6/2023



salah tawafsha

1200339

investigation using FTK-Imager and Active Disk Editor

Instructor: Dr. Mohammad Alkhanafseh

Contents

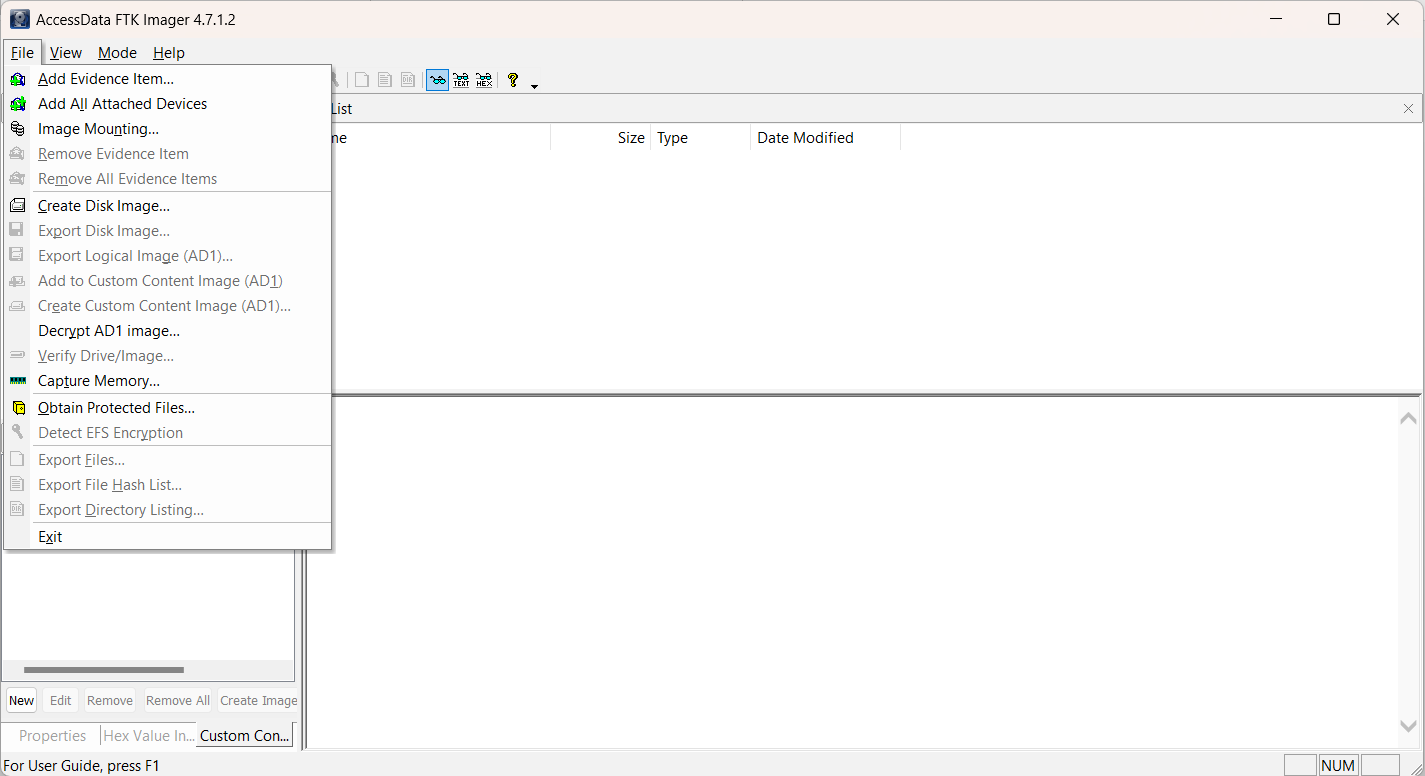
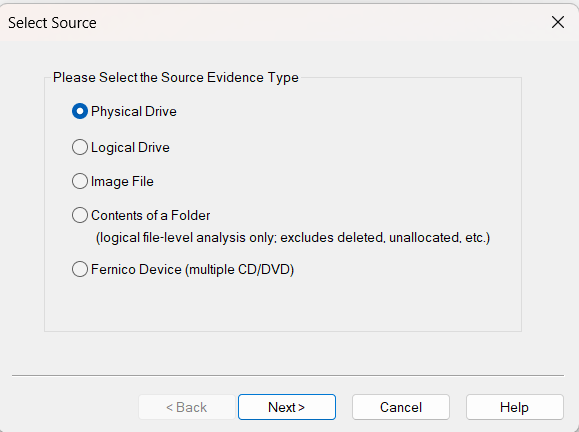
[First Requirement: build an image for Flash Memory 3](#_Toc136637748)

