Jasper Tenga Report for 10-13-19

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 in NTFS file system
* Create test cases with different file types (e.g. pdf, docs)

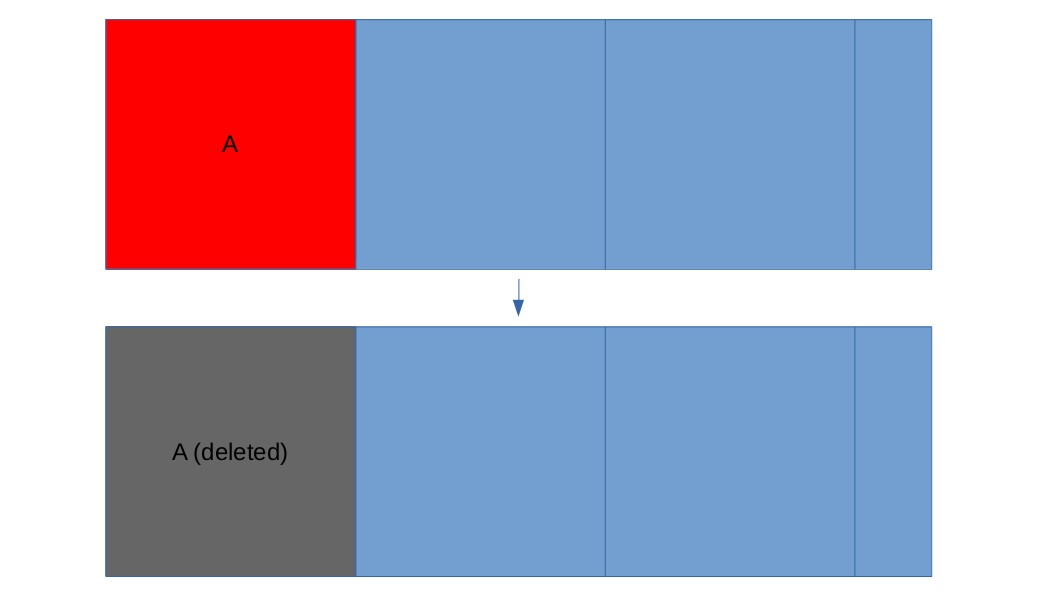
Thoughts/Concerns:

* Before adding file C after file B in test case 6i and 6ii, I had to write file D and delete it immediately before it is written in memory in order to make sure it was not written at the unallocated memory space that file A was. The concern was if it was written in memory.

**FAT test cases:**

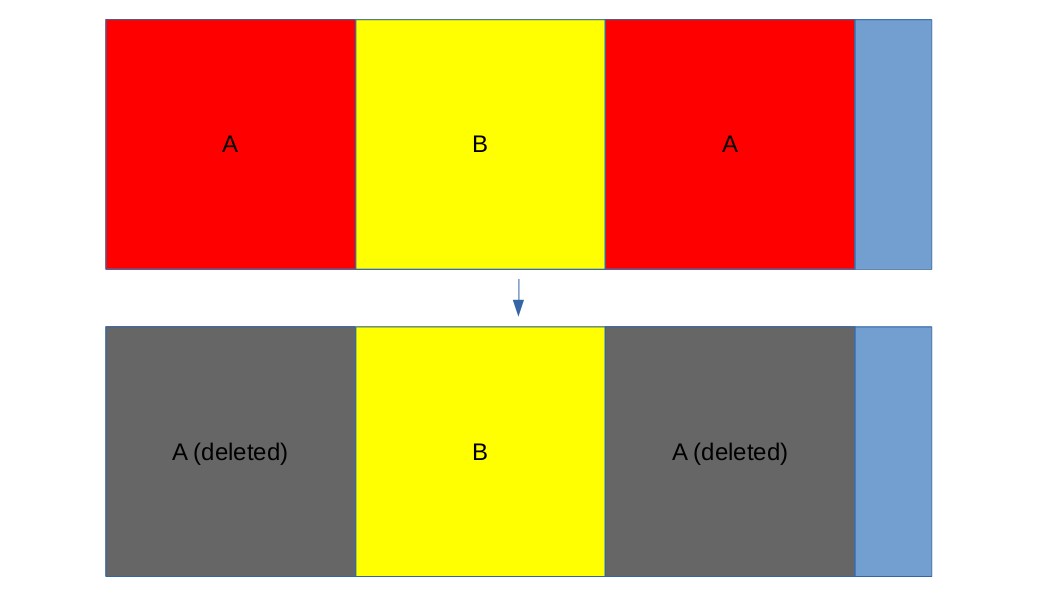
1. File A is written to contiguous clusters and deleted.
   * 1. Write file A
     2. Delete file A

