, just as the holidays are getting under way, I see stories in the press about spyware and adware.

This is software which is installed without your knowledge. There appear to be two ways in which this occurs.

Firstly with your consent when you install 'special packages' with unbelievable promises attached. The conditions to monitor your PC and spy on you are either hidden in the small print (how often do you read all those terms and conditions?) or 'accidentally' omitted. The types of promise include speeding up your download speed, removing spam from your email address, solving world peace - you get the idea.

Secondly, they are installed without your consent taking advantage of security weaknesses in Windows and Internet Explorer to install unwanted objects on your PC.

In the first case, if you remembered that you installed that 'useful package' you might know what caused the problem. In the second, you just don't know that the software is there.

Therefore the old dictum about 'not downloading unauthorised software' becomes even more relevant, however instead of merely causing software conflicts between your children's favourite computer games and your word processor, the software now installs modules which can compromise your PC and are difficult to remove without a complete Windows rebuild. I'm sure that versions for other operating systems are just around the corner.

Once installed, the software can perform any function, from a relatively harmless piece of internet site traffic monitoring (though traffic monitoring is in violation of the data protection act) to software capable of logging keystrokes or taking over your PC. I 'have a friend' - no really, I do! - whose PC only connects to the internet if an undesirable site is displayed first. If it isn't allowed to do this, then the internet is not available. The PC has been compromised without his or her knowledge, and needs a rebuild.

For companies, once again the advantages of good enterprise infrastructure management become apparent, all to maintain the integrity of systems and weed out unauthorised software installations. Hardly a new message, by any means.

So if you use Windows and have not checked out the Microsoft Update site, then you should consider doing so urgently!

BCS membership changes

I mentioned the changes to membership in the last corner. If you know someone (or indeed are someone) who has significant experience in the IT industry who would benefit from BCS membership, please contact the committee for more details. The new MBCS membership is based upon recommendation and experience. However, for those who have already gone the whole nine yards, becoming a chartered member is still as difficult as ever!

As ever, please contact the Management Committee with any ideas you have for courses to run, things you would like to see from IRMA, etc. Please email admin@bcs-irma.org.

Looking forward to the busy season .....

Alex Brewer (MBCS!)

The Down Under Column

Bob Ashton – IRMA Oceania Correspondent

Australian Information Risk Standards

Handbook 231:2004 Information security risk management guidelines (HB 231) has recently been published by Standards Australia (www.standards.com.au). This is a revision of the previous version of the handbook to be consistent with **BS7799.2:2002 Information security management Part 2: Specification with guidance for use**. It should therefore be useful to anyone applying information risk management consistent with the British Standards.

AS/NZS 4360:1995 Risk management set out to provide a generic framework for identification, analysis, assessment, treatment and monitoring of risk and is internationally recognized as an authoritative source in risk management. The original version of **HB 231** set out to align **ISO/IEC TR 13335, Information technology – Guidelines for the management of IT security** with **AS 4360**, while the current version builds on these foundations and goes on to reconcile these guidelines with **BS7799.2. ISO 17799** and **BS 7799.2** both require that a risk assessment process is used as the basis for selecting controls. HB 231 complements these standards by providing additional guidance concerning the management of information security risks, and may be applied at all stages in the life of an activity, function, project, product or asset.

The Handbook provides a good explanation of the reasons for information security risk management and provides examples of quantitative and qualitative evaluations and the various methods of risk treatment. The baseline approach to risk treatment is mentioned, but in a very cursory manner.

The Handbook will be useful to any organization wishing to apply information risk management in a standardized manner.

Failing to Cope

The third annual **Australian Computer Crime and Security Survey** was published in May, and is available from: www.auscert.org.au. Compiled by AusCert, Federal and state police forces and the Federal Attorney General's Department, the survey attempts to paint a broad picture of the state of computer security for organizations in Australia. The **2004 Survey** was adapted from the CSI/FBI Computer Crime and Security Survey, available from: www.gocsi.com and includes several new questions designed to deepen understanding of the key factors which contribute to electronic attacks and other forms of computer crime. **In a disturbing turn, the Survey concluded that efforts being made by respondent organizations to improve their readiness to protect their systems appear to be insufficient to cope with the changing nature of the threats and vulnerabilities to which they are exposed**. Although organizations are spending more money and are better prepared than ever in terms of security, the tide of malicious code is rising faster than many organizations can cope with. This includes the increased number and severity of system vulnerabilities and the number and rapid propagation of internet worms and viruses.

88% of respondents experienced externally sourced attacks, while 34% experienced internally sourced attacks. Threats were reported in the following order of importance:

- Infections from viruses, worms and Trojans
- Theft of laptops
- Abuse and misuse of computer network access or resources.

The readiness of organizations to protect their IT systems has improved in three key areas:

- The use of information security policies, practices and procedures
- The use of information security standards or guides
- The number of organizations with experienced, trained qualified or certified staff.

Unpatched or unprotected software vulnerabilities and inadequate staff training and education in security practices were identified as the two most common factors which contributed to harmful electronic attacks.

As well as providing an example of human wickedness, the following anecdote taken from the Survey raises serious questions in regard to the usefulness of auditors.

"Citing evidence of transactions made using a junior clerk's userid, an auditor claimed that the clerk was fraudulently diverting funds from the company's payroll. The clerk was summarily terminated and asked to repay the funds or face criminal charges. The company's lawyer engaged a computer forensic consultant who examined various company computers. The clerk's union-provided solicitor requested an independent examination of the evidence, which revealed the suspect transactions were in fact made by a company director pretending to be the clerk. Examination of company emails also revealed that the company requested its forensic consultant to make certain omissions in his report.

The clerk no longer wished to work at that company and agreed to a substantial termination payment along with signing a deed of confidentiality. The company director had already returned the money and resigned and the alleged fraud was never reported to the police."

The accompanying commentary also questioned the ethics of certain computer forensic examiners, who claim the status of independent witnesses in litigation. The Expert Witness Code of Conduct, as required by the New South Wales Supreme Court, states: "an expert witness has an overriding duty to assist the Court impartially on all matters relevant to the expert's area of expertise." In other words, an expert is duty bound to report both incriminating and exculpatory (ie, proving innocence) evidence. This duty is especially important when dealing with computer based evidence that is relatively easily misinterpreted (at best) or tampered with.

Australian "Nigerian"

The 39 year old Sydney disability pensioner mentioned in a previous edition of this column has not wasted his time since his arrest last October. In addition to his original scam which fleeced victims of more than $5 million, police have now charged him with 7 new offences, allegedly committed in custody, claiming he used false tax returns to obtain a $720,000 loan and wrote letters to his wife and girlfriend to pervert the course of justice.

Getting Case Analysis off to a Fast Start

Greg Krehel

This is the third in a series of articles which will deal with best practice in compiling information required for civil or criminal litigation. The best practices described are equally relevant to the audit process. In this article Greg explains the basics of identifying the principle and supporting characters in a case. – Ed

From your first conversation with a prospective client, you're learning about the dispute that led the individual or corporation to seek counsel. There are many benefits to taking a systematic approach to analyzing this knowledge. Not least of these is the favorable impression you'll make on those who retain you.

The following article presents a method for organizing and evaluating the facts about any case. And it illustrates how the early results of this dispute analysis process can be used to great effect in an initial case analysis session with your client.

Standardizing the Case Analysis Process and Work Product

My partners at DecisionQuest and I have spent the past 15 years conducting jury research studies on all manner of civil and criminal cases. In the course of this work, we've had the opportunity to try many methods for analyzing case knowledge. We've developed a process that I hope you'll find both simple and useful.

When you take this approach to case analysis, you'll gain a thorough understanding of the dispute and clarify your thinking about it. And, as you sort out what you do know about the case, you'll find it easy to identify what you don't know and need to find out.

The process focuses on creating four analysis reports – a Cast of Characters, a Chronology, an Issue List, and a Question List. These reports provide a framework for organizing and evaluating critical case knowledge. If multiple people are involved in the analysis process, the reports provide a way to divide responsibility and share results. Moreover, once you standardize the analysis work product, it's easy to compare the findings in one matter to the analysis results from other similar disputes.

You should begin the dispute analysis process as soon as you've had your first discussions regarding a new matter. Perform an initial round of case analysis to organize the limited information you have about the case. Then meet with your client to review the reports you've created.

You'll discover that a case review session conducted as a structured walk through of your dispute analysis reports produces far better results than an unstructured discussion of case details. It gives you a firm grasp on critical case details and confidence that you've eliminated any points of miscommunication between you and your client. We provide the agenda for such a meeting below.

Please note that the value of early organization and evaluation is not limited to instances when you've already been engaged. I believe you'll find that performing a quick dispute analysis and sharing the results with your prospective client is a terrific way to differentiate your firm from the others seeking to be retained on a matter.

I encourage you to make these analysis techniques standard operating procedure, a process you employ on every case, even ones that may be simple. Why? First, we're all familiar with disputes that appeared minor but which turned out to be costly disasters. By analyzing all cases, including those that seem small, you ensure that you aren't just seeing the tip of the iceberg. Second, even small matters have more facts, more players, and more issues than anyone can meaningfully organize and evaluate in his or her head. Third, the practice gained analyzing small cases makes you more proficient when working up larger ones. Finally, the amount of time required to analyze a case is proportionate to its size. If the case is as small as anticipated, it will take little time to do the analysis.

The Analysis Work Product

The analysis reports we encourage you to create are essentially tables listing critical information. They are long on knowledge and short on prose. They are tools that you use throughout the organizational process, not a summary created once analysis is complete. In fact, once you begin to employ these analysis reports, you may find a narrative summary unnecessary. When you write a narrative case summary, a great deal of the total effort must be devoted to working on the style of the report (the outline, phrasing, and grammar). Is the narrative summary adding enough value to the analysis to justify the hours spent eradicating split infinitives and other grammatical evils?

You should create your case analysis reports using database software, not a word processor. Database software makes the knowledge you're organizing far easier to explore and evaluate. For example, using database software, it's easy to filter your Chronology so that it displays only facts that have been evaluated as being particularly troublesome.

Another advantage database software has over word processors is support for replication and synchronization. A replica is a special copy of a database file. Synchronization is the process of merging the changes made to the information in the replica back into the master version of the file. When trial team members go on the road, they can take replicas of the case analysis file along, and make additions and updates to the Cast of Characters, Chronology, and other analysis reports. While these individuals work in replicas, trial team members back in the office are free to make changes to the master version of the case file. When a replica is returned to the office, it is synchronized with the master version of the case file, thereby automatically melding changes made in th replica with changes made in the master. These sophisticated features are available in some database packages. You won't find them in any word processor.

Here are the details that should be captured in each of our recommended dispute analysis reports:

Cast of Characters

Create a Cast of Characters that lists the individuals and organizations you know are involved in the dispute. This report should also catalogue key documents and other important pieces of physical evidence. Capture each player's name and a description of the role the person, organization, or document plays in the case.

Also include a column in which you can indicate your evaluation of cast members. Even if you don't evaluate every player, it's essential to note the people and documents that are particularly worrisome, as well as the basis for your concerns. If you follow my recommendation that you build your dispute analysis reports using database software, you will find it easy to filter the entire cast list down to the problem players you've identified.

Chronology

A Chronology of key facts is a critical tool for analyzing any dispute. As you create the chronology, important factual disputes and areas of strength and weakness become obvious.

Begin by listing the fact and the date on which it occurred. As you enter each fact, be sure to make the important details about the fact explicit. For example, rather than simply stating "Gayle phoned David," write "Gayle phoned David, and asked him to shred the Fritz Memo." Remember that your chronology should be a memory replacement, not a memory jogger.

Since you're analyzing the case within weeks of being retained, there will be many facts for which you have only partial date information. For example, you may know that Gayle called David about the Fritz Memo sometime in June of 1993, but be unsure as to the day within June. When you run into this problem, a simple solution is to substitute a question mark for the portion of the date that's undetermined, e.g., 6/?/99.

