Memory and Disk Imaging Lab

FOR-100

Insert Name Here

Insert Date Here

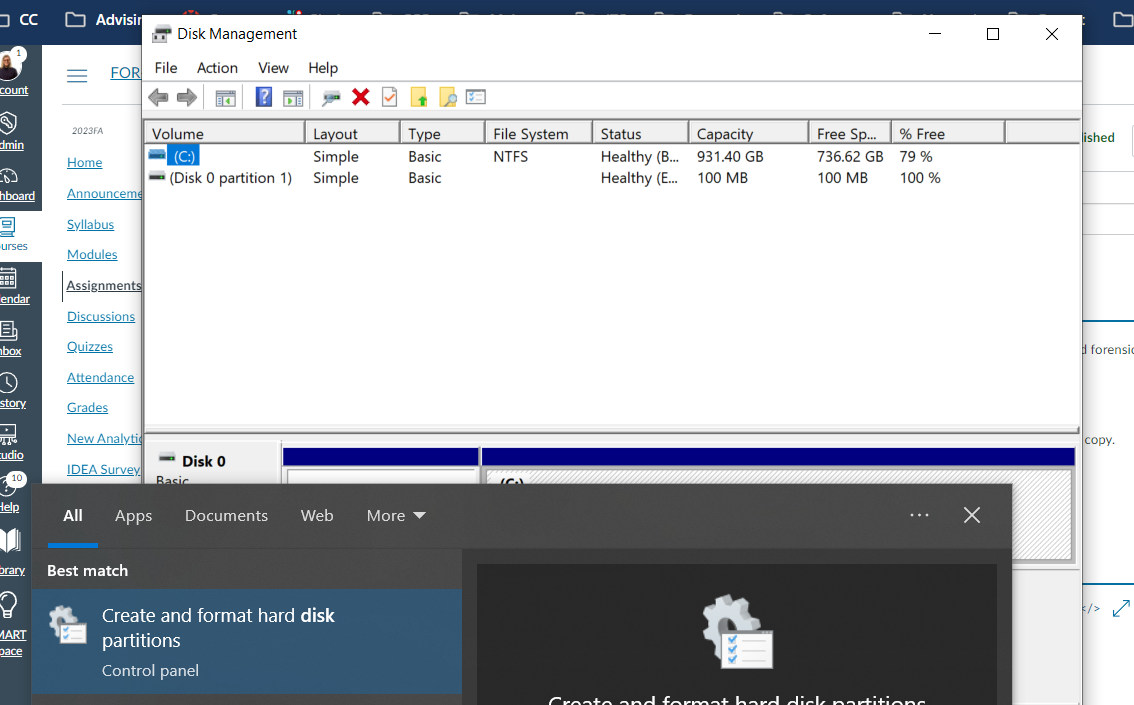
**Task**

You have been tasked to perform a forensic acquisition from a single volume contained on a hard disk provided to you by your client. Your boss and forensic lead in the lab has given you the following specific instructions.

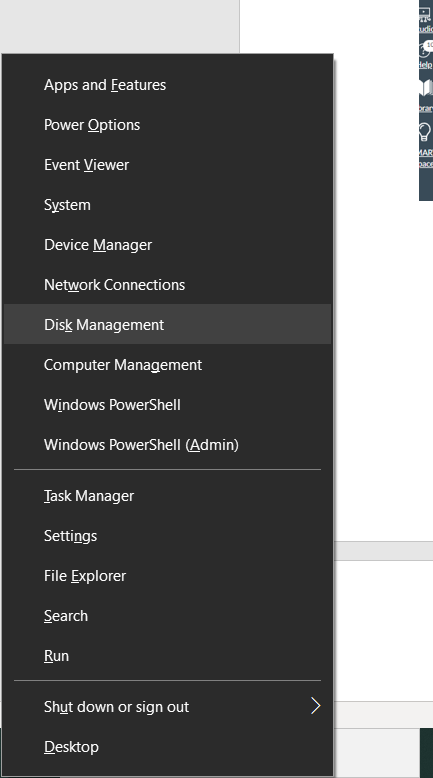
**Deliverables:** Lab write up (Can use this document as a template) and Chain of Custody Document (Use your previously created template).

Step 1: Create Virtual Evidence.

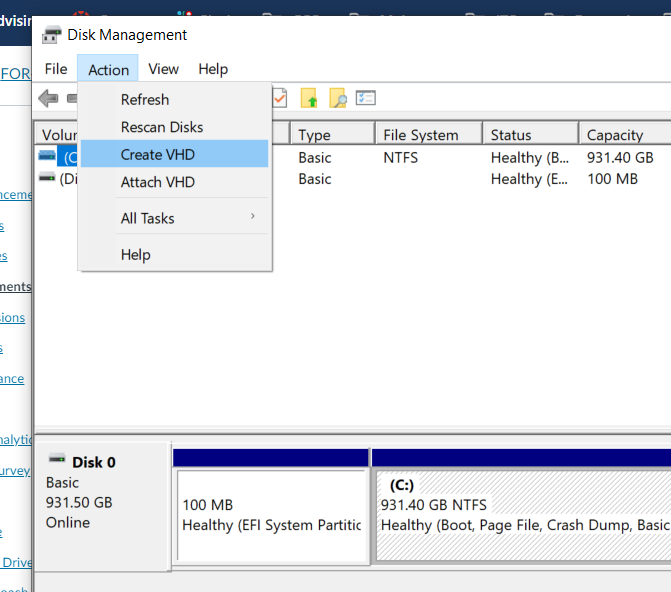
Note: Collect screenshots as you go for an easier write up (ctrl + Win +s)