[Second Set of Requirements: 7](#_Toc136637749)

[ divide the VHDD into 8 different partitions 7](#_Toc136637750)

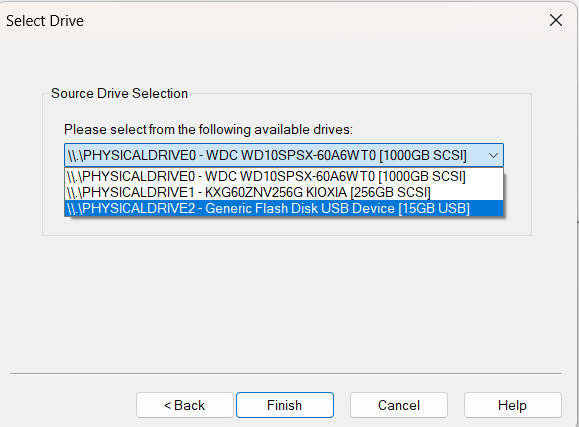
[ Find Type of each partition. 11](#_Toc136637751)

# First Requirement: build an image for Flash Memory

1. Install FTK imager and open it.
2. Open “File” from toolbar then go to “Create Disk Image”. 
3. Select “Physical Device” as a Source then click “Next”.   
   

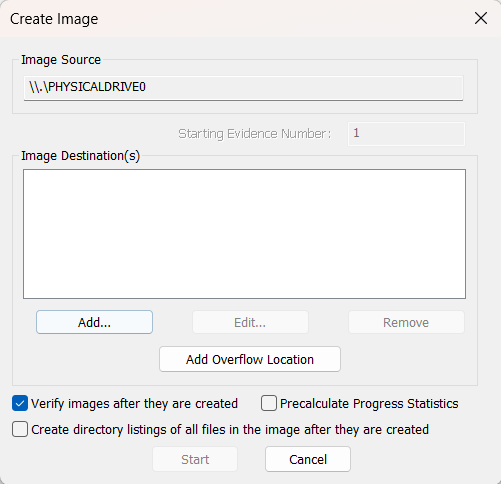
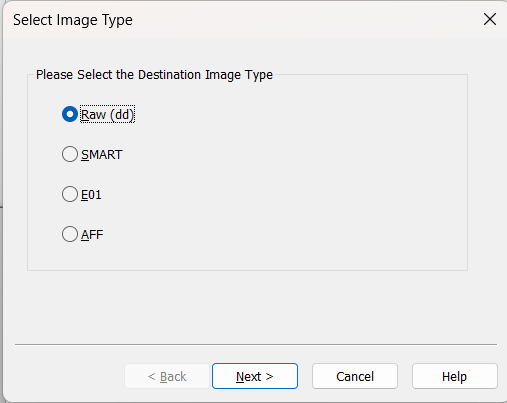
**2**

