Disk Recovery and Forensics

Who doesn't love the word "Forensics"? It's a word that brings out the inner geek in all of us, yet the reality is usually pretty grim – like when your only hard drive containing all your important files and photos fails.

The first thing you should do if you suspect your hard drive is failing or has failed is not attempt to write to it and if necessary hard shut the machine down asap by pushing and holding the power button on your PC. Any further writes could lunch the drive for good making recovery impossible. In otherwords STOPPP!!

Anyway, here's some notes from recent tinkerings with Ubuntu Rescue Remix (Google it, Download it). It's a bootable Live CD which boots a computer into a command line only Linux environment, and for the remaining 2% who are still reading, provides you with a good handful of tools that stand you the best chance of recovering data from a failing hard disk.

Assuming you've just booted it and your hard disk(s) are attached, the first thing to do is identify which disk corresponds to which device name in /dev. This can be done using lshw or fdisk -l

lshw > /tmp/hardware

cat /tmp/hardware | less

The next step is to clone the dodgy disk to either another disk, or to an image file or both. You choose.

ddrescue /dev/sda /dev/sdc

or (restartable clone to an image file)

ddrescue –direct –retrim –max-retries=3 /dev/sda imagefile logfile

If you've cloned to another healthy disk, then you should fsck /dev/sdc to fix any errors, then attempt to mount it with mount /dev/sdc1 /mnt/mydisk and see if you can read any data on it. You may be as good as done at this point with no further need to go on to employing other more targeted tools for recovering data off an unmountable drive. Failing that, try to stay calm (really – it helps), clone the disk to an imagefile the best you can, then read on. If you can't stay calm, then run testdisk and benefit from a more intuitive menu driven interface of various recovery options.

testdisk

Or if you're enjoying this new found challenge of getting the photos back before the missus finds out, read on about using foremost and other similar, powerful recovery commands.

sudo foremost -i imagefile -o /recovery/foremost -w
(list recoverable files only)

sudo foremost -i imagefile -o /recovery/foremost -t jpg (recover jpg files only)

If you suspect that the partitioning information on the drive is gone, then you can replace it using gpart to guess what the previous partitioning scheme was based upon whats on the drive. This is good if you're an overzealous techy who blanked the drive to install the latest OS without thinking about who else had an account on the computer and what they may have had stored. Not good. Don't do it again.

sudo gpart /dev/sda

Or instead of using foremost, you could try scalpel. Like foremost, but configurable and well, a bit better.

vi /etc/scalpel/scalpel.conf (to configure options)

sudo scalpel imagefile -o /recovery/scalpel/

Or maybe try magicrescue on the cloned disk if there's multiple file types to be recovered (requires the presence of recipes for the filetypes to be recovered).

/usr/share/magicrescue/recipes

Enable DMA on the cloned disk first to speed things up.

hdparm -d 1 -c 1 -u 1 /dev/hdc

sudo magicrescue -r gzip -r png -d /recovery/magicrescue /dev/sdc

If it's specificly photos you're wanting to recover, then there are two tools to choose from; photorec and recoverjpeg.

sudo photorec imagefile (imagefile is the disk imagefile, not an image as in picture)

sudo recoverjpeg /dev/sdc1 (recovers any obvious jpeg files on partition /dev/sdc1)

If the files you want to recover were deleted on the original drive, then assuming the drive has come from a windows computer and was formatted with NTFS, then you can use ntfsundelete to recover the deleted files.

ntfsundelete -s /dev/sdc1 (scans for inodes of deleted files which can be subsequently recovered)

ntfsundelete /dev/sdc1 -u -i 3689 -o work.doc -d /recovered/ntfsundelete

If you want to recover old files previously written to a disk containing a new FAT filesystem, then you're into using autopsy and dls, fls, icat and sorter from sleuthkit to create a secondary image of unallocated blocks contained in the image and list the inodes of files apparently contained within them, recover those files and optionally sort them by filetype, respectively.

sudo autopsy -d /media/disk/autopsy 192.168.0.1 (use your local ip address)

dls imagefile > imagefile_deletedblocks (create secondary, smaller imagefile)

fls imagefile_deletedblocks -r -f fat -i raw (list inode numbers of any deleted files found)

icat -r -f fat -i raw imagefile_deletedblocks inode_number > myfile.doc (recover a file)

sudo sorter -h -s -i raw -f fat -d out -C /usr/share/sleuthkit/windows.sort /imagefile

This just touches upon ways you can recover lost data, with a few useful examples, but remember each command in it’s own right has a multitude of options which can be perused using the man command and reading the accompanying manual. You can also google *man sorter* for example, and read the man page in a web browser. I hope you get some data back!