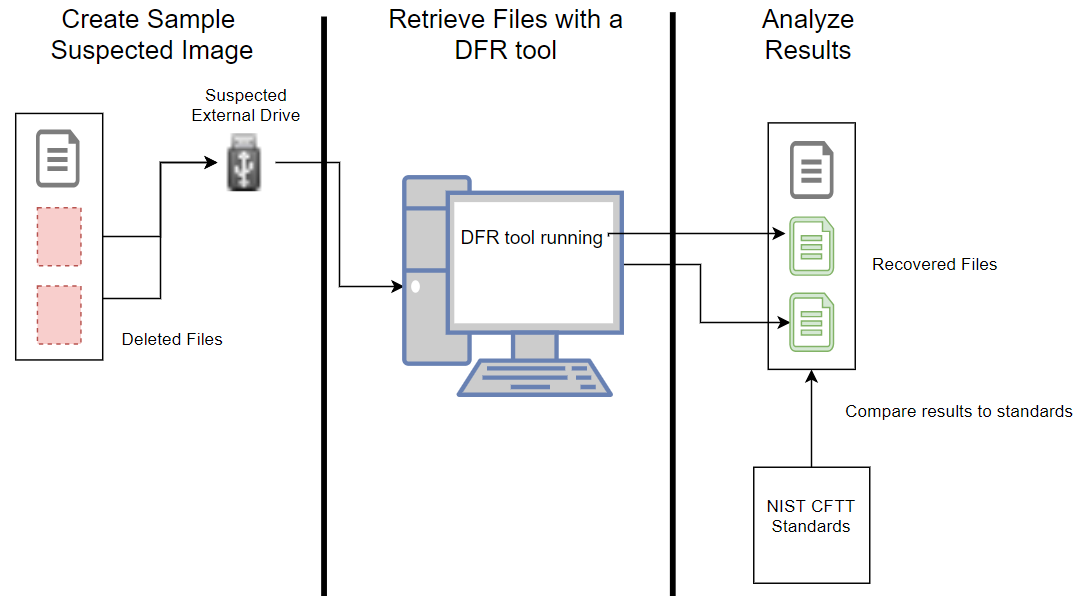
**Background**

Digital forensic tools are used for post-mortem investigation of cyber-crimes and cyber-attacks both in corporate and government organizations. National Institute of Standards and Technology (NIST)’s Computer Forensics Tool Testing Program (CFTT) established standards for digital forensic tools to help determine the quality and integrity of such tools. The quality and integrity of these tools are especially important in judicial proceedings. Using a forensic tool that does not follow the standards may cause evidence to be thrown out in court cases (which are increasingly reliant on digital data). Consequently, incorrect results from a forensic tool can also lead improper prosecution of an innocent defendant. The focus of our proposed research is about standardization of one class of forensic tools that are for Deleted File Recovery (DFR). The CFTT standard for DFR tools consists of four *core* features and a set of *optional* features

**Research question**

****A DFR tool is a software that can retrieve (residual data of) a file that was deleted from a storage device (e.g., computer hard disk, flash drive, and more). We plan to investigate a set of popular DFR tools to find which of these tools meet the standard set by CFTT. There are many companies and individuals marketing their software as the best recovery tool. As one task we will test the free tools’ effectiveness at recovering files compared to that of enterprise-level tools. Identifying if there are any errors for such as not recovering a deleted file or attempting to recover a file that was never there is also an important metric for a DFR tool (*Type I* and *Type II* errors). Type I and Type II errors of a tool can relate it to the standard.

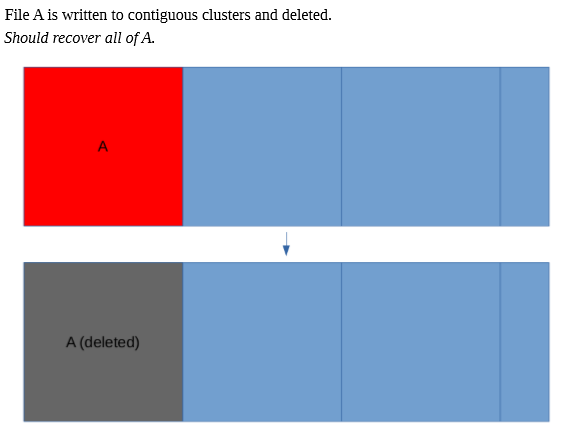
**Process**

We used the following process to create the cases into images that can be used against the softwares to get results and compare them.

