Jasper Tenga
Report for 10-31-19

Things that have been done:

- Created test cases in FAT file system for the test images shown below:

Goals for the next week:

- Create test cases with different file types (e.g. pdf, docs)
- Use the proprietary tools to test the test cases.

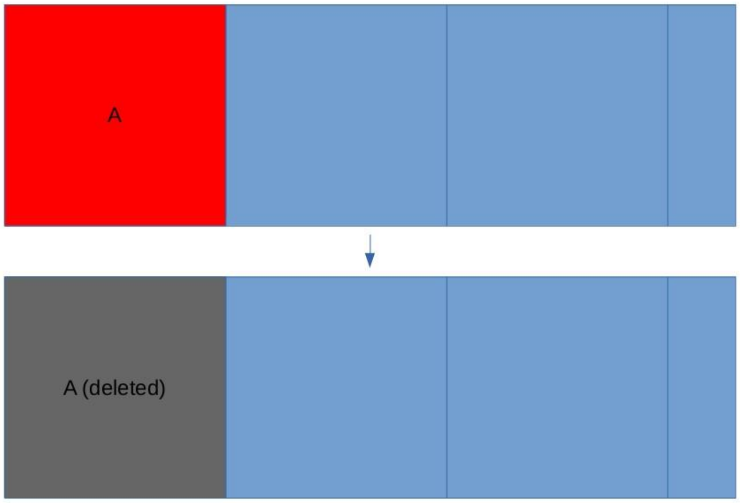
Thoughts/Concerns:

- Whether file carving would work as well with NTFS file system. Tried the first test case (the simplest test scenario) and Photorec (file carving tool) was not able to return file A. This is a concern since if the simplest test case is not retrieved, the complex ones will not.

FAT test cases:

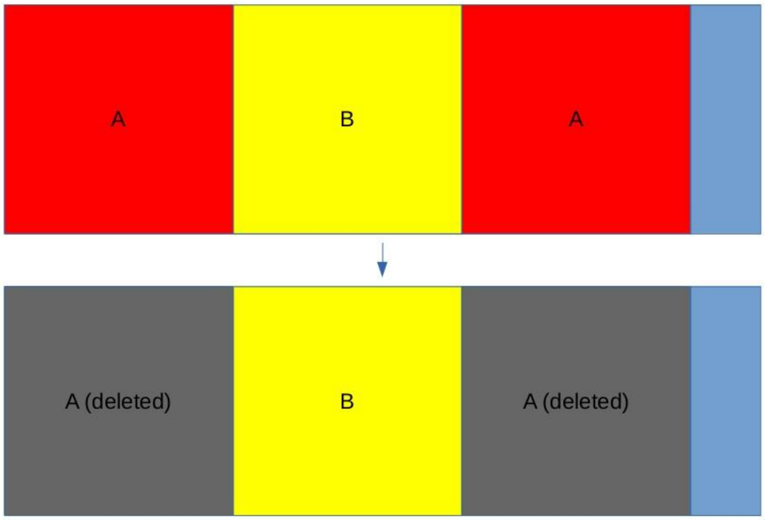
1. File A is written to contiguous clusters and deleted.
    1. Write file A
    2. Delete file A

    Should recover all of A.



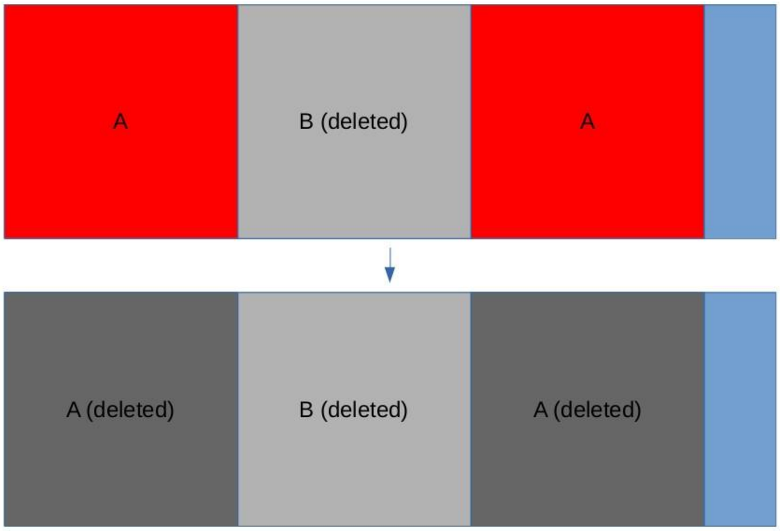
2. File A is written to non-contiguous clusters (A is fragmented) and deleted.
    1. Write file C
    2. Write file B
    3. Delete C
    4. Write and Fragment file A
    5. Delete file A

    Should recover all of A.



