

# Silent witnesses: the rise of computer forensics

In a business environment increasingly dominated by the use of technology, **Anthony Riem** and **Andrew Gilliland** examine how computer imaging orders can change the nature of commercial disputes by retrieving crucial evidence long after users think it has been deleted

AS THE USE OF TECHNOLOGY IN THE corporate world has grown in recent years, the importance of evidence obtained from computers for use in litigation has also increased. This article uses three recent cases in which PCB Litigation has been involved to look at the strategic uses of computer imaging orders to achieve a successful outcome in commercial disputes.

In particular, this article will concentrate on how the use of computer imaging orders in each of the three following scenarios can lead to an early and successful conclusion to a dispute:

- 1) computer imaging orders obtained as part of search and seizure orders to reveal a hidden bank account;
- 2) specific disclosure of images of a computer to establish the forgery of a key document; and
- 3) obtaining computer imaging orders when new evidence comes to light at a late stage in the run-up to trial to establish a smoking gun.

## SEARCH ORDERS AND THE HIDDEN BANK ACCOUNT

A search order is a key component in the arsenal of a litigator seeking to trace the assets of a fraudster. It is an order – made on a without notice application and requiring the permission of the court



By **Anthony Riem**, partner, and **Andrew Gilliland**, solicitor, international fraud and commercial litigation, PCB Litigation LLP

– for certain representatives of the claimant, and an independent supervising solicitor, to enter premises for the purposes of searching them and removing articles and documents. This occurs before the defendant has had an opportunity to put their side of the case to the court and in circumstances which could cause serious damage to their reputation. In *Bank Mellat v Nikpour*, Donaldson LJ described it as being one of the law's two nuclear weapons (the other being what is now called a freezing order).

Three of the pre-conditions that are required for the making of a search order are set out in *Anton Pillar KG v Manufacturing Processes Ltd*:

- 1) there must be 'an extremely strong prima facie case';
- 2) the potential or actual damage to the applicant must be 'very serious'; and
- 3) there must be clear evidence that the defendants are in possession of incriminating documents or other items and that there is a real possibility that the defendants may destroy such documents before any inter partes application can be made.

The Staughton Committee – which was set up by the Lord Chancellor's department to look into search order

relief – reported in 1992, adding a fourth pre-condition:

'The harm likely to be caused by the execution of the *Anton Piller* order to the respondent and his business affairs must not be excessive or out of proportion to the legitimate object of the order.'

In recent years the need to include computers and other electronic devices in any search order has become increasingly important. Computers are often the most fruitful source of incriminating evidence against the defendant, especially if the defendant thinks that they may have deleted the incriminating evidence from the computer. This demonstrates the importance of ensuring that a computer forensics expert is part of the team enforcing the search order.

Computer forensics experts are more than capable of recovering data from a hard drive of a computer long after the user thinks that they have deleted it. Therefore it is important to ensure that any search order allows for a computer expert to take an image of the hard drive of any computer found in the search. An image of the hard drive is a forensic copy of every piece of data contained on the computer. This allows the images to be inspected at a later date. The same can be done for any personal digital assistants

(PDAs), mobile phones or any other form of electronic data storage device that may be found on the premises.

The importance of using a trained expert was recently demonstrated in the case of *Aston v Rusal*, where spyware was installed on the computer system of the claimant, allegedly for the purpose of committing net espionage. The electronic evidence supported the claimant's assertion that the Russian defendant had placed the spyware on the system, and accordingly the claimant was able to bring proceedings in England. However, it should be noted that one of the features of the case was that the claimant had used its own computer technicians rather than computer forensics experts to carry out the initial investigation and this could have led to the destruction of valuable evidence.

The aim of a search order is to prevent a defendant from destroying incriminating evidence regarding the commission of the fraud and the concealment of its proceeds. The hope is to obtain sufficiently strong evidence (that would otherwise have been destroyed) to secure an early settlement on favourable terms.

In one case, PCB represented a leading casino in proceedings against a wealthy individual who owed it a substantial amount of money. First, a worldwide freezing order was obtained on behalf of the client, freezing all of the defendant's assets worldwide, up to the amount owed (together with an order requiring him to deliver up his passports). In his disclosure – provided in accordance with the freezing order – the defendant claimed to have almost no assets of any value. This caused the claimant great suspicion as the defendant was known to frequent casinos throughout the world and to live a lavish lifestyle.

