Ontrack®

Data Recovery **UK**

Case Study

The case of the fire damaged CCTV DVR

The Situation

Ontrack took receipt of a badly damaged DVR and upon initial inspection, it was found to have no original markings to show the manufacturer or model number.

The first task for the engineers was to open the DVR and remove the hard drive. To preserve all data on the hard drive a sector-by-sector copy, known as an “image” of the drive had to be taken. However, unsurprisingly the hard drive removed from the DVR was in a very poor physical condition and could not be operated in this state.

The hard drive was covered in soot and the plastic components both inside and outside the drive’s head/disk assembly (HDA) had melted due to radiated heat. There was also evidence of water damage from the subsequent extinguishing of the fire. It was determined that the disk platters, which carry the magnetic coating within which the data is stored, were dirty but had not been taken to a temperature high enough (the “Curie point”) to cause the loss of the stored data.

The Solution

In this instance, it was necessary to rebuild the drive within our class 100 cleanroom facility. This was done by fully disassembling the HDA, removing the disk platters and carefully cleaning the surfaces.

An ultrasonic cleaner was used to carefully remove deposits on the disk surfaces using a proprietary cleaning solution. The hard drive’s original printed circuit board (PCB) and heads were beyond salvage so the necessary data was extracted from the PCB memory to ensure that a replacement PCB was compatible with the drive firmware stored on the disk platters. Additionally, the head and pre-amplifier technology used by the drive was identified so that a compatible set of replacement read/write heads could be procured.

Once the drive had been reassembled and the critical mechanical alignment at the head-media interface had been restored to that of the original components, the drive was able to spin up and load firmware from the disk platters under controlled laboratory conditions. However, the drive was not ready to allow logical access to the stored data just yet. Analysis through the drive’s diagnostic interface identified that there was a problem with a defect list within the reserved system area of the disk platters. This required switching the drive into a factory mode and the defect list was corrected and re-written using Ontrack’s proprietary tools.

An image of the drive was then successfully taken and approximately 95% of the total sectors were read successfully.

With the exception of the unreadable sectors, the image is a faithful copy of the data that is stored on the hard drive. However, as with many CCTV DVRs, this DVR model used a proprietary file system and video compression algorithm to store the video footage. This is why a hard drive from a DVR cannot be simply connected to a PC in order to access and play the video, nor will many standard data recovery tools recognise and extract the video. Furthermore, in this case, it was not possible to create a "clone" copy of the recovered image on a new drive and use that within the DVR, even if the DVR had worked because the unreadable sectors had affected the DVR's indexing information which it uses to locate the stored video. Even forensic software tools designed specifically for DVR recovery could not process the image in this case due to the partially-missing index information and missing sectors of video data.

For cases such as this, Ontrack has developed software tools to maximise the recovery of video from partial hard drive images. These tools support a wide range of DVR formats and their variants, can be tweaked to support new DVR formats and can even recover video that had been considered overwritten. From a forensic perspective, it is almost always possible to generate a report on the available date and time range of recoverable video from a hard drive image, often down to the granularity of individual video frames and even if the DVR format is missing some meta-data that would be used to extract video, for example, a camera ID or timestamps, the software tools are still able to recover video.

The Resolution

After analysing the video data format, the necessary code was updated to support it and the image was processed to extract all available video footage.

The recovered video was returned in files organised by camera, date and time – making it a simple process to find the video leading up to the start of the fire. In this case, the fire was found to have started in the cab of a camper van on a garage forecourt. The footage revealed the start of the fire which evolved from a small trail of smoke to a full blaze within less than twenty minutes. The cause was believed to be an electrical fault.