In addition to capturing the fact and the date, be sure to list a source or sources for each fact. Now, in the early days of a case, it's likely that the sources of many of the facts you are entering in your chronology are not of a type that will pass muster come trial. However, by capturing a source such as "David Smith Interview Notes," you know to whom or what you will need to turn to develop a courtacceptable source.

The mission in early dispute analysis is to take a broad look at the potential evidence. Therefore, your chronology should be more than a list of undisputed facts. Be sure to include disputed facts and even prospective facts (i.e., facts that you suspect may turn up as the case proceeds toward trial). You'll want to distinguish the facts that are undisputed from those that are disputed or merely prospective. Include in your chronology a column that you use for this purpose.

Finally, include a column that you use to separate the critical facts from others of lesser importance. A simple solution is to have a column titled "Key" that you set up as a checkbox (checked means the fact is key, unchecked means its not). If you're using database software, filtering the chronology down to the key items should take you about 20 seconds.

Issue List

Build a list of case issues including both legal claims and critical factual disputes. If the case has yet to be filed, list the claims and counterclaims or crossclaims you anticipate.

Rather than listing just the top level issues, consider breaking each claim down to its component parts. For example, rather than listing Fraud, list Fraud: Intent, Fraud: Reliance, and so on as separate dimensions.

In addition to listing a name for each issue, create a more detailed description of it. The description might include a brief summary of each party's position on the issue and, if it's a legal issue, the potential language of the judge's instruction.

As your case proceeds to trial, your Issue List will increase in importance. You'll use the Issue List to return to the Cast of Characters and Chronology and establish relationships between each fact, each witness, each document and the issue or issues to which it relates. Once you've made these links, it will be easy to focus on the evidence that's being developed regarding each issue and to make decisions about case strategy based on this analysis.

Question List

When you start case analysis early, your knowledge of the dispute is sure to be incomplete. But as you map out what is known about the case, what is unknown and must be determined becomes clear.

Each time you come up with a question about the case that you can't readily answer, get it into your Question List. You'll want your report to include a column for the question and another column where you can capture notes regarding the answer. Also include a column for evaluating the criticality of each question. Use a simple A (extremely critical), B, C, and D scale to make your assessment. Other columns to consider for your Question List are "Assigned To" and "Due Date."

The Initial Case Review Session

Once you've completed your first round of case analysis, it's time to meet with your client to discuss the results. At the client review session, you'll: (1) confirm your initial understanding of the case and eliminate misunderstandings, (2) prompt your client to provide further details about the case, and (3) educate your client regarding case issues.

Before you head off to meet your client, decide whether you want to work offline or online during the client session. By offline, I mean using printed copies of your four analysis reports. By online, I mean working with a laptop and an LCD display, and capturing updates to your case knowledgebase in real time.

The first time you try our method, it probably makes sense to work offline. Once you're comfortable with the flow of the client review session, switch to working online; it's more efficient and more impressive to your client.

Here's the meeting agenda:

R**eview the Cast of Characters.** Ask your client: Who and what is missing? How would you improve on the description I've provided of each key player? Which members of the Cast of Characters do you consider particularly important? Why? Which of these players do you feel are the most problematic? Why?

Review the Chronology. Ask your client: Can you provide complete dates for these partial dates I have listed? Can you provide additional sources for these facts? What important facts are missing? There don't seem to be that many bad facts in our

chronology at this point. There must be other facts that will become problems for us. The sooner I know these facts, the more likely it is I can keep them from causing irreparable harm to our case. Are you aware of any such problem facts?

Review the Issue List. Use it to show your client about the legal and factual disputes likely to be at the heart of the matter. Ask your client: Do you see other issues in the case that I've overlooked? Do you know of any other facts, witnesses, or documents that pertain to these issues that you don't recall seeing in the Cast of Characters or Chronology?

Review the Question List. Use it to show your client the areas that will need to be investigated early in case preparation. Ask your client: Do you know the answer to any of these questions? What other questions do you have about the dispute that don't appear in my list? Which of the questions in the list can you take responsibility for getting answered?

If you've been working offline and marking up paper copies of your reports during the meeting, when you return to your office, transfer your notes into your computer. If you've worked online capturing information in your computer as the session proceeds, your work to update your analysis reports is effectively done when the client meeting ends. Either way, after the meeting, print updated reports and send a copy to your client and anyone else on the trial team.

The analysis reports you've begun are "living" ones. As you head towards trial, keep working on your Cast of Characters, your Chronology, your Issue List and your Question List. These analysis reports will do far more than help you think about your case. They'll serve a myriad of concrete purposes. They'll help you keep your client up to date, plan for discovery, prepare to take and defend depositions, create motions for summary judgment, and make your case at settlement conferences and at trial.

About the Author

Greg Krehel is CEO of DecisionQuest's CaseSoft division (www.casesoft.com). CaseSoft is the developer of litigation software tools including CaseMap and TimeMap. He can be contacted at gkrehel@casesoft.com.

HUMOUR SECTION

Adopt a Motto today!

☺ Experience is something you don't get until just after you need it.

☺ If at first you don't succeed, destroy all evidence that you ever tried.

☺ Success always occurs in private. Failure is always public.

☺ Borrow money from pessimists; they don't expect it back.

☺ A fool and his money are soon partying.

☺ The problem with the gene pool is that there is no lifeguard.

☺ A clear conscience is usually the sign of a bad memory.

☺ I'd kill for a Nobel Peace Prize.

☺ Ninety-nine per cent of lawyers give the rest a bad name.

Help Desk Humour?

I initially thought that the following was a joke. Sadly it was the real thing! - Ed

Please see the following which explains the recent changes to the Wide Area Network that enable the regional offices to access central IT systems based in London.

What is an IP VPN Network Using MPLS?

We have now migrated to a IP VPN utilising MPLS, this is privately owned by (name deleted). This private network is shared by (name deleted) customers but security and service levels are guaranteed by using the Multi Protocol Label Switching Protocol. With the capability of MPLS to segregate different customers traffic on the same equipment (before each customer had dedicated equipment) there is a very attractive cost saving and has enabled us to increase bandwidths significanlty *(sic)* to all locations.

MPLS labels traffic with a Quality of Service (QoS) indicator which allows the customer to define which traffic is more sensitive to time delays (Latency). Typically interactive traffic and voice/video traffic are time sensitive and will be guaranteed a percentage of the bandwidth. In our deployment this has enabled us to give priority to critcal *(sic)* applications using the AS/400.

The MPLS network also allows Any to Any connectivity which with additional changed to our infrastructure will allow for more efficient transfer of data across the network, for example if someone in New York emailed someone in Phoenix the email would go directly between the two sites whereas currently all email travels via London. It is aniticpated *(sic)* that this change will be implemented during Q1 2005.

(They can't even spell, let alone explain what the change does for the user - Ed)

Disaster Recovery and Business Continuity: Don't Forget The Paper

Priscilla Emery

Disasters Are A Fact of Life. You don't have to be addicted to watching the evening news or CNN to see the impact of different disasters on people, their communities and their livelihoods. Disasters can appear with little or no warning, can negatively impact people in a variety of ways, and can come in a variety of forms:

- Extreme weather conditions (Hurricane Floyd, which brought the eastern United States to a standstill in September 1999; the flooding of the Danube across Eastern and Central Europe in 2002)
- A sudden failure in power or communications infrastructure (the 2003 blackout in the Northeastern United States and regions of Canada; the recent blackout in Italy)
- Robbery or other criminal activity (the theft of credit card numbers from ***CDNOW*** and other e-commerce sites)
- Major hacking events (the I Love You virus; the Klez virus)
- Civil unrest (the riots at the ***World Trade Organisation*** conference in Seattle in 2000 and the ***Group of Eight*** summit in Genoa in 2001)
- Terrorist acts (New York World Trade Centre attack on 9/11; the Oklahoma City bombing)

Businesses are constantly at risk for both natural and man-made interruptions to their operations, any of which can have devastating consequences. ***Gartner***, a widely respected industry analyst group, has estimated that two out of five organisations that experience a disaster go out of business within five years. Making a speedy recovery from unforeseen interruption is imperative to staying solvent as a business. However, if a company does not develop and implement a disaster recovery and business continuity plan, one that is able to bring its systems back up in as short a time as possible, the potential for lost revenue can add up to millions of dollars within several days. Having no recovery strategy means the actual time to be fully functional can stretch out across several weeks or months.

Unfortunately, just like people sometimes hesitate to spend money on insurance for their personal interests, many organisations ignore the basic tenets of disaster recovery. And even those organisations that think they are prepared sometimes overlook the need to protect one of the most hard-to-recover assets - paper documentation.

Seeing the Signs But Not Taking Action

In the winter of 2000, Gartner conducted a survey of IT managers and discovered that over 60% of the businesses surveyed did not have a basic plan to mitigate the effects of a disaster. Unfortunately, even after the events of 9/11, many organisations still had not made serious preparations for quick disaster recovery. Almost a full year later, Gartner issued another report, which indicated a continuation of this trend: many businesses may be closely evaluating their level of disaster preparedness, but most haven't fully identified plans to address the disaster recovery shortcomings within their organisation.

Research by KPMG also helps illustrate the level of widespread avoidance of disaster contingency planning. This research found that 81% of U.S. companies believe their organisations are susceptible to attack by terrorists and/or other outside predators, and yet 47% of these organisations do NOT have a crisis plan in place or even a method to measure their readiness.

What is even more troubling is that the organisations that do develop disaster recovery and business continuity plans often do not have a recovery strategy for their paper-based documents in those plans. Some organisations may have records-management strategies in place for vital paper-based records stored off-site, but related documentation (such as faxes, paper in file cabinets, memos, reports and financial statements) is not backed up or stored securely off-site. Much of this additional paper is what feeds data-driven transactions and forms the paper trail that is a key component of any ongoing investigation or transaction adjudication. When this information is lost, complete data records cannot exist.

Paper Recovery Necessary, No Matter What Size the Disaster

In terms of information and data loss, any size disaster has significant consequences for your business. For example, in early December of 2002, the Old Town of Edinburgh, Scotland, was devastated by a fire, which ripped through the heart of the historic area. Council officials and property owners estimated that the cost of the damage ran into many millions of pounds. Almost every building affected by the fire had come down and many of the historic facades were affected. But the buildings were not the only great loss. ***The School of Informatics at the University of Edinburgh*** lost a major collection of books and journals. This collection, which included significant research papers on artificial intelligence, took years to accumulate and could not be replicated on the scale that it had existed before the fire. This paper had not been subject to a recovery plan, and now a great deal of globally important information is lost forever.

Another secondary but equally relevant issue when dealing with paper-based information relates to emergency

management during the course of a disaster. Of primary importance is the ability to get quick access to appropriate municipal information, including maps, drawing, inventory data and blueprints. This information can help pinpoint the location of underground pipes, tanks, wiring systems, and known stockpiles of hazardous materials in the area. If this information is lost, misplaced, out-of-date or damaged, it becomes a problem that can stop the emergency services in their tracks.

Being Prepared Is Not an Option – It's a Requirement

Gartner analyst French Caldwell says it best when he points out, "In this new kind of war, business readiness and resilience are your most effective deterrents to terrorism. We are not going to return to business as usual, but we can get back to business." Getting back to business includes developing a business continuity strategy that takes into consideration all the different types of catastrophes that can occur to a business, such as fire, electrical outages, flooding, and so on. In addition, taking into account the backup strategies for your paper-based documents is a critical component to any strategic recovery plan.

To ensure your business continuity plans are complete, a paper scanning and archiving application is vital. The integration of imaging and scanning technologies, together with strong search and retrieval capabilities, will allow you to:

- Easily add paper-based documents to your backup schedule and media storage strategy
- Backup vital paper documents with fast and easy archiving to a variety of media types
- Provide quick remote access to your paper-based reference information

Tools are available to help make important paper-based documents accessible, in terms of both increased processing productivity and information recoverability in case of disaster. Such tools provide:

- A single point of access, through any computer, to all relevant information that has been gathered from a variety of sources, including scanned and imaged paper files, electronic documents and e-mails.
- Advanced searching techniques and optional web tools, which improve the efficiency of any business processes.
- Improved auditability and activity logging. These functions are very important for recovering paper-based and electronic documents when mixed batches of overlapping information are involved.
- Easy export or printing of all relevant information to share with clients or team members.
- A system that is easy to restore. This "restorability" means improved responsiveness to citizens, constituents and clients when a recovery situation arises. Those companies that can bounce back quickly from an emergency situation are most likely to survive over the long term.

