C24 Graphic File Carving Tool Testing

Richard Ayers, MS, 100 Bureau Drive, Mail Stop 8970, Gaithersburg, MD 20899-8970; James R. Lyle, PhD, NIST, 100 Bureau Drive, Mail Stop 8970, Gaithersburg, MD 20899; and Jenise Reyes-Rodriguez, BS, NIST, 100 Bureau Drive, Gaithersburg, MD 20899*

After attending this presentation, attendees will be aware of the importance of tool testing and will have gained an understanding of the file-carving tool-testing process conducted within the Computer Forensics Tool Testing (CFTT) project.

This presentation will impact the forensic science community by increasing awareness of the impact tool testing has on informing the forensic community of tool capabilities and limitations. Test reports provide a foundation for toolmakers to improve tools, help users make informed choices, and provide interested parties with an overview of any anomalies found. This presentation will provide an overview of tools capabilities for carving graphics files and the CFTT test results produced for various tools.

The CFTT project has been researching and testing forensic tools capable of reassembling files from fragments in the absence of file system metadata, typically accomplished by searching an input for files based on content or header/footer file signatures. This presentation discusses all aspects of the testing process that are critical for producing a test report.

A summary for the test results of the graphic file carving tools examined will be discussed for each dd image created for performing the following test cases:

Nofill: Contiguous files with no other content between files.

Simple: Contiguous and sequential fragmented files with content separating the files.

Partial: Contiguous and partial (i.e., only a portion of the file is present) files.

Disordered: contiguous and disordered fragmented files separated by other content.

Braided: Contiguous and intertwined fragmented files.

Not-Shifted: Contiguous files that are aligned on sector boundaries.

Shifted: Contiguous files that are aligned on non-sector boundaries.

Each test report contains an associated table that identifies the test, the total number of files carved, and a classification based upon the data recovered. The categories classifying the recovered data for each test follow:

Viewable — Complete/Minor Alteration: Carved data appears to be unchanged from the original or the changes are so minor that the full content and most attributes of the video are maintained.

Viewable — Incomplete/Major Alteration: Include partial recoveries (i.e., only parts of the file are viewable), scrambled files in which the fragments are assembled incorrectly (making the content of the file unrecognizable), color shifts, and similar changes.

Not Viewable: Describes carved files that are not viewable, could not be opened, or had no content when opened.

False Positive: Reports a count of files that were incorrectly identified.

The presentation gives an overview of the CFTT process as applied to graphic file carving tools while providing information on file carving and scanning unallocated space enabling the recovery of specific file types with based-upon file signatures and various carving schemes.

The test reports are available from the Department of Homeland Security Cyber FETCH web site: https://www.cyberfetch.org/.

File Carving, Digital, Testing