JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

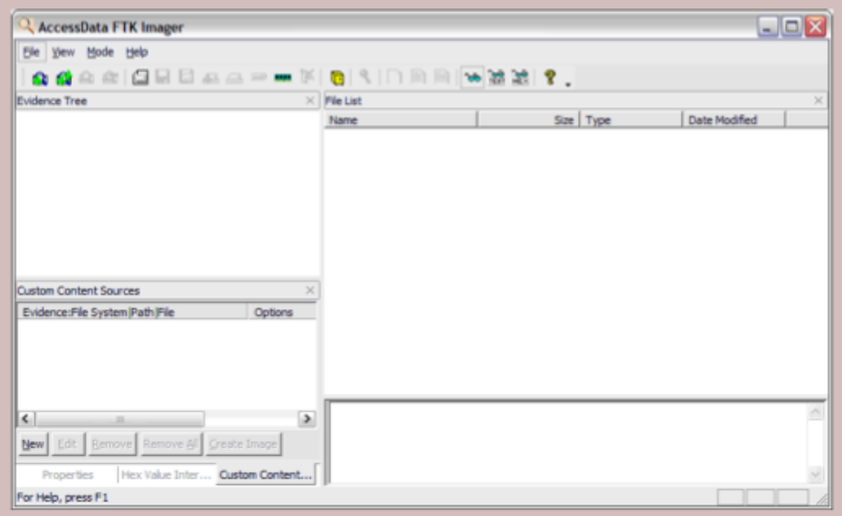
Disk Imaging

CYBER INCIDENT RESPONSE

Imaging Media and Drives

- Bit by bit copy of a drive, including the slack space and unallocated space

- FTK Imager
- EnCase Imager
- dd



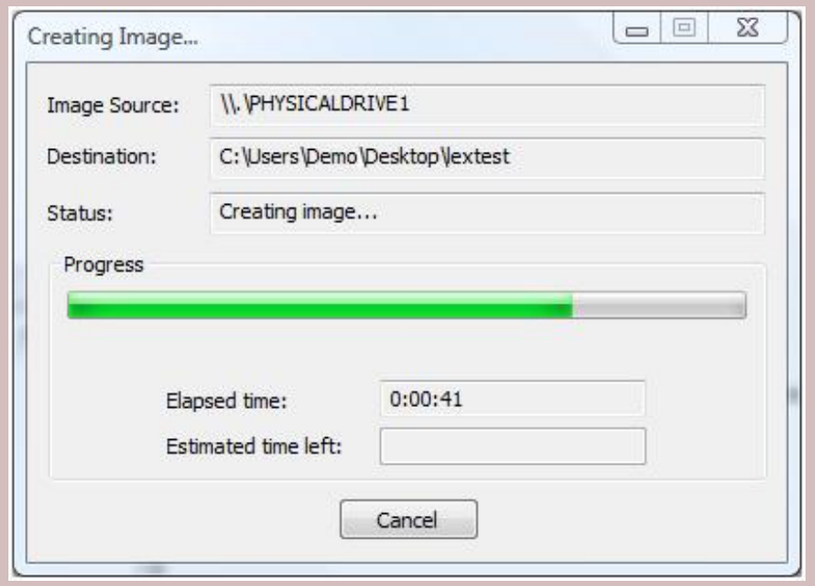
dd

- Standard Linux and UNIX tool
- Can clones drives using bit-by-bit copy

```
# dd bs-64k if=/dev/disk1/sda1 of=/mnt/usb1/sda1.img
```


FTK Imager

- Commercial product that is free to use
- Documents chain of custody, adds hash, and creates metadata tags for later analysis

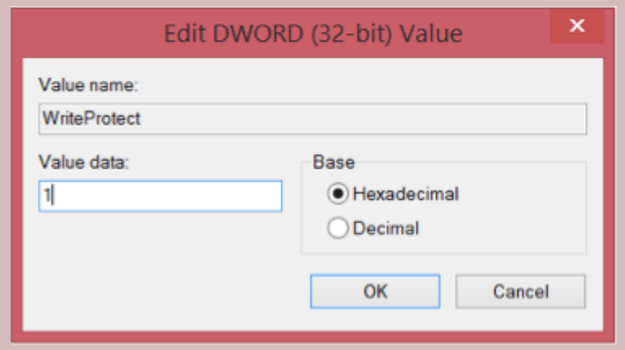


Forensic Drive Duplicators

- Very expensive, dedicated devices
- Creates images, hashes, and chain of custody metadata

Write Blockers

- Maintain data integrity on the source disk
- Hardware write blockers should be used for best forensic integrity



Encrypted Drives

- Try to find the password because brute forcing is VERY slow (if possible)
- Capture the computer while logged in to bypass drive encryption when possible