B1 The Potential Recoverability of Data From Hard Drives of Computers From Fire Scenes

Niamh Nic Daeid, PhD, Royal College, Strathclyde University, Center for Forensic Science, Department of Pure and Applied Chemistry, 204 George Street, Glasgow, Scotland G1 1XW, United Kingdom; and Angus Marshall, PhD, Centre for Forensic Investigation, University of Teeside, Teeside, TS1 3BA, United Kingdom*

After attending this presentation, attendees will understand the potential for recovery of data from computers recovered from fire scenes.

This presentation will impact the forensic community and/or humanity by demonstrating how computers that have been subjected to fire are often disregarded as potential evidential sources and the situations in which hard drive data can be recovered from computers that have been within full compartment fires.

With the ubiquitous nature of computers in modern society it is common to find these types of items during the investigation of a fire scene. One question which has arisen is whether or not it is possible to recover information from hard disc drives which have been damaged within a fire and secondly what parameters (exposure to heat, protection afforded by the computer case etc) define this recoverability.

A hard disk drive is a complex system: The disk pattern consists of a number of rotating platters with a ferro-magnetic coating. An electro- mechanical arm carries a number of read/write heads, which may be moved so that the heads (carried on the end of the arm) may be positioned over any spot on the disk. The arm and heads are controlled by the drive's interface electronics (usually mounted on a PCB which is an integral part of the drive). A hermetically sealed case surrounds the disk pattern. Provision is made for attaching the interface electronics to the host computer via a set of multipole connectors.

Data is only irrevocably lost from such a disk by the (usually deliberate) alteration of the magnetic pattern on the disk (logical destruction) or by the corruption of the disk's magnetic coating (physical destruction). Destruction (by fire or other means) of the electronics, connectors, or even the arm/head mechanism may leave the magnetic surface and hence the data unharmed.

It has been assumed that the recovery of evidence such as hard drive data (both pictures and documents) has not been possible once the computer housing the hard drive has been exposed to fire conditions. A preliminary study was undertaken to test this hypothesis. A number of computers containing hard drives with stored documentary files were placed into a fully furnished compartment which was set on fire. The compartment fire was allowed to develop until flashover or near flashover was achieved.

The drives were subject to three stages of analysis: firstly a preliminary visual inspection was made. Secondly the drives (where possible) were connected to a forensic data capture station for interface testing and retrieval of basic drive parameters. Finally the drives (where possible) were imaged and a search performed.

Visual inspection: The serial number and drive parameters were retrieved from any extant labels. The feasibility of connecting power and data cables to the drive (in the light of the degree of damage) was assessed. The general appearance of the drives was recorded.

Interface testing and parameter retrieval: If a drive was sufficiently intact to permit the connection of data and power cables, it was mounted in a test caddy and inserted into a digital forensics workstation. The functioning of the interface electronics, drive motors,

head mechanism was tested using the Hitachi Drive Function Test (DFT) program, and the results recorded.

Imaging and search: If a drive was found to be sufficiently functional, an attempt was made to recover partition information using *fdisk*. Where partition information was recovered, an image of the drive was taken using the *dd* utility. The image was mounted and searched using the *Autopsy* digital forensics toolkit. A simple ASCII search for a 12-byte string was made ("autoexec.bat" in the case of a Windows file system - none of the Apple drives were sufficiently undamaged to allow a search to be made) and the results of the search recorded. All tools used in this stage where based on the Helix V distribution of Linux.

It was possible to rapidly recover some data from the test disks without resorting to removal of disk pattens.

Data Retrieval, Computers, Fire Damaged

 ** Presenting Author*