D33 Identification and Reconstruction of Deleted, Fragmented DNA Digital Files

Jessica Reust, MFS, and Ryan Sommers, BS*, Stroz Friedberg, LLC, 850 Northstar West, 625 Marquette Avenue South, Minneapolis, MN 55402*

The objective of this case study is to describe a methodology to identify, reconstruct, and validate deleted file fragments. This methodology is predicated on a thorough understanding of the content structure of the file format and file-system level structures.

This presentation will provide the forensic community with details about a process used to identify and recover files from a reformatted drive by using file structure and file-system characteristics, which in turn were utilized to develop a programmatic and elegant solution to a challenging and complicated task. The case presented involved not only identifying the file fragments of the deleted file, but also reconstructing the history of the drive, including the file-system structure of the drive before it was reformatted.

Identification and reconstruction of deleted, fragmented files is a time consuming and often difficult process but it can be worth the effort, particularly when the results are a matter of life or death. The case study presented will detail the identification and recovery of deleted files from a hard drive that had been re-initialized with different volume parameters from the original drive format. The recovered files contained the DNA analysis results of a crime scene sample that were relevant to a multiple homicide investigation and death penalty trial.

Traditionally, identification of deleted files has been most successful when plain text content is searched for in unallocated space. Documents such as word processing documents, spreadsheets or Internet HTML files may be identified with relative ease in unallocated space, even in fragmented form. Nevertheless, in only a few cases is an original file able to be reconstructed from recovered file fragments.

This case study provides an example in which only the first fragment contained a searchable keyword. Fragmentation on the drive made it impossible to reconstruct the files using available tools. The existence and location of the first file fragments were identified through keyword searches formulated by researching the file format and the standard nomenclature used by the laboratory that had analyzed the original DNA samples. One method available to identify the remaining associated file fragments would require a manual "trial and error" approach to combine random clusters and attempt to validate the combined file.

Instead, the authors developed, and will present, an alternative method using a customized program to search for and identify the associated file fragments that relies upon the characteristics of DNA digital files and individual attributes of the specific, relevant files. The program searched through every cluster of the relevant hard drive for the associated second file fragments, and returned only one hit for each deleted file fragment. The file fragments were reconstituted, and the resulting files tested and validated with DNA analysis software.

Fragmented Files, Reconstruction, Deleted Files

** Presenting Author*