*Should recover all of A.*



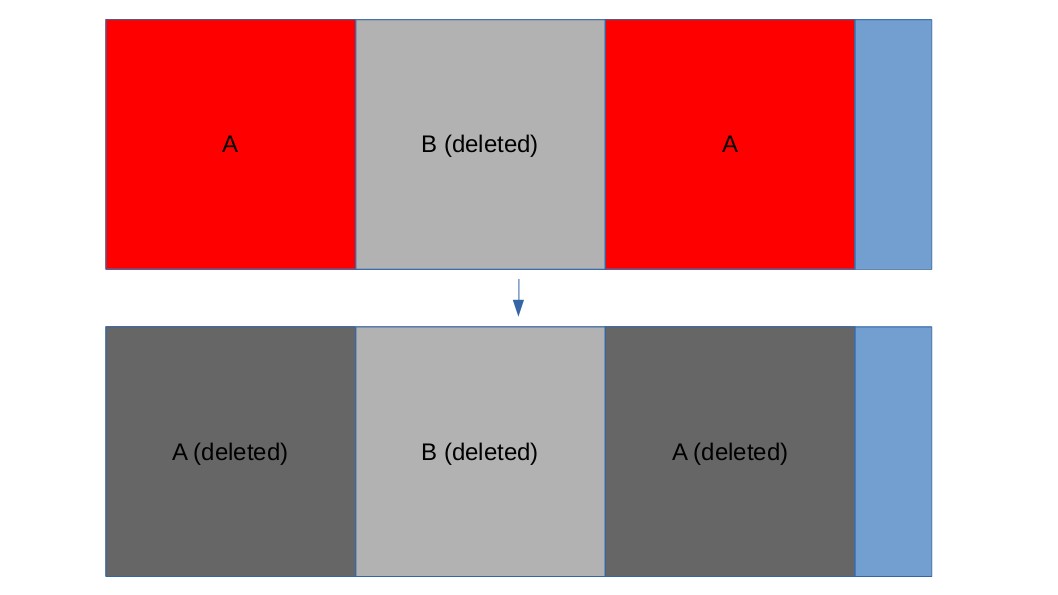
1. File A is written to non-contiguous clusters (A is fragmented) and deleted.
   * 1. Write file C
     2. Write file B
     3. Delete C
     4. Write and Fragment file A
     5. Delete file A

*Should recover either all of A or only the first fragment of A.*



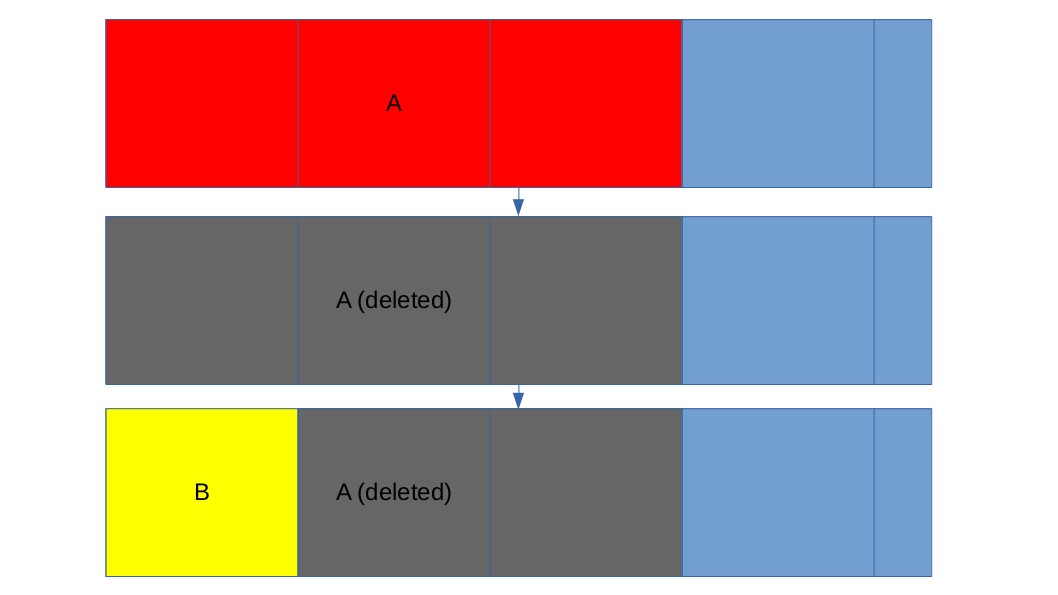
1. File A is written to non-contiguous clusters and deleted, and clusters between the fragments are de-allocated.
   1. Create drive 2
   2. Delete file B

