

Computer forensics and data recovery

From laptops thrown in the river to hard drives that have been damaged in an attempt to destroy any evidence of wrongdoing, Kroll Ontrack's engineers and consultants have successfully assisted hundreds of law enforcement and government agencies, law firms and corporations to recover evidential data that was pivotal for their case.

Computer forensics is the science behind the investigation of computer media while data recovery, on the other hand, is the technique used for the retrieval of data from damaged media. This damage can be physical, when a hard drive has suffered a crash or is malfunctioning, for example, or can be logical, when the data structures are corrupt.

In many instances the media at the centre of an investigation, either as the tool used to commit a crime or a repository of evidence of a crime, might be damaged or unreadable. The failures could be caused by a myriad of reasons such as intentional damage, technical failure, fire or water among many others.

Kroll Ontrack has been engaged in many investigations over the past two decades where media has been seriously damaged. A recent test of our expertise took place when we were instructed to recover data from computer hard drives which sustained fire damage following an explosion in a residential building.

The generally accepted protocols used by computer forensics specialists in the UK are drawn out of the ACPO (Association of Chief Police Officers) guidelines. The practice guidelines to computer-based evidence offer good and

sound advice on how to handle media from the seizure, to the handling, copying, processing and final analysis.

One of these accepted guidelines is that data held on a computer should not be changed in any shape or form. Another of these is that proper documentation and a chain of custody needs to be in place. This documentation explains the procedures so that another expert would be able to reproduce the same results.

In all cases, it is vital that these guidelines and protocols are followed. It is also crucial that the expert analysing the media has the skills and experience required to handle and analyse electronic data storage devices.

A recent case handled by Kroll Ontrack for a foreign Magistrates Court involved a hard drive that was used to record CCTV images. There was the possibility that footage captured contained evidence of a murder being committed. Unfortunately for the local investigation team, the drive was not operational and they called in our experts to assist.

The damaged drive was flown into London by personal escort and after a cursory examination, the media seemed to suffer from electronics failure. Further examination revealed that the drive also suffered from media corruption damage. Media corruption means that there is no physical damage to the media, but certain areas on the drive have been mistakenly overwritten, which renders the data unrecoverable. In these instances the fault lies with the storage device, not a virus or the operating system. In many cases, it is not

Two decades of successful investigations...

only the data that is overwritten, but also the low-level information that is critical to the basic operation of the hard drive.

Despite this level of corruption, Kroll Ontrack managed to copy 99% of the raw data. Unfortunately the data structures were affected, which meant that, in order to recover the files, they needed to be repaired. As it is often the case with CCTV systems, the operating system is of a proprietary nature. However, Kroll Ontrack was able to bypass the damaged structures and recover image files that could be used by the court.

In general, you will get one shot at recovering data from damaged media. Therefore it is paramount to engage the assistance of experts with the right level of skills, qualifications and experience. Kroll Ontrack has amassed years of experience in the data recovery field, experience that can now be used by our computer forensics experts in the recovery and analysis of evidence from computer media.

KROLL ONTRACK®

Jérôme Torres Lozano
Senior Computer Forensics
Project Manager

Kroll Ontrack
Cardinal Tower
12 Farringdon Rd
London EC1M 3HS

Tel: 020 7549 9600
Fax: 020 7549 9636

jtorres@krollontrack.co.uk
www.krollontrack.co.uk