

## Corporate Evidence Collection: The Unique Challenges



Ashwell Point, Babraham Road, Sawston, Cambridge CB2 4LJ, United Kingdom  
t +44 (0)870 600 1667 f +44 (0)870 600 1668 w www.7safe.com

**7safe**  
information security

### About the author:

Jim Kent (CSTP, CFIA) is a senior forensic consultant & instructor for 7Safe - an independent Information Security practice delivering an innovative portfolio of services including: forensic investigation; ISO 27001 consulting; penetration testing & university-accredited information security training. 15/01/2006

### The Unique Challenges of Collecting Corporate Evidence

“If your organisation was asked to produce reliable evidence of what has happened within its computers, perhaps after a suspected crime or attack, or to resolve a legal dispute – how well would it respond?” This is the question posed in a white paper entitled “Directors and Corporate Advisors’ Guide to Digital Investigations and Evidence”, prepared by Peter Sommer for the Information Assurance Advisory Council<sup>1</sup>.

According to the paper, nearly all organisations underestimate how often they may be called upon to produce reliable evidence of what has happened in and around their information and communication technology (ICT) systems. “They also underestimate the demands that the legal system makes in terms of ensuring the admissibility and reliability of digital evidence. Both of these can have a profound impact on business welfare”<sup>2</sup>.

This article discusses issues surrounding corporate evidence collection. The views and opinions expressed within are based on experience and findings from our work in the field.

The corporate world is slowly realising the importance and implications of computer-based or digitally-based evidence. However, many organisations believe that the challenges surrounding the collection and production of corporate evidence are unique to them and differ from those facing other organisations and law enforcement. Whilst there are situations that can create additional complexities, the issues are not necessarily unique; we believe that the processes surrounding evidence collection and production within the corporate environment have many traits and characteristics in common with those utilised by law enforcement. Perhaps the biggest problem and therefore challenge facing the corporate world is the lack of forensic readiness within organisations today.

It is probably fair to say that the approaches to evidence collection and production adopted by law enforcement are different to those of the majority of organisations. These differences stem from the fact that law enforcement agencies have had a head start in the field of computer forensics and over the past few years have established very high standards regarding the preservation and presentation of evidence found on digital media. In our experience, a large number of organisations have no processes or procedures in place for handling events that result in the requirement to produce reliable evidence. In comparison to the corporate world, the law enforcement arena is generally, but not exclusively, task orientated and the need to be pro-active in the same sense as the corporate world does not exist.

There are strict protocols and guidelines governing law enforcement and computer forensics, covering aspects of evidence continuity and best practice. Many of these practices should be adopted by the private sector as they provide an excellent foundation for corporate organisations. Adherence to a common set of policies, procedures and practices would help ensure continuity and smooth transfers of evidence from the corporate to

<sup>1</sup> <http://www.iaac.org.uk>

<sup>2</sup> Directors and Corporate Advisors’ Guide to Digital Investigations and Evidence; September 2005, Sommer, Peter, IAAC

the law enforcement environment, in the event that law enforcement involvement is required.

In our experience, a large number of organisations do not consider the issues surrounding incidents that require the production of evidence and have no procedures in place for handling the resulting evidential requirements. When such an incident does occur, these organisations tend to resort to following a fire-fighting approach which, in turn, means making snap decisions with little information. Fundamental mistakes are often made when attempting to do the 'right thing' while handling the event. In the worst case, this can have a seriously detrimental effect on the collected evidence and even, perhaps, on the running and functioning of the organisation.

Adopting a more pro-active approach naturally results in improved handling of incidents. An organisation may elect to train certain members of staff in the area of computer forensics thus enabling them to handle potential incidents in the correct manner. Drawbacks to this option include the training and equipment costs and, potentially, a lack of impartiality resulting from staff being investigated by their colleagues. An alternative option for organisations to consider is the employment of an external forensic firm or investigator. A good firm or investigator will have experience, training and independence but these attributes may carry a high price tag. Whatever the approach, all organisations should ensure they adopt practices that assist them in becoming forensically ready. Failure to do so could result in missed, lost or contaminated evidence or the mishandling of suspects, any of which could result in a large financial loss for the business.

