Digital forensics in a liquidator's investigation

David Ingram and Carmel King follow up their previous article by considering the tools available to us when interrogating electronic evidence

DAVID INGRAM
Insolvency practitioner,
Grant Thornton UK LLP, London

CARMEL KING
Advisory,
Grant Thornton UK LLP, London

In the Summer 2014 edition of Eurofenix, we considered the importance of the golden hour, that is how the first actions taken by a liquidator can dictate the outcome of the case, particularly where fraud is suspected, and the risk of asset dissipation and missing company records is high.

We looked at the initial information gathering phase, which involved the assessment of various threats and the identification, securing and collection of evidence. We will now consider the tools available to us when interrogating electronic evidence. These can be used to reduce costs and improve efficiency, contributing significantly to a meaningful investigation and the development of a strategy that will result in the recovery of misappropriated assets for the benefit of creditors.

Size matters

The electronic records uplifted from the company are likely to be very substantial in size. How big is a gigabyte? Say, for example, that the data from the email servers, file servers, the cloud and various data sources such as usb memory drives, laptops, company mobile phones and tablets of a company in liquidation amounts to 210GB. This could be as much as 580,000 Word documents, plus 139,000 Excel documents, 4 million emails, 26,000 PowerPoint presentations and 46,000 images. When we consider the storage capacity of various electronic items, 210GB is a very modest estimate. It is not unusual for laptops to have 1 terabyte hard drives, my mobile phone has a 16GB capacity, the usb memory drives on my desk each have a 4GB capacity. Such an overwhelming amount of data is likely to give even the most determined (or deep-pocketed) liquidator pause for thought. By combining your knowledge of the case with the skills of a digital forensics team to process, analyse and review the data, the liquidator can approach this volume in a sensible way.

The digital forensics team will provide the liquidator with the essential details he needs to start the process. They should report the valuable information – the volume, file types, languages and size of the data. Essentially, they should communicate the time and cost required to process the data for the liquidator.

Culling and analysing the data

It is at this stage that the liquidator's steer is required to process and cull the electronic records, in order to reduce them to a manageable size for review. Culling the data in a methodical way will result in a reduced review, which reduces cost and improves efficiency. It is essential to be aware of the various methods available to the liquidator, this is a more sophisticated exercise than a basic keyword search. Some simple processing, for example the application of a date filter to the records can, in our example, reduce 210GB right down to 80GB. The liquidator's case knowledge will be required to identify the relevant dates. A de-duplication of the data held could further reduce this down to 18GB. This volume is likely to be unwieldy, still too much to manually review in any efficient way. Fortunately further tools are at the liquidator's disposal for an intelligent review of the company records.

When a computer program requires memory from a computer system, it is allocated in clusters. The clusters allocated are sometimes larger than is required, and the excess allocated memory is known as slack space. Slack space is another storage area that can be interrogated by the digital forensics team, which can hold information such as data dumped

when a file is closed at the end of a work session. This can be particularly useful when the liquidator suspects fraud, and there is every chance that those involved made efforts to avoid saving documents to their system. In a recent case, we suspected that a fraudster was using one or more web-based email accounts to avoid conducting his illegitimate business using the company email server. We identified partial pages for web-based email accounts in the slack space, the contents of which confirmed our suspicion, and enabled us to identify a number of web-based email addresses used by the fraudster.

Similar to slack space is unallocated space. We should all by now be familiar with the concept that deleted items don't disappear entirely. This applies to digital material stored on a system as well as that shared online. When we delete a file, it is not entirely removed, but the allocated cluster is classified as available for reallocation. Accordingly, prior to being overwritten the unallocated space can be host to a wealth of deleted files or data which may be of interest.