**1**

1. Select The device and click “next”.  
   

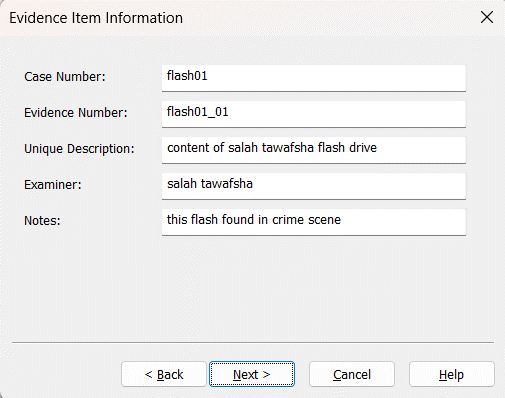
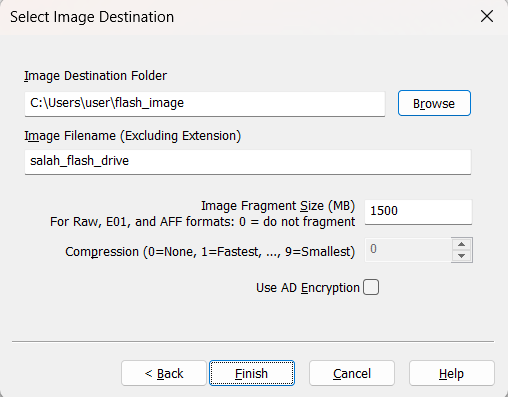
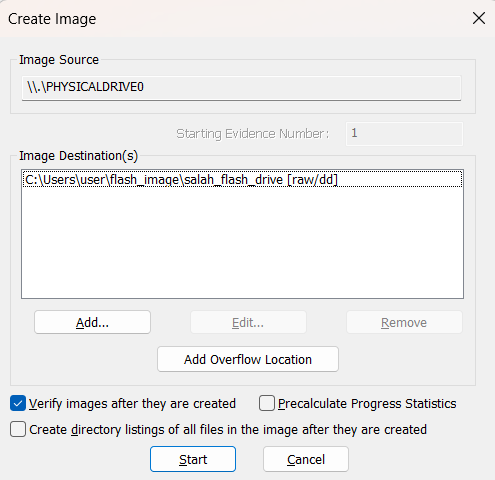
**2**

**1**

1. Now, we want to add destination that to save the image. So, click on “add”.  
   
2. First, we will select the type of image file. Raw is a bit-by-bit uncompressed copy of the original, while the other three alternatives are designed for use with a specific forensics program. I will use Raw, which is an EnCase forensic image file format.   
   

