ARTICLE:

AN INVESTIGATOR'S APPROACH TO DIGITAL EVIDENCE

By **Paul Lund**

For investigators acting in the State or the private sector, the gathering of digital evidence occupies a steadily increasing proportion of work. A principal and growing problem lies in the volume of material obtained, and then extracting what is considered to be relevant. This article will briefly outline the approach that Bishop International takes to digital data to advance the enquiries made during the course of an investigation. It is anticipated that the reader will acknowledge that client confidentiality is paramount in such matters. Many of the investigations lead to the settlement of a case before litigation is considered and others become a matter for law enforcement. It is for those reasons that none of the examples given in this article is in the public domain. Nevertheless, the examples have occurred, and will continue to occur, and the anonymity afforded to the examples does not detract from their relevance.

It is normal for digital material to be recovered as part of almost every investigation. For purposes of this article, it is presumed that the client has given their written consent to enable the investigator to obtain access to the relevant systems, that the imaging has been correctly completed, that an audit trail is preserved and that the evidence will be admissible. Regardless of whether the potential litigation as the result of an investigation will be civil proceedings or a complaint to the police, the aim is to gather the evidence to satisfy criminal standards of admissibility. Material will be gathered from all those sources that can be viewed, and the data will then be formatted to allow searches to take place. The re-formatting always takes place with a copy of the copy.

Before examining a number of examples, there are some preliminary points to consider. First, there is the issue of the timing of the investigation. The longer it takes to locate the relevant hardware and take an image of the stored information, the greater the risk of sabotage by the suspects or their accomplices. For portable devices, ensuring there is a record of custody and anyone that might have access can be vital. For example, when laptops are re-assigned to a new user within an organization, the preservation of the original hard drive will secure material for the future. This is, for instance, particularly important when an employee leaves a company.

Second, an investigation often exposes flaws in existing procedures. Digital forensic investigations are no exception. No system is perfect. Anyone with expertise and access to a system or hardware will be able to exploit them if they so choose. However, when a digital forensic investigation takes place, it becomes an ideal opportunity to conduct a security audit to prevent any further exploitation.

Investigations inevitably include a thorough trawl of international databases and the internet. It has been suggested by some commentators that anyone can obtain access to such material. However, a comprehensive understanding of search techniques is as important as an understanding of the investigation's objectives. The results of professional searches are likely to identify additional potential sources of information. Such work will generally have a direct bearing on the later interrogation of the digital data that is recovered.

The contractors had unimpeded access to the entire system with the ultimate result that the new system was manipulated by the alleged fraudster, allowing fraudulent orders to be issued at the expense of the client.

Evidence of bribes from a supplier

The first case involved a senior manager in one of Britain's largest companies. He approved very significant contracts for services to the company. He was suspected (via a whistleblower) of receiving bribes. The purpose of the investigation was to provide evidence of sufficient quality to justify his dismissal and the withholding of his pension and share-incentive scheme. The suspect had the use of a company laptop, but the client took the view that he rarely used it. Nevertheless, the client was persuaded of its potential value as a source of evidence. An image of the hard drive was taken, and the data searched using key words selected from the results of the traditional form of enquiries.

A range of useful material was found, and the most striking document was a letter from a marine surveyor valuing a £500,000 yacht. It was addressed to the suspect at his home address. Interposed between his name and his address at the head of the letter was the name of a sub-contractor who had benefitted from a series of lucrative contracts commissioned by the suspect. This evidence was put to the sub-contractor who confessed his involvement. As a result, the company felt sufficiently confident in the results of the investigation to report the matter to the police.

Substantial breach of contract

In the second case, an international trading business was threatened by a mass resignation of important members of staff, apparently intent on moving to a competitor. Under extreme pressure of time, evidence was required to support applications to the courts for injunctions without notice to the other party in several jurisdictions. Images were taken of many gigabytes of data from servers, mainframes, laptops and organizers around the world. Predictably, nothing so obvious as letters of intent or contract terms were found – the sensitivities of both sides were well known. Random searches would have been too slow, too expensive and offered limited prospects of success.

