

eDisclosure & Forensics

What do I need to know?

Authors: James Kent & Chris Dale

The purpose of this white paper

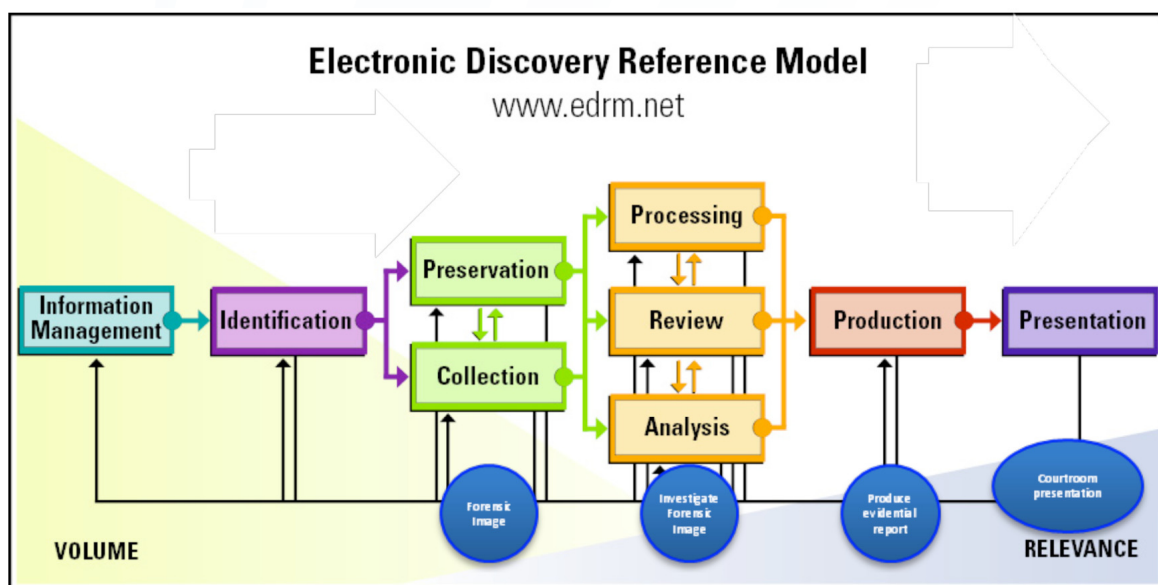
Computer forensics is necessarily a new science. It has two broad components – the application of technological skills and equipment to the preservation and collection of electronic data from computers and other electronic devices, and the interpretation of the results of that collection to help lawyers and law enforcement bodies to make use of it in civil or criminal proceedings.

The purpose of this paper is to show how the evolving computer forensics units in various law enforcement teams went through growing pains developing ways to preserve, collect, interpret and present the evidence, and how a similar path is evolving in the electronic disclosure market place. The key element is the integrity of the findings. Anyone involved with presenting any form of digital evidence must be sure that the final document presented in a court bundle or on a screen is identical in every way to the original item and be able to prove that.

How much do you need to understand?

Informed thinking about digital evidence can sometimes make the difference between a successful and an unsuccessful outcome. The solution must be proportionate to the purpose, especially in the current economic climate. The better you understand what is possible and what is involved, the easier it is to frame instructions to the company making the collection. The clearer the instructions the easier it is to get a clear description of the proposed deliverables and the likely cost.

The Electronic Discovery Reference Model shows the stages through which digital evidence passes from its source to presentation in court. In its simplest form, a digital forensic investigation consists of taking a forensic image of the data, investigating and analysing the data and finally producing a report. Thereafter the investigator may have to stand up in court to present as an expert witness.



Although much evidentiary material is still paper-based, it is estimated that 90% of new documentary material is digital in origin and remains so throughout its life, most of it never being printed. That which exists only as paper can be converted to digital form by scanning it to ease the handling and review process. Technology has brought with it some significant leaps in case management. Complex email, word processed, spreadsheets and other user-created documents are now reviewable through a litigation support review platform. However, with this new ability there are new issues to consider, such as metadata, file slack and deleted space. These never arose when using paper.

