Andrew Meyer
DFR project weeks 9-10

What I have done:

- Prepared 11 NTFS images
  - cases 1, 2, 3, 4i, 4iii, 4iv, 5i, 5iii, 5iv, 6, 7
- Completed tests on Autopsy for Linux
- Added miscellaneous documentation and notes

What remains to be done:

- Running tests
  - FAT
    - TestDisk
    - FTK
    - Magnet Axiom
  - NTFS
    - Autopsy Windows (partial)
    - Recuva (partial)
    - TestDisk
    - FTK
    - Magnet Axiom

- Documents for CURS (**Due August 24**)
  - Project Report
  - Project Reflections
  - PowerPoint Presentation
  - Financial Disclosure Statement

Notes:

NTFS MFT entries behave similarly to FAT directory entries, they are not removed upon file deletion but are reallocated on a “first-available” basis.

We found the main weakness of the DFR tools tested is dealing with cases where files were overwritten. In particular, when a file is written over the beginning of a deleted one, the tool should recognize that those clusters are allocated, and thus no longer part of the deleted file. Both TSK/Autopsy and Recuva fail in this case, for both FAT and NTFS. The FAT case in particular causes strange behavior; TSK recovers only a single cluster (from the overwritten file), while Recuva recovers only the overwritten clusters and appends for the length of the deleted file.

The primary difference between TSK/Autopsy and Recuva is that TSK in some FAT cases can reason about the allocated clusters between fragments of a deleted file, and skip them when recovering a fragmented file, while Recuva assumes no fragmentation and blindly recovers the length of the deleted file.

Due to the “best fit” file allocation algorithm in NTFS, cases 4ii and 5ii seem impossible to occur through normal file operations, so we will not create them. The technique that created them in FAT depends on the “next fit” algorithm.

Due to the way fragmentation is handled in NTFS, we decided cases 8, 9, and 10 would not test anything that the other fragmentation cases didn’t also cover, so they do not need NTFS equivalents.

Magnet Axiom apparently cannot recover files with no file extension, so we had to remake the test images, adding a .txt extension to every file.