

A Comprehensive Data Carving Architecture for Digital Forensics

Golden G. Richard III and Lodovico Marziale
Department of Computer Science, University of New Orleans



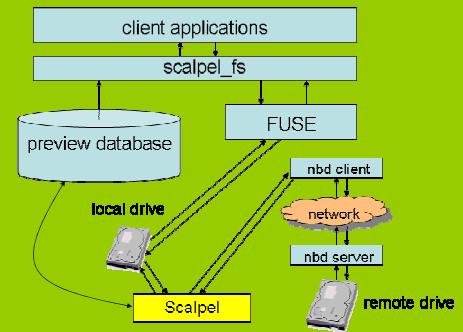
“Next Generation” Data Carving Techniques

File carving recovers documents and document fragments from block devices by searching for headers, footers, “milestones” and by performing deeper analysis of the contents of individual blocks. Current generation file carvers suffer from high false positive rates, offer little support for recovery of document fragments, require large amounts of disk space, and have difficulty carving extremely large targets. This research investigates techniques for efficient, rule-based, data carving for block devices, RAM, and network flows.

File carving is an important, practical technique for data recovery in digital forensics investigation and is particularly useful when filesystem metadata is unavailable or damaged.

Current project collaborators:

Vassil Roussev (University of New Orleans)
Dutch Police Department



In-place carving is an example of a “next generation” data carving technique. With in-place carving, a custom FUSE filesystem allows carving large forensic targets with minimal additional storage. The in-place carving application populates a preview database that the custom filesystem uses to create an overlay on the forensic target.

Approaches

- ✓ Rules-based carver configuration
- ✓ Recovery of document fragments
- ✓ In-place carving
- ✓ RAM carving
- ✓ Integration into distributed forensics framework

Research Impact

- ✓ Development of a open framework for design and deployment of new carving strategies
- ✓ Carving-based malware detection
- ✓ Application execution fingerprinting
- ✓ RAM carving for memory analysis

The Scalpel file carver, developed by the PI in 2005, is largely a response to the poor design of most commonly available file carving tools. Its contributions are primarily: *performance* (i.e., it is significantly faster and less resource-hungry than most available file carving tools) and *awareness* (i.e., many in the digital forensics community were surprised at the performance gains possible with a fresh look at a commonly used type of tool). A next generation data carving architecture must provide much more than the basic performance improvements illustrated by Scalpel, however.

Automatic pattern generation for new document types is necessary to reduce human effort and to increase the effectiveness and accuracy of file carving. Techniques for reducing the time and disk space necessary for carving large targets are also necessary. Our in-place carving technique, now being developed in cooperation with the Dutch police department, uses a custom filesystem to “wrap” a forensic target, exposing recovered documents and document fragments while requiring very little additional disk space. We are also developing techniques for file carving during the acquisition phase of an investigation, useful for data reduction, “targeted” carving operations, and for triage purposes.

Our carving strategies are also useful in live forensics investigations. By identifying characteristic patterns of application code and data layouts in physical memory and directly carving physical RAM dumps, it is possible to mine fragments of recently accessed documents and previously executed (or executing) malware, even on machines with no secondary storage.

Finally, we are a strong advocates of using distributed computing principles in next generation digital forensics. These data carving techniques will be incorporated into our cluster-based DELV (Distributed Environment for Large Scale Investigation) framework.