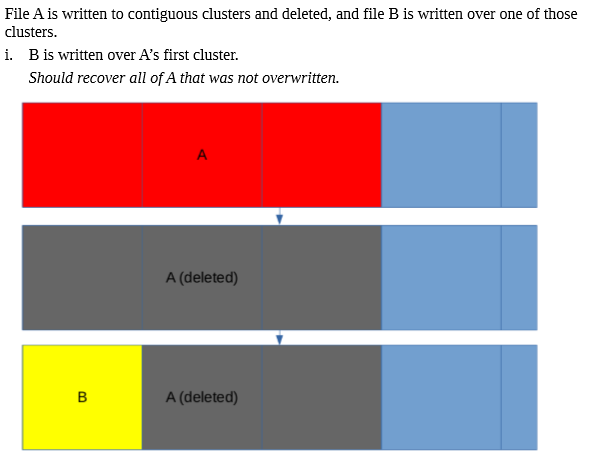
1. Use standard files (size and contents) to fill up flash drive with scenario
   1. Files were created in 1 Megabyte (MB) block sizes unless specified otherwise
2. Delete appropriate files that we are testing to be found
3. Create image of drive using dd tool in Linux
4. Mount image in Linux for DFR software to recognize and run against  
   **OR**
5. Use the image file directly in the DFR software
6. Export results and upload to GitHub for team
7. Analyze results compared to expected

We created the cases with different scenarios in mind and possibilities of users deleting data. All diagrams can be found on attached PDF or at <https://github.com/quintoc/CURS-DFR-Research/blob/master/docs/test_cases.pdf>. For a few examples of very common instances:

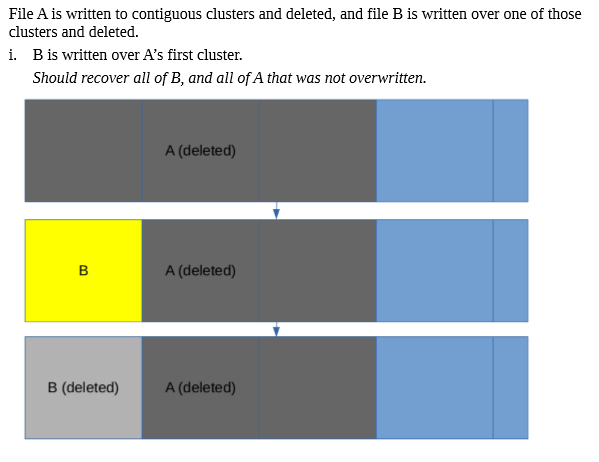
Case 1 (Data is deleted):



Case 4i (Data is deleted and overwritten in hopes of not being found):



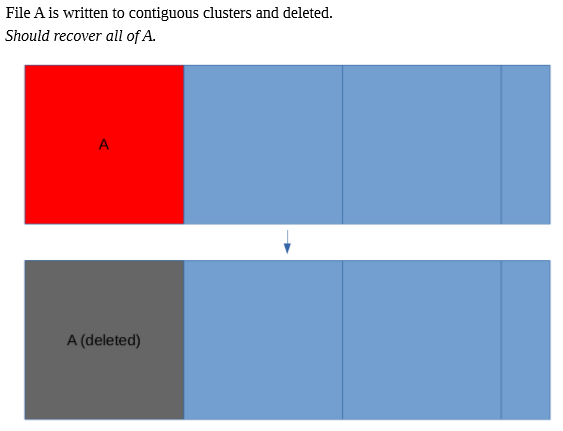
Case 5i (Data is deleted and overwritten and deleted again in hopes of only the most recently deleted data is retrieved):