Organizations and companies using this technique include:

- ***The Conference Division of the International Maritime Organization (IMO)*** was able to assist The American Bureau of Shipping (ABS) - which lost all its paper in the World Trade Centre attacks - in converting ABS's microfilmed documents (1958 - 1998) back to searchable archives.
- ***Akzo Nobel Chemicals,*** which converted many of its Research & Development files after a small fire hit part of the library. Although the loss was not significant, the company heeded the warning and ordered the system several days later to protect against any similar problems in the future.
- Several government agencies backup paper files as part of their HIPAA and/or DoD compliance efforts.

Some of these organizations learned the hard way the importance of being prepared for the worst. Ignoring the backup and recovery of paper-based reference information that permeates your organization is like playing Russian Roulette with your business. Maybe you will be lucky and won't become a victim of disastrous circumstances, but if disaster does strike, will you be prepared to put your entire business at risk?

Priscilla Emery is President and founder of e-Nterprise Advisors. She can be contacted at pemery@e-nterpriseadvisors.com

ZyLAB UK Limited
Is a leading provider of document imaging and paper filing software. The company has offices in the U.K, the U.S., Germany, Spain, France, the Netherlands, Singapore and Australia. base. For more information access www.zylab.com

Computer Forensics Science

Celeste Rush

This is the first of a two part series dealing with this very interesting subject – Ed

1. Historical perspective

The science of Computer Forensics was developed largely due to a demand for addressing the specific and articulated needs of the law enforcement community. [Whitcomb 2002]

The first known employment of computer forensic techniques was by the United States military and intelligence agencies in the 1970s. Due to their classified environments, very little is known regarding their activities but it is assumed it would have involved counterintelligence using mainframe computer systems. [Mohay *et al* 2003, pp. 113]

The Federal Bureau of Investigations (FBI) and other law enforcement agencies developed programs to examine computer evidence as early as 1984. The Computer Analysis and Response Team (CART) was incorporated by the FBI to properly address the demands of investigators and prosecutors in a structured and programmatic way; the general organisation and function of which are mirrored in many other law enforcement agencies in the United States and other countries. [Noblett *et al* 2000]

Special agent Mark Pollitt of the FBI gives a definition of Computer Forensics as: *"Computer forensics is the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and law".* [—Mark Pollitt (undated) *'Computer Forensics: An Approach to Evidence in Cyberspace'*, Federal Bureau of Investigation, Baltimore, MD, USA]

The discipline of computer forensic science differs from other forensic sciences in some important aspects. In computer forensics the objects examined and techniques used are products of the market-driven private sector. Examinations are expected to take place at virtually any physical location including a controlled laboratory setting. What is produced from the examinations is direct information and data that may be a significant factor in a case rather than interpretative conclusions that are produced in other forensic science disciplines. This type of direct data collection has far reaching implications in the relationship of all parties involved in a forensic computer examination. [Noblett et al, 2000]

Pollitt states: *"Rarely is determining that the (paper) document physically exists or where it came from, a problem. With digital evidence, this is often a problem. What does this binary string represent? Where did it come from? While these questions, to the computer literate, may seem obvious at first glance, they are neither obvious nor understandable to the layman. These problems then require a substantial foundation being laid prior to their admission into evidence at trial."* [—Mark Pollitt (undated) *'Computer Forensics: An Approach to Evidence in Cyberspace'*, Federal Bureau of Investigation, Baltimore, MD, USA]

Another difference between computer forensic science and some of its traditional forensic counterparts is that computer forensics cannot rely on receiving similar evidence in every submission. For example, a forensic DNA analysis, once cleared of contaminants and reduced to its elemental form, is generic and may be applied similarly to all submissions. Indeed, the justice system has come to expect a valid and reliable result using those DNA protocols. However computer forensic science can rarely expect to receive the same elements from standardised repetitive testing in many submissions. This is largely is due to the many different manufacturers of computer software and hardware, making storage methods unique to both the device and the media. [Noblett *et al* 2000]

Due to the large volume of information contained on modern computers and with time or other judicial constraints, a computer forensic investigator can create a list of key words (for a *keyword* search) to obtain specific, probative, and case-related information. On the other hand, other forensic disciplines will attempt to gather as much information as possible from an evidence sample. This difference shows a clear requirement of a computer forensic scientist to make their examinations more efficient and effective thus making it a more demanding science than what traditional forensic science requires. [*Ibid*.]

From a 1995 survey conducted by the US Secret Service it was identified that 48 percent of the agencies had computer forensic laboratories and 68 percent of computer evidence seized was forwarded to experts working in those laboratories. However, the survey also reported that 70 percent of these agencies were doing the work without a written procedure manual. [Noblett et al, 2000]

Since the early 1990's there have been ongoing efforts to develop standards and protocols in how computer forensic examinations are conducted. This has led to the formation of various working groups:

- The Technical Working Groups (TWGs) whose name was change to Scientific Working Groups (SWGs) in 1999;
- The Technical Working Group on Digital Evidence (TWGDE) whose name was changed to The Scientific Working Group on Digital Evidence (SWGDE) also in 1999;
- The formation of the International Organization on Computer Evidence (IOCE).
- The Scientific Working Group on Imaging Technology (SWGIT) which is closely associated with and was originally part of the SWGDE. An example would be the taking of a digital picture as evidence at a crime scene or the digital picture itself as evidence.

A set of definitions, standards and principles were drafted by the SWGDE and presented at the International Hi-Tech Crime and Forensics Conference held in London, October 1999.

Using the same overriding principles, the 'Good Practice Guide for Computer Based Evidence of the UK Association of Chief Police Officers (ACPO) Computer Crime Group' was first published in 1998. This document was written for the Police Service personnel and used as a good practice guide in specific circumstances while dealing with computers in the possession of a suspect. [ACPO 1998]

Because the electronic world and the manner in which it is investigated had changed considerably since the first

publication, the ACPO revised the original document and produced two other versions to take into account these changes. The most recent, Version 3.0, entitled, 'Good Practice Guide for Computer Based Electronic Evidence', was published in the summer of 2003 in conjunction with the National High-Tech Crime Unit (NHTCU). As the title suggests, the document is specifically intended for use in the recovery of computer based electronic evidence, but it is not a comprehensive guide to the examination of that evidence. Although aimed again at police officers, other organisations that comprise the law enforcement community are expected to make use of the guide. [ACPO 2003]

Noel Bonczoszek, Chairman of the British Computer Society Information Security Specialist Group, commented at the publication of Version 3: "One major issue relating to the investigation of computer crime is the extent to which well-meaning but untutored people can damage the integrity of gathered computer evidence. This often renders it unusable in criminal cases and usually happens in the early stages of an investigation, before police experts are called in."

"Great care will also be needed in applying the guidelines on child pornography to ensure the defence is not prejudiced by the access restrictions which do not apply in other cases. However, these new guidelines will greatly improve understanding amongst our membership and the wider IT community of the procedures to be followed with obvious benefit to all." [BCS 2003]

The four principles from the document, listed in Appendix B, are consistent with the principles adopted by the G8 Lyon group as a basis for international co-operation [ACPO 2003]

The principles adopted as G8 recommendations are published in the 2002 International Organization on Computer Evidence (IOCE) draft v1.0, 'Guidelines for Best Practice in the Forensic Examination of Digital Technology'. These principles are also listed in Appendix B for comparison.

Other working groups have published similar guidelines, such as the Internet Society's 'Request for Comments: 3227 - Guidelines for Evidence Collection and Archiving'. [Brezinski *et al* 2002]

Computer evidence represented by the physical components such as chips, motherboards, storage media, monitors, printers, etc. may be easily identified and acceptable methods for handling these are well detailed. However, the evidence stored within these components is latent and exists only in a metaphysical electronic form. The forensic report is based on the recovery of this latent information and the challenge to computer forensic science is to provide accurate and reliable results without harm to the evidence.

A major factor involved is that computer evidence almost never exists in isolation. It is a product of the data stored, the application used to create and store it and the computer system directing these activities. [Noblett *et al* 2000]

Reliable and valid methods are required to recover data from seized computers to ensure the original data is unaltered in any way or form so evidence in criminal investigations can be legally defensible.

A hierarchical model of computer forensic science protocols may be applied so that the overarching principles may remain constant but examination techniques are readily adaptable to the computer system to be examined. [Noblett *et al* 2000]

'A Three-Level Hierarchical Model for Developing Guidelines for Computer Forensic Evidence', published by the FBI, provides a model that would encompass more than one policy or set of guidelines. This is shown in Figure 1.

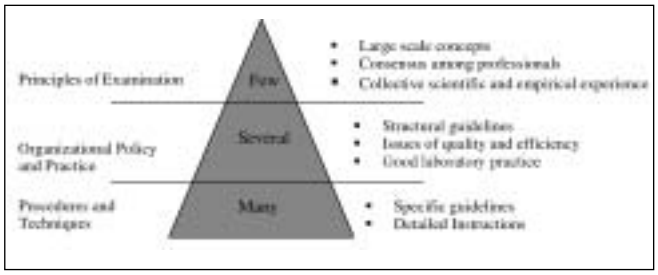


Figure 1 – A Three-Level Hierarchical Model for Developing Guidelines for Computer Forensic Evidence [Noblett *et al* 2000]

2. Rules of Evidence

There are five rules of collecting electronic evidence, encompassing five properties the evidence must have in order for it to be useful. These are:

Admissible – Considered the most basic rule, evidence must be able to be used in court or otherwise and so conform to certain legal rules before it may be submitted before a court.

Authentic – Evidence must be positively tied to the incident and the relevancy of the evidence to the incident shown.

Complete – Evidence must be complete and tell the entire story and not just a particular perspective. Not only should evidence be collected to prove a case against a defendant in a crime but also evidence that could prove innocence. For example, it may be shown that an attacker was logged in at the time of an incident but it must also be shown who else was logged in at the same time and the reasons why *they* were not the guilty party. This is called *exculpatory evidence*. [Vacca 2002]

Reliable – The evidence collected must be reliable. Nothing about how the evidence was collected and subsequently handled may cast doubt about its authenticity and veracity.

Believable – The evidence must be readily believable and understandable by the members of a court. For example, presenting a binary dump from process memory would not be understandable to a jury. Likewise by presenting evidence in an understandable format it must be shown to relate to the original binary information.

3. Basic Guiding Principles during Evidence Collection

Applying the five rules above, certain guiding principles have been recommended in the literature of current best practice. These principles include:

Minimising the handling or corruption of the original data – A master copy should be made of the original data. This is usually done through imaging the media containing the evidence bit by bit or bitwise so to capture and preserve all data on a disk. Steps should be taken to avoid any alteration of any part of the original. (Using a write block while imaging would prevent the inadvertent writing to the original.) The original media should be stored securely in an appropriate environment. Secondary copies may be handled for examination.

Chain of custody – Logging the chain of custody of any evidence

collected would show at all steps what was done with original, who did what, how was it done, and when was it done. This should also include how the evidence was stored and when and how it changed custody. Detailed notes should be kept and include dates and times. Any notes and printouts should be signed and dated. A message digest algorithm (e.g. MD5) should be applied to all storage devices to prove its authenticity and that it has not been altered in any way.

Account for any alterations to the original data and keep a detailed log of any actions taken – Sometimes evidence alteration is unavoidable and should this occur, the nature, extent, and reasons for the changes need to be documented. This would include any changes to the physical location of the original (e.g. removal of hardware components).

Ensure that any actions are repeatable – Any actions taken to recover data must be able to be repeatable and achieve the same results.