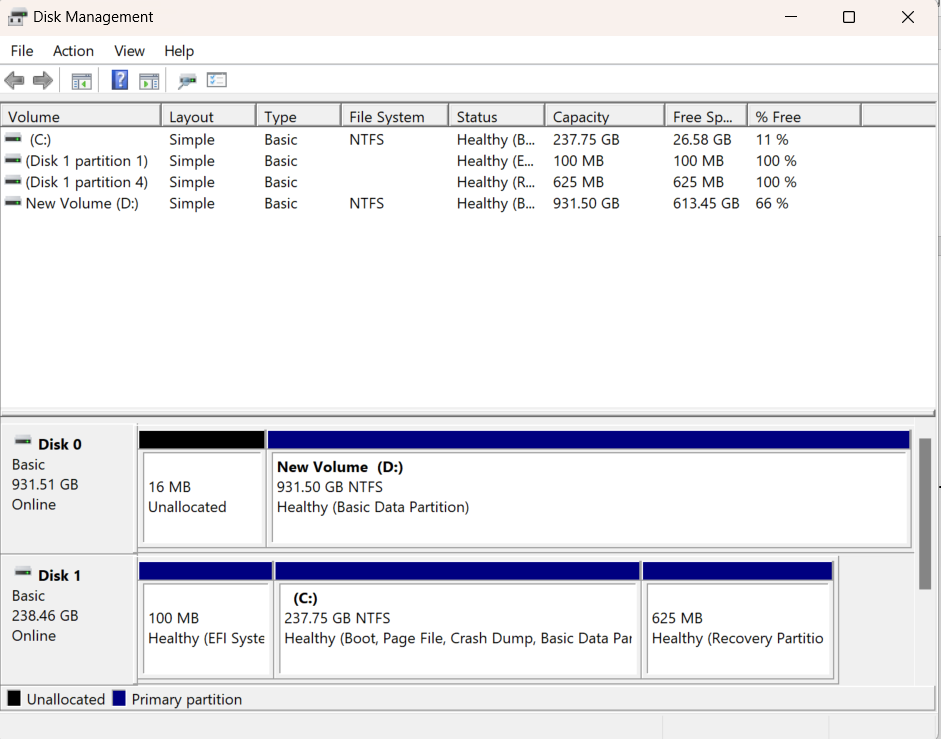
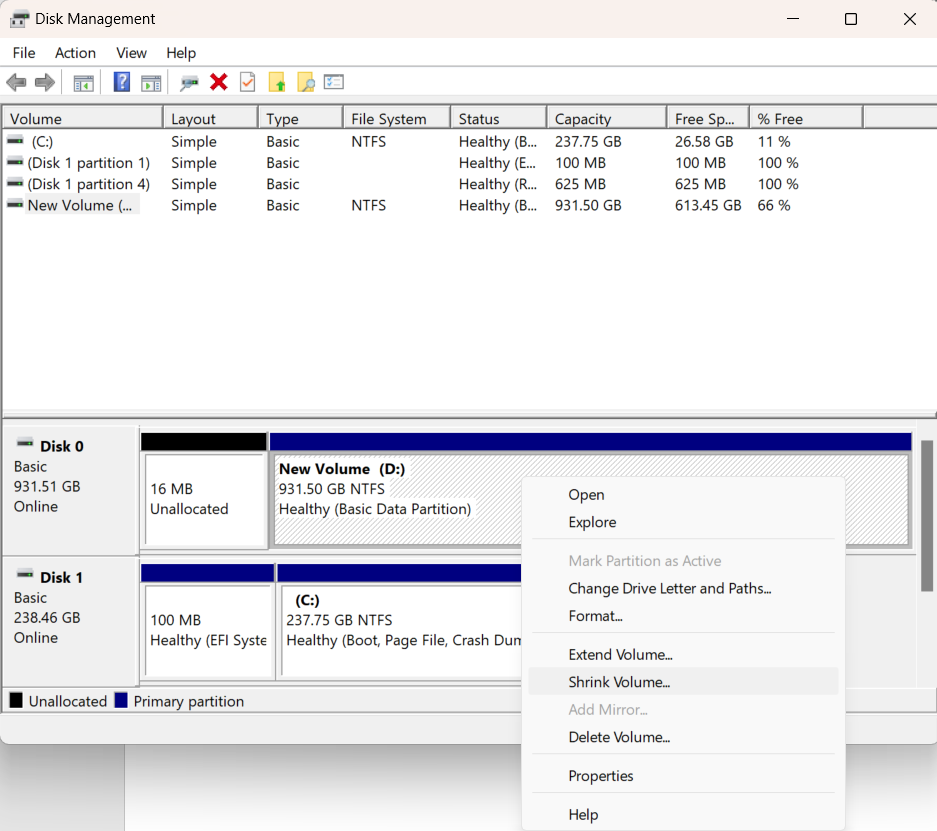
**2**