*Should recover either all of A or only the first fragment of A.*



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

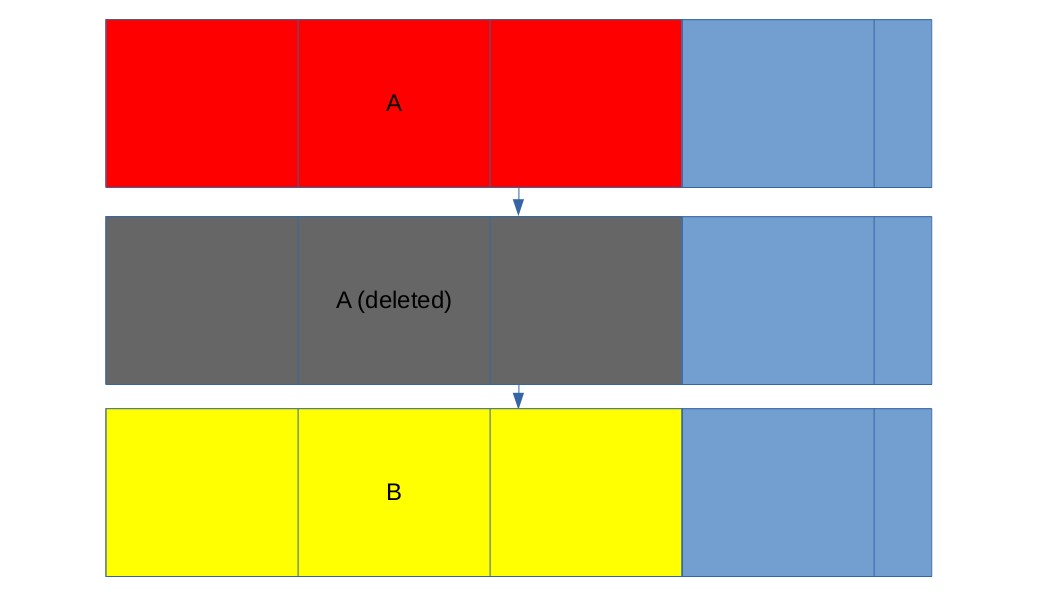
*Should recover all of A that was not overwritten.*



ii. B completely overwrites A.