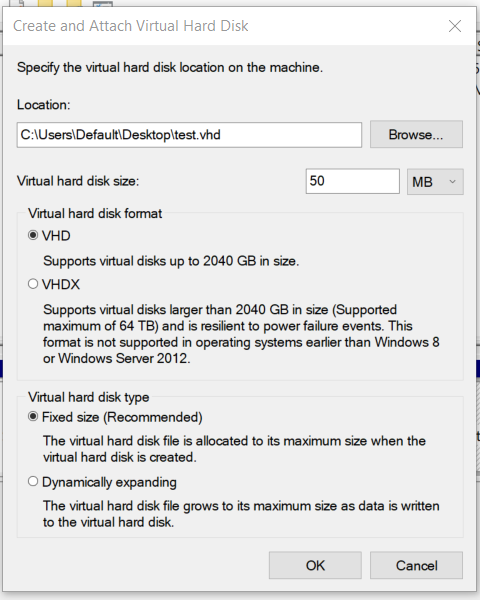
* 1. Type Disk Management or Create and format hard disk in Windows Search. Reference documentation on how to use Disk Management: <https://learn.microsoft.com/en-us/windows-server/storage/disk-management/manage-virtual-hard-disks>



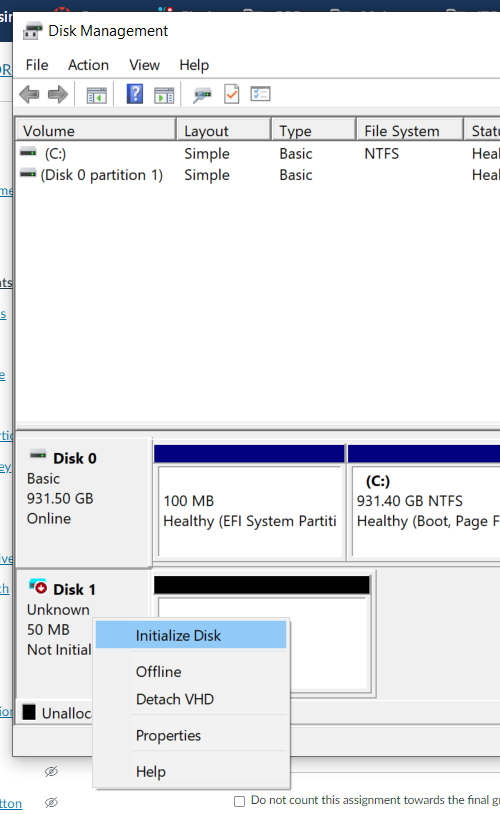
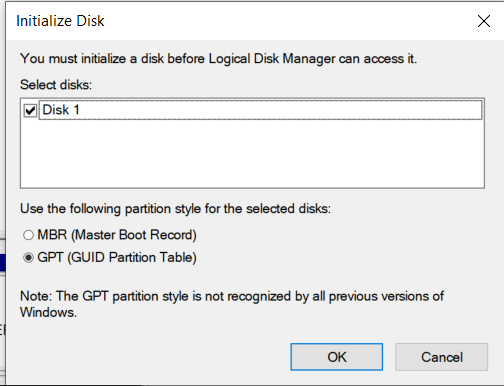
Or use keyboard shortcut Windows Key (Bottom Left between ctrl and alt) + x to open system shortcuts. Select Disk Management to open storage management wizard. You can also use this program to modify and add new storage devices to Windows.



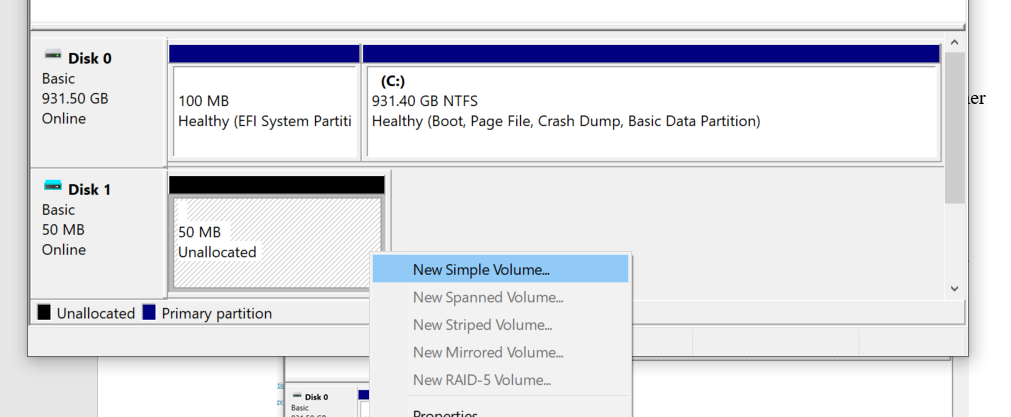
1. Select Action and Create VHD (Virtual Hard Disk).



