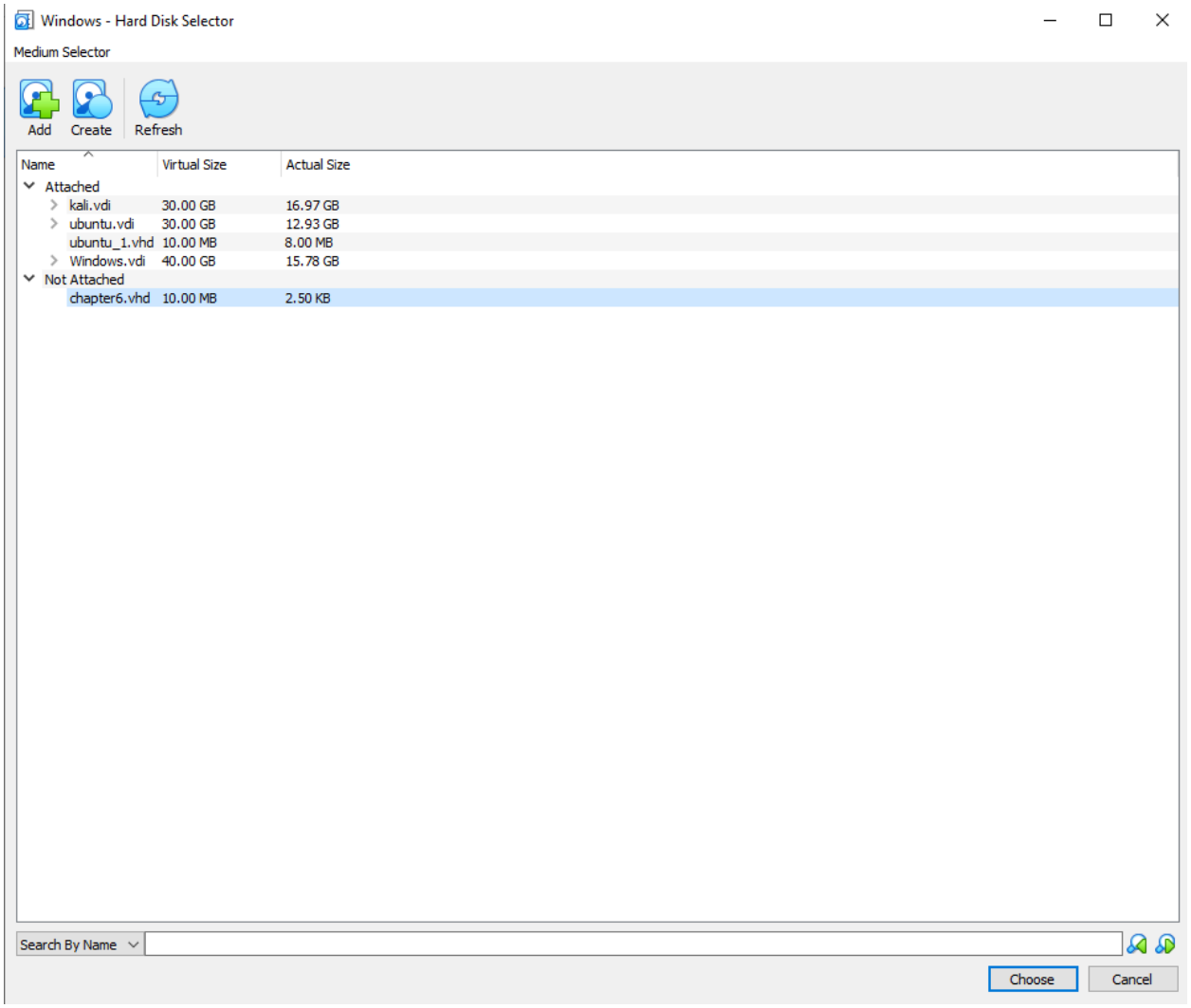
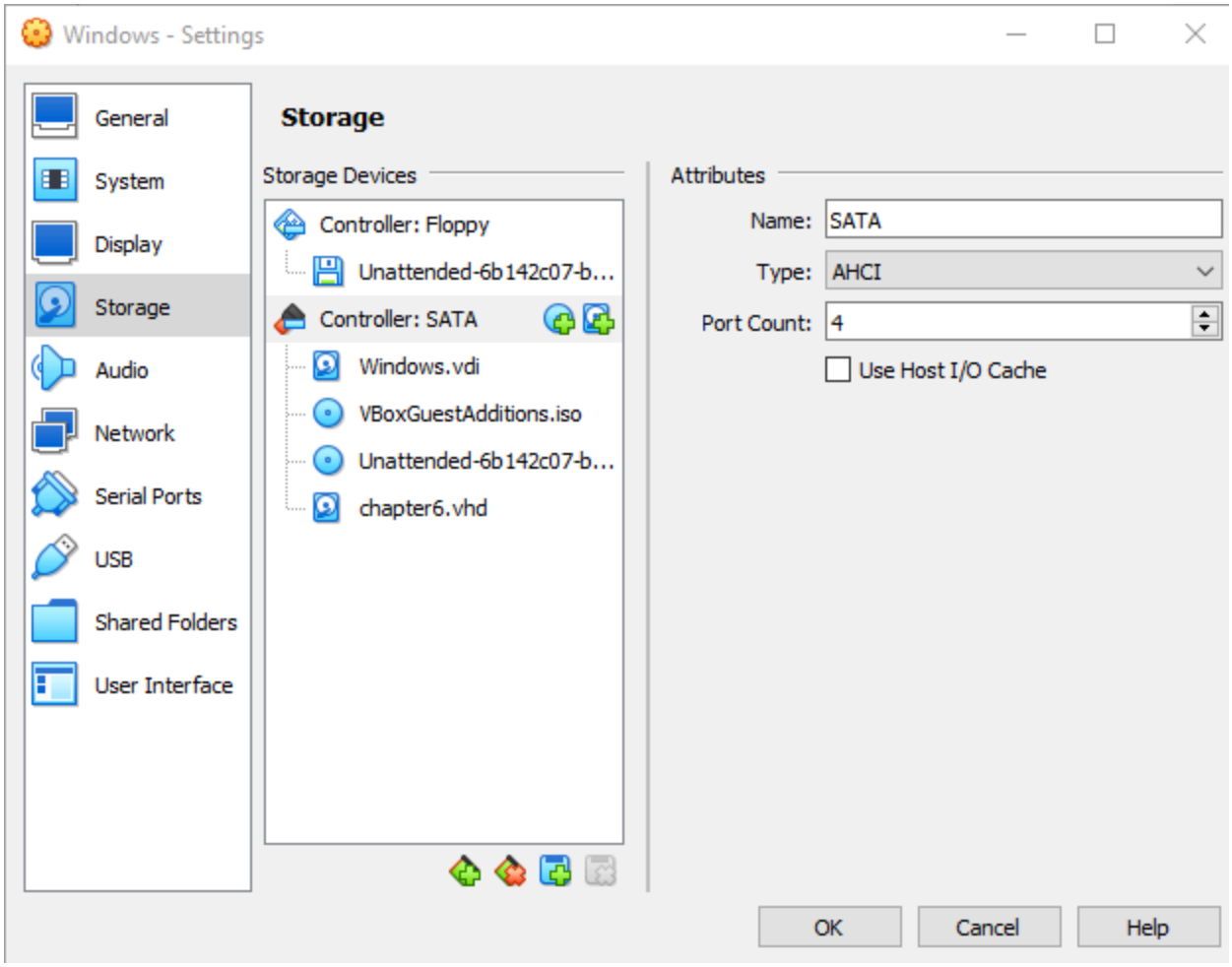
