Andrew Meyer
DFR project report week 8

What I have done:

- Continued studying NTFS
- Fixed my Autopsy installation problems on Linux
- Familiarized myself with relevant Windows command line utilities for creating the test cases

Work for next week:

- Begin creating NTFS images
- Run FAT tests for Autopsy Linux version and (testdisk or easeUs)

Alternatives to PhotoRec: **TestDisk** or **easeUs**

- TestDisk is free and open source, easeUs is freeware/freemium
- As far as I can tell, TestDisk is more popular or at least better known, and supports more platforms.
  - TestDisk has a Wikipedia page
  - alternativeto.net has TestDisk as the second most popular alternative to easeUs (after recuva), while easeUs is far lower on other DFR tools' pages.
- I couldn't tell from easeUs's website if it is metadata based or file-carving based.

I recommend we go with TestDisk as it is companion software to PhotoRec, probably better known than easeUs, and gives us a better balance of free vs proprietary tools: 2 free and open source (Autopsy, TestDisk), 1 freemium (Recuva), 2 proprietary (FTK, Magnet Axiom).

Useful commands for creating test images on Windows:

format
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/format
format X: /fs:NTFS /v:CASE_X /p:1
(formats drive X as NTFS with label CASE_X after zeroing over every sector once)

sync
part of MS sysinternals, installed from https://docs.microsoft.com/en-us/sysinternals/downloads/sync
equivalent of unix/linux *sync*, flushes write buffers to the disk

type
equivalent of unix/linux *cat*, passes contents of a file to standard output

mountvol
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/mountvol
probably unnecessary to ever remount volumes as NTFS (according to Carrier) uses best-fit allocation algorithm, so there's no "last written" pointer to reset

copy

del