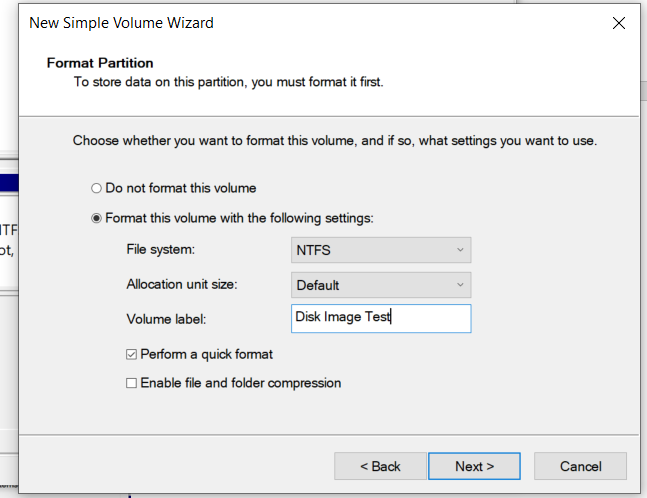
1. Create and Attach Virtual Disk: Save as test on the Desktop and make size 50MB. Other options as default.

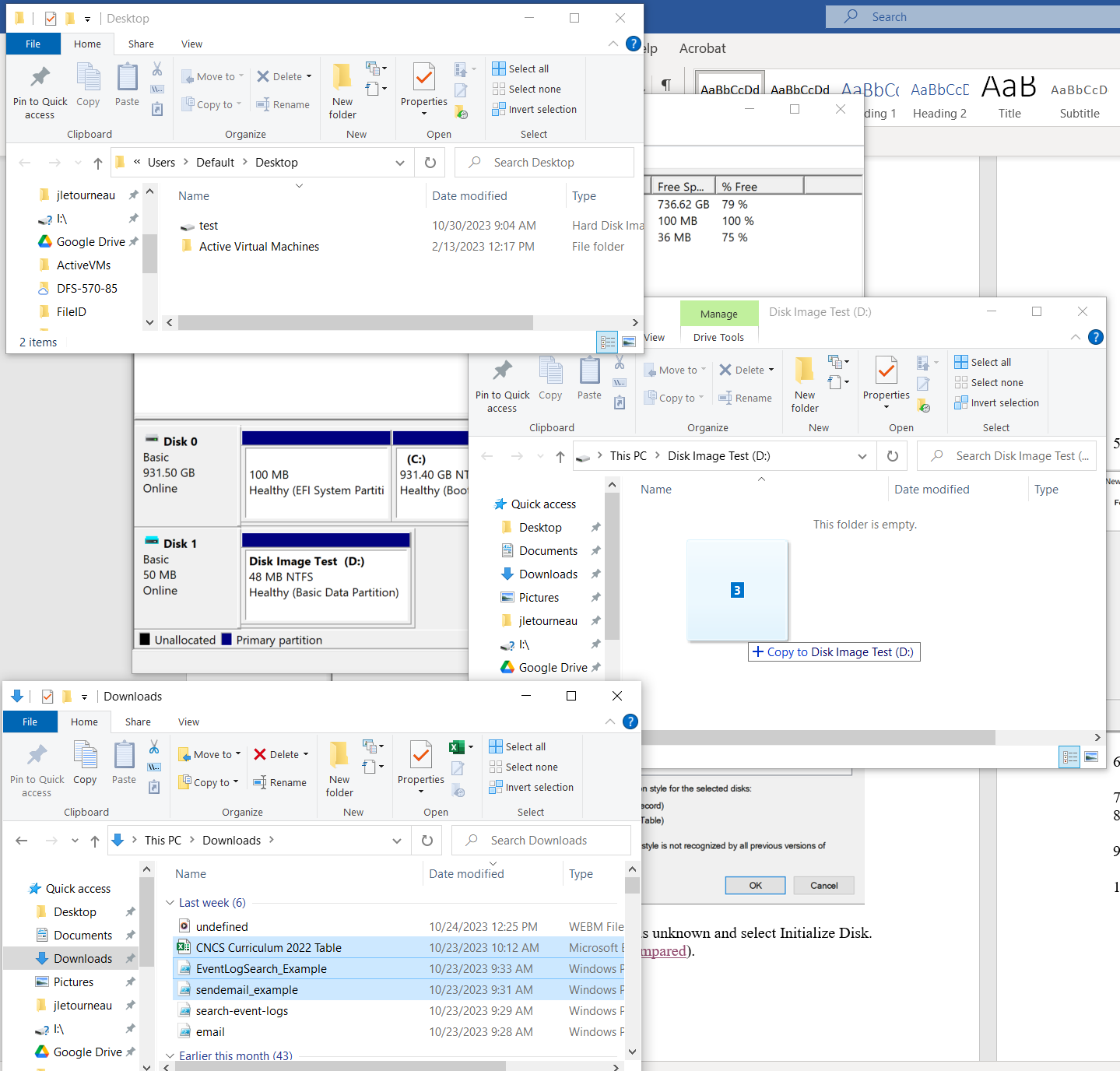
1. Once disk is created, right click new disk labeled as unknown and select Initialize Disk. Select default option for GPT. ([MBR and GPT Compared](https://learn.microsoft.com/en-us/windows-server/storage/disk-management/initialize-new-disks#compare-partition-styles---gpt-and-mbr)).



