Fields Associates
Litigation Consultants

Speak directly to a qualified member of staff
0845 301 5778

Anti-Forensics: An Overview

To put it simply, anti-forensics is a term used to describe techniques that individuals may use in order to hinder investigators from gathering the digital evidence that is stored on any type of device used to store electronic media. It has only recently been recognised as a legitimate field of study, but there can be little doubt that it is essential that any forensic investigator is familiar with such techniques and, indeed, how to circumvent them. Below is a summary of some of the most common techniques utilised by unscrupulous individuals looking to hide their 'digital tracks':

Encryption

When data is encrypted, it will appear as little more than a series of random characters that are completely meaningless. Following the device that holds the data having been provided with the relevant encryption key, the data is 'unscrambled,' allowing the user to once again access this data.

Encryption is an extremely popular form of anti-forensics and can, depending on the complexity of the algorithm used, make it difficult for a forensic investigator to gain access to the required data.

Fortunately, in criminal proceedings, it would be an offence for the accused to refuse to disclose the relevant encryption key. However, in civil cases it will be necessary to obtain a court order before it would be necessary for this key to be disclosed.

Steganography

Steganography is, essentially, the act of hiding or disguising data. Imagine, for example, if an incriminating text file had been stored as an MP3 file. Under such circumstances, the file may appear to be little more than a music file and, as it would therefore appear to be entirely innocuous, a forensic investigator may not notice that it actually contained incriminating data.

Whilst some would argue that such techniques are not widely used they can, when used correctly, prove to be a difficult obstacle for a forensic investigator to overcome.

Data Wiping

The act of deleting data from a computer does not mean the data cannot be recovered. The deletion of data by a user will merely inform the storage device in question that the data can be overwritten (meaning that it still exists and can therefore be recovered), the forensic deletion of data is both a common and effective means of permanently destroying incriminating data on computers and other digital devices.

From continuously overwriting data to – in extreme circumstances – magnetic degasing, if data is permanently deleted, then there is very little that a forensic investigator can do to recover it. Consequently, to account and proactively explore instances of anti-forensics in the recovery and investigation of computer data and evidence, it is imperative to seek the services of proven experts in the area of data recovery and digital forensics.