File Carving and Its Use in Digital Investigations

[redacted]

Abstract

This summary paper goes over the fundamentals of what file carving is and how it is relevant to digital forensic investigations, as well has what challenges people that use the method face.

Introduction/Methods

Since the early to mid 1990s, the explosion in popularity and pervasiveness of the internet has demanded comparable increases in both the ability of organizations to product their data and assets from cyber attacks, as well as an increase in the ability for law enforcement and associated professionals to recover data from computers to assist in prosecution of certain crimes. These could be newer offenses such as piracy/intellectual copyright violation or more typical crimes, facilitated in a new way by the internet (child pornography, drug selling, etc). This paper is meant as an overview of several other published sources of information on the practice of file carving, which is a means of recovering deleted data without using file system metadata.

Results

File carving (also sometimes referred to as "data carving" or simply "carving") is a newer method developed to recover deleted files from physical storage mediums such as hard disk drives and flash memory. Deleted file recovery has always been possible but only under certain circumstances. Beek (2011) describes traditional file recovery as a process that relies on residual data that resides within the file system information that describes the location of the deleted data on the disk. Contrary to popular belief, deleted data is not truly gone, but the file system instead goes to the cluster links in the FAT (file allocation table) and sets the hex value to 00, indicating that they have been unallocated rather than zeroing out all of the data (Pal & Memon, 2009).

Unfortunately, if the data in the file system is corrupted or the drive is formatted, this traditional method of file recovery will not work. In addition, if a file is not stored in contiguous sectors (fragmented), file recovery will also not work. This is where file carving comes in.

File carving as we know it now was pioneered by Simon Garfinkel and Joachim Metz in 2008 (Merola, 2008). The method is file system agnostic, meaning that it will work on any file system (FAT32, NTFS, ISO 9660, etc). An early version of this method was to search for headers and footers unique to each file type in order to determine where a certain file's data begins and ends. For example, a JPEG image file begins with the header 0xFFD8 and ends with 0xFFD9. Things again become difficult when files are fragmented, but with the advent of much larger storage media, most hardware will opt to write a file to contiguous sectors rather than fragmenting it, unless storage capacity runs low (Merola 2008). If a file is indeed fragmented, a deep knowledge of a file's internal structure helps a forensic investigator recover a file and identify where the data starts and stops. An example of this is a Windows BMP file which contains the size of the file in bytes where the footer would normally be (Pal & Memon, 2009) and Microsoft Word files include unique byte strings that contain Author, Company, Keywords, etc. and JPEG files also contain a sequence of metadata that can help with recovery. Pal & Memon (2009) also note that in cases of high fragmentation, there is also a risk that you could end up splicing multiple images together during the carving process, so it does involve some meticulous searching and trial and error.

Conclusion

The advent of file carving has provided law enforcement and technology professionals another tool they can use to recover deleted data. Although not perfect and continually refined, tools such as *Foremost, Scalpel,* and *Photorec* have made it easier than ever for files to be recovered even after deletion (Beek, 2011).

References

Merola, Antonio, (2008). Data Carving Concepts. *SANS Institute InfoSec Reading Room.* Retrieved from: https://www.sans.org/reading-room/whitepapers/forensics/data-carving-concepts-32969

Pal, A., Memon, N., (2009). The Evolution of File Carving: The benefits and problems of forensics recovery. *IEEE Signal Processing Magazine,* 59-71. Retrieved from: https://isis.poly.edu/memon/pdf/2009_file_carving.pdf

Beek, Christiaan, (2011). Introduction to File Carving. McAfee White Paper. Retrieved from: http://www.mcafee.com/us/resources/white-papers/foundstone/wp-intro-to-file-carving.pdf