1. Right click Unallocated space and select New Simple Volume.



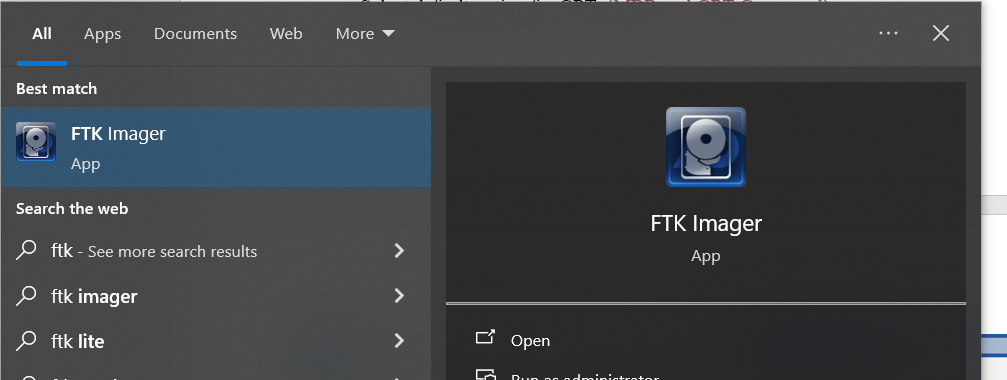
1. Select all default options in New Simple Volume Wizard until it asks for a Volume label where you should label it Disk Image Test.



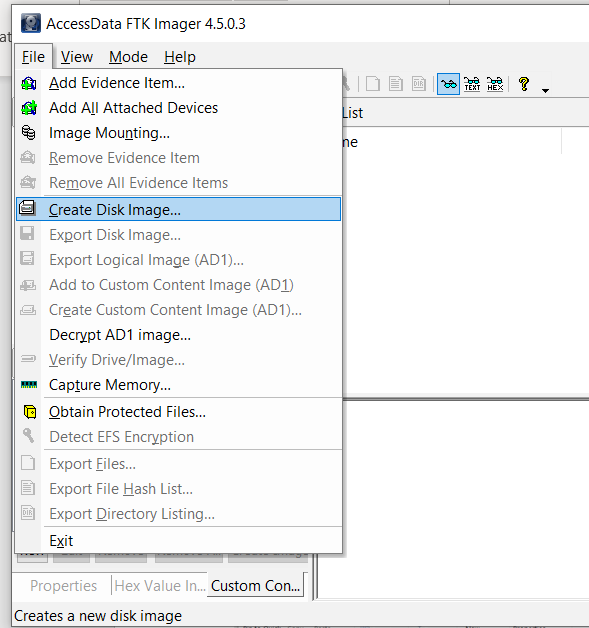
1. Now there should be a new drive letter mapped to the system as a letter incremented from the existing drives such as D, E, F, or G. In my case, D.

You can see the virtual hard disk image of the drive on the desktop as well in the upper right. (This is essentially a pretend storage device similar to a virtual computer but just the storage).

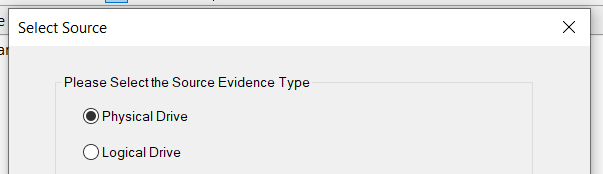
Copy some existing files from the downloads/pictures folder and move to the new blank Disk Image Test drive location. You can always search file explorer in Windows to pull up multiple file explorer windows side by side but in different places like above.