Proceed from the volatile to the less volatile – Some electronic evidence is transitory by their nature and exists when power is applied. By collecting evidence in order of volatility the recovery of such data may be ensured. (See Hide and Seek)

Note the difference between the system clock and the Coordinated Universal Time (UTC) – Previously known as Greenwich Mean Time (GMT), UTC uses a 24-hour system of time notation provided by precise atomic clocks, shortwave time signals and satellites for accuracy. Other terms used to refer to it include 'real time', 'Zulu time' (after the 'Z' often used after UTC times), 'universal time', and 'world time'. [DXing 2003]

Follow any local security policy – Failing to comply with a company's security policy regarding search and seizure of evidence, the evidence may become unusable. Engage the appropriate Incident Handling and Law Enforcement personnel. [Brezinski *et al* 2002]

Be aware of global jurisdiction issues – Evidence that crosses national boundaries will be subject to issues with respect to sovereignty and jurisdiction in how criminal offences are dealt with. Evidence obtained in one jurisdiction, which is perfectly acceptable to the legal system, may be completely inadmissible in the judicial system of its immediate neighbour. [Mohay *et al* 2003, pp 123]

Be prepared to testify – Outlining all actions taken during an investigation may have to be presented in court, perhaps even years after the fact. Detailed notes will be vital. [Brezinski *et al* 2002]

*When confronted with a choice between collection and analysis one should do collection first and analysis lat*er – Sometimes evidence may be part of a larger network and retrieval of hardware may not be appropriate. If possible, all evidence including peripheral components should be collected using the appropriate seizure guidelines. If the equipment is found switched off it should not be switched on, as the act of powering on a computer will alter data. If the equipment is found switched on, the power source should be removed first from the computer device without closing down any programs. This would avoid data being written to the hard drive if an uninterruptible power protection device is fitted. [APCO 2003] One must bear in mind the affect on volatile information from this action.

Although the above guidelines are general in context and certainly not comprehensive, from these, an idea of the importance of data collection and how it is executed may be appreciated.

2

Information

Computer systems may hold and process many different types and forms of data. Any information extracted from this data is the result of analysis and an interpretation of the data for some perceived purpose. By extracting this data in an accurate and meaningful way the information obtained may be presented as evidence in a court of law. This presupposes that interpretative rules are applied to the data so the intended information is found. However, which rules are applied and how the receiving person perceives the information require that the difference between the data and the interpreted information need to be preserved.

1. Number systems

A computer system almost always represents data in a *binary* pattern, which can take many different forms. The binary system is a two-state system. This type of system is easy to engineer and can represent almost any kind of information. As the term implies, each data element is implemented through a physical device that may be in one of two stable states. Examples of two-state or binary devices include a memory chip which contains a transistor that may be on or off or a magnetic disk that may be magnetised to one polarity or the other.

A system of millions of transistor switches may be called *memory*. Mathematics provide symbols to represent the state of a device in each memory element as "0" for off and "1" for on. A set of interpretative rules is required to apply to a particular segment of a sequence of these symbols in order to extract the intended information. As such, each of the two symbols "0" and "1" are referred to as a binary digit or bit (the acronym of which comes from the beginning of binary and the end of digit).

There is an ordered sequence of bits to convey information. This information may be a character of text, a specific mathematical number, or a set of instructions for a specific process among many others. A uniquely identifying number of bits is known as the *address* and is associated with eight bits called a *byte*. The bytes are ordered from address 0 numerically upwards to the highest possible address in the memory. (See figure 1) For a modern personal computer, it would not be unusual for the highest address in memory to exceed 64 million. [Sammes *et al* 2000, pp 9]

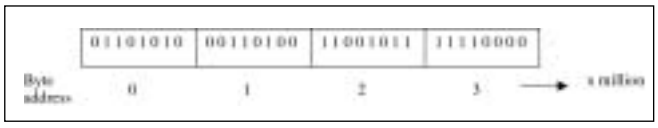


Figure 2 – Byte addressing [Sammes et al 2000, pp 9]

The byte is the known as the basic measure of memory size but other terms are also used. Table 1 lists these terms for units of memory.

Nibble	= half a byte	= 4 bits
Byte	= 1 byte	= 8 bits
Word	= 2 bytes	= 16 bits
Double word	= 4 bytes	= 32 bits
Kilobyte	= 1024 bytes	= 2^{10} bits
Megabyte	= 1 048 576 bytes	= 2^{20} bits
Gigabyte	= 1 073 741 824 bytes	= 2^{30} bits
Terabyte	= 1 099 511 627 776 bytes	= 2^{40} bits

Table 1 – Units of memory

In any computer system, associations can be made with any sequence of bytes and can be changed at any time. However, there are standard interpretative rules which will be looked at which will be used later in this section for analysis.

In any number system, the position of a digit in a pattern is significant. In the decimal number system the values 0 – 9 are used with a multiplying factor of a power of 10, thus *decimal*. The actual position relative to the left of the decimal point will give the particular power of 10. Moving one step either way will either increase or decrease the multiplying factor. Thus a whole number sequence of 8492.00 in decimal may be interpreted as:

8 x 1000 + 4 x 100 + 9 x 10 + 2 x 1

= 8492.00

OR

$8 \times 10^3 + 4 \times 10^2 + 9 \times 10^1 + 2 \times 10^0$

= 8492.00

The same interpretative rules can be applied to other number systems. The particular number of digits used is known as the *base*. The following are other number systems:

- Eight digits (0 – 7), base 8 or an *octal* system with a multiplying factor of eight,
- Three digits (0 – 2), base 3 or a *ternary* system with a multiplying factor of three,
- Two digits (0 and 1), base 2 or *binary* system with a multiplying factor of two.

The *hexadecimal* number system is base 16 with a multiplying factor of 16 and uses digits 0 – 9 and the letters A – F representing the decimal equivalent of 10, 11, 12, 13, 14, and 15 respectively.

As in the decimal system the multiplying power of two in the binary system will depend on the actual position of the digit relative to the *binary point*. Therefore applying the same interpreted rules to the binary data given in byte address 0 in figure 2 (01101010) the following may be interpreted:

(0 x 128) + (1 x 64) + (1 x 32) + (0 x 16) + (1 x 8) + (0 x 4) + (1 x 2) + (0 x 1)
= 106 decimal
OR
(0 x 27) + (1 x 26) + (1 x 25) + (0 x 24) + (1 x 23) + (0 x 22) + (1 x 21) + (0 x 20)
=106 decimal

The total possible values in a single byte (eight bits) is 0 to 255 (11111111 = 255 decimal). Two bytes or a *word* will be frequently taken together to represent whole numbers. The range of two bytes is now 00000000 00000000 to 11111111 11111111. (that is 65535 maximum in decimal). Where greater precision is required, four bytes, or a *double word*, are used together.

2. Big Endian, Little Endian

When addressing multibyte numbers there are two ways to consider the order. One way would be to have ascending number for the addresses i.e. from left to right as in figure 2. However, this would mean that the least significant bit (smallest value) would be in the larger address number as illustrated in figure 3 and so the number would appear 'backwards'. This is known as *big endian format*.

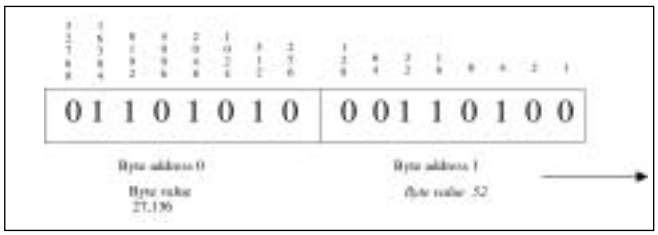


Figure 3 – Binary word number in big endian format equivalent to 27,188 in decimal

It is argued that the lower powers of two should be in the lower byte value address and the higher powers of two in the higher byte value address. This would then change the value of the same two-byte sequence to 13,418 decimal as shown in figure 4, which is known as *little endian format.*

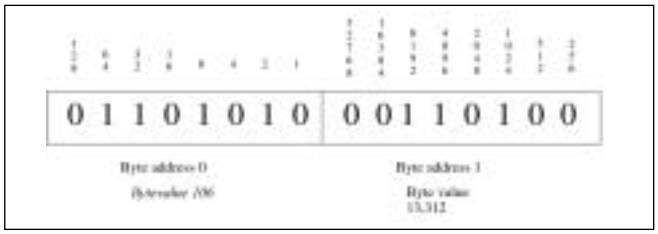


Figure 4 - Binary word number in little endian format equivalent to 13,418 in decimal.

Motorola processors (used in Mac's) use big endian byte order and Intel processors (used in PCs) use little endian byte order.

In 'An Essay on Endian Order', Dr. Verts describes the merits of the two formats:

"In "Little Endian" form, assembly language instructions for picking up a 1, 2, 4, or longer byte number proceed in exactly the same way for all formats: first pick up the lowest order byte at offset 0. Also, because of the 1:1 relationship between address offset and byte number (offset 0 is byte 0), multiple precision math routines are correspondingly easy to write.

In "Big Endian" form, by having the high-order byte come first, you can always test whether the number is positive or negative by looking at the byte at offset zero. You don't have to know how long the number is, nor do you have to skip over any bytes to find the byte containing the sign information. The numbers are also stored in the order in which they are printed out, so binary to decimal routines are particularly efficient."

[—Dr. William Verts, (19 April1996) 'An Essay on Endian Order' available at Internet < http://www.cs.umass.edu/~verts/cs32/endian.html >]

For an analyst the endian order requires knowledge of how numbers are written to a file. For example, Windows Bitmap (.BMP) files are developed on a little endian architecture. If graphics file integers are written as a Bitmap file on a machine with big endian integers, the byte order must be reversed and saved in little endian format to be processed correctly.

The use of endian formats is illustrated in the hexadecimal analysis of graphic files in the following section.

Other considerations are binary representations of negative numbers, which use a *signed bit*, fractions and mixed numbers where the binary point is at some other position other than the extreme right of the digit sequence, and floating point numbers, which is the representation of the *scientific notation*. Another format often used is the *binary coded decimal* (BCD) where the binary value in a sequence of bytes will directly represent a decimal number. Except for the mention of these other formats they will not be covered in more depth here.

3. Hexadecimal

As previously mentioned, hexadecimal is a base 16 number system and has 16 digit symbols. It is a convenient system for interpreting long binary sequences as four binary digits, or a 'nibble', may be represented by one hexadecimal digit. This means that there is a reduction in the size of the binary sequence from 4 to 1, as it would take two hexadecimal digits to represent one full byte.

Table 2 lists the binary and decimal equivalents to each hexadecimal digit.

Hex	Binary	Decimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
A	1010	10
B	1011	11
C	1100	12
D	1101	13
E	1110	14
F	1111	15

Table 2 – Hexadecimal code table

Hexadecimal letters may be written in either upper or lower case and hexadecimal numbers may be identified by an upper or lower case 'H' immediately afterwards.

To illustrate, the binary numbers used in figures 3 and 4 may be represented in hexadecimal as in figure 5.

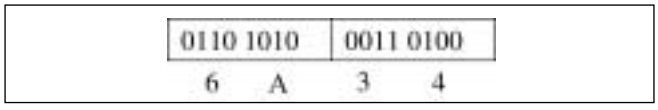


Figure 5 – Hexadecimal representation of two bytes.

This would be written as 6AH and 34H or 6ah and 34h. Another way hexadecimal numbers may be represented is by putting '0x' in *front* of the number; thus, 0x6a and 0x34.

4. ASCII

The hexadecimal number system is also very important in that it is used to represent *characters* of the American Standard Code for Information Interchange, or ASCII as it is universally known. A character in this instance means a single symbol that is to be visually displayed or printed, within the set of all letters of the alphabet, both upper and lower case, and the digits 0 to 9. In binary a single character is represented by one byte, thus two hexadecimal digits. The two hexadecimal bytes in Figure 3, 6ah and 34h, correspond to the ASCII code characters "j" and "4" respectively.

The ASCII set uses 127 unique symbols out of the 255 total available (one byte value may be from 0 to 255). The first 32 are *control characters* originally designed to control data communications equipment and computer displays and printers. A sequence of characters is often known as a *string*. The end of a text string is marked by a byte of all zeros in binary and is referred to as an *ASCIIZ string*. [Sammes *et al* 2000, pp 22]

IBM introduced an *extended ASCII* code for its personal computers (PC) that extends the basic ASCII character set in the binary value range of 128 to 255. The extra characters represent characters from foreign languages and special symbols for drawing pictures. The Windows ANSI (American National Standards Institute) code is the Windows version of the extended ASCII code, which typically assigns different characters for each of the binary values, 128 to 255.