The idea of being pro-active in this field is not new but one which is taking time to filter through to organisations that see no need to act until an incident arises. Alongside many of the suggestions proposed in the IAAC paper prepared by Peter Sommer, some organisations are also considering the idea of obtaining forensically sound 'snapshots' of random computers within the organisation. These snapshots are then analysed in terms of the organisation's acceptable usage policies (private data and emails are not examined). This approach can be compared to the random drugs tests that are conducted in the professional sporting arena, with the same obvious benefits. Further, when a member of staff leaves the organisation, it makes sound sense to take an image of the drive before wiping, re-installing and handing the system over to the new member of staff. Before this process can be implemented, the organisation must ensure it has the necessary policies and procedures in place to reflect this approach and all staff must be made aware of the 'dip' sampling of computer systems. This is fair to both the users and the organisation and shows consideration of data protection and human rights issues.

The lack of forensic readiness is a common problem. Let us consider a hypothetical scenario. This scenario is based on previous experience but should by no means be considered a detrimental view of any particular organisation or individual; it is purely an opportunity to highlight the need for sound planning and readiness. In our scenario we will consider inappropriate material. However, there are numerous reasons why digital evidence may need to be secured, ranging from fraud or industrial espionage to harassment, blackmail or network compromises. The advancement of technology has been a fantastic leap but has also introduced the ability to carry out old style crimes in a new way.

In our scenario, we receive a telephone call from a member of staff within an organisation. During the call, they explain that they believe another employee to be accessing inappropriate material and ask what they should do next.

The first point for the forensic investigator to take into consideration is who has made the call, why and whether it was within their remit to do so. Once this has been established and contact with the correct individual has been made, maintaining this single point of contact is crucial for the integrity of the investigation.

After a few questions, it becomes clear that, prior to the telephone call, several mistakes were made. The laptop was given to the IT Department for examination in an attempt to locate evidence. Once it was clear to the IT Department that there were a large number of folders containing inappropriate material, the HR department was approached by the manager of the suspected employee and discussions were held as to how to handle the case. It was decided that disciplinary action should be taken; it was also decided that an external company should be contacted for assistance 'just in case'.



When organisations deal with such an issue, the above process is not uncommon but there are potential problems with it. It is possible that evidence has been destroyed, compromised or missed. For example, the suspected member of staff's PDA or mobile telephone may also contain useful evidence and should be seized. It is also highly likely that someone in the IT department has stamped their digital footprints all over the data to be secured: for example, the date and time stamps associated with the files and folders containing the inappropriate material may have been altered during the IT department's investigation. While this is not an insurmountable problem, it introduces unnecessary complications into the investigation.

The telephone call has also highlighted how many people in the organisation are now aware of the issue and there is a risk of partiality if details of the investigations are leaked to this member of staff (e.g. the removal of evidence from network servers or home computers if applicable). This naturally brings the admissibility of the evidence into question, should the investigation proceed to civil or criminal litigation.

Before we can advise the client how to proceed, we first have to establish what current policies and procedures the organisation has in place - to ensure we meet any legal obligations that result from them. We must also assess the potential impact on the company, such as loss of productivity, data loss, possible compromise of records and the overall impact to its reputation.

There are of course facts to be established as part of the initial investigation process and reviewed as the investigation proceeds, such as: who the recipient of the initial reports will be; what the implications of any findings for the organisation will be; and the next steps in the investigation, especially if it has to be handed over to law enforcement. It is then necessary to identify what steps are required to identify and secure the relevant digital evidence. Its physical location must be established (e.g. laptop, desktop, network storage). Its geographical location must also be established, for example, the user may be located in the UK but the digital evidence may be stored on a server in the USA. This information will have real implications on any investigation. Understanding management's objectives throughout the investigation is also important: their objectives often change as the investigation evolves.

A crucial part of any investigation is the proper collection of evidence and ensuring a correct chain of custody of the suspect computer systems, hard drives, PDAs or mobile telephones. Forensic investigators need to be sure they can identify what the evidence is, who seized it, the time and date it was seized and from where it was seized. If evidence changes hands multiple times, this must be documented and signed: best practice necessitates keeping track of all items.

When a third party becomes involved in an investigation, as in this scenario, investigators will usually require an area in which they can work acquiring evidence and possibly conducting interviews. This often presents problems as not all areas are necessarily appropriate. In the past, we have found ourselves in a building basement and conversely also in the middle of an open office in a glass meeting room with all eyes on us. Ideally, the area should be forensically sterile and secure, away from other members of staff. It may also be appropriate for the client to have a back-up story to explain the presence of the investigators to deflect questions from ever-inquisitive staff.