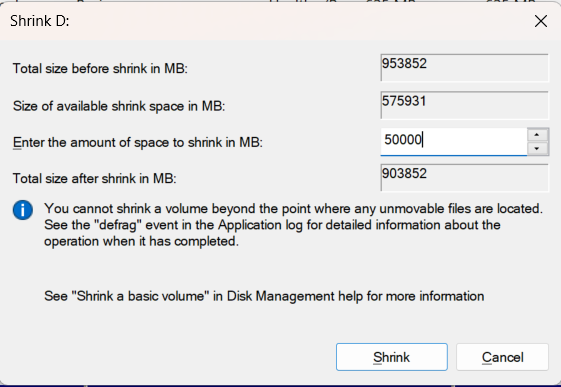
**1**

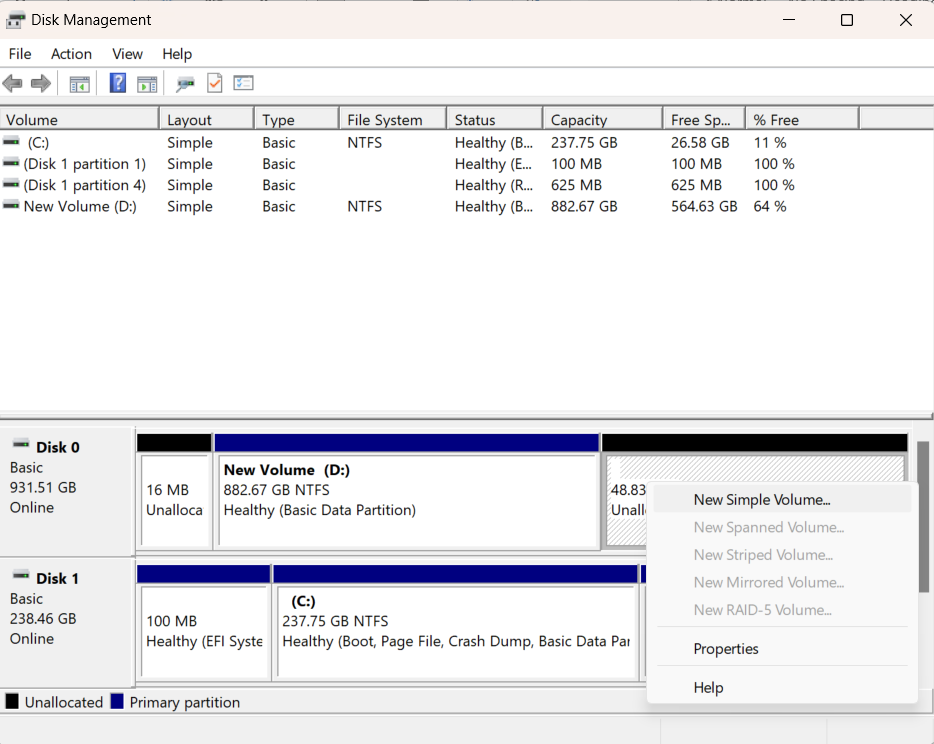
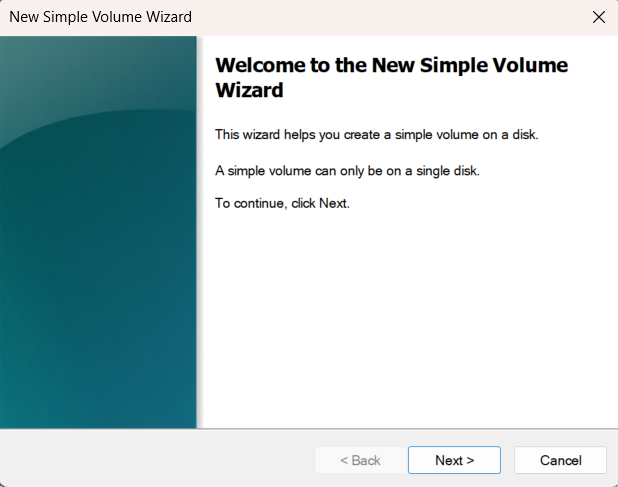
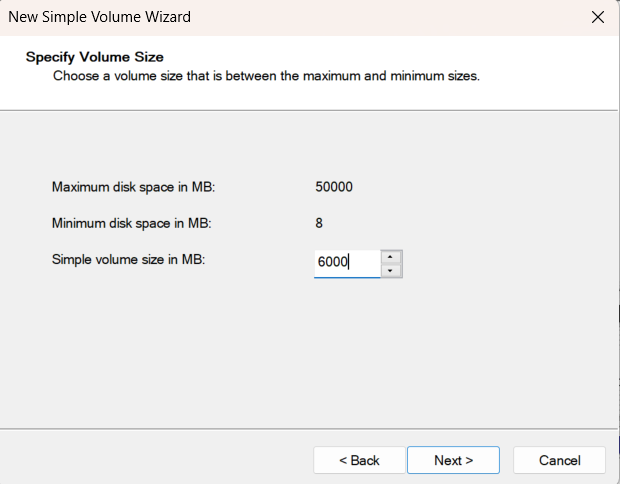
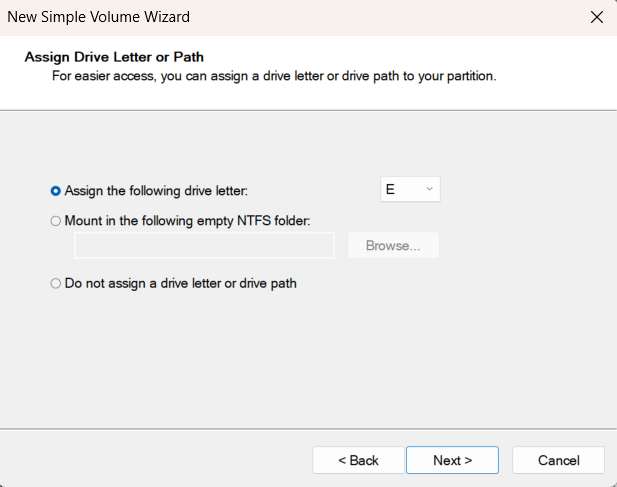
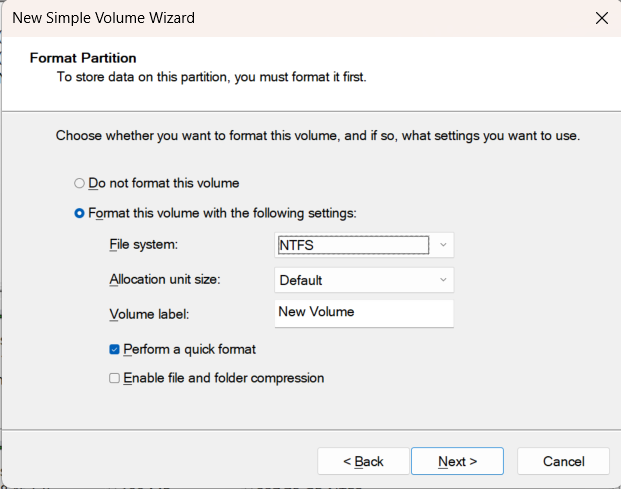
1. Then, enter key information about the evidence item and click “next”. I add this information.   
   