* + 1. Write file A
    2. Delete file A
    3. Write file B

*Should recover nothing.*



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

1. File A and B are jpeg

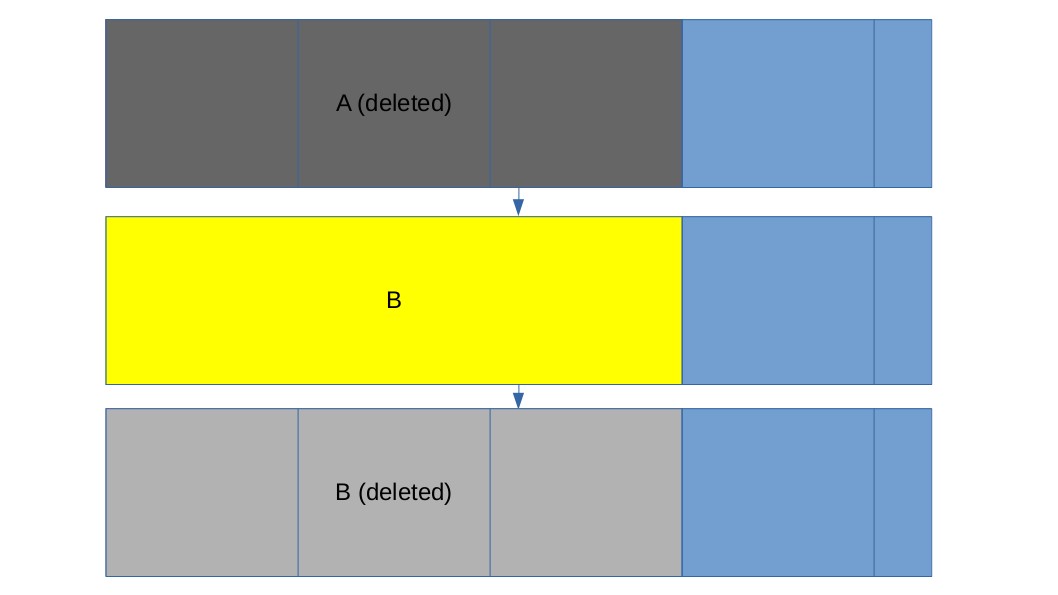
1. Write file A

2. Delete file A

3. Write file B

4. Delete file B

*Should recover file B*



1. File A is a pdf and file B is jpeg

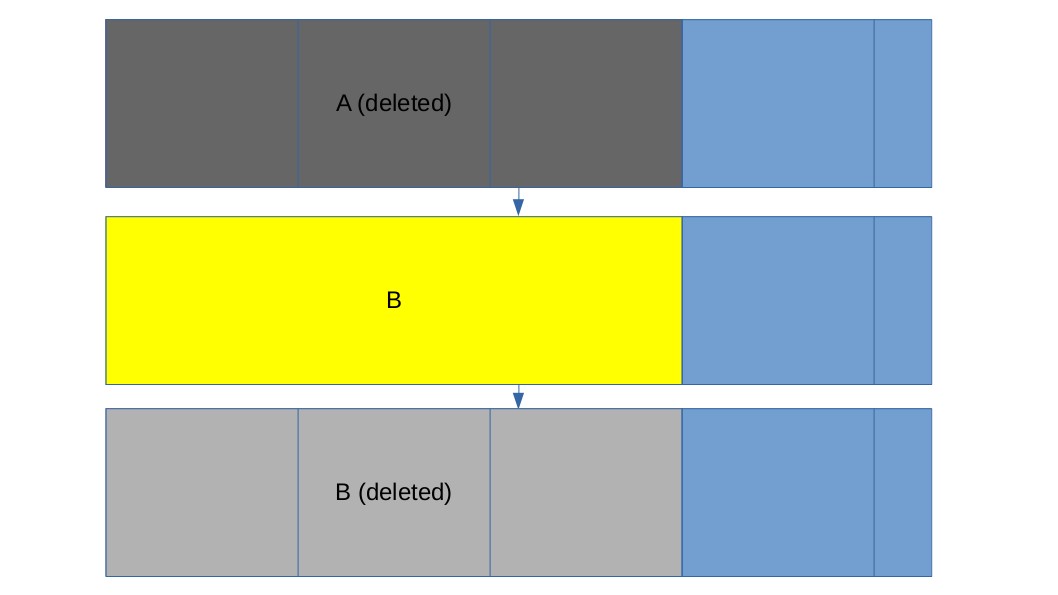
1. Write file A

2. Delete file A

3. Write file B

4. Delete file B

*Should recover B without A contents.*

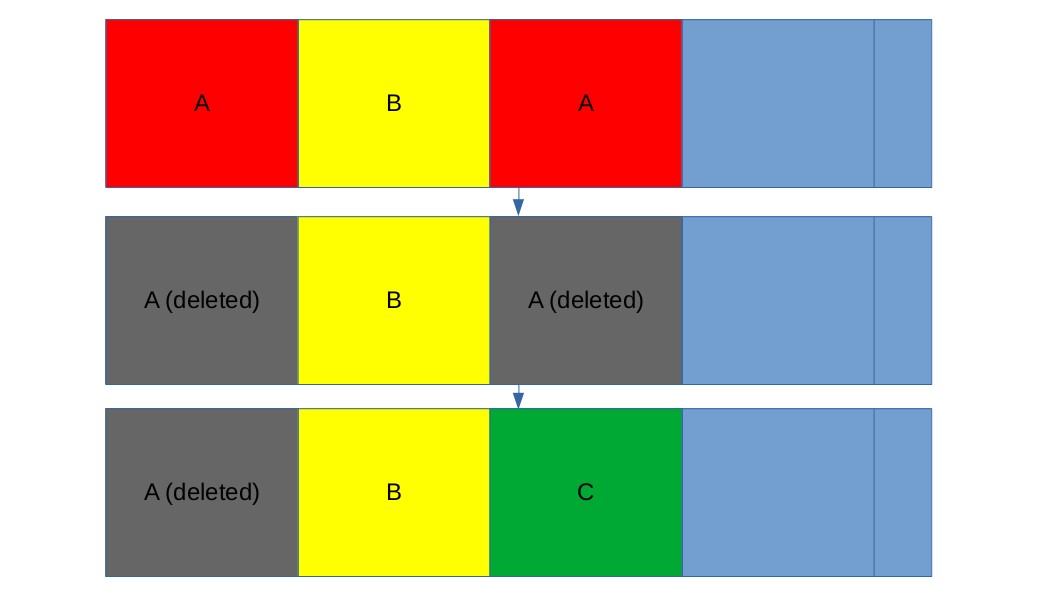


6. File A is written to discontinuous clusters and deleted, and file C is written over the second fragment.

i. File C is not deleted

* 1. Create drive 2
  2. Write file C*.*

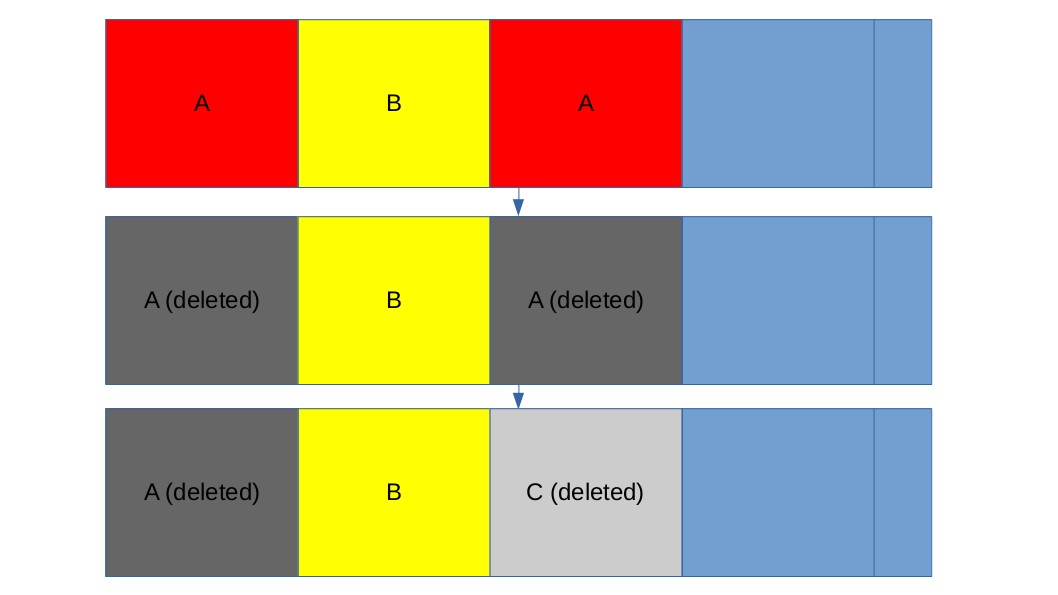
*Should recover first fragment of file A*



ii. File C is deleted.

* + 1. Create drive 6
    2. Delete file C

*Should recover first fragment of 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 5ii 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).

1. Zero over partition (**host or guest OS)** *dd if=/dev/zero of=/dev/sdb1*
2. Unmount file system (**guest OS**) *umount /dev/sdb1*
3. Write file system **(guest OS)** *mkfs.fat -n “CASE\_1” /dev/sdb1*
4. Mount file system **(guest OS)** *mount /dev/sdb1 /mnt*
5. Write and delete files **(guest OS)**

*cp test\_files/pic1.jpg /mnt sync rm /mnt/pic1.jpg*

1. Unmount file system **(guest OS)** *umount /mnt*
2. Make image of file system **(host OS)** *dd if=/dev/sdb1 of=.../case\_1.raw*
3. Inspect the file system image to make the result is as expected. (To view raw image use hexedit or similar tool.)