

The Ethics Of Computer-Based Electronic Evidence

Technology is present in every aspect of modern life. Information Technology is constantly growing & every new development gets a larger role in our lives. Criminals are exploiting the same technological advances which are driving forward the evolution of society.

Computers can be used in the commission of crime, they can contain evidence of crime and can even be targets of crime. Understanding the role and nature of electronic evidence that might be found, how to process a crime scene containing potential electronic evidence and how an agency might respond to such situations is crucial. It cannot be over emphasized that the rules of evidence apply equally to computer-based electronic evidence as much as they do to material obtained from other sources. It is always the responsibility of the case officer to ensure compliance with legislation and, in particular, to be sure that the procedures adopted in the seizure of any property are performed in accordance with statute and current case law.

Electronic evidence is valuable evidence and it should be treated in the same manner as traditional forensic evidence with respect and care. The recovery of evidence from electronic devices like computers, tapes, CD/DVD, flash drives, is now firmly part of investigative activity in both public and private sector domains. The methods of recovering electronic evidence, whilst maintaining evidential continuity and integrity may seem complex and costly, but experience has shown that, if dealt with correctly, it will produce evidence that is both compelling and cost effective.

Computer-based electronic evidence is information and data of investigative value that is stored on or transmitted by a computer. As such, this evidence is latent evidence in the same sense that fingerprints or DNA(deoxyribonucleic acid) evidence is latent. Computer-based electronic evidence is very delicate. It can be easily altered, damaged, or destroyed if not handled properly or by improper examination, For this reason special precautions are taken to document, collect, preserve and examine this type of evidence. Failure to do so may make it unusable or lead to an inaccurate conclusion.

In its natural state, we cannot see what is contained in the physical object that holds our evidence. Equipment and software are required to make the evidence available. Testimony may be required to explain the examination and any process limitations.

Four principles are involved:

Principle 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3:

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Explanation of the principles

Computer-based electronic evidence is subject to the same rules and laws that apply to documentary evidence. The principle of documentary evidence may be explained thus: the responsibility is on the prosecution to show to the court that the evidence produced is as it is since the first possession of police.

Sometimes Operating systems and other programs alter and add to the contents of electronic storage automatically even user may not aware of changes being made by such programs. Wherever practicable, an image should be made of the entire target device. If creating image of incomplete or selective file which is considered as an alternative in certain circumstances, investigators should be careful to ensure that all relevant evidence is captured.

In a some cases, it may not be possible to get an image using a recognized imaging device. In these conditions, its necessary o access original machine to recover the evidence. While doing this it is important that a witness, who is able to give evidence to a court of law makes any such access.

It is essential to display objectivity in a court, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court.

About the Author

Author is an international computer forensics consultant. He is president of Data Triage Technologies, LLC.(<http://www.datatriage.com>), a [Computer forensics](#) and [Electronic discovery](#) firm based in Los Angeles, California .