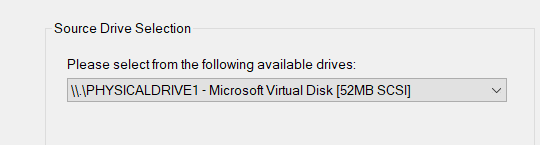


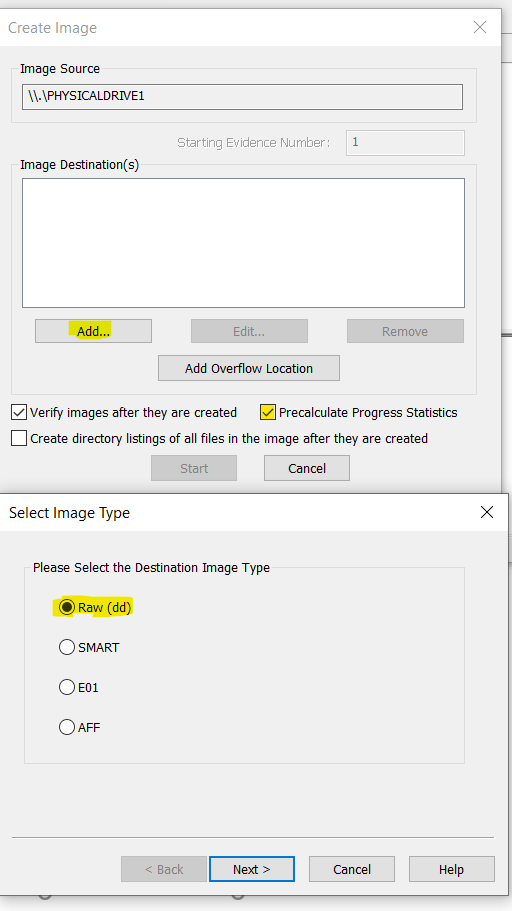
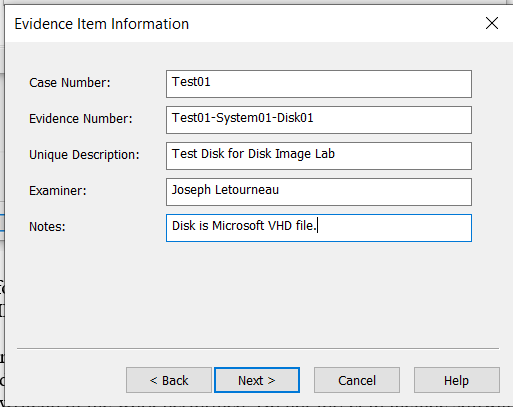
1. Search for FTK Imager in Windows and open the program.

