Evaluating Deleted File Recovery Tools on NIST Standards

Quinton Currier

1 Introduction

The National Institute of Standards and Technology (NIST) has a subdivision named the Computer Forensics Tool Testing Program (CFTT). The CFTT has standards regarding digital forensic tools to help determine the quality and integrity of these tools. The integrity of such tools is important in many cases such as corporate, security, and especially in judicial proceedings. Using a software that does not follow these standards has the potential to recover files incorrectly, corrupted, or mislabeled, which has the potential to throw out evidence in court cases that are increasingly reliable on digital data. On the other hand, incorrectly recovered files can also lead to jail sentence of innocent defendants. One important task in digital forensics is deleted file recovery (DFR), which is the focus of our proposed research. CFTT standards for DFR tools consists of 4 core features and a set of *optional* features. We have already done a few preliminary experiments with the popular digital forensics tool Autopsy (The SluethKit), which shows importance of a similar study in a bigger scale.

2 Research Topic

Define what does a deleted file recovery tool do. I am interested in investigating which software meet the standards set by CFTT. There are many companies and individuals marketing their software as the best recovery tool. My research question encompasses this software as well to test their effectiveness at recovering files compared to a standard for enterprise level tools. I aim to use Autopsy as a base comparison to the other software and what they can do. The question also expands to the different types of file systems. While there are 3 operating systems that have different file systems, there are even more file systems that each store data and meta data differently. Looking out for Type I and Type II errors are also a large part of evaluating each software. Many other factors also play a part, including the condition of the filesystem (is it full, was the tool installed after the file was deleted, etc.) and how the file was deleted (Recycle bin, permanent delete, reformat of disk etc.). All of these additional variables can be tested and compared, especially using the optional requirements of the CFTT to create a comprehensive comparison for readers at both the consumer and student levels.

3 Description

3.1 Motivation

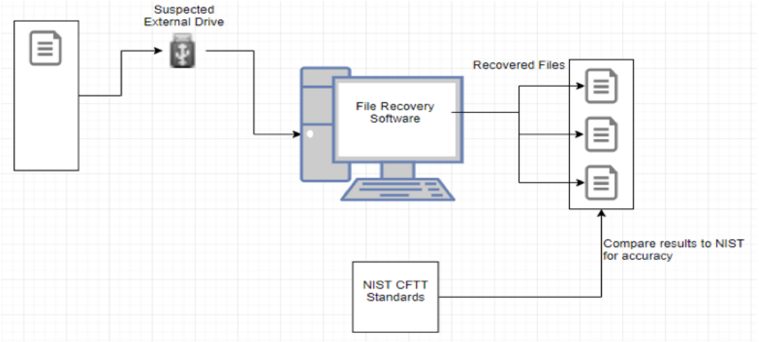
As an example, many arrests and court cases hinge on the finding of recovered files like the infamous Craigslist Killer. Data from deleted files can prove ones innocence or guilt just as much as DNA proof can. Information like created times, who wrote the file, and even past versions can make or break a case for law enforcement. Having knowledge of which software will perform best for each instance can save a lot of time for investigators to find the guilty party.

3.2 Preliminary Findings

I have already done a set of experiments with Autopsy tool against the CFTT Core standards with one filesystem. This experiment showed it is possible to replicate the same process multiple time for each software to test. This experiment also showed the value of changing the complexity of how the files were deleted. Sometimes a new file can overwrite the desired deleted file, and it has to be pieced back together.

3.3 Testing Plans

My desktop is powerful enough (i7 8700k CPU, 32GB RAM, GTX 1060 GPU) to run multiple instances of virtual machines that I can test with multiple Operating Systems(Windows, Mac and Linux). Using these virtual machines, I can also test multiple file types (Pictures, Word Docs, PDFs, etc.). See Figure**??** below for diagram of testing setup.



I plan to test with popular free and paid versions of popular open source and enterprise file recovery software to show if the open source maintains the same standards This can also help future students in understanding the difference in capabilities that different software has. Some example software that I plan to use are Recuva, PhotoRec, Magnet Axiom, FTK or EnCase, SR: We should select two free (autopsy and something) and two enterprise (magnet and ftk). QC: Removed some tools and left open for more if I have the time and others as possible. By testing multiple tools on multiple operating systems, it will give a universal resource for others to understand the various software capabilities and restrictions.

3.4 Reporting

The CFTT already has a few published reports of different file recovery software. However, they should be expanded and retested to ensure their reliability is consistent as new patches and features come out for file recovery tools. By adding new reports to the website that other researchers can test and confirm will allow developers a chance to continually develop their tool for the better.

4 Anticipated Outcomes

I anticipate the free consumer tools will not meet as many standards compared to the professional or more complex software because the time and effort developing them. Each software I will be testing is unique in their own way, but when providing a use to recover a deleted file, the CFTT Standards act as a guideline to what the software should retrieve. I estimate that while there are more tools for windows file systems, the ones developed primarily for Linux will have the most versatility and highest passing mark for recovering files.SR: We also aim to find out possible underlying causes of failure of a tool in a scenario, which can lead to better design of future tools.

I aim to turn this research into a published paper with the assistance of Professor Roy if I am able to discover enough information about the various tools. I am hoping that this will inspire future readers to test different software for themselves and show the importance of having a standard that can be used to *grade* a software. As students look more and more into file recovery, relating software back to which standards they pass will help students understand why the standards are important and what can happen to deleted files if they do not pass.