B9 Intelligently Combining Carving Results to Reduce Examiner Workload and Improve Output

David G. Ferguson, MS, 5338 Gunston Hall Drive, Woodbridge, VA 22193*

After attending this presentation, attendees will understand why combining carving results can be useful and understand some of the many issues combining these results can create. Discussion will include some of the more common carving tools with respect to accuracy (false positive/false negative results). Current activities across the community to identify intelligent ways to combine and display the results will also be shown. Finally, the potential issues that solid state devices may have on carving will be discussed.

This presentation will impact the forensic science community by showing the research that has been done in this area over the preceding months and the potential approaches to make this work.

The digital and multimedia forensics community is always looking for ways to improve processes. Improvements in carver results such as: reduction of false positives, false negatives, and greater accuracy can reduce examiner work load and improve accuracy of results. Combining the results of multiple tools, selecting the best results, and discarding the junk should improve overall results. The problem with this approach is knowing what is good and what is bad.

The research presented assumes that different carving tools perform better with some file types then with others. Based on this assumption, with appropriate testing we should be able to improve overall performance by intelligently combining the result of multiple carving tools. Performance attributes of some specific commercial and open source tools will be discussed.

Combining the output of multiple tools is not simply intermixing the results and displaying them. This simple approach will likely increase the number of unique files found and will also likely drastically increase workload for examiners because of the massive amount of duplication that will occur. In addition to the obvious issues with duplication, there are significant less-obvious obstacles to reducing work load for examiners. As an example, many carving tools are said to be “better” than others because they have low false positive rates on some file types. If one combines the better carver with the results from poorer carvers (with higher false positive rates), the bad tool will simply add back in the false positives that the better tool rejected. So, intelligently combining these results may mean ignoring part of the output of each tool and only keeping the best of the results.

In addition to combining the outputs from the different carvers, this study looked at workflow and ways to improve carving efficiency by making a number of passes, removing items found and only carving the remainder.

Finally, this presentation will show the research that has been done in this area over the preceding months and potential approaches to make this work.

Carving, Tool Integration, Improved Output

 ** Presenting Author*