**Results**

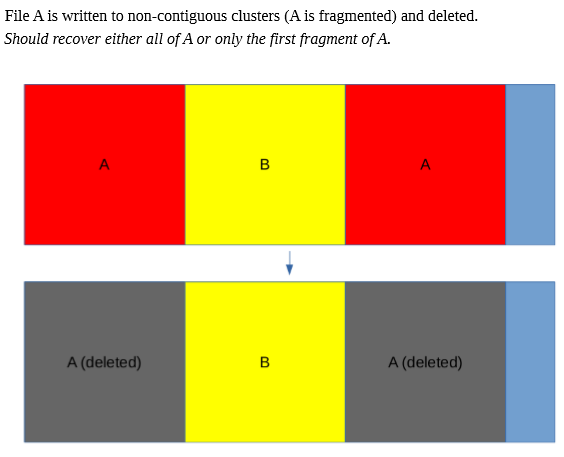
**FAT**

Case 1:



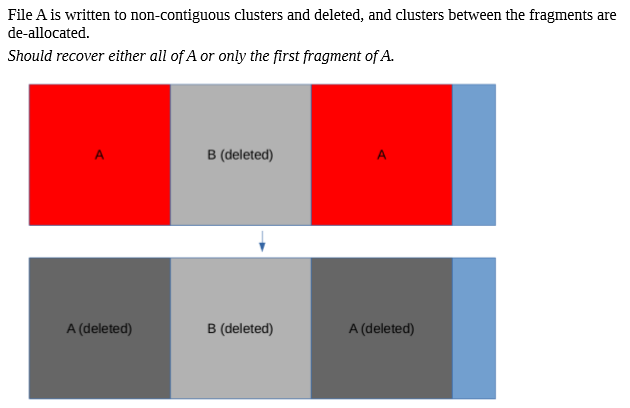
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 1 Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered A | Recovered A | Recovered A | Recovered A | Recovered A | Recovered A |

Case 2:



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 2 Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered all of A | Recovered all of A | Recovered first half of A | Recovered first half of A and seconds half of B | Recovered first half of A and seconds half of B | Recovered all of A |

Case 3:



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 3 Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered first half of A and second half of B | Recovered first half of A and second half of B | Recovered first half of A and second half of B | Recovered first half of A and second half of B | Recovered first half of A and second half of B | Recovered first half of A and second half of B |
| Recovered B (separate file) | Recovered B (separate file) | Recovered B (separate file) | Recovered B (separate file) | Recovered B (separate file) | Recovered B (separate file) |

Case 4i:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 4i Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered 2kb of file B | Recovered 2kb of file B | Empty file (0 Bytes) | Recovered size of A, but data was B and then zero’s | Recovered size of A, but data was B and then zero’s | Recovered B and last portion of A |

Case 4ii:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 4ii Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered 2kb of zero’s | Recovered 2kb of zero’s | Recovered 1MB of A | Recovered 1MB of A, 1MB of B, then 1MB of Zero’s | Recovered 1MB of A, 1MB of B, then 1MB of Zero’s | Recovered 1MB of A, then 2MB of zero’s |

Case 4iii:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 4iii Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered 2kb of B | Recovered 2kb of B | Recovered 0kb file | Recovered B, 1 kb of zeros and 1kb of A | Recovered B, 1 kb of zeros and 1kb of A | Recovered B, 1 kb of zeros and 1kb of A |

Case 4iv:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 4iv Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered 2kb of B | Recovered 2kb of B | Recovered 0kb file of A | Recovered B | Recovered B | Recovered B |

Cave 5i:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 5i Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered B and rest of A | Recovered B and rest of A | Recovered B and rest of A | Recovered B and rest of A | Recovered B and rest of A | Recovered B and rest of A |
| Recovered B | Recovered B | Recovered B | Recovered B | Recovered B | Recovered B |

Case 5ii:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 5ii Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered B in the middle of A | Recovered B in the middle of A | Recovered B in the middle of A | Recovered B in the middle of A | Recovered B in the middle of A | Recovered B in the middle of A |
| Recovered B | Recovered B | Recovered B | Recovered B | Recovered B | Recovered B |