Looking back at the criminal side, as law enforcement grew into the world of hi-tech crime (in the latter half of the nineties); it became clear that electronic evidence was not always collected in a consistent manner between units. Evidence was potentially altered due to lack of knowledge or process, and training became a key element. It was increasingly obvious that certain basic skill sets and experience had to be in place before police forces and other authorities could produce forensic work acceptable to a court. All of this naturally evolved at different rates throughout the UK until 'centres of excellence' emerged in different areas.

Principles of computer-based evidence

It became clear that there was a need for a simple set of rules which could be followed to ensure uniformity, integrity and repeatability. As a result the Association of Chief Police Officers (ACPO) commissioned the production of a guide to be written and produced for all Hi-Tech Crime Units which handle digital evidence. The ACPO Good Practice Guide contains four 'Principles of Computer Based Electronic Evidence' designed to cover all computer-based evidence, including eDisclosure cases.

Principle 1: No action taken should change data held on a computer or storage media, which may subsequently be relied upon in court.

This requirement is less straightforward than may appear. The integrity of digital evidence is easily compromised if it is handled incorrectly, so specialist hardware, software, training and experience all need to be used to ensure that evidence is correctly captured in the first place. Even the simple act of powering up or shutting down a machine causes changes to be made to many files on a computer's hard drive. Copying emails or Word documents to a CD can cause the loss of or change to extremely important metadata, but the implications of mishandling electronic evidence are not obvious because these changes go on behind the scenes and thus do not appear in printed copies of the documents.

An enthusiastic IT department can innocently make damaging changes whilst they diligently look for relevant information in a litigation case, deleting or changing vital information. Such changes may also not be so innocent, as altering electronic documents and their accompanying metadata is easily achieved deliberately by people with malicious intent. It may be then necessary to prove that changes were accidental in the face of an opponent's suggestions to the contrary.

The ultimate solution is to make an exact 'mirror image' of the media (e.g. hard drives) because it maintains the integrity of any evidence which may later be relied upon. This includes data that has actually been deleted (yes, beyond the Recycle Bin), another potentially significant benefit.

To ensure that the data on the mirror image is not altered in any way during the imaging process, hardware known as a 'write blocking' device is used. An integrity check is made to verify that the original hard drive and mirror image hard drive are exactly the same. Once a mirror image has been made it is effectively a preserved snapshot, frozen in time.

You cannot assume that your clients will know about or have the in-house ability to cope with these procedures. Generally, even technically-skilled IT departments do not necessarily have the tools or knowledge required to perform the operations described above.

Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or on storage media, the person must be competent to do so and able to give evidence explaining the relevance and the implications of their actions.

In many eDisclosure cases these circumstances are likely to be the rule rather than the exception, as documents will be collected from live, running servers that need to remain continually operational in a business setting. To achieve this requires a higher level of skill both in terms of the exercise itself and the evidence needed to prove the condition of the data at the moment of collection, since that will have changed minutes later and the original will not be available for inspection.

Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

This principle is of paramount importance, and is only workable if standardised best practices for evidence collection and analysis procedures are agreed upon and strictly adhered to. It is probable that this does not currently happen in the majority of eDisclosure cases.

The final principle is fairly self-explanatory:

Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Expense proportionate to the problem

Inevitably, a proper collection of data involves some expense, but if electronic evidence is not correctly handled at the outset, the potential for future disputes exists. It is possible that the entire case is inherently flawed from then onwards. The failure to follow evidentially sound guidelines could therefore prove to be a false economy, particularly where the lawyers on the other side have the skills and knowledge to challenge the basis on which collection was made. Judges will have to learn to discriminate between points which are genuinely made and those whose purpose is purely tactical.