In these circumstances, two applications were made to the High Court. One application was made on notice to the defendant for an order that he be cross-examined on his disclosure. The other application was made without notice to the defendant for a search order to include a provision that an image be taken of the hard drive of the defendant's computer. The orders were granted and the information obtained from the defendant and the evidence

obtained from the defendant's computer led to the claimant locating an additional bank account that the defendant had not previously disclosed in accordance with the freezing order.

Evidence gathered during the course of the search order was then used during the cross-examination and the Court ruled that the defendant had not given full disclosure. The pressure brought on the defendant and the danger of the defendant being found in contempt and possibly sent to prison led to the defendant settling the claim, thereby saving the costs of the proceedings continuing and going to trial.

#### SPECIFIC DISCLOSURE AND THE FORGED LETTER OF ADVICE

Rule 31.4 of the Civil Procedure Rules defines a document as follows:

'... "document" means anything in which information of any description is recorded; and "copy", in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly.'

A computer database is clearly potentially discloseable. This is supported by *Derby & Co Ltd v Weldon (No 9)*, where a computer database was found to be a 'document' for the purposes of rule 31.4. Since a database contains information capable of being retrieved and converted into readable form, it is therefore susceptible to disclosure. Indeed the disclosure statement served with a list of documents now requires all parties to confirm what searches have been carried out with regard to locating relevant electronic documents, including searches of computer databases.

If a party to the litigation is unhappy with the disclosure of electronic documents provided, they can seek an order for specific disclosure. If they feel that relevant documents may be located by a forensic inspection of the opposing party's computers, this can be in the form of a computer imaging order. If such an order is made it will enable a computer forensics expert to take an image of a computer and, in many cases, may allow them to recover deleted

'The aim of a search order is to prevent a defendant from destroying incriminating evidence regarding the commission of the fraud and the concealment of its proceeds.'

e-mails or other hidden data which the computer user is completely unaware of, for example, information embedded in a computer file or cached to disk about the sequence of access and editing of a document, when and by whom. The order may lead to the production of strong evidence and successful, early conclusion to the litigation.

The following case study demonstrates how obtaining a computer hard drive through specific disclosure can shorten the litigation process and produce a successful result for the client.

PCB was instructed by a client whose former solicitors had sent a letter before action seeking to recover unpaid fees relating to work carried out in an earlier litigation. The client objected to paying the fees and wished to recover damages against the solicitors on the basis that they had been negligent in the previous proceedings. Documents were requested from the solicitors in order to be able to respond to the letter before action. Amongst the documents supplied was a letter of advice purportedly sent by the solicitors to the client. The letter was suspicious in that it conveniently addressed all the allegations of negligence set out in previous inter-solicitor correspondence.

On further consideration, it was apparent that the letter before action was inconsistent with subsequent

>

‘Obtaining a computer hard drive through specific disclosure can shorten the litigation process and produce a successful result for the client.’

correspondence. In particular, the client had previously made complaints about the advice he had received and, in the responses from the former solicitors, no reference was ever made to the advice given in the suspect letter. In addition, there was no reference in the solicitors’ bill narratives to the drafting of the suspect letter. Finally, the client had no recollection of having seen the suspect letter before.

A letter was therefore written to the former solicitors requesting that a computer forensics expert be permitted to take a forensic image of the relevant computer and for undertakings to preserve the evidence in the meantime. The solicitor refused to allow access or provide the requested undertakings. Instead the solicitors purported to rely on computer printouts to show that the suspect letter was created on the date on which the solicitors claimed it was created.

In answer to this, a computer forensics expert was commissioned to prepare a report on the reliability of such printouts. The report stated that the dates on such printouts could be altered by adjusting the computer’s clock and were therefore of no evidential value.

Proceedings were issued by the former solicitors for payment of the fees and the client counterclaimed for negligence. An application was made in

these proceedings for specific disclosure of the hard drive of the computer on which the suspect letter was drafted. The draft order included undertakings to be given by the computer forensics expert to prevent disclosure of confidential and privileged information contained on the computer.

Despite vigorous opposition to the application, the court ordered specific disclosure of the hard drive. When the computer forensics expert inspected the computer, he was unable to find a copy of the suspect letter in the directory in which (according to the printouts previously disclosed by the solicitors) it should have been located. Instead a copy was found in unallocated space on the computer. The solicitors claimed that they were unable to explain how this had occurred.

On the basis of the expert’s preliminary report, PCB sought the court’s permission to rely upon expert evidence and directions for:

- the solicitors to explain precisely what had happened to the electronic copy of the suspect letter and the hard drive and any other media on which it has been stored, including the provision of certain disclosure; and
- the exchange of expert reports.