Another 8-bit code found particularly on IBM mainframes is the *extended binary-coded decimal interchange code* (EBCDIC). Also, different personal organisers and information managers use their own particular version of ASCII, which are not usually published but which an analyst would need to know for internal investigations. [Sammes *et al* 2000, pp 23]

The ASCII, Windows ANSI, and EBCDIC Character Sets are listed in Appendix A.

5. Unicode Standard

"Unicode Worldwide Character Standard"
"Unicode provides a unique number for every character,
no matter what the platform,
no matter what the program,
no matter what the language."

[—-The Unicode Consortium (2003b), 'What is Unicode', Unicode, Inc. available at Internet http://www.unicode.org/standard/WhatIsUnicode.html]

The *Unicode Worldwide Character Standard* is a more recent code developed by The Unicode Consortium designed to support the worldwide interchange, processing and display of diverse languages and technical disciplines of the modern world. [The Unicode Consortium, 2003a]

The Unicode Standard began as a two-byte (16-bit) encoding to provide numeric values, or *code points*, for more than 65,000 characters. The standard now supports three encoding forms that use common characters but also allow for encoding as much as a million more. This allows for encoding of all known characters as well as historical scripts and common notational systems worldwide.

The Unicode Consortium and the International Organization for Standarization (ISO) Working Group responsible for ISO/IEC 10646 have worked closely together to synchronise their respective extended versions for coding multilingual text. However, the Unicode Standard imposes additional constraints on implementations to ensure characters are treated uniformly across platforms and applications. To this end, it supplies an extensive set of functional character specifications, character data, algorithms and substantial background material that is *not* in ISO/IEC 10646. [The Unicode Consortium 2003]

The three encoding forms defined by the Unicode Standard allow the same data to be transmitted in a byte, word, or double word format (8, 16 or 32-bits). All three may be transformed into one another without loss of data due to the common character formats in each. All three encoding forms need at most 4 bytes (or 32-bits) of data for each character.

The three formats begin with UCS Transformation Format (UTF) and end with the length encoding of bytes; thus, UTF-8, UTF-16 and UTF-32. The latest version is the Unicode Standard Version 4.0 (2003)

UTF-8 is used with HTML and similar protocols and transforms all Unicode characters into a variable length encoding of bytes. The format corresponds to ASCII character values and may be used with many existing software programs as is.

UTF-16 is used in many environments that need to balance efficient access to characters with economical use of storage. It fits the most heavily used characters into a single 16-bit code unit, while all others are accessible via pairs of 16-bit code units.

UTF-32 is used where memory space is no concern, but fixed width, single code unit access to characters is desired. [The Unicode Consortium 2003a]

6. Records and Files

The byte is generally the fundamental unit for making *records* and *files*. A record is a sequence of bytes that will have different sets of interpretative rules associated with different parts of the byte sequence. A *file* is a sequence of records, which may be of the same or different type and may be simple or complex. A *file system* stores files which are often given a name and type description. [Sammes *et al* 2000, pp 24]

For instance, a file in a Microsoft file system will be given a name and a file type of up to three characters. A dot or period character separates the name from the type as in 'Example.txt'. This is a file called *Example* and the file type is a *text file*.

Some common file types are investigated and analysed in the following section.

3 File types and signatures

1. File signatures

Files are given extensions after their name to signify they are of a certain file type and would be suitable for processing with certain software packages. The extension is also useful to an analyst whom would be able to apply the appropriate set of criteria to interpret the file as required. Some files have a sequence of bytes at the beginning of the file that specifies a type of file. This is called the *file signature*.

The idea of a file signature has been around for some time. The Unix community, in particular, would indicate a file type in the first few bytes of a binary data file. These were known as their *magic number*. Attempts have been made to standardise magic numbers and specify certain rules for future selection. The rfc-draft, v1.2 1996/11/20 is one such attempt geared toward a uniform semantic file type system for the Internet. In the document, *MAGIC* is defined as 'Magic Against Galloping Internet Complexity'.

"In such an environment, it is very desirable that files should generally present themselves as self-describing objects from which an application launcher or navigation tool can readily deduce both their uses and at least some of the semantics of their contents. An effective set of such conventions can enable tools such as Web browsers to inform users according to such deductions, and to dispatch to appropriate sub-interpreters and user agents on the file object's semantic type."
[Rfc-draft v1.2, 1996, available at Internet
< http://www.catb.org/~esr/magic-numbers/rfc-draft >]

2. File Analysis

Some of the most common files will be examined here with an evaluation copy of the hexadecimal editor tool, WinHex 11.0 (by Stephan Fleischmann), downloaded from Internet <http://www.winhex.com >. The full version provides several forensic tools useful to a specialist investigator.

Those files analysed include document type files, image type files and compressed files.

2.1 Plain text

The most common and simplest is the *plain-text file* with the .txt extension, which are sometime called *ASCII files*. One byte represents one ASCII character in records of single bytes.

In Notepad the following text was saved to a file called 'Example.txt'.

> This is an example of a text file.
>
> That was a carriage return. Those were spaces. This is a question mark?

Figure 6 – A printout of Example.txt

Below, in figure7 is a screenshot of the file viewed with WinHex

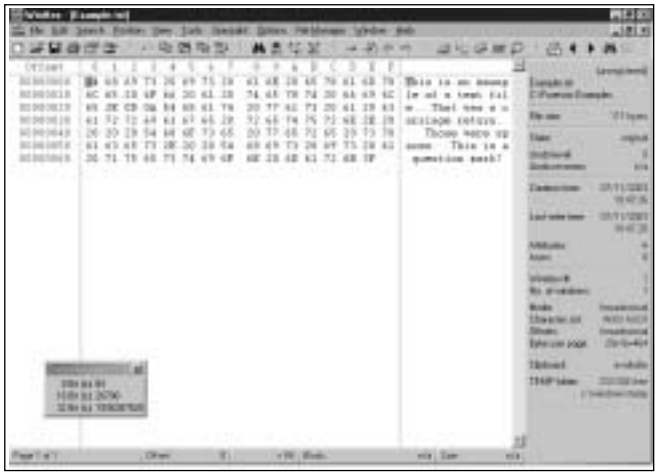


Figure 7– Screenshot of a text file in WinHex

The text in ASCII character form can be seen on the right column and the corresponding hexadecimal number in the middle column. The address of a specific character is a sum of the row number and column number. For instance, the carriage

return is indicated by the hex values 0d, "carriage return", and 0a, "line feed", at address 22h (20h + 2h) and 23h (20 + 3). Sometimes a carriage return may be represented as just 0d *or* 0a. All addresses start from 0. Spaces are recognised as hex value 20 and can be found sequentially at addresses 3Fh-42h and individually found at other addresses corresponding to the text format. A question mark corresponds to hex value 3F at address 6Eh.

It can be noted that non-text characters do not appear in ASCII character form. For example, the carriage return and line feed are indicated by two dots and nothing is visible for any spaces between text.

The simplicity of the ASCII text file is not a challenge for an analyst. However, most word processors use a modified form of ASCII to represent text with their own word processing codes, which are embedded in the file. These codes indicate different bits of information regarding the appearance of the document, for example, the page layout, font size and type, underlined, bold, italic, etc. These files also have a file signature.

2.2 Microsoft Word

> This is an example of a word document file.
>
> That was a carriage return. Those were spaces. This is a question mark?

Figure 8 – A printout of Example.doc

The text in figure was saved as a document file (.doc extension) in Microsoft Word 97 with the file name 'Example.doc'. The basic text format was duplicated for comparison with other document formats. Figure 9 is a screenshot of the first part of the file. At the far right of the screen in the WinHex application window, information about the file is shown including the size of the file, which is much greater for the.doc file (19,456 bytes) than the .txt file (111 bytes).

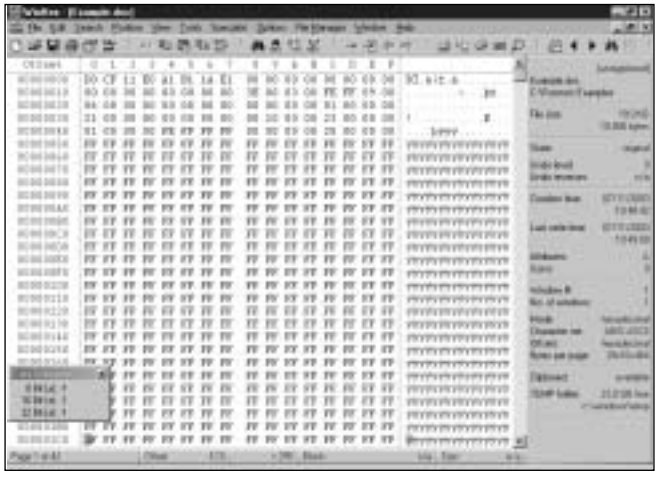


Figure 9 – File signature of .doc file

In addresses 00h to 07h the file signature can be seen as eight hexadecimal codes: D0 CF 11 E0 A1 B1 1A E1. This is a "wrapper" file for a variety of Microsoft applications, including the latest versions of Word, Excel and PowerPoint. The right column displays the signature as encoded characters instead of ASCII characters.

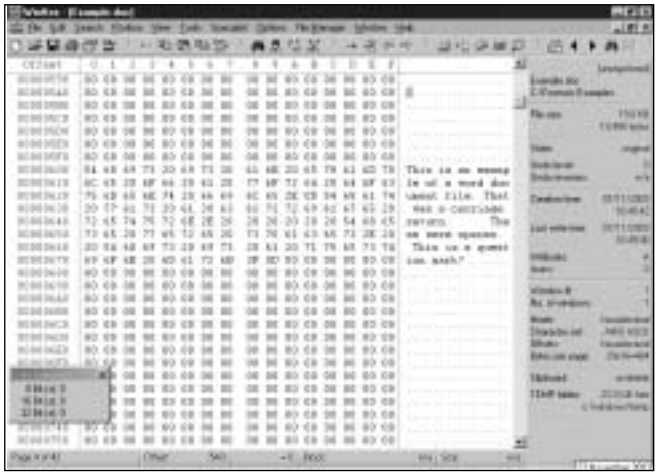


Figure 10 - Start of ASCII text in .doc file

The text does not begin until address 600, shown in figure, and as with the .txt file, the ASCII characters are represented in hexadecimal code with some notable differences. At address 62Bh the carriage return is represented by the hex value 0D without a following line feed character value 0a. Also, one corresponding dot is displayed in the ASCII text area instead of two. As before, 20 represents a space and 3F a question mark.

Details for the Microsoft Word format is not publicised. However, it is known that memory blocks used in one application are reused in the Word files unmodified. [Sammes *et al* 2000, pp 28]

This would mean that sensitive information from one application could be inadvertently saved to a Word document and accessed through a hexadecimal listing program such as WinHex.

Another concerning aspect about Word is the data that is kept within the document including the time of creation, when it was modified and by whom, but more revealing, what information was original and what alterations took place. The effect of this metadata could have far reaching implications for any document containing sensitive information.

The current British Government illustrated this breach of privacy in February 2003 with the publication in Microsoft Word called "IRAQ – ITS INFRASTRUCTURE OF CONCEALMENT, DECEPTION AND INTIMIDATION". All who worked on and altered the document were clearly visible in the metadata of the document and evidence of plagiarism could also be found. Subsequent publications of the document were in the *portable document file* (.pdf) format to avoid a similar embarrassment. [Smith 2003]

One way to avoid this scenario is to change the default *Allow fast saves* setting in Tools/Options/Save in Microsoft Word by unchecking this option. The 'allow fast saves' option, when selected, means that the new changes are saved but the previous version is left alone. [Caloyannides 2002, pp 113]

2.3 Rich text format

The *rich text format* (RTF) was designed by Microsoft as a convenient format for text and graphics to easily be transferred between different applications. This format does not contain the same metadata as the .doc format and was designed to use only the displayable ASCII characters. The RTF is a useful format that is supported by many applications. [Sammes *et al* 2000, pp 29]

As in the other examples above the same basic text was

saved in the rich text format, keeping the same text format for comparison and given the name Example.rtf. Figure 11 shows the beginning of the file in WinHex. The file signature is highlighted on the top row as "{\rtf1\ansi". The file is considerably smaller than the .doc at 2,152 bytes.

