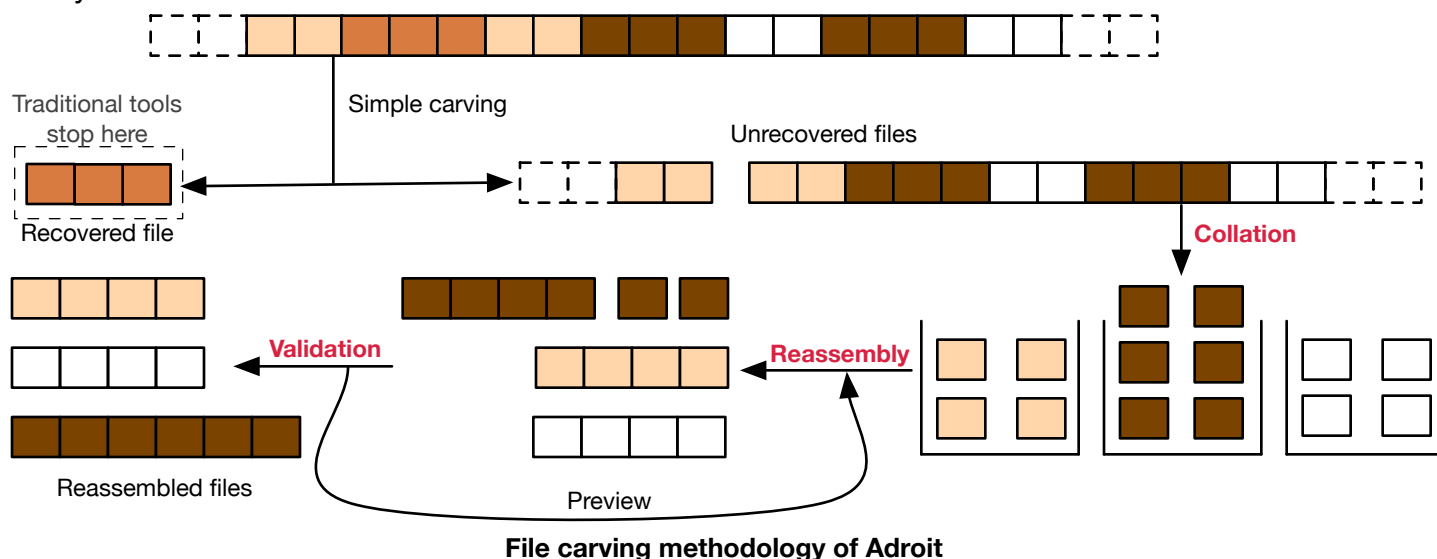


Adroit by Digital Assembly

Advanced Digital Recovery & Investigative Toolkit

The proliferation of digital media devices and increasing storage of information in digital form has highlighted the need for newer and better data recovery, forensics, and e-discovery tools. Adroit employs technology researched and developed by Digital Assembly to recover files in the absence of file table information—an operation popularly known as *file carving*. Adroit is a state-of-the-art file carver that employs a three-tier system to recover files. It matches data blocks based on content and can recover files even if they are highly fragmented—a task no other tool can perform today.



Collation. For efficient recovery, fragments that belong to a document type must be grouped together. Adroit utilizes various techniques to collate fragments belonging to specific file types, such as Microsoft Office files, JPEG images, GZipped files, etc. Adroit uses a sequence of semantic, syntactic, and statistical tests for collation. In addition, specialized decoders and file validators are employed to further improve this process. Once Adroit has fragments of different file types collated, it can then perform reassembly to recover individual files.

Reassembly. At its heart, reassembly is a two-step process. The first step estimates the likelihood of adjacency between all the fragments of a file type. This likelihood is estimated using a statistical model that does not require a dictionary. These statistical computations are then combined with disk geometry information and higher-level semantic information. The second step involves solving a graph theoretic combinatorial optimization problem, which then results in candidate reassemblies of the collection of files under consideration.

Validation. No matter how good a file carver is, with the absence of file table information, mistakes will occasionally be made. Adroit's GUI has unique

visualization tools that provide the user with the results of reassembly and the ability to evaluate the results. This includes, merging correct portions of reconstructions, disallowing incorrect pairings of data, and examining data down to the cluster level of the media. Just a few simple iterations can result in correct reassembly even when correlation computations between candidate pairings are not highly discriminative and result in false pairings.

Combined test results on DFRWS 2006/2007 Forensic Challenge disk images of 49MB and 346MB respectively.

FILE TYPE	ADROIT	BEST CURRENT TOOL
27 JPEG Images	25 (7 mins 40 secs)	7
6 HTML Files	6 (40 seconds)	2

Digital Assembly is a Brooklyn-based start-up developing advanced file-carving technology. The company's premier product, Adroit, helps customers recover files from digital media for forensics, e-discovery, and data recovery. A beta version of Adroit is available for evaluation. For more information, email beta-adroit-photos@digassembly.com