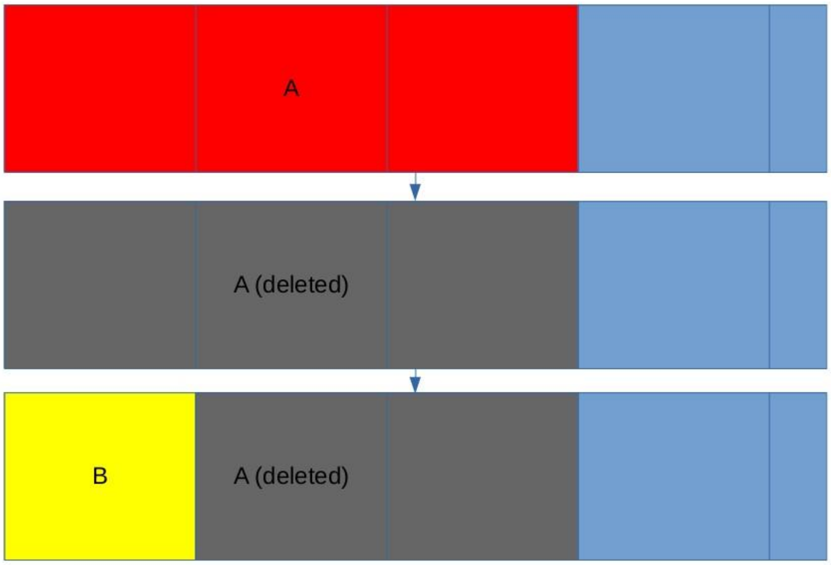
3. File A is written to non-contiguous clusters and deleted, and clusters between the fragments are de-allocated.
    1. Create drive 2
    2. Delete file B

    Should recover all of A.



4. File A is written to contiguous clusters and deleted, and file B is written over one of those clusters.
    1. Write file A
    2. Delete file A
    3. Write file B

    Should not recover A.