Part of the liquidator's strategy should be a methodical interrogation of the slack space and unallocated space, in addition to the live digital materials delivered up. This may seem the opposite of culling the data, however the liquidator will ignore the depositories of deleted or less-obvious materials at his peril. Keyword searches have become very sophisticated, and are infinitely preferable and more useful than trawling through vast amounts of data. Some examples of the smarter types of keyword searches include:

- **Proximity searches:** Allowing for keywords within a set distance of each other. Useful for example where parties of interest use middle or family names on occasion, and all variations must be considered.
- **Boolean searches:** Combining keywords with instructions such as AND, OR, NOT in order to produce more relevant results.
- **Fuzzy searches:** Allowing for minor variations in the keywords to produce a match. Useful for overcoming variations in spelling or spelling errors.
- **Wildcard searches:** Using * and ? to search for words containing a certain combination of characters, as determined by the person setting the search parameters.

Other types of searches will be able to automatically identify such things as email addresses, telephone numbers, locations and currencies. Using these instruments, in our example the liquidator has culled the relevant digital material down to 7GB, which, with the application of his practical knowledge of the liquidation, is a manageable amount for review purposes.

A timeline analysis can be constructed using the metadata stored in the digital material, and is a good technique for structuring the material in an accessible, chronological order. The

> A DIGITAL FORENSICS TEAM WON'T WORK FOR FREE, ANY MORE THAN THE LIQUIDATOR IS LIKELY TO

> WE SHOULD ALL BY NOW BE FAMILIAR WITH THE CONCEPT THAT DELETED ITEMS DON'T DISAPPEAR ENTIRELY

Share your views!

metadata provides information about various aspects of the digital material. For example, the time and date of creation, the identity of the author, details of changes to the material, and in some instances the applicable geographical location where the material was created, sent, received etc. The metadata is essentially an electronic audit history of digital material. The liquidator accordingly can identify when files were created, accessed and modified; he can assess various users' access to certain accounts and browser usage, downloads and usb memory drive usage.

The application of a timeline analysis to the liquidator's knowledge of the operation of the company can be very powerful. How do the director's daily usage patterns compare to his own account of his daily routine, his role and responsibilities? Who accessed the company's online banking facility at the time of a suspicious payment out? Where hard copies of correspondence were not retained by the company, do the date stamps on the electronic copies fit with the estimated date of postage, or have the documents been modified since?

Other tools that the liquidator will have readily available when reviewing the digital material should include the ability to sort and filter the material, to tag or categorise items, to add comments, highlight sections of the material or redact as required. This will be provided by the digital forensics team using an appropriate e-discovery platform. The more commonly-used platforms have a web interface, which not only enables the liquidator to carry out his review from his preferred location in the event the digital forensics team is not in-house, but it will also allow the liquidator to share the digital material with his legal advisors in consideration of litigation.

Cost

Cost, of course, is a major factor. Industry articles refer to digital forensics as a billion-dollar sector with huge potential for growth and expansion. A digital forensics team won't work for free, any more than the liquidator is likely to. There are obvious considerations to be made prior to embarking upon a potentially costly digital forensic review exercise, such as budget and proportionality of work carried out in relation to the size of company or complexity of the case.

It is important to appreciate however, that whilst it may seem an extravagance to instruct a digital forensics team, a meaningful interrogation of the electronic materials is increasingly unlikely to be possible without some employment of the tools available. It doesn't have to be extortionate. Smaller tools for use by the liquidator without the need to instruct a digital forensics team can be purchased online, along with training, support and upgrades.

A digital forensics team can use automation of processes where possible in order to control costs. It can be more cost-effective: a colleague has advised just today that our digital forensic team was able to extract data (with time-stamps stored in the metadata) to a spread sheet in a very short period of time and at reasonable cost, when the same exercise conducted manually would have been cumbersome, complicated and costly. Our colleague has also managed to practically eliminate the risk of human error, and as we know, where significant data is overlooked it can be a costly mistake to make.

Conclusion

Our lives are increasingly lived electronically, and the same can be said for the majority of companies. We email rather than write letters or make telephone calls, spread sheets have replaced ledgers, we strive for paperless offices in place of shelves full of files. This is probably the most significant change in workplace life in recent years. Liquidators are going to need to be familiar with the tools available to them in order to conduct a successful investigation, pursue fraudsters and recover company property for the benefit of creditors. ■