The acquisition of evidence may entail making a number of decisions and it is perhaps some of these that corporate entities feel are unique when compared to those taken by law enforcement. It is commonly believed that law enforcement has to take systems away for imaging or that they will take images of all systems even if it is financially detrimental to an organisation, such as an eCommerce server running 24 hours every day. While this may have been the case in the past, law enforcement are very much aware of the implications of their actions and will certainly review alternate possibilities for obtaining best evidence.

Whilst corporate organisations may have some complex issues, such as large RAID arrays or 24x7x365 services that require additional consideration, the majority of issues surrounding digital evidence are not unique to them. There are a number of options that can be considered when looking to acquire evidence from within an organisation; the appropriate option will depend upon the organisation's requirements. For example, can the organisation continue to operate without the offending machine or must it remain in operation? Can the offending machine be reviewed during office hours, or is there a requirement for this to take place (covertly)



after hours? It is possible, when dealing with systems that must remain in operation, to conduct a live analysis and obtain evidence in compliance with accepted guidelines, e.g. the Association of Chief Police Officers (ACPO) guidelines. In the majority of cases, including our scenario, it is usually possible to image the suspect workstation. However, servers containing data can only be accessed out of working hours or using a live analysis technique.

There are many ways to create a forensically sound image of the digital media using tried and tested software. Discussing the various software products utilised for this purpose is outside the scope of this article, but there are a number of products that are legally acceptable and used regularly all over the world.

Whilst the corporate environment offers up a few complexities associated with the gathering of digital evidence, it also offers a number of resources that can greatly assist an investigation. For example, most organisations re-distribute centralised resources, such as e-mail servers, authentication servers and file servers. In addition to these resources, organisations often deploy perimeter security devices such as firewalls and proxy servers. Many of these devices provide some form of logging. These log files can prove invaluable to an investigation and can often be used to corroborate or clarify findings.

In our scenario, we were able to obtain a number of log files that helped demonstrate the suspect had repeatedly retrieved inappropriate material. The log file entries could be matched with the times and dates of the items on the workstation. The logs also showed that the user was utilising the system at the time these items were actually retrieved. We did however experience issues with the log files that affected the time required to complete the investigation as well as the overall complexity of the same. The organisation did not synchronise the time for the various resources in use in the company. The proxy server, firewall and authentication servers all had differing time configurations: indeed one of the devices was configured for an incorrect time zone!

Our scenario proved relatively straightforward, but not all cases turn out that way. Sometimes, during analysis, certain events may unfold or new issues may be raised. For example, the investigator may discover illegal content, such as paedophilia, in which case the evidence must be handed over to law enforcement. We have seen cases in which a number of staff are implicated, such as in the case of fraud, rapidly changing the face and complexity of the investigation. We have also seen cases that started as simple disciplinary hearings turn into civil or criminal cases. It is essential that all processes prior to this point are forensically sound and comply with the accepted principles so the investigation is not compromised.

Although there were minor issues surrounding the evidence in our case, such as the corruption of the digital scene by the IT department and the lack of time synchronisation amongst network resources, it was still possible to demonstrate that the member of staff had contravened the acceptable usage policies. As all work was conducted in a forensically sound manner, the case would stand up in a court of law. The organisation was able to complete the disciplinary action without incident.

Our hypothetical (but fairly typical) organisation learned some valuable lessons from the experience. They have since implemented a number of policies and procedures that map to the best practice forensic guidelines. They are now ready for any further incidents – they have become forensically prepared.

The future is in planning. The white paper recently released by the Information Assurance Advisory Council, titled “Directors and Corporate Advisors’ Guide to Digital Investigations and Evidence”, prepared by Peter Sommer, aims, “to help directors, senior managers and their legal advisers to understand the key strategic and management issues. It is designed to anticipate the need for provision of digital evidence and investigations by setting up management procedures, acquiring appropriate resources and identifying third-party sources of emergency assistance.” This paper is well worth reading and serves as an excellent reference point.

Although the field of computer forensics, data, transfer speeds, and storage sizes appears to grow daily, it is almost impossible to predict what the future holds. Neglect, however, is not an option. It may only be a matter of time before your organisation is thrown into the grip of securing digital evidence and held accountable for it. To truly overcome the challenges facing the collection of corporate evidence, it is time to become forensically ready!