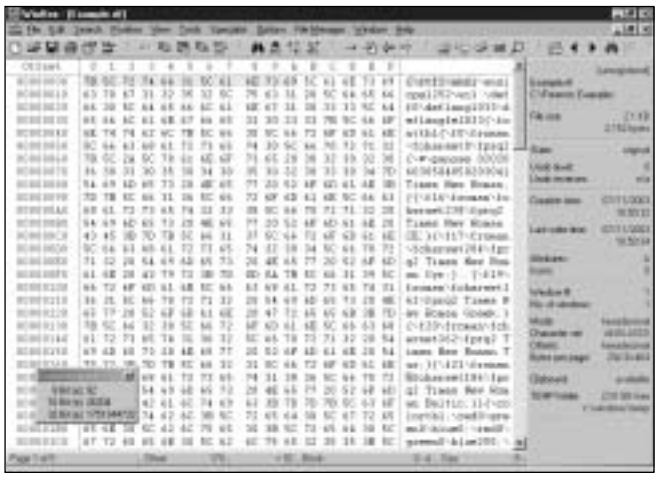


Figure 11 – RTF file signature

Also, unlike the .doc file, the formatting information is displayed in text form and the corresponding ASCII character details about the font type colour, etc. can be seen.

Figure 12 shows the beginning of the text at address 7DBh. The carriage return is included with the line feed at address 80Ch and 80Dh with two corresponding dots in the text area. Unlike before, however, the '\par' formatting information is also included afterwards and again at the end of the text.

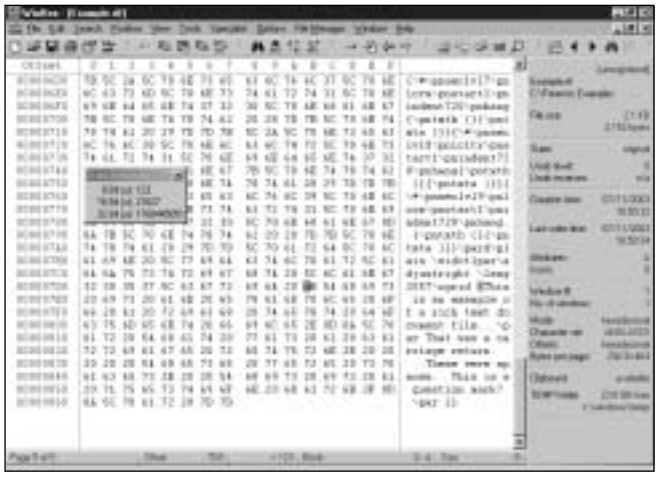


Figure 12 – RTF start of text

2.4 Graphic Formats

2.4.1 Graphic Interchange Format (GIF)

The Graphic Interchange Format (GIF) enables several pictures to be stored in one file and, to reduce the size of the file, uses the loss-free compression algorithm. The GIF file for this example is known as "GIF89a", which is an extended version of the "GIF87a". Figure 13 shows the file, Cat.gif, in the WinHex editor. The picture, shown here in a reduced size, follows.

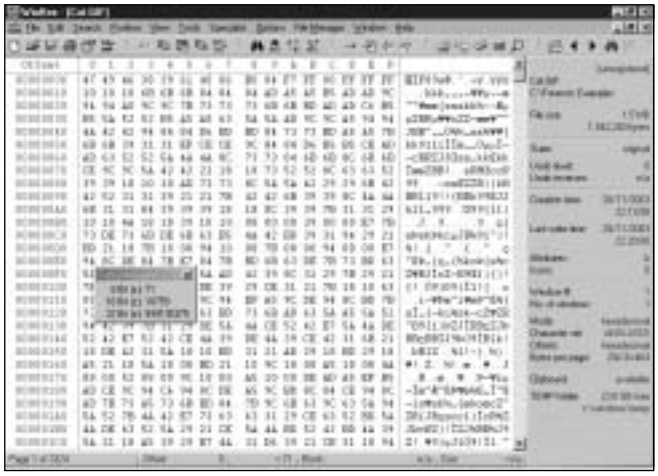


Figure 13 – File signature of GIF and picture below.

The file signature can be seen in the first six bytes in hexadecimal code 47 49 46 38 39 61, which corresponds to "GIF89a" in text. Following this at address 06h is the logical screen descriptor block, which specifies the width of the logical screen in pixels as 40 06 and the height as B0 04. This becomes 0640h and 04B0h in little endian or 1600 decimal and 1200 decimal respectively.

At the following address 0Ah indicates that there is a *global colour table* with a resolution of 8 bits for each primary colour in the table. The table begins at address 0Dh with 256 triplets of red, green, and blue (RGB) intensity values corresponding to all the possible colours in the 256 palette. As each group of three are not all the same value throughout, this indicates these are not grey-scale colours (which would result in a palette of only grey and black tones) but colour.

Figure 14 in the highlighted area, shows the last entry of the colour table at address 312h with the values 00 FF 00. The next value, 2C, signals the start of a GIF picture bearing in mind that there may be more than one picture in the file (though not in this example).

Address 316h is the first byte of the *image descriptor block*, showing the left coordinate of the picture in pixels as 0000. Immediately following at address 318h starts the top coordinated of the picture in pixels also as 0000. The addresses immediately following will again show the width and height of the picture in pixels, 40 06 and B0 04 or little endian 0640h and 04B0h respectively.

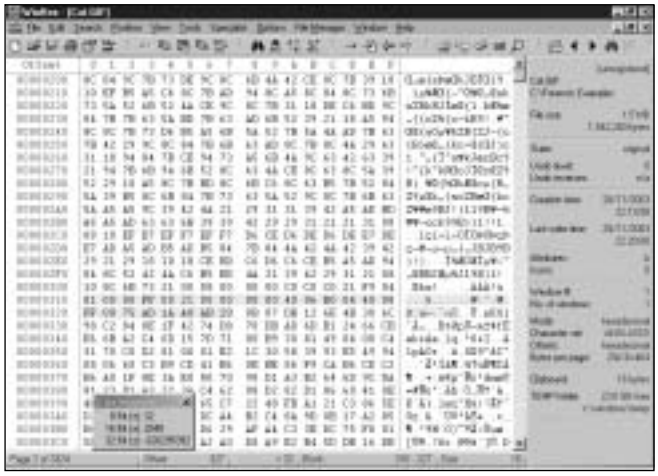


Figure 14 – Start of GIF picture

A single flags byte follows at address 31Eh with the first *raster data block* at 31Fh giving the value 08. This is the *code size* byte used in the LZW decompression process. The following address, 320h begins the first raster data block with the length value of FF. The compressed data for this block will then start at 321h. This will be followed by a number of *raster data sub-blocks.*

The LZ compression algorithms were first developed by Abraham Lempel and Jakob Ziv in 1977, known as LZ77 and are found in archiving programs such as *zoo, lha* and *pkzip*. Terry Welch produced a modified version known as the LZW algorithm and is used in the GIF and TIFF graphic formats. Due to licensing restrictions imposed on the GIF file format by Unisys in 1995, there has been a move away from GIF and towards the Portable Network Graphic (PNG) format ('PNG's Not GIF'). PNG uses a variant of the LZ77 algorithm, which is not subject to the Unisys patent. [Sammes *et al* 2000, pp 33]

2.4.2 Portable Network Graphic (PNG)

The PNG format image uses a variation of the deflate compression method developed by Phil Katz, the author of the pkzip archiving program.

Figure 15 is a screenshot of the same picture in PNG format.

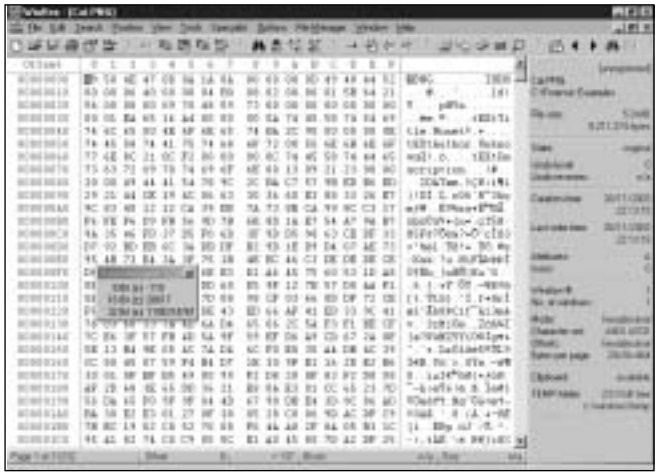


Figure 15 – PNG file screenshot

The file signature in the first eight bytes will always be 89 50 4E 47 0D 0A 1A 0A. The values are used to assist in detecting various kinds of errors. For example, 89 is used to detect whether the file has passed through a 7 bit data transmission channel, and if so, would change to 09. "PNG" (values 50 4E 47) is a recognisable signature in text form. 0D 0A are used together to determine whether or not the file has been manipulated by software in regards to carriage returns and newline sequences. The byte 1A prevents the MS-DOS operating system from listing the file, as it is also the value of Control-Z, the MS-DOS end of file marker. [Sammes *et al* 2000, pp 33]

Just after the signature is the Header data block of 00 00 00 0D which gives the double word length equivalent value in decimal as 13. Following this, in address 0Ch, is the signature for the data block as the characters "IHDR". The 13 data byes start at address 10h and first gives the double word width of the image in pixels 00 00 06 04, then the double word height in pixels 00 00 04 B0. These values are given in big endian format (1600 and 1200 decimal) and are exactly the same results obtained in the GIF file. The next five bytes starting at address 1Ch with the values 08 02 00 00 01 indicated a colour resolution of 8 bits followed by the colour information. The data block ends at address 1Dh with a double word cyclic redundancy check.

The next data block starts at address 7Eh which gives the data length as 00 00 20 00, or decimal value 8192, followed by the character signature for this block "IDAT", the Image Data, at address 82h. The 8192 bytes of compressed data begin at 86h.

2.4.3 JPEG File Interchange Format (JFIF)

The two previous graphic format examples use lossless compression methods. This enables the file size to be reduced by only around a half. The JPEG format differs in that it primarily uses lossy methods for compression. This means that information is discarded that would not be visible to the human eye to achieve compression ratios of the order of 20:1.

The Joint Photographic Experts Group (JPEG), formed in 1987, is a standards committee formed from sub-groups of two separate bodies: the International Telegraph and Telephone Consultative Committee (CCITT), and the International Organization for Standardization (ISO). Together they established the JPEG ISO standard (undated), a single standard in compression methods for the transmission of graphics. The JPEG File Interchange Format (JFIF) was designed to define a common file interchange format to enable JPEG bitstreams to be exchanged between a variety of platforms and applications. [Sammes *et al* 2000, pp 34]

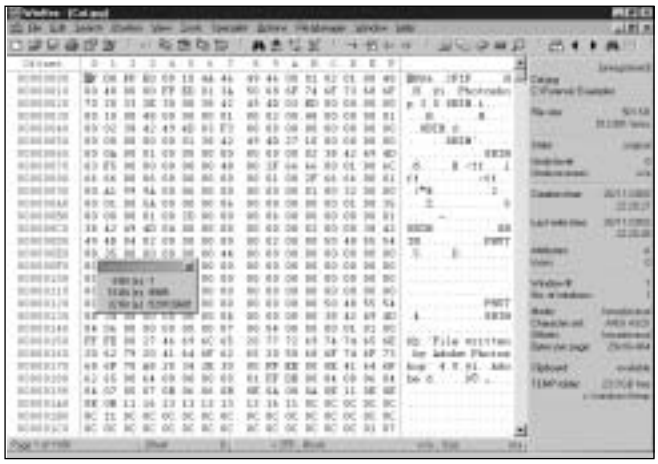
JPEG is based on more than one compression method and can be altered to fit the needs of the user. File types such as JPG, JPEG, JIF or JFIF are most likely to be in JFIF format.

