



Case Study— Professional Negligence

A national government medical organisation contacted CY4OR following concerns that a member was engaged in the illegal sale of prescription only medicines. Medicines of this type can only be prescribed by a medical practitioner having evaluated the nature of each patient's case. The organisation were naturally concerned about the risk to public health should the suspected member be trading illegally as a business.

CY4OR have had extensive experience implementing search and seize orders, and have been appointed by the court on a number of occasions. Once instructed, CY4OR executed a search and seize order on the suspect's office and subsequently seized four personal computers for forensic analysis. The organisation requested that CY4OR provide information on how long the fraudulent business had been operating, its financial records, and who was supplying the suspect with medicine.

“The organisation required that CY4OR provide information on how long the fraudulent business had been operating, its financial records, and who was supplying the suspect with medicine.”

An examination of the Outlook email identified correspondence between the suspect and his web designers, which indicated that the business had been launched in September 2003. In order to confirm this, an internet query (known as a Whois Query) of the suspects trading website was conducted.

The Whois is a central database that stores information on domain name registrants and their registration dates. The domain names relating to the suspect's business were all registered at around the same date as the correspondence to the web designer. The date of this set up was further confirmed by business plans found on the personal computers.

Continued overleaf





Case Study— Professional Negligence

The review of databases located on the computers successfully highlighted information on drug suppliers to the company. Furthermore, the associated metadata provided confirmation of the database's origin. Metadata is hidden information relating to the document; in this case the metadata contained information completed during the database program installation. The metadata confirmed that the database had originated from the suspects machine.

The financial information relating to the business appeared to have been deleted at some point. A common misconception is that file deletion completely removes the data from the media; this is not the case. When a user deletes a file, the area of disk that occupies the file is simply marked as being available for re-use. The operating system may then choose to overwrite that area, or a portion of it with another file.

Although this information would not be recoverable by the average IT user, using advanced techniques it was possible to recover a deleted file, apparently containing relevant financial information. Again the metadata allowed CY4OR to review hidden information; this time on the document history. It identified the history of saving the file and that the company's accountant had been involved in the falsification of accounts.

The forensic investigation provided the organisation with sufficient information to approach the suspect and successfully prosecute. The information collected adhered to ACPO guidelines and was retrieved in a forensically sound manner, so that it was entirely admissible in court.

“Using advanced techniques CY4OR recovered a deleted file and analysed its Metadata for hidden information; identifying the history of saving the file and that the company's accountant had been involved in falsification of accounts.”

HEAD OFFICE

TEL 0161 7978123
Fax 0161 7978122

AYLESBURY OFFICE

TEL 01296 488123
Fax 01296 488124

LONDON OFFICE

Tel 0207 8368123
Fax 0207 2402225

If you require an office address, please contact the relevant office and someone will be glad to help.

E-MAIL info@CY4OR.co.uk
WEB www.CY4OR.co.uk

EMERGENCY OUT OF HOURS CONTACT
07879 49 42 47