

# Data Recovery Services: The Golden Combination of Data Security and Computer Forensics

By [Chris Vermaak](#)

Data recovery services entail the recovery of data from a computer's hard drive. The hard drive may have been formatted or damaged. Computer forensics is a special branch of computing that deals with complex data recovery to ensure that valuable data that has been lost is recovered in as much of its original state as possible, and to trace the data security path to determine why the data was lost in the first place in instances where foul play is suspected.

To facilitate data recovery services, a data security specialist will use special tools and equipment to identify three types of data: active data, archival data and latent data. Active data refers to normal files that can be seen by anyone using a normal computer system while archival data refers to encrypted files stored in backups. These two types of data are easy to recover and can be transferred to a disk or any other storage medium once identified.

Latent data is a bit trickier, since it refers to files that have been deleted, or files that have been stored on a disk that has been quick formatted. These files are still recoverable with the use of specialist software capable of viewing the content of the drive without relying on the partitioning table of the drive. Said software also typically offers data recovery services to restore the files to their active state for transfer to a different storage medium. Once transferred, these files can again be inserted into an active file system to minimise any potential losses incurred due to a lack of the data in question.

Adding computer forensics to the mix will entail a detailed analysis of the information contained on the drive. The aim here is not only to provide data recovery services, but to determine how the information was lost, when it was lost and, most importantly, who was involved. In this instance special computer forensic techniques and methodologies are employed in addition to specialist hardware to examine file fragments still stored on areas of the drives that have as yet not been overwritten. At the same time a chain of custody will be established with the client to ensure that all parties concerned are aware of the location of the data (or a copy thereof) being examined.

Data recovery services experts that specialise in computer forensics will then proceed to catalogue all active, archival and latent data. This includes files that have been deleted, password-protected files, encrypted files as well as attempts at hiding data. An examination of relevant server logs, firewall logs, proxy logs and the like will also be conducted to further recreate the conditions under which the data was lost. The final step in the computer forensics process is to provide the client with a detailed report along with the recovered data.

It should be noted that data recovery services and computer forensics cannot be applied to hard drives that have been low-level formatted, since these drives are completely and actively overwritten in their entirety by the computer system. Luckily, this type of exercise can take many hours to complete, which means it can be stopped in time by simply cutting the computer's power supply.

Keep in mind that data loss as a result of human error or active intention is often attributable to slack data security. The data recovery services expert will therefore also advise on proven data security principles, methods and routines that can help the organisation avoid future incidents, thereby minimising expenditures. Examples of enhanced data security include a recommendation for strengthened passwords, offsite backups, restricted access to certain computers, frequent computer log analysis, and daily reports of network traffic.

Further data security measures can be taken to avoid future data recovery services and computer forensics costs by keeping computers containing valuable information in a dedicated server room or safe, completely disconnected from the network, or with access almost entirely restricted.

The combination of data recovery services, computer forensics and added data security can help recreate events that led up to the loss of important organisational data. It is, however, the responsibility of the organisation and those in charge of its IT infrastructure to ensure that the risk of such losses are minimised to the utmost extent.

<http://www.intratec.co.za/>

Article Source: [http://EzineArticles.com/?expert=Chris\\_Vermaak](http://EzineArticles.com/?expert=Chris_Vermaak)