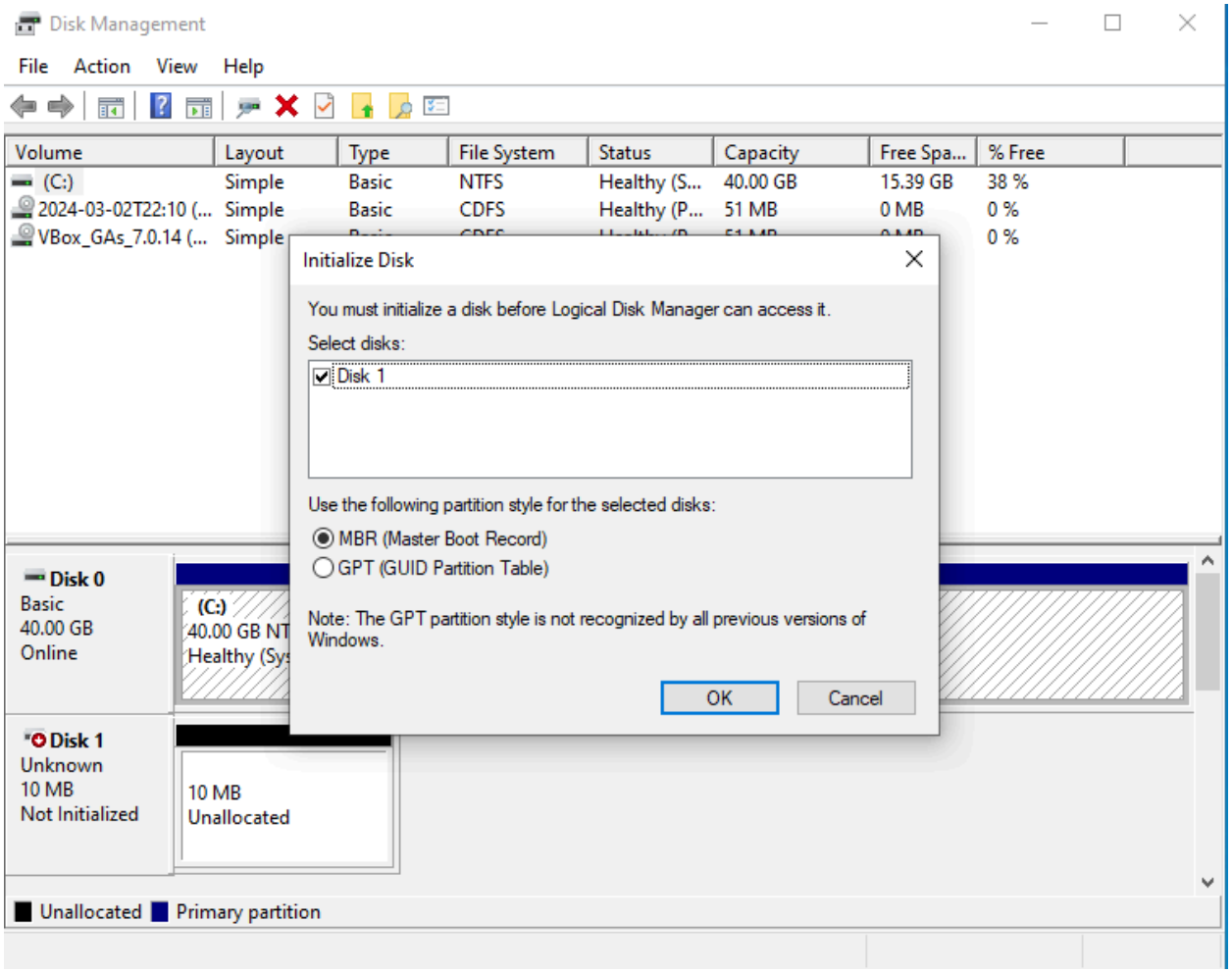
Task 1:



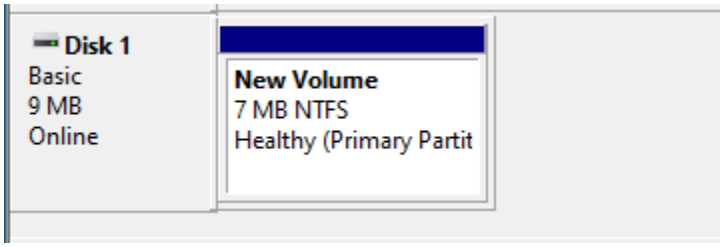
In this step, I have created a new virtual hard disk for my Windows VM and I am about to attach it to the VM.



