Windows Disk Image

- Assumes basic setup from setup
- All command below should be
  - copied to a “IR log” text/md file
  - edited as needed
  - executed with output copied back to “IR log”
    - recommendation: move commands/output from “useless commands” to second “IR dump” text/md file
- ## is a placeholder for a number

setup

```
echo 'source $HOME/.case.env' >> ~/.bashrc
```

Env variables

```
pwd
WD=/case/working/folder && echo 'WD=$WD' >> ~/.case.env
E=/case/working/folder/evidence/evidence.E01 && echo 'E=$E' >> ~/.case.env
```

Disk Image

```
mmls -r $E
sudo -E ~/.local/bin/imount -p -o ## $E
# -p has 'pretty' & predictable folder name, fails if in use
# new tab or crtl-z
DISK_C=<imount_dir> & echo 'DISK_C=$DISK_C' >> ~/.case.env
```

Extended disk image anaylsis

```
fsstat -o <offset> $E
istat -o <offset> $E 5 # root node
istat -o <offset> $E <inode from fsstat>

fls -o <offset> -m C: -r $E > data/bodyfile
mactime -b data/bodyfile -d -z UTC yyyy-mm-ddThh:mm:ss >
output/disk_timeline.csv

mactime -b data/bodyfile -d -z UTC yyyy-mm-ddThh:mm:ss..yyyy-mm-dd >
output/disk_timeline.csv
```