With a thorough understanding of best practice, and what can be achieved with digital forensics, eDisclosure and many other types of cases could take very different twists.

Examples of what digital forensic experts are able to do using a robustly-documented, evidentially sound process include:

- Calling on many types of data as evidence, including calendar files, web sites visited, search engine phrases used, instant messenger logs, images, audio files, and malicious software as well as more conventional things like emails, spreadsheets and word processing documents
- Fraudulent document alteration detection (e.g. metadata edits)
- Recovery of deliberately (or otherwise) deleted documents
- Finding evidence of attempts (successful or unsuccessful) to permanently erase or 'scrub' data from hard drives
- Using evidence from additional, commonly used devices holding communications data such as mobile phones.

An everyday scenario

A scenario for a solicitor to ponder: A client calls about a new matter, telling you that he is clear as to what must be collected, that he has found everything relevant and is about to set his very capable IT team to copy off the data to a hard disk. He is not really asking for your view, just telling you what he plans to do to get you the documents to advise on.

There are many cases in which this is entirely the right thing to do. Indeed, many cases can be dealt with without any reliance on electronic data at all and printing or copying a few documents may be the best and most proportionate course. The next level up from that is where the custodians (the people in whose care the documents are) are few, the date range limited and a sensible filing system (e.g. by e-mail and document folders) exists and is used. In such circumstances, it might be entirely right to get the IT department simply to make copies, subject to the proviso that the case is one in which no question is likely to arise as to the condition, the authenticity or the genuineness of the documents. Many straightforward commercial cases are like this.

At the opposite extreme, imagine a scenario in which the relevant custodians are both numerous and uncertain, where the documents are scattered at random throughout their mail systems and across the network, and where there are or might be unconventional data sources such as BlackBerries, instant messaging, and home computers, C:\ drives and other sources which were not necessarily subject to network control or even readily identified. Add the possibility that relevant information is in large databases such as HR systems, accounts systems or other large resources which are not readily copied and which contain much information which has no bearing on the case at all. Now add in another factor - that the case may be one which involves activity which will not necessarily be obvious and which is not susceptible to conventional collection methods. These may include web pages visited

by an employee, deleted files or file fragments, or evidence that an external device such as a USB drive has been connected to a computer.

These factors raise issues regardless of volume. Once you add the other element that the outer selection of data (that is, the maximum scope of the collection from which the disclosable documents will come) is very large, then some pause for thought is needed. Lastly, consider the points made above about the way in which data may be damaged and lose its authenticity or value as evidence if it is not collected properly.

You do not need to find all these elements at once to stand back a little before encouraging the clients to set their IT department to work on the collection. Any one of them is enough to warrant the engagement of an expert. Quite apart from anything else, you may find that the costs of making a collection in this way are in fact no greater, in real terms, than having your IT department do it, particularly when you consider the downstream costs of sorting out what has been collected. You may find that the true expense of a professional (and possibly a forensic) collection are no greater than would be incurred by self help.

How much do you need to know?

A lawyer assimilates a great deal of information in the early days (and sometimes the early hours) of a new case. The immediate focus will be on what the issues are likely to be, what must be proved in relation to them, and what categories of material are likely to be disclosable or, if not necessarily disclosable, will be at least prudent to capture.

It is necessary to identify what sort of case this is for the reasons given above - some cases will require a proper forensic collection and some will not; some will raise problems, if only of sheer volume, which do not arise in other cases. The lawyer needs to be alert to what might have been done, and what it is possible to achieve by a professional collection.



He/She also needs some idea of what the relative costs are or, at least, how to estimate them.

There is a further reason for acquiring these skills. It is not enough merely to be able to collect your own clients' data in a defensible and cost effective manner. One needs also to be able to challenge opponents who have not collected their data properly in circumstances where it matters. Examples might include messages, documents or calendar entries purportedly proving a meeting which were not created on the right date or by the right person, or data which you have which draws attention to data which has not been provided by the other side. The point is not to incite a US-style battle over immaterial technical points but to enable challenges to evidence which, if unchallenged, may lose the case.