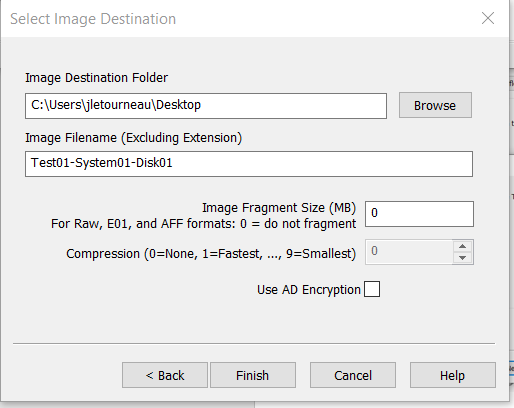


1. Select File/Create Disk Image.

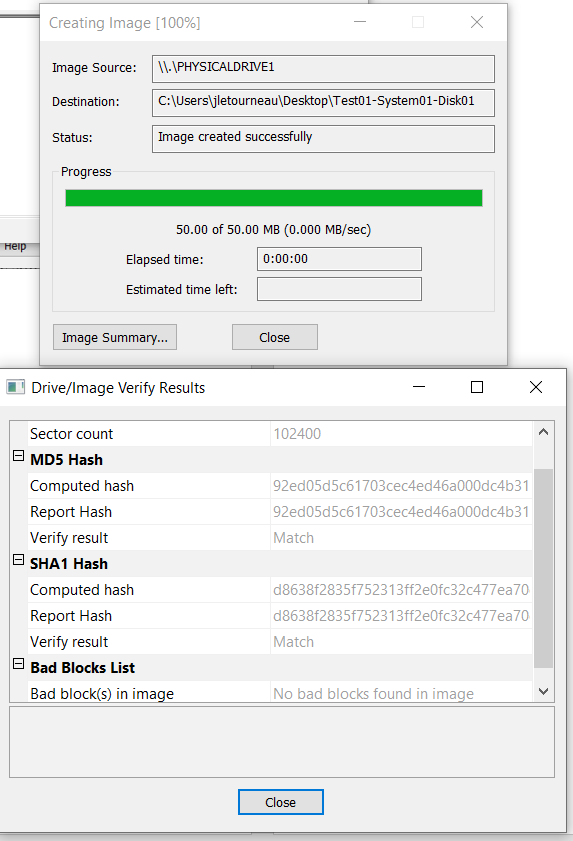
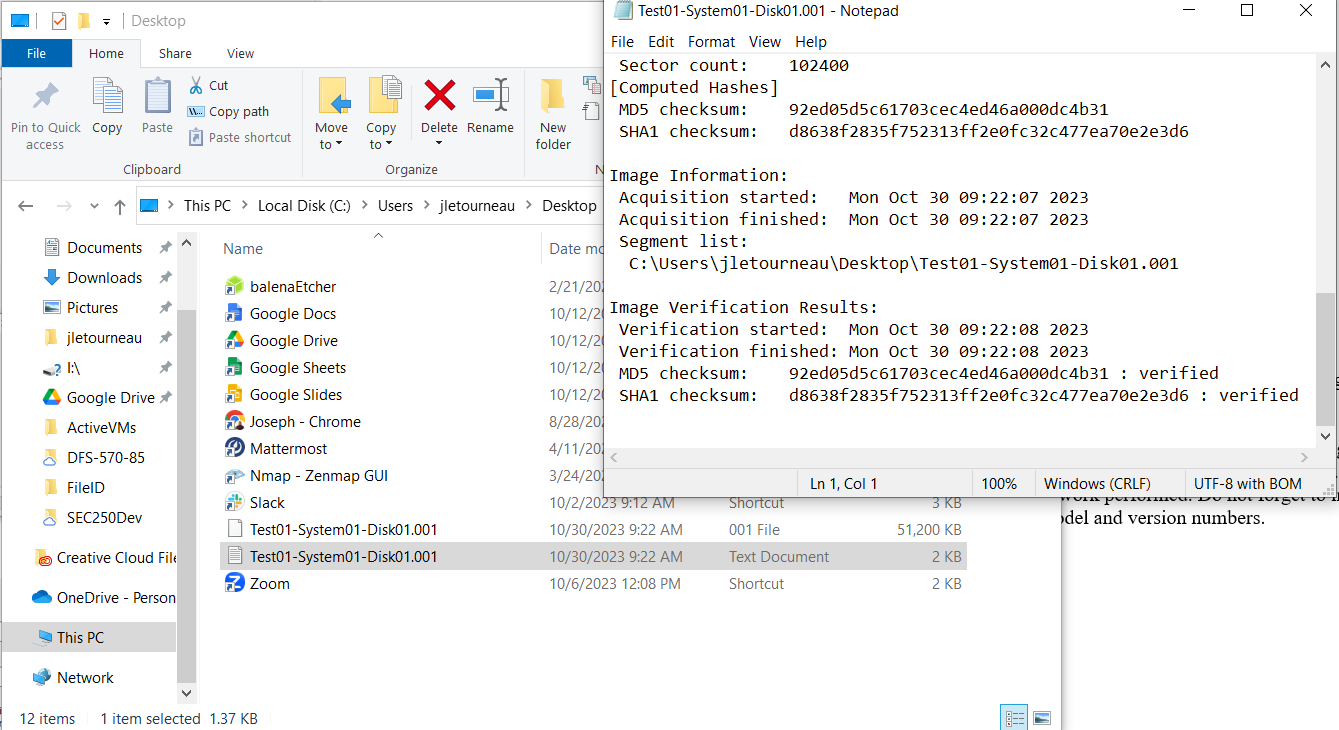




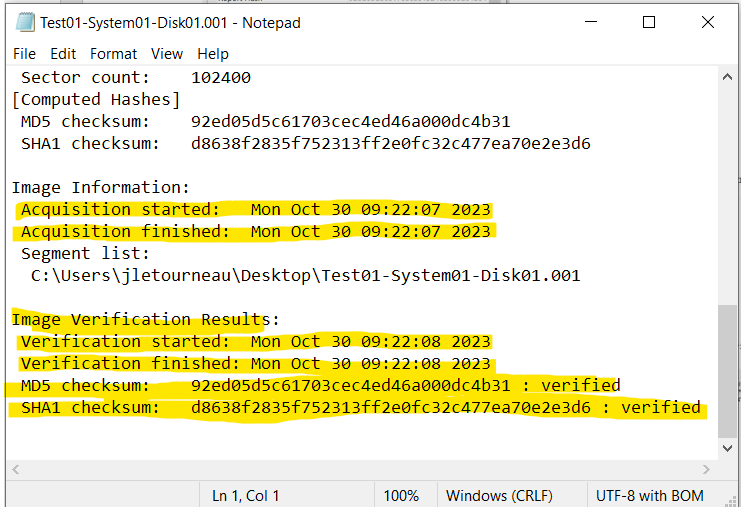
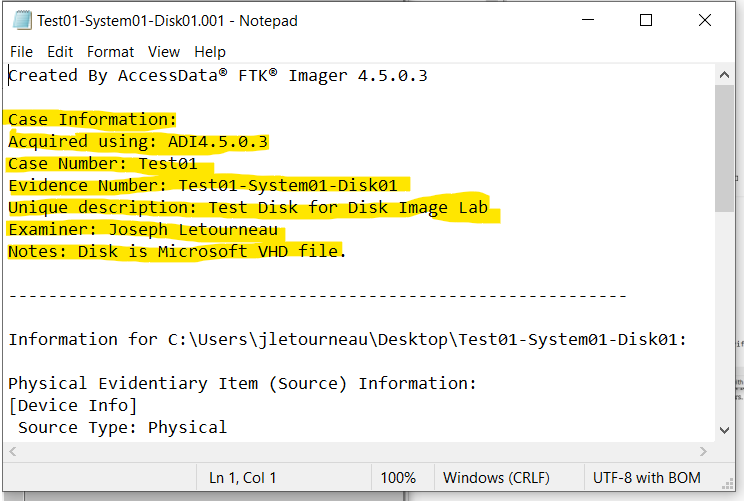
 



