

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 ## $E  
# -p has 'pretty' & predictable folder name, fails if in use  
# new tab or ctrl-z  
DISK_C=<imount_dir> & echo 'DISK_C=$DISK_C' >> ~/.case.env
```

Extended disk image analysis

```
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  
TZ=UTC mactime -b data/bodyfile -d > output/disk_timeline.csv
```