As in the first example, investigations of a traditional nature helped to identify the relevant search terms for the digital data. Investigators were put in place and briefed. Potential sources of information were identified, particularly previous employees of both businesses. The patterns of behaviour of the most important members of staff had been researched. Interviews were conducted with confidential sources, which enabled targeted searches to be conducted on the data retrieved. The results enabled the client to resume control of the situation and to resolve the matter on his terms.

Manipulating data for fraudulent purposes

A third case demonstrates the risks inherent when technology is employed without adequate security controls. The client engaged contractors to modernize its computer-controlled commissioning and delivery processes. The contractors had unimpeded access to the entire system with the ultimate result that the new system was manipulated by the alleged fraudster, allowing fraudulent orders to be issued at the expense of the client.

To explain more fully: the system allowed the assembly of finished products from the inventory of components. At the start of assembly each item carried a unique identity. Once the product was assembled, the system was meant to initiate and monitor delivery to the customer. However, certain mistakes in making entries on the system would cause the order to be placed in an error file, effectively losing it from the system, since the error file went unchecked.

The alleged fraudster entered the system using enhanced access and administration rights and placed orders for assembly. However, once the order was

processed beyond a point that it could not be cancelled, but before the goods were uniquely identified, the fraudster was able to manipulate the system. He caused the order to be classed as an error and effectively go unrecorded. Thereafter, in the absence of notification to the assembly shop, the order could be made to proceed to despatch without an identity. The items left the factory despite a security procedure that required all products to be cleared at the gate before leaving the factory. The fraudster was well aware of weaknesses in the security procedures.

The client identified a suspect based on his unusually high level of access to the system and his supervisory role in the plant. Research identified that, without the company's knowledge, the suspect had established a haulage business and a wholesale operation selling goods similar to those that were missing. Using traditional investigative techniques, dockets were traced to shipping manifests overseas. Specifications on those dockets could potentially match missing stock. The suspect had positioned himself within the company as the informal point of contact for solving problems between the manufacturing process and the IT system. He had established close ties to a number of members of staff in the IT department who, it was later discovered, had given him unwarranted and extended access to the system, enabling him to manipulate the data and conceal the changes.

When a discrepancy was eventually uncovered, the company, in its innocence, made sure that the still highly-regarded suspect was actually one of the first people to be made aware of it. He responded by offering a complicated explanation of how the system had malfunctioned. At the same time he also took steps to delete any incriminating evidence from his personal computer and laptops.

By the time the thefts had been confirmed and the investigation had begun, the suspect had left the company and his laptops had been reissued to other members of staff. The IT department was requested to find the original laptops, but despite several being provided, the correct machine was not found. Whether this was a result of incompetence or collusion with the suspect remains uncertain. In either event, allowing the recovery of the machines to be controlled by an internal team in a piecemeal fashion frustrated the process and may have allowed vital evidence to be lost.

The good news was that a secondary laptop was recovered, and despite extensive cleansing of data, it was possible to extract important evidence. The report, which included both the digital forensic work and parallel lines of inquiry, was ultimately presented to the police, a prima facie case having been established. Meanwhile the flaws in the system were addressed and rectified. Improved audit procedures were initiated to monitor the flow of orders and components to the assembly shop and off the site more precisely. In addition, all devices and the people to whom the devices had been allocated began to be rigorously logged.

Conclusion: an integrated approach

The factor that unites the three examples in this article is the need to provide a focus to any forensic examination of digital information, and to integrate it with more traditional forms of investigation to enable digital evidence to be searched effectively. Material that is recovered increases in volume exponentially. As the proportion of irrelevant material increases, so do the chances of missing relevant evidence if investigators have failed to follow traditional investigative methods, such as researching the background and speaking to appropriate employees and others who have relevant information.

Paul Lund is the Director of Corporate Investigations for Bishop International Limited. A solicitor, he has served as a Director of Compliance, and as a prosecutor for the Serious Fraud Office. Since joining Bishop International, he has supervised investigations of fraud and corruption for European and American banks and corporations.

http://www.bishop-group.com