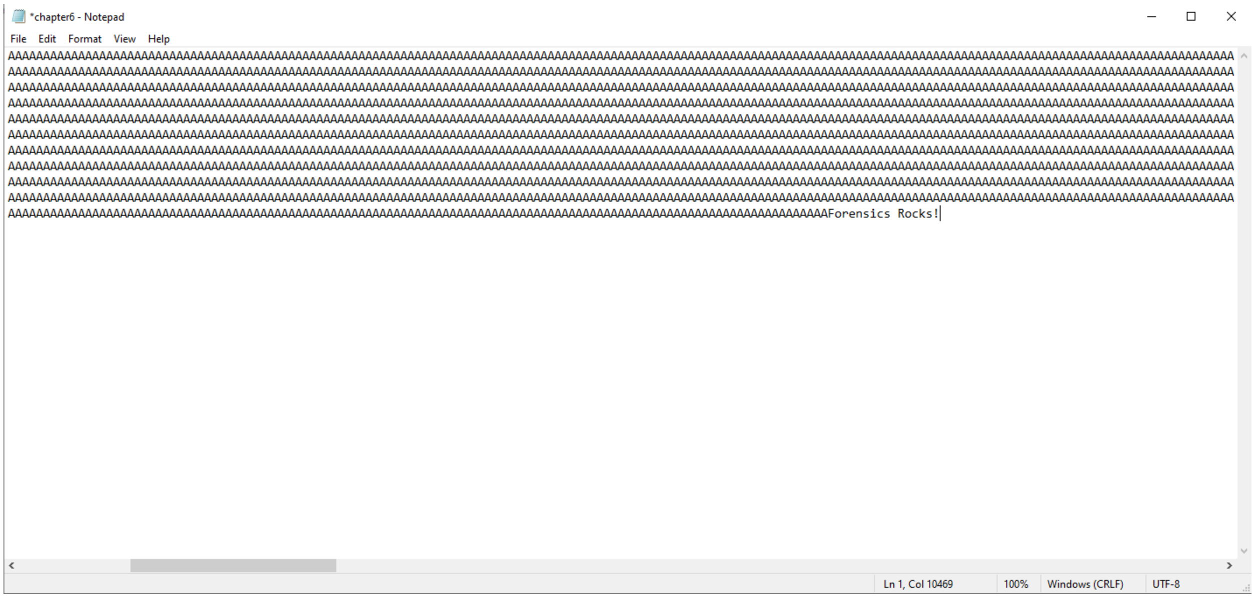
The VHD is attached to the Windows VM.



