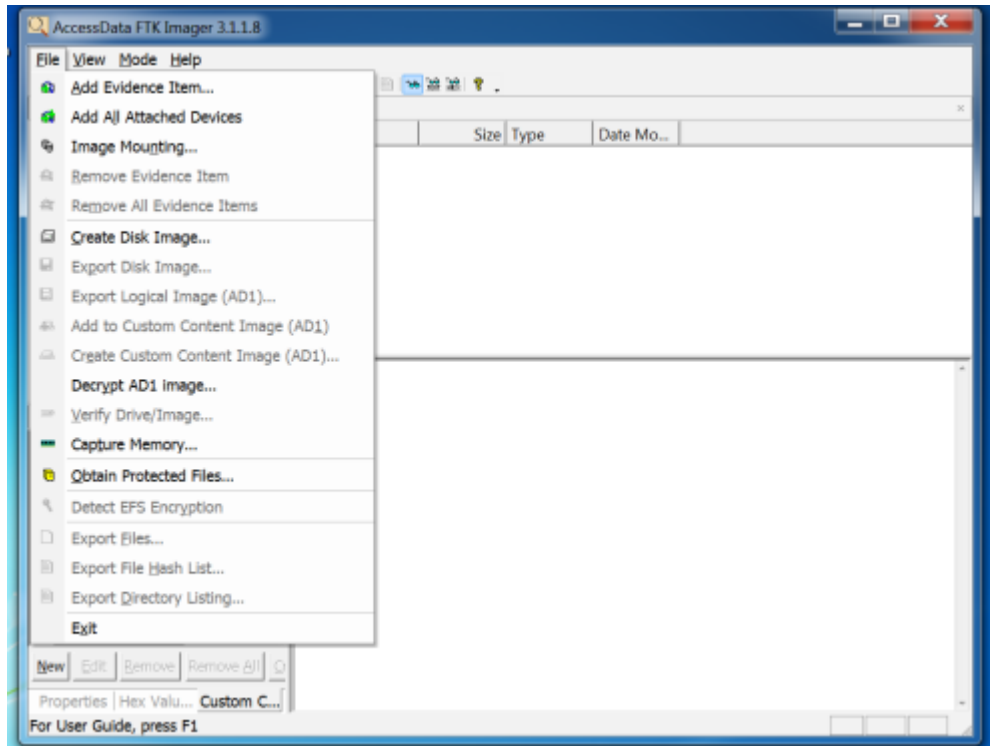
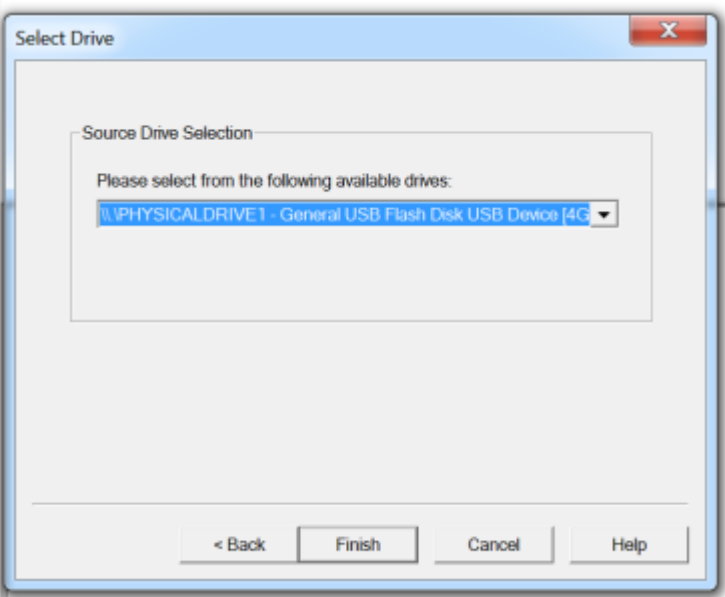
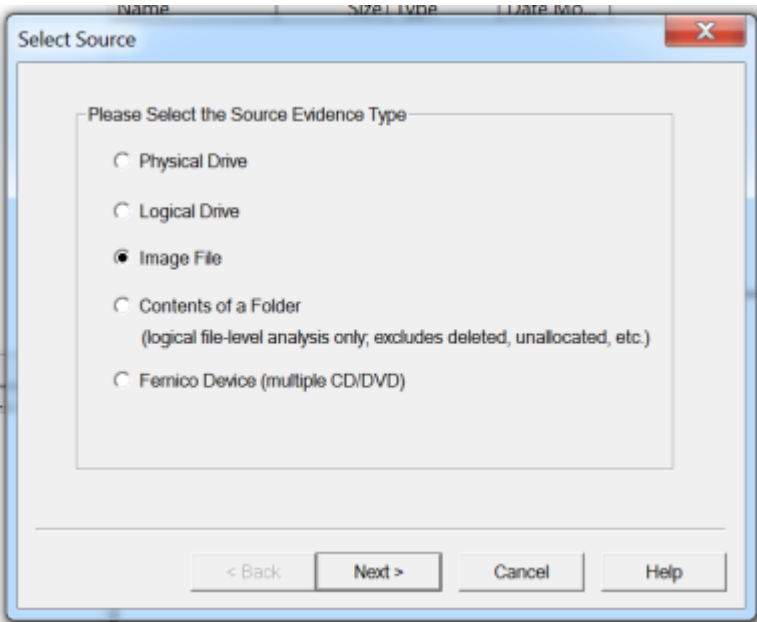