The solicitors argued that they should not have to provide witness evidence until they had seen the final report of the expert. Nevertheless, the court ordered that witness evidence should be provided. The solicitors served a witness statement which disclosed for the first time that there was a diskette on which the suspect letter had been saved.

Following service of the witness statement, the expert finalised his report which, in summary, stated the following:

- 1) There are a set of rules as to the order of the date and time data contained within documents, provided the computer clock is not altered.
- 2) These rules were breached on both the computer on which the suspect letter was drafted and on the diskette.

- 3) The date and time data was consistent with the suspect letter being created six months after the solicitors claimed it had been created and the computer clock backdated to falsify records as to when the suspect letter was created.
- 4) The suspect letter was found in unallocated space on the computer. This was consistent with an attempt having been made to delete it.
- 5) Deletion software was run on the computer the evening before the inspection of the hard drive.

The difficulty facing the client was that, even absented the suspect letter, the solicitors were on balance likely to succeed in defending the negligence claims. It was therefore decided to take the unconventional step of seeking summary judgment on the issue of whether the suspect letter was a forgery.

Although the issue of whether the suspect letter was a forgery would not itself be determinative of the proceedings, the (successful) argument was that the matter should be resolved before trial. As it was likely that substantial parts of the solicitors’ claims for fees and defence to the negligence claim would be struck out, a fair trial would no longer be possible. In support of this there was evidence of other concerns about the authenticity of certain handwritten notes, as well as the evidence of the destruction of the electronic evidence.

By the end of the first day of the summary judgment hearing, it was apparent that the judge was, as a result of the expert’s report and other circumstantial evidence presented on behalf of the client, very receptive to the allegations of forgery and the consequent attempt to destroy the evidence. This led to the firm agreeing to drop its fees claim and pay a substantial proportion of the client’s costs and damages claim before the summary judgment hearing resumed.

#### COMPUTER IMAGING ORDERS AND THE SMOKING GUN

Even with trial approaching, it is possible to obtain evidence through a computer imaging order that may give you the tactical edge at trial. Shortly before trial

*Bank Mellat v Nikpour* [1985] FSR 87

*Anton Pillar KG v Manufacturing Processes Ltd* [1976] Ch 55

*Aston v Rusal* [2006] EWHC 2545 (Comm)

*Derby & Co Ltd v Weldon (No 9)* [1991] 2 All ER 901

*L v L & H* [2007] EWHC 140 QB

the claimant provided supplemental disclosure of documents obtained from its Moscow office and informed the client that there were a further two suitcases of documents which they did not consider relevant, but were also available for inspection. Three days were spent reviewing the documents and a 'smoking gun' document was discovered, namely a draft of an agreement which cut across the central plank of the claimant's case.

During cross-examination at trial, the claimant's finance director referred to having looked at the draft agreement on his laptop. An application was therefore made to the trial judge for a hybrid computer imaging/search order. The order provided for the defendant's computer expert to take images of the claimant's laptops and the server to which they were backed up, under the supervision of an independent supervising solicitor.

The court further ordered that the claimant's solicitor and leading counsel were to review and to disclose any electronic versions of the draft agreement. This resulted in the disclosure of numerous versions of the draft agreement together with other documents which had not been previously disclosed. Shortly after this episode, the claimant agreed to settle the claim on confidential terms.

#### CONCLUSION

The use of computer imaging orders is a vital tool for the astute litigator. Computers hold a huge amount of evidence which can be used strategically to lead to the early settlement of disputes. However, it is important to ensure that all the correct steps are followed. A party must ensure that the necessary orders are obtained from the court.

In the recent case of *L v L & H*, computer images of a husband's laptop were obtained by his wife in relation to divorce proceedings. Although she used a computer forensics expert, she did not seek the appropriate court orders and the images had to be delivered up to the husband. Further, she may well have committed criminal offences by breaching the Computer Misuse Act 1990 and the Data Protection Act 1998. It is therefore important to ensure that the right team of lawyers and forensics experts is in place when handling electronic data to ensure that all possible evidence is obtained. **IHL**

*By Anthony Riem, partner, and Andrew Gilliland, solicitor, international fraud and commercial litigation, PCB Litigation LLP.*

*E-mail: [ajr@pcblitigation.com](mailto:ajr@pcblitigation.com),  
[arg@pcblitigation.com](mailto:arg@pcblitigation.com).*

*Tel: 020 7831 2691.  
[www.pcblitigation.com](http://www.pcblitigation.com).*