Intro to File Carving

UofSC Cybersecurity Club - SWGN 2A14
April 12th, 2019 6:30 P.M.
Austin Staton

Forensics Overview

What are Forensics?

- Computer Forensics - The application of the scientific method in reconstructing a sequence of events involving computers and information.

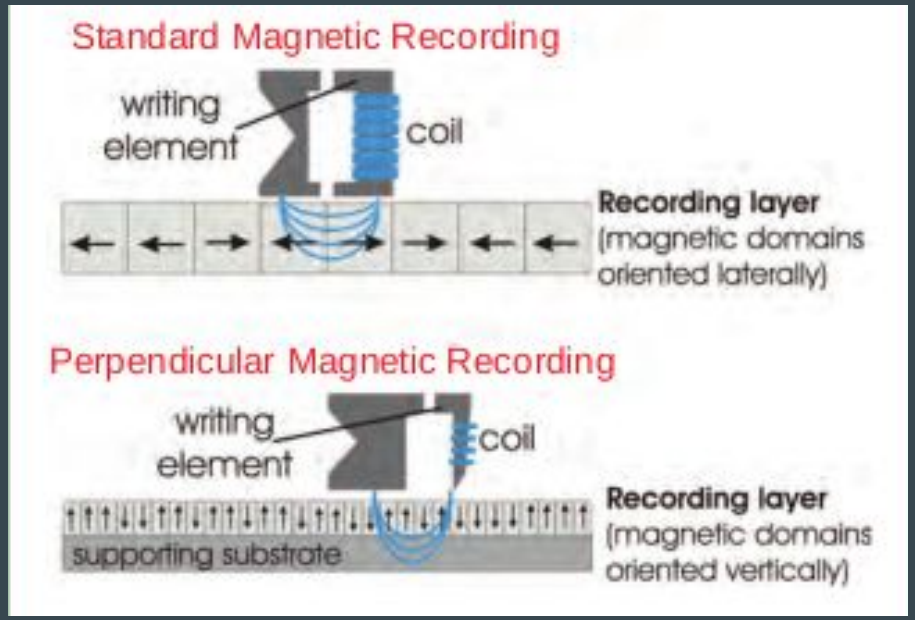
  - U.S. Naval Academy

What is a File?

“A file is a container in a computer system for storing information.”

-Techopedia

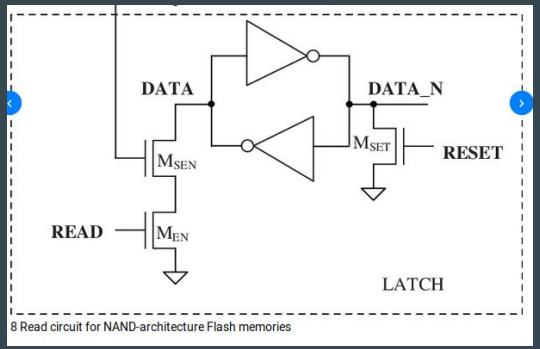
How Are Files Stored on a Disk?



When a strong magnetic field is applied across a small area of the disc, it causes the atoms in that area to align along the orientation of the field, providing the mechanism for writing bits of data onto the disc. Conversely, by detecting the aligned field, data can be read back from the disc (Ulaby).

The Case of SSDs

- SSDs store data in NAND flash (i.e. “flash memory) circuits.
- This is different from the transistors in DRAM because the NAND flash stores electrons/charge without external power supplies.
    - This means non-volatile data is stored.



8 Read circuit for NAND-architecture Flash memories

Magic Numbers

File Signatures (a.k.a. “Magic Numbers”) identify the leading, and occasionally trailing, bits of a file.

- Example:

File Type	Leading Bits	Trailing Bits
JPEG	0xFFD8FFE3	0xFFD9

https://filesignatures.net/index.php

“Deleting” Files

- Files must be overwritten to be truly deleted. Otherwise, the data remains intact, but there is no organization/structure to the data.
- Meaning, the computer recognizes the “deleted space”; but, the space is waiting to be reused.

File Carving

File Carving uses the concepts of Magic Numbers to search for patterns in bits. With the patterns, portions of data are then extracted. These portions of data are then placed in a new container, which recreates the file.

The carve does not rely on any specific file system (FAT32, ext3, ext4) to execute effectively.

Demo

We will be using a tool called “Scalpel.” This tool is a modified successor to the tool, “Foremost”, developed by the USAF Office of Special Investigations.

```
$ sudo apt-get install scalpel
```

Retrieve the disk image:

```
$ wget https://cse.sc.edu/~ajstaton/nist_docs.dd
```

Demo (cont.)

Scalpel uses a configuration file that allows users to select exactly what files they would like to have retrieved.

```
$ sudo vi /etc/scalpel/scalpel.conf
```

Once files (PDFs) have been specified, run the scalpel command on the retrieved disk image.

```
$ scalpel nist_docs.dd
```

Limitations

- By no means is File Carving a perfect plan for recovering all data from a disk. The structure of the data can be altered with:
  - Fragmented Files (moves bits to different locations)
  - Compressed Files (removes non-essential bits
  - Disk Encrption
- Identifying a source of malware on an infected machine with file carving has its risks. Ensure that you are in a secure environment.

Real-World Examples

- Osama Bin Laden's compound was raided in 2011. There were 10 HDDs, among 5 computers. Forensics were used to gain other intel.

- In 2016, Hillary Clinton's personal emails were recovered by the use of file carving.

Sources

- https://www.us-cert.gov
- HIGHLY recommend: https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l30/lec.html