FTK Imager Exercise

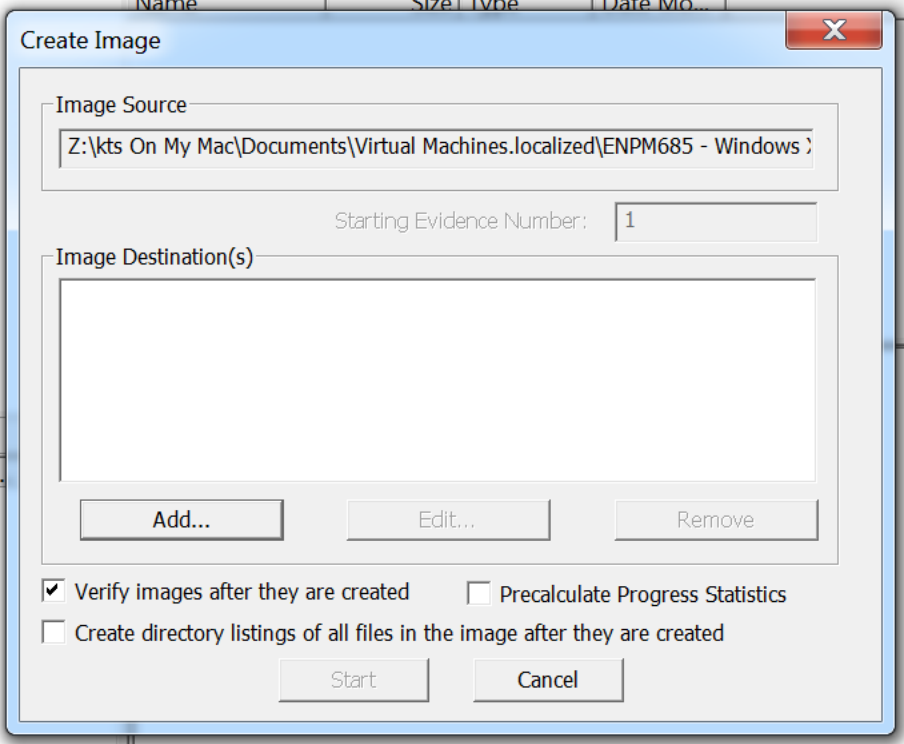
0. Download FTK Image Lite from <http://accessdata.com/product-download/ftk-imager-lite-version-3.1.1>
1. Unzip FTK Image ZIP file
2. File -> **Create Disk Image...**