2. Now, click on browse to select folder to save image, type the filename and enter image fragment size, Image Fragment Size indicates the size of each fragment when you want to break a larger image file into multiple parts. Note that: in Raw files, compression is always 0. Finally, click “Finish”.  
     
   
3. Finally, click on start and image will start generating. And when finished we can show summary about the image.  
   

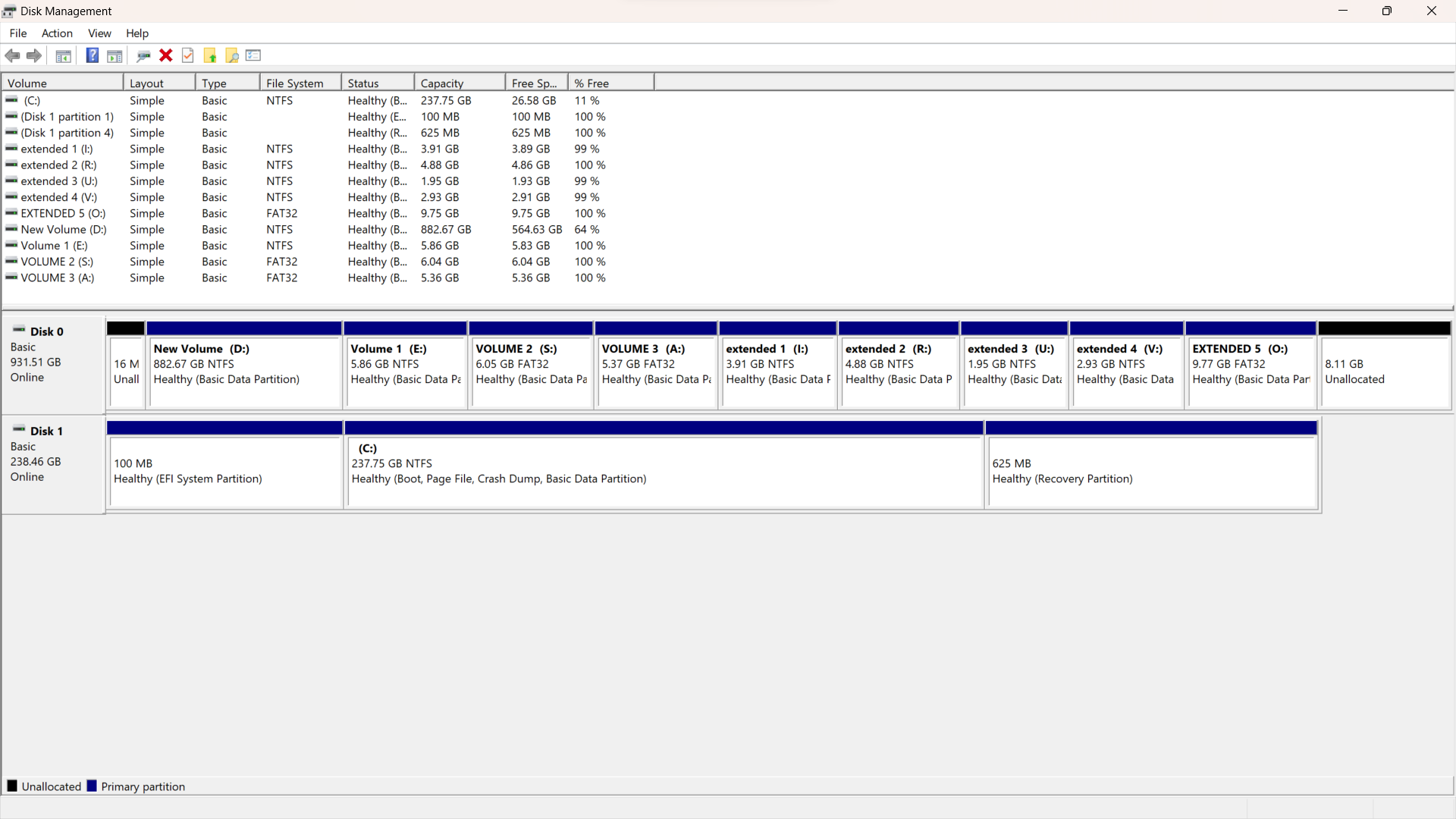
# Second Set of Requirements:

