

# Computer forensics and litigation support

## What is computer forensics?

We all know that computers and other electronic devices are capable of storing and retrieving vast quantities of data, cheaply and reliably. What is less well known is that, as a consequence of this ability, they are correspondingly inefficient at deleting the information stored on them when it is no longer needed. Deleting a file from a computer by no means removes it from the hard drive, and computers accumulate large amounts of data users may know little or nothing about.

### What can we recover using computer forensics?

- files deleted days, weeks or months previously;
- records of the editing history and authorship of files;
- records of the times and dates files were created, accessed, copied, modified and deleted;
- web-searches run on the computer using Google, Yahoo and other search engines – sometimes years before;
- web pages visited by a computer's users;
- web-mail and e-mail messages written and read by a computer's users;
- files printed on a computer;
- programs recently run on a computer;
- devices recently attached to a computer (including USB pens and other data storage devices);
- CDs and DVD's burned on the computer; and
- much more.

## Why should I be interested

Because any organisation, sooner or later, has to carry out some kind of internal investigation, and computer forensics could be the key to any investigation you might find yourself involved in. From simple internal disciplinary cases like employee misconduct or bullying, to complex cases of intellectual property theft and fraud, computer forensics can produce evidence that may be the difference between finding the truth or being left in the dark.

Few offences these days are not carried out in some way without the help of a computer. In many frauds computers are not simply used to move the money, but to research how to steal it in the first place, to track its movements after it has been stolen and even to plan how it is going to be spent. Computer forensics can tell you exactly what has happened. We can quickly find out who your suspects have been talking to and what they have been talking about, what websites they have been visiting, what documents they have prepared. In many cases computer forensics can tell you exactly what has happened, right down to times, dates and locations.

Fraud doesn't just involve money being stolen. Many of your organisations most important assets are stored on your computers as electronic data. Your computers hold client lists and correspondence, strategic, business and marketing plans, software code, product designs, personnel records and, of course financial information and records. But do you know what information is being lost to your organisation when people leave? Do you know if any crucial data is being passed to people who should not have it? Modern criminals, at least the more intelligent ones, know that information can be every bit as valuable as money, and it is a great deal easier to steal.

#### And it's not just computers

Data can be retrieved from most modern electronic devices. We have recovered data from Blackberries and other PDAs, mobile phones, USB pens, backup tapes, portable hard drives, even iPods and digital cameras. These can all retain large amounts of crucial evidence long after it appears to have been deleted.

#### But isn't it expensive?

No. The technology and procedures used by Grant Thornton allow us quickly copy and analyse computer evidence to the highest international standards. Our professionals have the experience to know where the best places are to look for evidence in the different kinds of cases they deal with, so they do not waste our client's time and money following false trails. Our technology, our techniques and our experience allows us to give our clients the answers they need quickly and to the highest standards of evidence, without charging them unnecessary or unreasonable fees.

#### Discretion is part of the service

We can visit your premises at a time of your choosing. We can quickly make evidentially sound copies of computers and other equipment without anyone even knowing we have been there. We can let you retrieve evidence in investigations without tipping-off suspects, and let you help you positively identify offenders before anyone knows there is even an investigation under way.

#### Why Grant Thornton?

Grant Thornton's IT forensic procedures are based on accepted international best practice. They comply with the standards set-out in the UK Association of Chief Police Officers *Good Practice Guide to Electronic Evidence* (on which Garda Siochana IT forensic standards are also based), the US *NIST Incident Handling Guides*, and on the ISF Standard of Good Practice. The standards and procedures used by Grant Thornton have been proved in hundreds of different cases in Ireland and worldwide.

Grant Thornton operate a law-enforcement grade IT forensic laboratory at our premises in Dublin. We operate to the same procedural and evidential standards as An Garda Siochana, and a former Garda officer is part of our team to ensure these standards are maintained. We use similar IT forensic hardware, software and investigative techniques to the Gardai's own Computer Crime Investigation Unit (CCIU).

Our Irish IT forensics team is equipped with the same equipment as the Garda Computer Crime Investigation Unit. Our specialists have extensive experience of investigating a wide

range of different cases from large scale financial frauds, to industrial espionage, to employee misconduct and many others.

We maintain computer forensics units in locations as varied as New York, Chicago, Toronto, London, Singapore and Hong Kong.

### Contact

**Paul Jacobs**

Partner, Forensic & Investigation Services  
D +353 (0)1 6805 835  
E [paul.jacobs@grantthornton.ie](mailto:paul.jacobs@grantthornton.ie)

**Andrew Harbison**

Director, IT Forensics & Investigation Services  
D +353 (0)1 6805 766  
M +353 (0)86 040 7211  
E [andrew.harbison@grantthornton.ie](mailto:andrew.harbison@grantthornton.ie)

24-26 City Quay, Dublin 2

Offices also in Limerick and Kildare

This briefing is provided for general information purposes only and is not a comprehensive or complete statement of the issues to which it relates. It should not be used as a substitute for advice on individual cases. Before acting or refraining from acting in particular circumstances, specialist advice should always be obtained. No liability can be accepted by Grant Thornton for any loss occasioned to any person acting or refraining from acting as a result of any material in this briefing. Grant Thornton is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

