What happened when we create a file

- Each file has data stored in **blocks, inodes and directory entries**
  - A free inode is chosen from inode bitmap
  - The superblock free-inode values are decremented
  - Add an entry in the parent directory
  - Fill in the inode contents
  - Choose a free data block from data bitmap to contain the file contents

How files are deleted…

- http://www.porcupine.org/forensics/forensic-discovery/chapter4.html
- When the link-count in the inode reaches zero (0):
  - The Data blocks in the Block Bitmap are marked as free
  - The inode in the Inode Bitmap is marked as free
  - The deletion time is set in the inode.
  - The directory entry is invalidated.

What happens when a file is deleted in ext3/ext4?

- The file size in the inode is set to zero.
- The data blocks info in the inode is cleared.
- http://linux.sys-con.com/node/117909
- An analysis of Ext4 for digital forensics, Kevin Fairbanks, 2012, http://www.dfrws.org/2012/proceedings/DFRWS2012-p13.pdf

Why do I care about deletion?

- Data still exists on disk
  - Fully recoverable until space is overwritten
  - Larger disks less likely to overwrite formerly-used space
- Therefore, you can (usually) recover deleted files
  - Unless the disk blocks are “wiped” before the file is deleted (e.g. “srm” or “shred”) (dd if=/dev/zero or /dev/random)