Case 5iii:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 5iii Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered B, 1kb of zeros, and 1kb of A | Recovered B, 1kb of zeros, and 1kb of A | Recovered B, 1kb of zeros, and 1kb of A | Recovered B, 1kb of zeros, and 1kb of A | Recovered B, 1kb of zeros, and 1kb of A | Recovered B, 1kb of zeros, and 1kb of A |
| Recovered B | Recovered B | Recovered B | Recovered B | Recovered B | Recovered B |

Case 5iv:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 5iv Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered B as A | Recovered B as A | Recovered B as A | Recovered B as A | Recovered B as A | Recovered B as A |
| Recovered B (separate file) | Recovered B (separate file) | Recovered B (separate file) | Recovered B (separate file) | Recovered B (separate file) | Recovered B (separate file) |

Case 6:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 6 Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered 2kb file of zeros | Recovered 2kb file of zeros | Recovered first half of A | Recovered first half of A, and B as 2nd half | Recovered first half of A, and B as 2nd half | Recovered first half of A, then 1MB of zeros |

Case 7:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 7 Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered first half of A, and C | Recovered first half of A, and C | Recovered first half of A | Recovered all of A \*\*\*\* | Recovered first half of A, and B | Recovered first half of A, and C |
| Recovered C | Recovered C | Recovered C | Recovered C | Recovered C | Recovered C |

Case 8:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 8 Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered 2kb of zeros in A’s name | Recovered 2kb of zeros in A’s name | Recovered first half of A | \*\*\*  Recovered B and C | Recovered half of A and 52kb of zeros | Recovered half of A and 4kb of zeros |

Case 9:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 9 Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered 2kb of zeros in A’s name | Recovered 2kb of zeros in A’s name | Recovered first half of A | \*\*\*  Recovered B and C | Recovered half of A and 52kb of zeros | \*\*\*  Recovered C |

Case 10:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Case 10 Results | | | | | |
| Autopsy (Linux) | Autopsy (Windows) | FTK Imager | Magnet Axiom | Recuva | TestDisk |
| Recovered 2kb of zeros in A’s name | Recovered 2kb of zeros in A’s name | Recovered first half of A | \*\*\*  Recovered C | Recovered half of A and 52kb of zeros | Recovered half of A and 4kb of zeros |
| Recovered B | Recovered B | Recovered B | Recovered B | Recovered B | Recovered B |

Case1: aa1m  
Case2: aa2m **or** first half of aa2m  
Case3: bb1m **and** aa2m **or** first half of aa2m  
Case4i: aa3m that was not overwritten  
Case4ii: aa3m that was not overwritten  
Case4iii: aa3m that was not overwritten  
Case4iv: nothing  
Case5i: bb1m **and** aa3m that was not overwritten  
Case5ii: bb1m **and** aa3m that was not overwritten  
Case5iii: bb1m **and** aa3m that was not overwritten  
Case5iv: bb3m **only**  
Case6: First fragment of aa3m  
Case7: cc1m **and** first fragment of aa3m  
Case8: aa1m **or** first fragment of aa1m  
Case9: aa1m **or** first fragment of aa1m  
Case10: bb1m **and** aa1m **or** first fragment of aa1m

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| FAT Test Results | | | | | | | |
| Tool | Case 1 | Case 2 | Case 3 | Case 4i | Case 4ii | Case 4iii | Case 4iv |
| Autopsy (Linux) |  |  |  |  |  |  |  |
| Autopsy (Windows) |  |  |  |  |  |  |  |
| FTK Imager |  |  |  |  |  |  |  |
| Magnet Axiom |  |  |  |  |  |  |  |
| Recuva |  |  |  |  |  |  |  |
| Testdisk |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FAT Test Results | | | | | | | | | |
| Tool | Case 5i | Case 5ii | Case 5iii | Case 5iv | Case 6 | Case 7 | Case 8 | Case 9 | Case 10 |
| Autopsy (Linux) |  |  |  |  |  |  |  |  |  |
| Autopsy (Windows) |  |  |  |  |  |  |  |  |  |
| FTK Imager |  |  |  |  |  |  |  |  |  |
| Magnet Axiom |  |  |  |  |  |  |  |  |  |
| Recuva |  |  |  |  |  |  |  |  |  |
| Testdisk |  |  |  |  |  |  |  |  |  |

**Larger picture**