C21 Case Study - Imaging the Memory of a Digital Audio Recorder

Kenneth W. Marr, BSEE, MS, David J. Snyder, BSET, and Jeffrey Edwards, MSEE, Federal Bureau of Investigation, Forensic Audio, Video and Image Analysis Unit, Engineering Research Facility, Quantico, VA 22135*

The goal of this presentation is to review the procedures and precautions for making an exact digital copy of the memory contents of a handheld digital audio recorder.

This presentation will impact the forensic community and/or humanity by providing to the digital evidence examiner procedures and precautions for making an exact digital copy of the memory contents of a digital audio recorder.

Commercial digital audio recorders are used throughout society today. This case involved a commercial off-the-shelf digital recorder that the submitting agency requested to be examined to determine the contents of the recorder's memory. Since there were questions involving alleged alterations of the recorded information, an image of the recorder's memory was required. This is the same concept in use by computer analysis response teams when downloading the contents of a computer's hard drive. The image of the hard drive is an exact digital copy of the contents of the original drive. This allows the examiner the opportunity to review and analyze the image contents without affecting any parameters of the contents of the original drive. Potentially vulnerable information on a hard drive includes file names and the dates/times files were stored.

Since this case involved an unknown recorder system, a thorough search of law enforcement and Internet forensic sources was made to find existing forensic tools which could be used to image the recorder memory. None were found but valuable forensic consultation information was obtained. It was determined that a new procedure must be validated and approved before the image could be obtained. The same make and model recorder with the same characteristics and features was used to conduct the validation testing.

Established forensic principles of write-protection, data verification by use of MD5 Hash calculations, and use of validated procedures were followed. Consultation with the recorder manufacturer confirmed the design and operating specifications. Digital tools used in the validation included a forensically approved digital hex editor program, a commercial monitoring utility for USB interfaces, a computer utility written to query the recorder memory contents, and a high-quality computer and operating system. All steps of the procedure were conducted with repeated tests using the same make and model recorder to verify and validate the procedure. MD5 Hash calculations confirmed that the image of the test recorder memory matched the contents of the test recorder.

After validation and approval of the procedure, the memory content of the original digital recorder was downloaded and the exact image of the recorder's memory was returned to the requesting agency.

Digital evidence is taking a more and more important role in law enforcement in today's society. Analysis of digital files requires a high degree of knowledge and expertise to maintain the integrity of the memory contents of digital storage systems.

Digital Evidence, Computer Forensics, Computer Image

 ** Presenting Author*