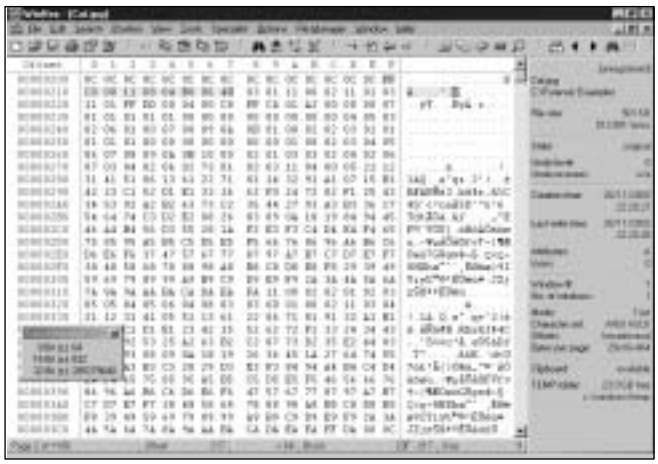
The same picture as the previous two examples was saved in JPEG format and is shown in the WinHex editor in figure 16. Three screenshots of different address locations are presented together to show main points of interest for analysis.

The size is noticeably smaller at only 501 kilobytes instead of 1.5 Megabytes for GIF and 5 Megabytes for PNG; however, there is a discernible difference of quality. See Cat.jpg in figure 13 for comparison.

The first four bytes are effectively the JPEG file signature. The first two bytes, FF D8, are the *start of image marker* block and the next two, FF E0, indicate an *application marker* block. These along with the characters starting at address 06h, "JFIF" values 4A 46 49 46, identifies this as a JFIF file.

Cat.jpg





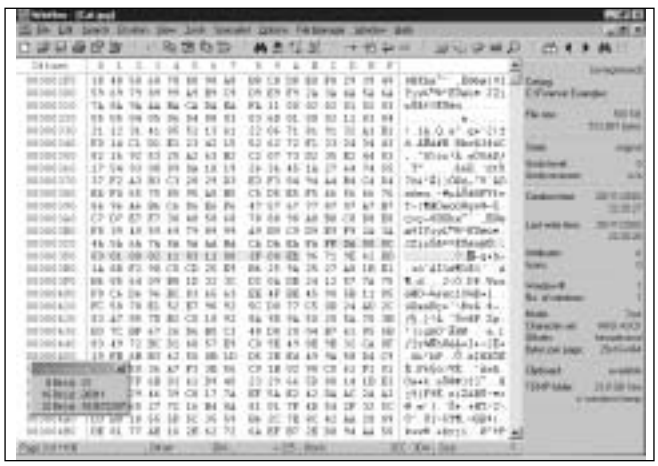


Figure 16 – Three WinHex screenshots with different sequences of Cat.jpg shown above

The sequence beginning at address 20Fh of value FF C0 is a *start of frame marker* block. The value of 08 bits per pixel is given at address 213h followed by the height of the image in pixels, 04 B0, and width of the image in pixels, 06 40, both in big endian formats (1200 and 1600 decimal). These are exactly the same results obtained from both the GIF and PNG files.

In the last sequence, starting at address 3CCh, is the *start of scan marker*, FF DA, and the compressed data begins at address 3DAh.

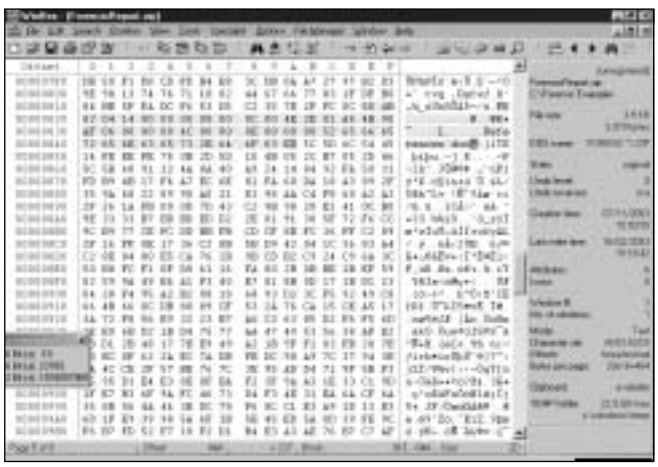
2.5 Pkzip

As mentioned previously, pkzip is an archive format that uses LZ compression algorithms. Archiving involves two functions: one or more files are compressed using lossless compression and the compressed files are archived into a single file. In pkzip this is given the file type ZIP (.zip).

Figure 17 shows three different sequences of a ZIP file with two documents called ForensicReport.doc and References.doc. These two documents are compressed into one file called ForensicReport.zip.

The file signature is shown in the first four bytes with the values 50 4B 03 04 with the characters "PK" visible in text. The signature is part of the *local file header*, which is repeated for every file in the archive. Immediately after the signature are a series of bytes detailing the *pkzip* version number, general-purpose flags, the compression method used, the last modified date and time of the file, a cyclic redundancy check, the compressed and uncompressed file sizes and the filename in characters. [Sammes *et al* 2000, pp 36]

At address 1Eh the first file in the archive is listed as ForensicReport.doc. The compressed file size begins at address 12h with the values EE 07 00 00. Put into little endian double word format this becomes 00 00 07 EE, or 2030 in decimal. The original size is listed in 16h with the values 00 4C 00 00, or 00 00 4C 00 in little endian double word format or 19,456 decimal. At address 30h immediately following the filename starts the compressed file data. The pattern of a local file header followed by the compressed file data is repeated for each of the files as can be seen at address 81Eh where the References.doc file is found. At the end of the file sequence a central directory record is established. Address EF9 the signature 50 4B 01 02 of the first file header in the central directory record. The second appears in address F39h. Similar information is shown as in the local file header and each filename is displayed in character form. The central directory record and ZIP file is terminated by an end of central directory record, with the signature 50 4B 05 06 starting at address F75h.



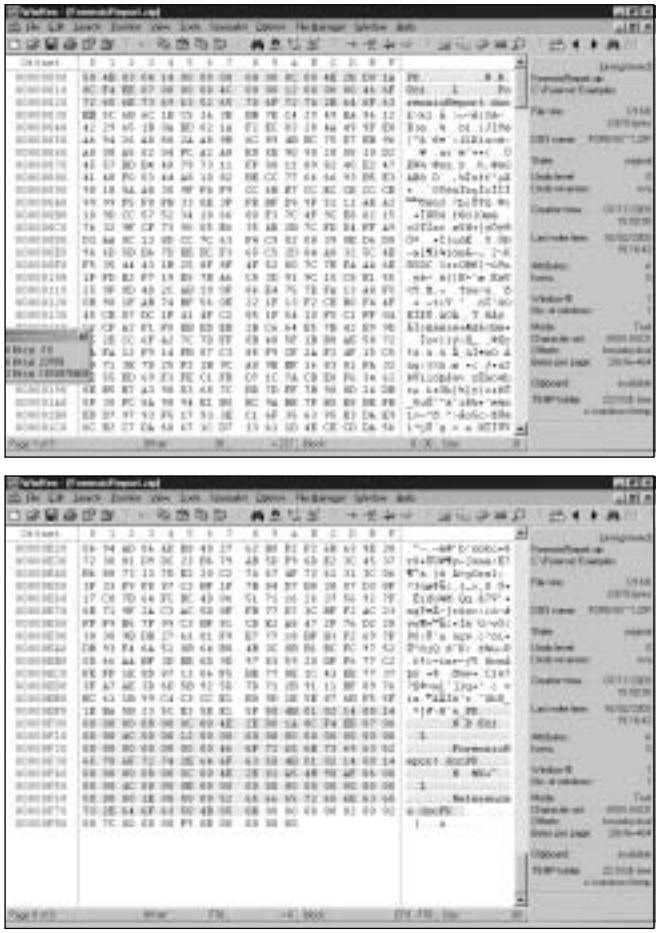


Figure 17 – Three sequences of ForensicReport.zip in WinHex

It is interesting to note that the display of the filenames and other details are still available in both the local file headers and central directory record even if the ZIP file has been password-protected. [Sammes *et al* 2000, pp 37]

To be continued in the next IRMA Journal

Celeste has recently completed an MSc in Information Security at Westminster University. She can be contacted on RushLSE97@aol.com

Care of your data

1. Never leave diskettes in the disk drive, as data can leak out of the disk and corrode the inner mechanics of the drive. Diskettes should be rolled up and stored in pencil holders.
2. Diskettes should be cleaned and waxed once a week. Microscopic metal particles can be removed by waving a powerful magnet over the surface of the disk. Any stubborn metallic shavings can be removed with scouring powder and soap. When waxing diskettes, make sure application is even. This will allow the diskettes to spin faster, resulting in better access time.
3. Do not fold diskettes unless they do not fit in the drive. "Big" diskettes may be folded and used in "little" disk drives.
4. Never insert a disk into the drive upside down. The data can fall off the surface of the disk and jam the intricate mechanism of the drive.
5. Diskettes cannot be backed up by running them through the Xerox machine. If your data needs to be backed up, simply insert two diskettes together into the drive whenever you update a document; the data will be recorded on both diskettes.
6. Diskettes should not be inserted into or removed from the drive while the red light is flashing. Doing so could result in smeared or possibly unreadable text. Occasionally the red light continues to flash in what is known as a "hung" or "hooked" state. If your system is "hooking" you, you will probably need to insert several dollars before being allowed to access the disk drive.
7. If your diskette is full and you need more storage space, remove the disk from the drive and shake vigorously for two minutes. This will pack the data ("data compression") enough to allow for more storage. Be sure to cover all the openings with scotch tape to prevent loss of data.

BCS MATTERS!

Colin Thompson
BCS Deputy Chief Executive

New Grading Structure Boosts Member Recruitment

The new BCS grading structure, introduced on 1 May this year has resulted in a 10% increase in membership numbers in just 3 months.

Up to 31 July, more than 3,500 new members had joined, including over 2,600 new professional members. This compares with a total of only 200 new professional members in the same 3 month period in 2003. This puts the Society well on track to hit its target of 10,000 new professional grade members in the first year of the new arrangements.

As expected, the new *'Trusted Source'* arrangements have played a major part in this early success. Nomination by existing members under those arrangements have been directly responsible for around half the new member applications and a significant proportion of others reporting that their application was prompted by a colleague recommendation.

The trusted source arrangements are designed to provide an invitation-based approach to professional membership with a target of 3 days for the completion of admission processing when the nominee responds. At present these arrangements operate only at the MBCS level but, I mentioned in this column in the summer edition, that we were piloting similar arrangements for direct election to FBCS. That pilot has now been completed very successfully and all existing Fellows are being invited to nominate colleagues with sufficient seniority, eminence or authority to justify an invitation to join the BCS as a Fellow. If the pattern from the pilot is replicated in the broader scheme, this will result in the recruitment of a significant number very senior new entrants to BCS, many of whom are keen to make an active contribution.

The trusted source concept is also an important element in the new relationships now being forged with some of the key employers of IT staff. Companies who have signed up to the new BCS Corporate Professional Partnership scheme include GCHQ, Royal Bank of Scotland, British Energy, and the Department of Works and Pensions. And discussions are in progress with 15 other companies.

A New London Base for BCS

The BCS leaves its London office at 11 Mansfield Street later this year and moves to new accommodation in Southampton Street, Covent Garden. The lease on the Mansfield Street building runs out in 2005 and the process of finding somewhere new was started over a year ago. Deputy President David Morriss led the project with a requirement for a combination of office space, various sizes of conference rooms, open space for multiple uses and a drop-in facility, all of which should have maximum flexibility. The location had to be within easy reach of the London rail termini and it had to meet all the requirements of the Disability Discrimination Act. The new building has a magnificent Edwardian façade which conceals a completely modern open plan building. It is situated in the Davidson Building, Southampton Street, with its main entrance just off the Strand in easy walking distance of Covent Garden, Charing Cross and Embankment underground stations. We are on the first office floor and have 7,300 square feet of space. A facility we did not have at Mansfield Street was a large conference room. We now have the capability to house 100 delegates in the new building. Nearby institutional neighbours include the Royal Society of Arts and the Institution of Electrical Engineers.

