DIGITAL FORENSICS

ACQUISITION

= Generally, police do not turn the device on and search it. Evidence must be acquired carefully and preserved to authenticate it.

Mirror (or "Forensic") Image = complete duplication of hard drive through the use of computer forensic tools

- Demonstrates evidence integrity by copying every bit of data — far different from merely copying files because that would miss a great deal of hidden data
- Made without turning computer on
  - Note: booting a computer up will alter data on the hard drive

AUTHENTICATE

= Part of authentication, requires the verification of mirror images

Hash algorithms - mathematical formula that provide verification of evidence accuracy, ensuring two data sets are the exact same content

- Technically, a hash function takes binary data, called the message, and produces a condensed representation, called the "message digest"
- The mathematical certitude is higher than DNA
- MD5 and SHA-1 are two of the most widely used

National Center of Justice & the Rule of Law

Source: Michael J. Hannon, DIGITAL EVIDENCE: COMPUTER FORENSICS AND LEGAL ISSUES ARISING FROM COMPUTER INVESTIGATIONS (2012)

Computer Forensic Tools

Computer forensic tools are very sophisticated programs. The major computer forensic software programs contain a suite of tools to facilitate different aspects of data recovery, sorting, interpreting, organizing, and reporting. EnCase by Guidance Software and Forensic Toolkit (FTK) by Access Data are two of the most widely used programs.

File Recovery

What happens when a file is deleted?

When a file is deleted on a computer, the operating system essentially masks the file from being recognized by the computer user or the operating system. The file system also marks as "unallocated" the cluster or clusters in which this deleted file is stored so that they are now available to store a new file. Until a new file overwrites the "deleted" file in these unallocated clusters it can be recovered easily with computer forensic tools.

How is a file completely overwritten?

Files that have been completely overwritten with new files are not recoverable. This can be achieved through the operation of file wiping software, but the efficacy of these programs is subject to some debate. It can also be achieved through regular computer usage. How soon deleted files are overwritten by subsequent usage varies based on several factors including how often the computer is used, especially to store new files.

It is important to note that computer forensic tools can identify if file wiping software was used.

How is file slack created?

File slack occurs when a deleted file is partially overwritten by a smaller file. The part of the deleted file not overwritten now resides in file slack. But file slack is actually not in unallocated clusters. This part of the file (the file slack) is recoverable with computer forensic tools. File slack is also called drive slack, slack space, or just slack.

The recoverable information consists of fragments of the previous file and its value would of course depend on what was found.