## divide the VHDD into 8 different partitions

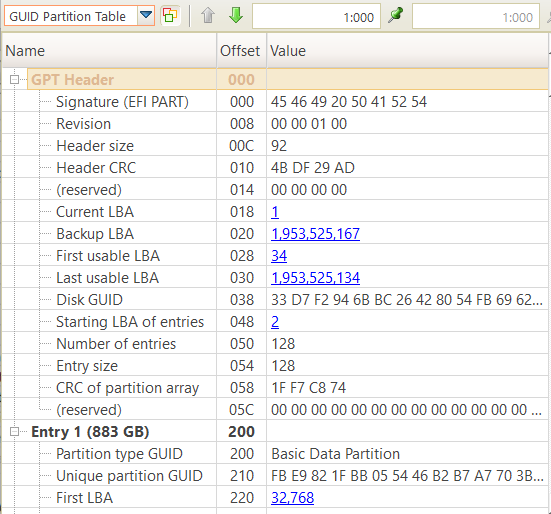
1. Press Windows key + X on your keyboard and select Disk Management.
2. Look at disk that you want to create partitions for it.  
   if you have unallocated space (as in RED) to make partitions in it go to step 4.  
   
3. If no unallocated space, then we must make shrink for disk, this will make the disk in smaller space and allow to make partitions in the unallocated space.
4. Click on right click while mouse hover the disk and click on “Shrink Volume”  
   
5. Here, we will enter how much unallocated space that we want to create.  
   I set 50000 that nearly 50 GB to be free. Finally click “Shrink”



1. Right click on unallocated space of disk and click on “New Simple Volume”  
   
2. Click on “next”  
   
3. Now, select the size of partition and click “Next”, I set it to 6000.  
   
4. Now, we can assign letter to show drive as disk in “This PC” folder. Then click “Next”.
5. Now, select format of disk (file system technology, allocation unit size and volume label). Then click “Next”. You will show page have overview of disk (just click finish).  
   

**REPEAT 1-8 for 7 times and we will find these partitions.**

## Find Type of each partition.

1. Open active disk editor
2. Select the disk: From the list of available disks, choose the disk containing the partitions you want to inspect.
3. now I want to know what is my partitioning scheme. When we open the disk it will shown as below.  
   
4. This is the scheme of GPT, each of Entry 1, Entry 2, Entry 2 … etc. represent partition. So will get information from it