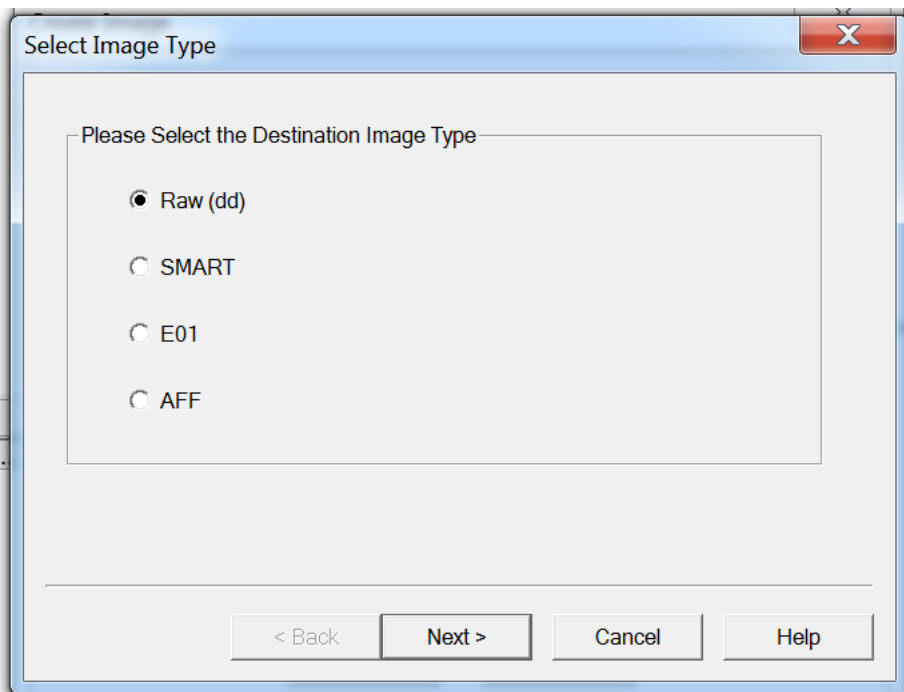
3. Select the source type
 - Physical Drive if doing a USB key, physical/VM drive
 - Image file if imaging the VMware .vmdk file



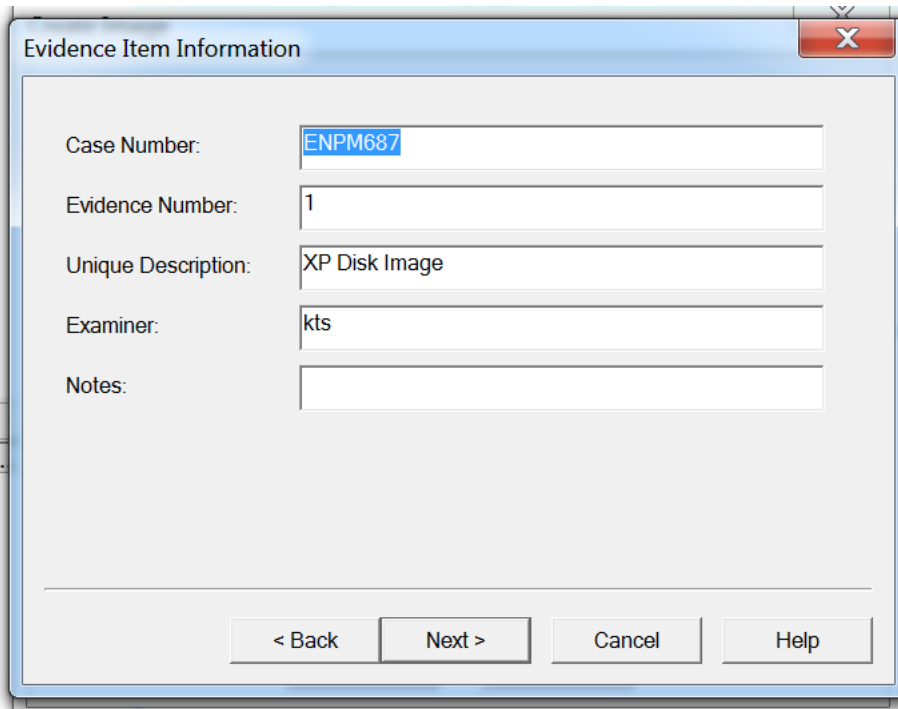
4. Click **Add...** and select a folder location to save output