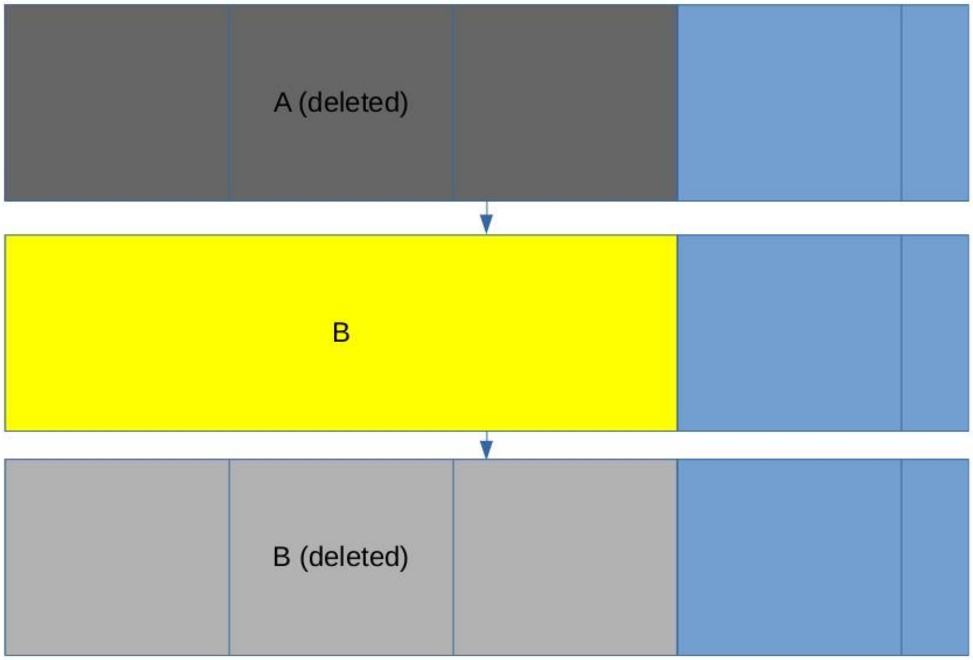


5. File A is written in continuous clusters and deleted, and file B is written over file A and is deleted.

File A is a pdf and file B is jpeg

1. Write file A
2. Delete file A
3. Write file B
4. Delete file B

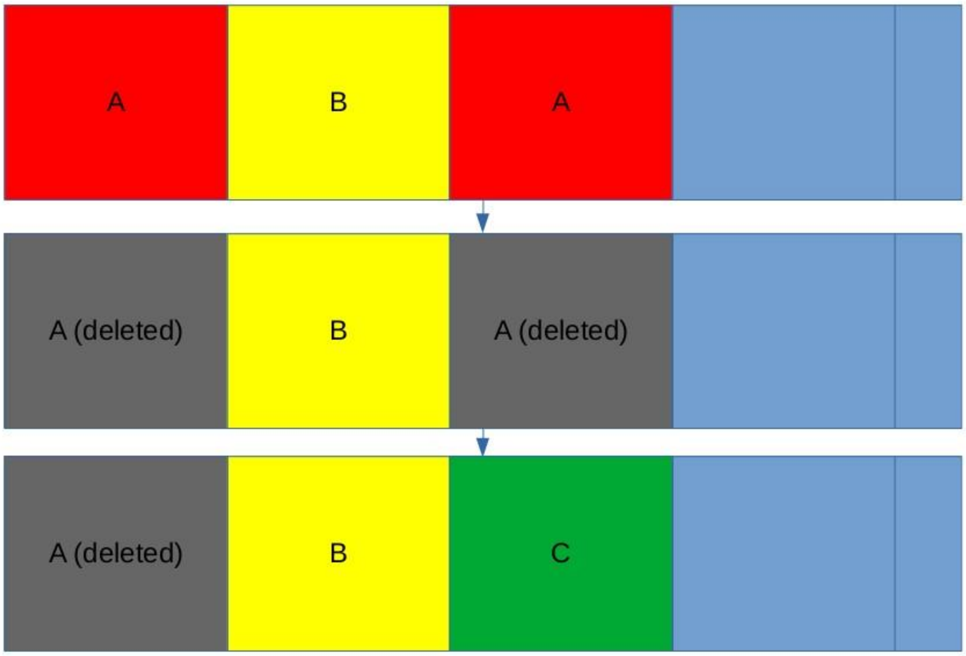
Should recover B without A contents.



6. File A is written to discontinuous clusters and deleted, and file C is written over the second fragment.

    1. Create drive 2
    2. Write file C.

       Should not recover A.



Test procedure:

Command line tools from the Virtual Machine (VM) were used to create the images in order to make it easier to reproduce the test cases. Kali linux was the Operating System used to perform the test cases.

Test case 5 used a pdf file filled with 1.2 MB of character ‘a’.

1. Partition USB drive **(host or guest OS)**

   gdisk was used to create 10MiB partitions.

The following are similar commands used in creating test images. (Test case 1 example).

2. Zero over partition (**host or guest OS)**

   dd if=/dev/zero of=/dev/sdb1

3. Unmount file system (**guest OS**)

   umount /dev/sdb1

4. Write file system **(guest OS)**

   mkfs.fat -n “CASE_1” /dev/sdb1

5. Mount file system **(guest OS)**

   ```
   mount /dev/sdb1 /mnt
   ```

6. Write and delete files **(guest OS)**

   ```
   cp test_files/pic1.jpg /mnt
   sync
   rm /mnt/pic1.jpg
   ```

7. Unmount file system **(guest OS)**

   ```
   umount /mnt
   ```

8. Make image of file system **(host OS)**

   ```
   dd if=/dev/sdb1 of=.../case_1.raw
   ```

9. Inspect the file system image to make the result is as expected. (To view raw image use hexedit or similar tool.)