

## EVIDENTIARY ISSUES

Computers are not just tools for processing and analysing data. They are also storage devices and therefore have evidentiary value. But because of their interactive capabilities, they must be treated very differently to other storage media. Most computer storage media are magnetic and can therefore be erased if they pass through a magnetic field. When seizing a computer, do not turn on an idle machine immediately. Law enforcement agents have come across computers with start-up traps which could wipe out all data from a computer hard drive if the system is booted without special precautions known only to the user.

Investigators should also be aware of the fact that even the simple viewing of files on a system could trigger changes in the system data logs, making it difficult to prove identity and intent. Any use of a system subsequent to seizure could change the system from its state at the time of the seizure, providing opportunities for defence lawyers to attack the evidence. That is why trained investigators create copies of all computer-based media and search the copies, leaving the originals relatively untouched.

Prosecutors must make sure that they know exactly how the investigating officer handled the evidence in every computer-related case. Even investigators working from copies could have created openings for defence lawyers to exploit. For example, copies can be made by connecting two computers. If one of the computers is routinely used for child pornography investigations, you must be sure that there is no inadvertent transfer of data from the investigator's computer (which, if routinely used for child pornography investigations will most likely contain child pornography) to the seized computer.

Investigators should also make sure that previously-used computer components have not been installed in the seized computer. For example, if the accused purchased a hard drive from a prior owner, there may be information on the hard drive which may have come from the previous user. It is not unknown also for hard drives to be contaminated by maintenance and repair, without the user being any the wiser.

Most importantly, the prosecutor must be a near an expert as an expert would be in order to present a case in such a way as to be understood by the presiding officer. The prosecutor must be prepared to explain how the evidence was seized, examined and preserved. A statement that the accused was found in possession of child abuse images downloaded from a website is not enough. One should go further and identify the website and explain how that website is accessed, what happens when it is accessed, and so on – and, if necessary and the website is still accessible, demonstrate the whole process. Presiding officers must be made to understand how computers work and the difference between digital and analogue information. Using a photocopier to make copies of an image is not the same as downloading an image from the Internet. That difference must be explained, particularly where an accused is charged with the offences of possession and creation.

Iyavar (2005)