Fields Associates
Litigation Consultants

Speak directly to a qualified member of staff
0845 301 5778

You may assume that all of the pertinent evidence on a computer or any other device will all be present within its storage media. Indeed, until recently many law enforcement agencies felt the same way and what we in the industry refer to as 'volatile data' was not deemed important. Fortunately, this attitude is changing and 'live forensics' is now rightfully seen as a vital means of gleaning all of the evidence contained within any type of device.

All digital evidence is, of course, unstable and must be 'handled' carefully. This, however, is particularly true of 'volatile data' as, to put it simply, it exists at one moment and not the next. This is data that is temporarily stored on the devices RAM – which can include, but is not limited to, browsing history, system information, messages etc. – which is lost permanently if the device is powered down. The solution to this is to capture a record of this data at the time that a live machine is acquisitioned.

The data in question is collected by simply connecting a collection device (such as a USB flash drive) to the machine in question. This device is then activated and the data collected. The device is then safely removed from the machine and the data collection verified on a separate machine. Following this having been completed, the acquisitioned device can be powered down.

As you will no doubt be aware, one of the most significant challenges concerning the acquisition and presentation of digital evidence stems from the fact that the vast majority of actions that an individual takes on a device are recorded. Unfortunately, the process of collecting data from an active device is no different as it leaves a 'digital footprint' which can, under certain circumstances, result in any evidence collected from the device becoming inadmissible – not just the data collected from the active device.

Fortunately, the vast majority of courts are now aware of the fact that collecting data from an active machine leaves traces and also how these traces manifest themselves meaning that the evidence will be accepted provided that the process of acquiring the data has been carefully executed and documented.

Nevertheless, it is essential that an assessment be carried out prior to collecting a copy of the data held on a device's RAM and that the benefits of collecting such data be weighed against the drawbacks until robust universal procedures on the collection of such data has been agreed.

-ooOoo-