5. Select the format. I'd recommend **Raw (dd)** or **E01**



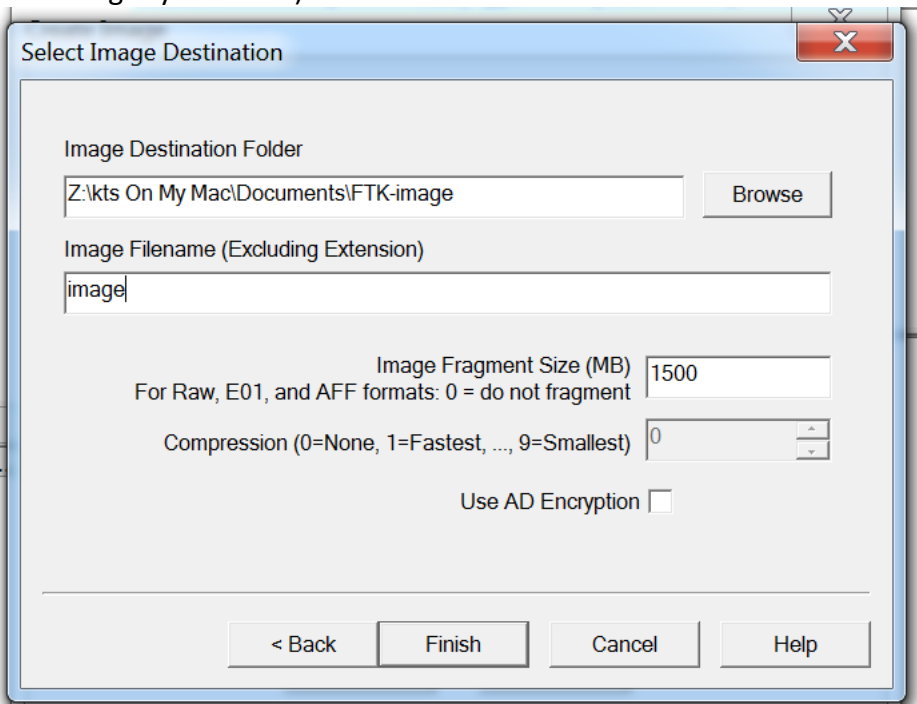
6. Enter case Information



The 'Evidence Item Information' dialog box contains the following fields and controls:

- Case Number: ENPM687
- Evidence Number: 1
- Unique Description: XP Disk Image
- Examiner: kts
- Notes: (empty text area)
- Navigation buttons: < Back, Next >, Cancel, Help

7. Select destination folder. I'd recommend the "shared" drive of your host system to save on space. (Computer -> "Shared Folder \\vmware-host Z:" on my VM, your may be slightly different)



The 'Select Image Destination' dialog box contains the following fields and controls:

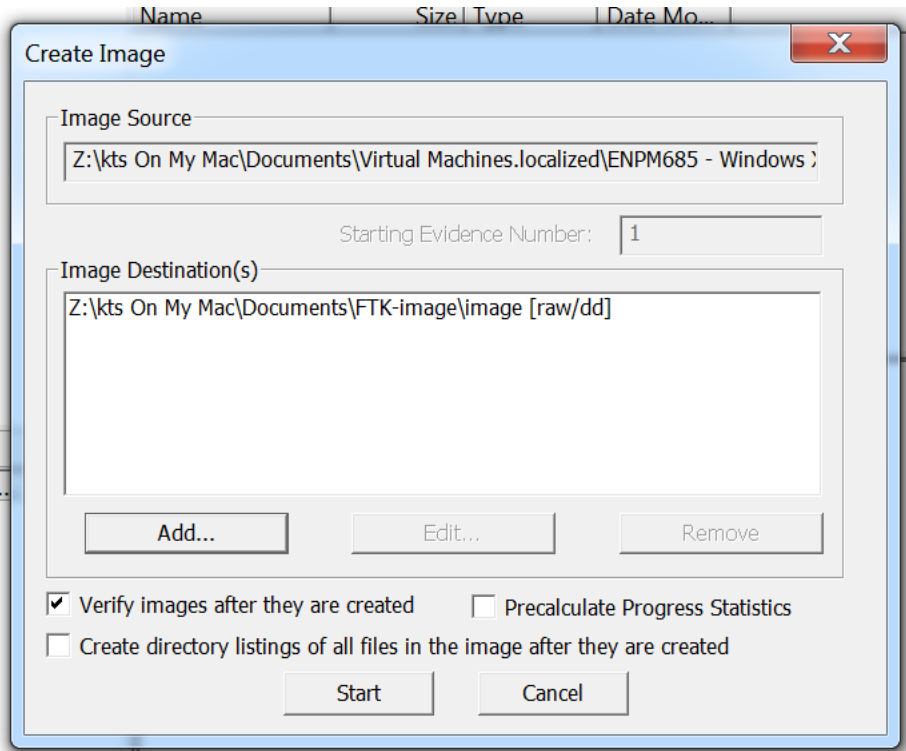
- Image Destination Folder: Z:\kts On My Mac\Documents\FTK-image (with a Browse button)
- Image Filename (Excluding Extension): image
- Image Fragment Size (MB): 1500 (with a note: For Raw, E01, and AFF formats: 0 = do not fragment)
- Compression (0=None, 1=Fastest, ..., 9=Smallest): 0
- Use AD Encryption: ☐
- Navigation buttons: < Back, Finish, Cancel, Help

8. Give a file image name (ex: usbkey)

9. Select the Image size if you want. 1.5GB is standard, for smaller images may make sense to keep as a single image vs splitting.

10. Select Finish

11. Click Start.



You'll see a progress bar and when it finishes you'll get a window with the status of the image along with the hash values