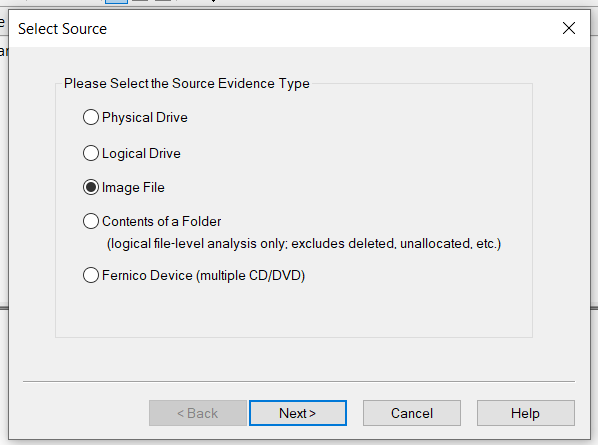
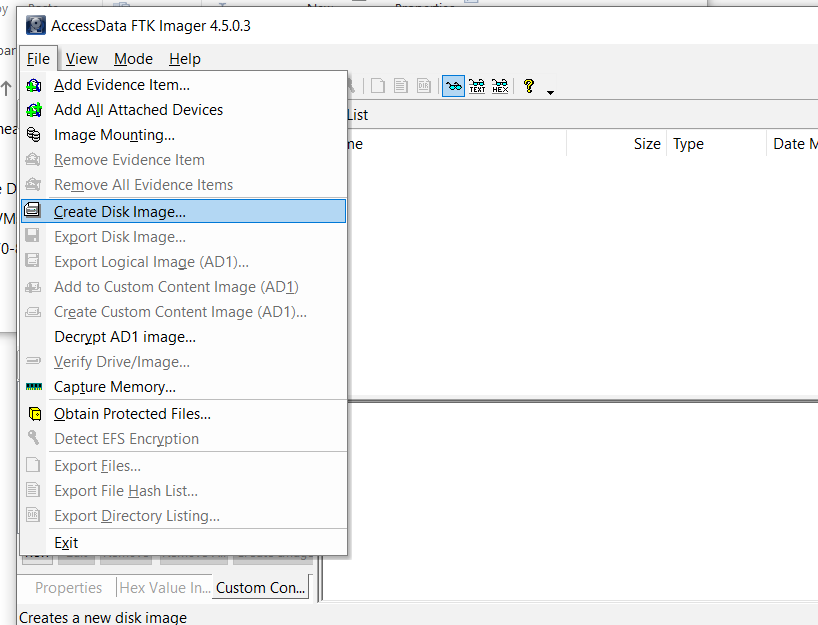
1. Follow Disk Image creation wizard. Select Physical Drive, Microsoft Virtual Disk, Raw(dd) format, enter evidence item information similar to example above. Label file name similar to Evidence number and save to desktop.

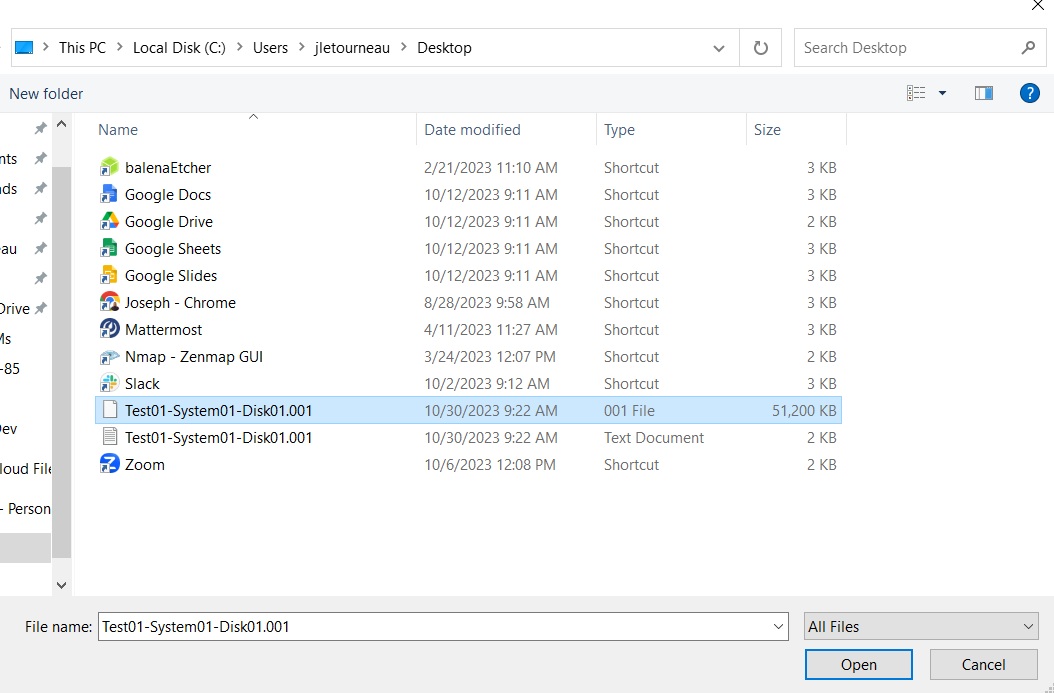
 

1. Program will complete imaging quickly but normally may take up to several hours for large systems. Disk image should be saved as Test01-System01-Disk01.001 file and accompanied by Test01-System01-Disk01.001.txt file which contains acquisition and verification information.

