**IDENTIFYING**

This is the process of identifying things such as what evidence is present, where and how it is stored, and which operating system is being used. From this information the investigator can identify the appropriate recovery methodologies, and the tools to be used.

**PRESERVING**

This is the process of preserving the integrity of digital evidence, ensuring the chain of custody is not broken. The data needs to preserved (copied) on stable media such as CD-ROM, using reproducible methodologies. All steps taken to capture the data must be documented. Any changes to the evidence should be documented, including what the change was and the reason for the change. You may need to prove the integrity of the data in the court of law.

**ANALYSING**

This is the process of reviewing and examining the data. The advantage of copying this data onto CD-ROMs is the fact it can be viewed without the risk of accidental changes, therefore maintaining the integrity whilst examining the changes

**PRESENTING**

This is the process of presenting the evidence in a legally acceptable and understandable manner. If the matter is presented in court the jury who may have little or no computer experience, must all be able to understand what is presented and how it relates to the original, otherwise all efforts could be futile.

Far more information is retained on the computer than most people realize. Its also more difficult to completely remove information than is generally thought. For these reasons (and many more), computer forensics can often find evidence or even completely recover, lost or deleted information, even if the information was intentionally deleted.