New Professional Development Products Launched

Career Developer, the latest in the line of new BCS professional development products was launched on 23 September. Like the other products in the portfolio, Career Developer has been developed in partnership with Infobasis and has, at its core, the SFIAPlus skills framework. It complements Skills Manager, launched earlier this year and is aimed at organisations that want to go beyond identifying and managing their IT skills to provide integrated career development planning.

Skills Manager and Career Developer are supported with both consultancy and training services and BCS will provide fully supported and accredited development schemes similar to the long-standing Professional Development Scheme.

Development work on a product known as Professional Experience Record (PER) is also well advanced. PER is aimed primarily at independent consultants and contractors and will provide a validated record of experience and achievements.

New Code of Practice

A new Code of Good Practice, the guidance dealing with how a member performs technically, has been approved. The work, undertaken by the Ethics Expert Panel, contains a core of common practices applicable to all members followed by sections covering good practices particular to such areas as project management, education, research functions and business functions such as software development.

The new Code is designed primarily as a web-based document and is intended to be read in parallel with the BCS Code of Conduct, which is also on the website.

The new Code has been rewritten to take account of both the increasing public concern about the ethical uses of IT, and new legislation such as the Freedom of Information Act and the Public Disclosure Act.

EUCIP Moves Forward

The status of the new European Certification of Informatics Professionals (EUCIP) qualifications scheme run in the UK by the BCS has been boosted by its approval as a funded qualification for further education. The approval by the UK Qualifications and Curriculum Authority follows acceptance by the Learning and

Skills Council into its education credits framework.

EUCIP, an initiative of the Council of European Professional Informatics Societies, was launched in the UK late last year and is aimed both at those entering IT and at existing specialists seeking continuing professional development.

BCS Expanding Internationally

Around 14% of BCS members are located outside the UK and more BCS international sections (the equivalent to a branch in the UK) are in prospect after enquiries from members across the world. And meanwhile the BCS's standing in Mauritius and Sri Lanka is being enhanced further by forthcoming graduation and awards events.

Consideration is also being given to the possibility of a regional section in the Gulf, covering Bahrain, Jordan, Kuwait, Oman, Qatar, Saudi Arabia, UAE and Yemen.

In the USA a preliminary meeting is being set up in October, aiming to elect a committee and discuss possible events. Regional sub-sections may be set up later, depending on the spread of members.

A new Hellenic Section in Greece is having its inaugural event on 21 October, when Charles Hughes, the BCS Vice President Member Services and Deputy President elect will give a presentation.

The Switzerland Section had its first major meeting last month in Bern and the Isle of Man Section has its first event this week.

The Mauritius Section is holding its fourth annual graduation event on 2 October for people taking the BCS Professional Examination – with speakers including the Mauritian prime minister and BCS President Wendy Hall. Around 150 people will receive their awards at Certificate, Diploma and Professional Graduate Diploma levels.

The Sri Lanka Section is holding its annual BCS graduation event on 7 October and its National Best Quality Software Awards event the day after. The awards, at business, higher education and school level, are said to be the most prestigious in Sri Lanka, if not the whole region. Last year 26 companies, 40 university students and 70 schools took part. Almost 300 people attended the awards gala dinner – including Sri Lanka's science and technology minister and BCS Vice President Charles Hughes.

And Finally.....

Some dates for the diary

The Awards presentation night for the BCS Professional Awards will, once again, be a black-tie event at the London Hilton on Park Lane on Tuesday 19 October 2004.

The Oscar-style Awards ceremony will be honouring the medallists and winners – individual and teams – who are being recognised for their skills, innovation and leading edge solutions. The dinner itself takes place in the magnificent ballroom, suitably dressed for the occasion. The evening will include entertainment and surprises to keep the audience occupied whilst they are waiting to for the announcement of the winners.

And the BCS Annual General Meeting will be held the new BCS London offices, **First** Floor, The Davidson Building, 5 Southampton Street, London WC2E 7HA on Wednesday 3 November 2004 at 3.30 p.m.

Further information on these or any other BCS related issues may be found on the BCS Web site (http://www.bcs.org). Information is also available from Customer Services at The British Computer Society, 1 Sanford Street, Swindon, SN11HJ (*e-mail to marketing@hq.bcs.org.uk*)

Member Benefits Discounts

Mark Smith

We have negotiated further discounts for IRMA members since the last journal, including 20% off the Unicom Outsourcing conference, which is held on 12th and 13th October. Contact details for these discounts and more are below:

Software

Product	*Discount Negotiated*	*Supplier*
Caseware Examiner for IDEA (mines security log files for Windows 2000, NT, XP)	15%	Auditware Systems (www.auditware.co.uk)
IDEA (Interactive Data Extraction and Analysis)	15%	Auditware Systems (www.auditware.co.uk)
Wizrule (data auditing and cleansing application)	20%	Wizsoft (www.wizsoft.com)
Wizwhy (data mining tool)	20%	Wizsoft (www.wizsoft.com)

Events

Event	*Discount Negotiated*	*Contact*
Computer and Internet Crime 2005 (www.cic-exhibition.com)	15%	Paul Webster paul@panpres.co.uk
Risk Management Congress 2004 (www.iir-conferences.com)	20%	Sindi Chong schong@iirltd.co.uk
SANS Amsterdam 2004 (www.sans.org/amsterdam04/)	10%	Ross Patel rpatel@sans.org
All Unicom events (www.unicom.co.uk)	20%	Julie Valentine julie@unicom.co.uk

We are looking to extend this range of discounts to include additional events, training courses, computer software or other products that our members may find beneficial. If you have any suggestions for products we could add to the list, please contact Mark Smith (mark.smith@lhp.nhs.uk), our Members' Benefits Officer, and he will be happy to approach suppliers.

IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

Membership Application

(Membership runs from July to the following June each year)

I wish to APPLY FOR membership of the Group in the following category and enclose the appropriate subscription.

CORPORATE MEMBERSHIP (Up to 5 members)* *Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal *(see over)*	£75
INDIVIDUAL MEMBERSHIP *(NOT a member of the BCS)*	£25
INDIVIDUAL MEMBERSHIP *(A members of the BCS)* BCS membership number: _____	£15
STUDENT MEMBERSHIP (Full-time only and must be supported by a letter from the educational establishment). Educational Establishment: _____	£10

Please circle the appropriate subscription amount and complete the details below.

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
E-mail:
PROFESSIONAL CATEGORY: (Please circle) 1 = Internal Audit — 4 = Academic 2 = External Audit — 5 = Full-Time Student 3 = Data Processor — 6 = Other (please specify)
SIGNATURE: DATE:

PLEASE MAKE CHEQUES PAYABLE TO "BCS IRMA"AND RETURN WITH THIS FORM TO

Janet Cardell-Williams, IRMA Administrator, 49 Grangewood, Potters Bar, Herts EN6 1SL. Fax: 01707 646275

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

CHAIRMAN	Alex Brewer	alex.brewer@morganstanley.com
SECRETARY	Siobhan Tracey	siobhan.tracey@booker.co.uk
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Celeste Rush	rushlse97@aol.com
JOURNAL EDITOR & SECURITY PANEL LIAISON	John Mitchell	john@lhscontrol.com
WEBMASTER	Allan Boardman	allan@internetworking4u.co.uk
EVENTS PROGRAMME CONSULTANT	Raghu Iyer	raguriyer@aol.com
LIAISON - IIA & NHS	Mark Smith	mark.smith@lhp.nhs.uk
LIAISON - LOCAL AUTHORITY	Peter Murray	cass@peterm.demon.co.uk
LIAISON - ISACA	Ross Palmer	ross.palmer@hrplc.co.uk
MARKETING	Wal Robertson	williamr@bdq.com
ACADEMIC RELATIONS	David Chadwick	d.r.chadwick@greenwich.ac.uk
	David Lilburn Watson	dlwatson@bcrm.co.uk

SUPPORT SERVICES

ADMINISTRATION	Janet Cardell-Williams t: 01707 852384 f: 01707 646275	admin@bcs-irma.org
OR VISIT OUR WEBSITE AT	**www.bcs-irma.org**	Members' area Userid = irmamembers Password = irma2004

BCS IRMA SPECIALIST GROUP ADVERTISING RATES

Reach the top professionals in the field of EDP Audit, Control and Security by advertising in the BCS IRMA SG Journal. Our advertising policy allows advertising for any security and control related products, service or jobs.

For more information, contact John Mitchell on 01707 851454, fax 01707 851455 email john@lhscontrol.com.

There are three ways of advertising with the BCS IRMA Specialist Group:

The Journal is the Group's award winning quarterly magazine with a very defined target audience of 350 information systems audit, risk management and security professionals.

Display Advertisements (Monochrome Only) Rates:

- Inside Front Cover £400
- Inside Back Cover £400
- Full Page £350 (£375 for right facing page)
- Half page £200 (£225 for right facing page)
- Quarter Page £125 (£150 for right facing page)
- Layout & artwork charged @ £30 per hour

Inserts can be included with the Journal for varying advertising purposes, for example: job vacancies, new products, software.

Insertion Rates:

For inserts weighing less than 60grams a flat fee of £300 will be charged. Weight in excess of this will incur additional charges:

- 60-100grams: 14p per insert
- 101-150g: 25p per insert
- 151-300g: 60p per insert
- 301-400g 85p per insert
- 401-500 105p per insert

Thus for an insert weighing 250g it would cost the standard £300 plus weight supplement of £210 (350 x 60pence) totalling £510.

Discounts:

Orders for Insert distribution in four or more consecutive editions of the Journal, if accompanied by advance payment, will attract a 25% discount on quoted prices.

Direct mailing

We can undertake direct mailing to our members on your behalf at any time outside our normal distribution timetable as a 'special mailing'. Items for distribution MUST be received at the office at least 5 WORKING DAYS before the distribution is required. Prices are based upon an access charge to our members plus a handling charge.
Access Charge £350. Please note photocopies will be charged at 21p per A4 side.

Personalised letters:

We can provide a service to personalise letters sent to our members on your behalf. This service can only be provided for standard A4 letters, (i.e. we cannot personalise calendars, pens etc.). The headed stationery that you wish us to use must be received at the Office at least ten working days before the distribution is required. Please confirm quantities with our advertising manager before dispatch. If you require this service please add £315 to the Direct mailing rates quoted above.

Discounts: Orders for six or more direct mailings will attract a discount of 25% on the quoted rates if accompanied by advance payment

Contacts

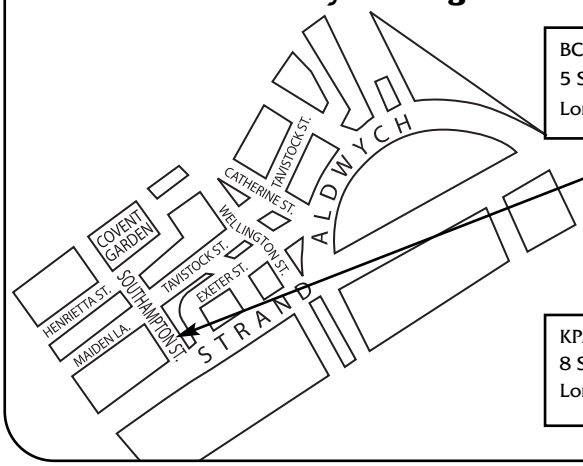
Administration

Janet Cardell-Williams,
49 Grangewood, Potters Bar, Hertfordshire EN6 1SL
Email: admin@bcs-irma.org
Website : www.bcs-irma.org

BCS IRMA Specialist Group Advertising Manager

Eva Nash Tel: 01707 852384
Email: admin@bcs-irma.org

Venue for Full Day Briefings



BCS, The Davidson Building,
5 Southampton Street,
London WC2 7HA

KPMG
8 Salisbury Square
London EC4

Venue for Late Afternoon Meetings