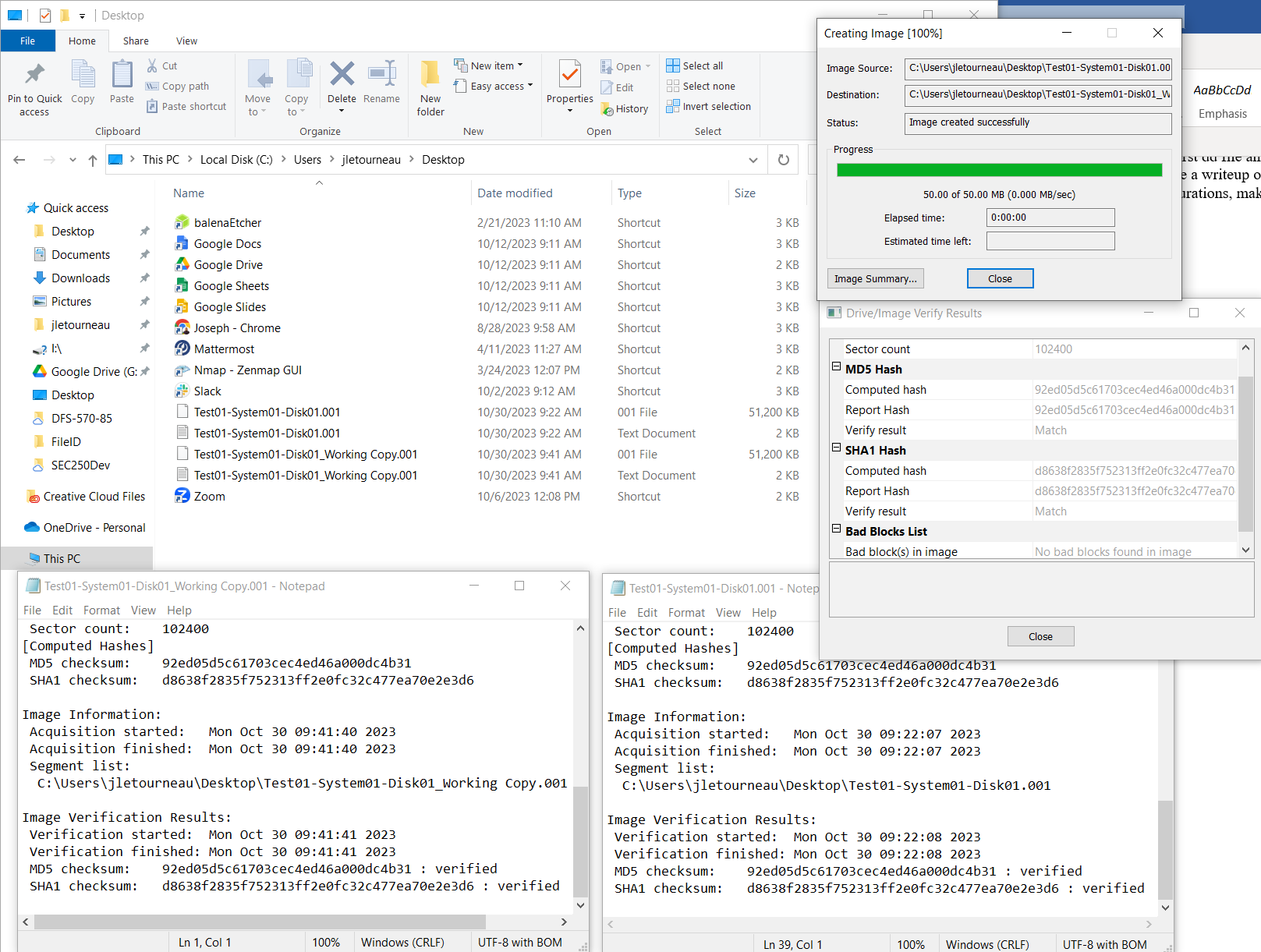


1. Record important information such as Case Information, when image was collected and the Image Verification Results including: Verification finish time, MD5 checksum, SHA1 checksum and that they were successfully verified. (The program uses these hashing algorithms to check that the copy we made is the same as the original).





1. Create a working copy of the disk image. Repeat steps 9 through 12 but when running the Imager again, select create image file. Select your new 51MB Test01-System01-Disk01.001 file as the source to copy.

Note: there are two copies of the original disk image now; a golden copy which should be secured with the chain of custody and a working copy which can be used for analysis. We can see above the verification hashes are the same from the original disk through to the working copy which proves the data has been preserved and unaltered. 

1. Complete your lab writeup detailing actions and screenshots.
2. Create a Chain of Custody Document using the Case information, acquisition and verification times along with the hash information.