Digital forensics is in part a physical thing - you can see what is being done and, whilst the lawyer may not need to understand the full implications of the hardware, software and skills being applied to the job, it is easy to envisage what is involved if you actually see it happening. It lends itself to demonstrations which, once seen, make it easier to get your mind around what is likely to be involved in any case which may turn up tomorrow.

It makes sense, therefore, to invite a forensic collection expert to come and demonstrate what is involved. The opportunity can be taken at the same time to discuss, at least in principle, what the costs are likely to be of broad classes of cases. You can also discuss the terms and conditions upon which the forensic collections company takes on engagements - these are unlikely to cause difficulty, but it is something you can do without having to consider at the moment when an urgent problem arises. Lastly, you can get to know the people - it is much easier to ring up someone you know rather than to search a directory in a hurry.

All this amounts to preparation for reactive scenarios, that is, putting you in a position to respond quickly and proportionately when a new case comes in. There are strong arguments going one step further and using your relationship with an eDisclosure and collections company to promote your litigation business, whether by making a joint presentation or merely by being able to describe on a beauty parade what process would be followed in certain situations, and who the players will be.

This moves the discussion about digital forensics away from mere mechanics and into risk management and practice development.

The primary purpose of such a relationship is, however, reactive and defensive - reactive for the reasons given above, defensive for the obvious reason that if you foul up this, the very beginning stage of a litigation matter, it is unlikely that you will set it right again without major expense for the solicitor. In *Hedrich v Standard Bank London*¹, the downside for the solicitor of not understanding his own client's data, and the deficiencies in it, was having to face a wasted costs application which was beaten off only in the Court of Appeal. For the defendants in *Earles v Barclays Bank*², the downside of not being able to produce documents was an extended trial, a missed opportunity for summary disposal, and a severe reduction in the costs recovered from the losing side. Whilst these cases may appear to be extreme ones, they are similar in potential to everyday cases of all sizes. A modest amount of learning and an alliance with a litigation support and forensics collections company such as 7Safe seems a worthwhile investment.

About 7Safe

7Safe and its employees have collectively been involved with civil litigation, regulatory and criminal cases since the mid-nineties. For the past five years, 7Safe's focus has been on digital evidence, how to preserve and interpret digital evidence and how to present the findings. The computer forensic industry has moved over the last decade from being primarily a government and law enforcement activity to being a concern of the legal and commercial sector. 7Safe has been at the forefront of this evolution, building one of the largest commercial digital forensics teams in Europe, dealing with high-profile court cases as expert witnesses and, more recently over the past two years, growing into the electronic disclosure market place with an approach that is both forensic and proportionate.

About the authors

Dr. James Kent is Director of eDiscovery services at 7Safe. A former hi-tech crime unit detective, Jim utilises his expertise in the field of electronic legal evidence to ensure delivery of a highly efficient and effective end to end solution. One of the UK's leading computer forensics analysts, Jim is a leading pioneer in the area of 'intrusion forensics': a recent development which allows investigators to analyse data in its operational environment. He is also a registered expert witness and is UK Government security cleared to SC level.

Chris Dale qualified as an English solicitor in 1980 after reading History at Oxford. He was a litigation partner in London and then a litigation software developer and litigation support consultant before turning to commentary on electronic disclosure / discovery. He runs the e-Disclosure Information Project which disseminates information about the court rules, the problems, and the technology to lawyers and their clients, to judges, and to suppliers. He writes an objective web site and blog on the subject and is a well-known speaker and commentator in the UK, the US and other common law jurisdictions.

Footnotes:

1. Earles v Barclays Bank Plc [2009] EWHC 2500 (Mercantile) (08 October 2009)
2. Hedrich & Anor v Standard Bank London Ltd [2007] EWHC 1656 (QB) (25 June 2007)