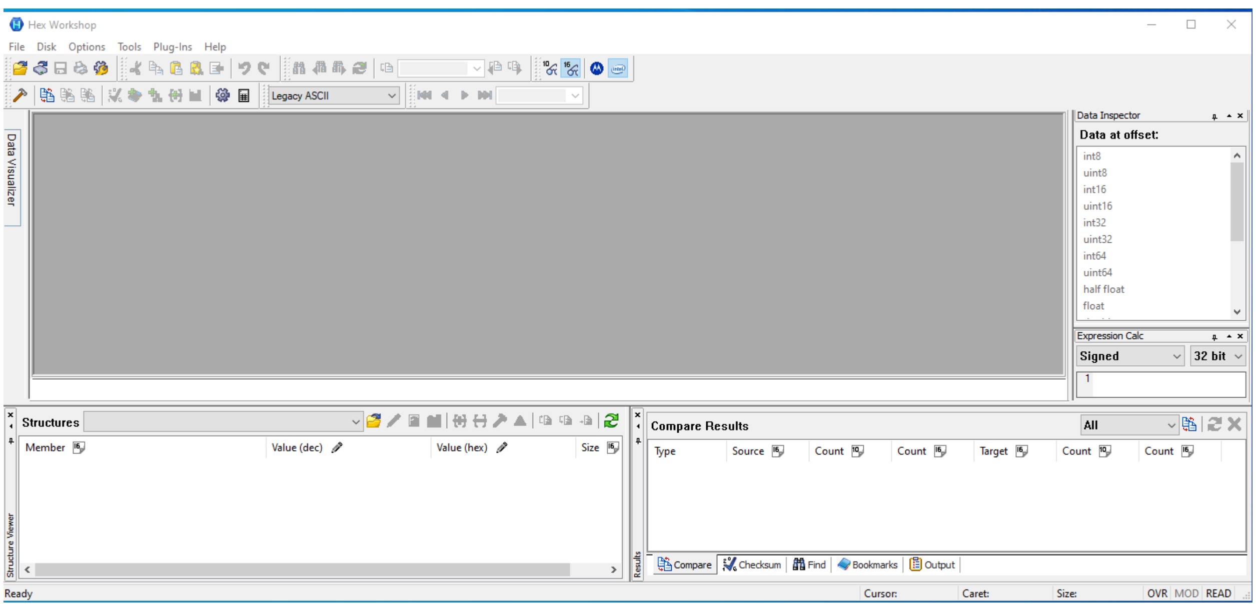
In this step, I am in the Windows VM and have opened the Disk Management Utility and am initializing disk 1.



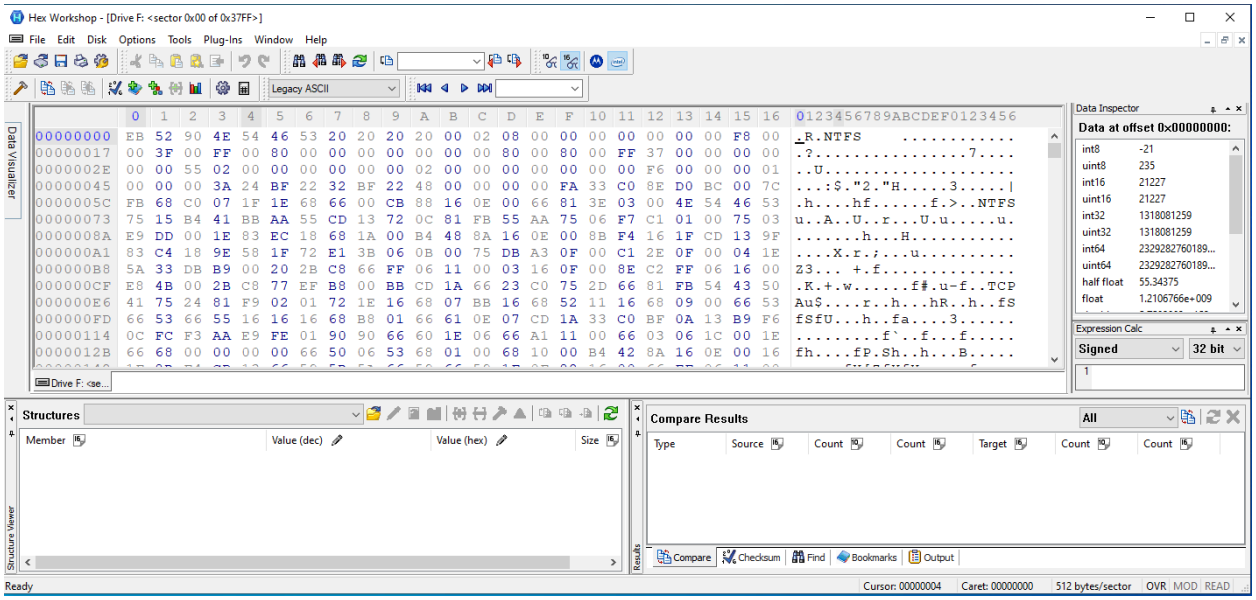
In this step, I have created a partition for Disk 1.



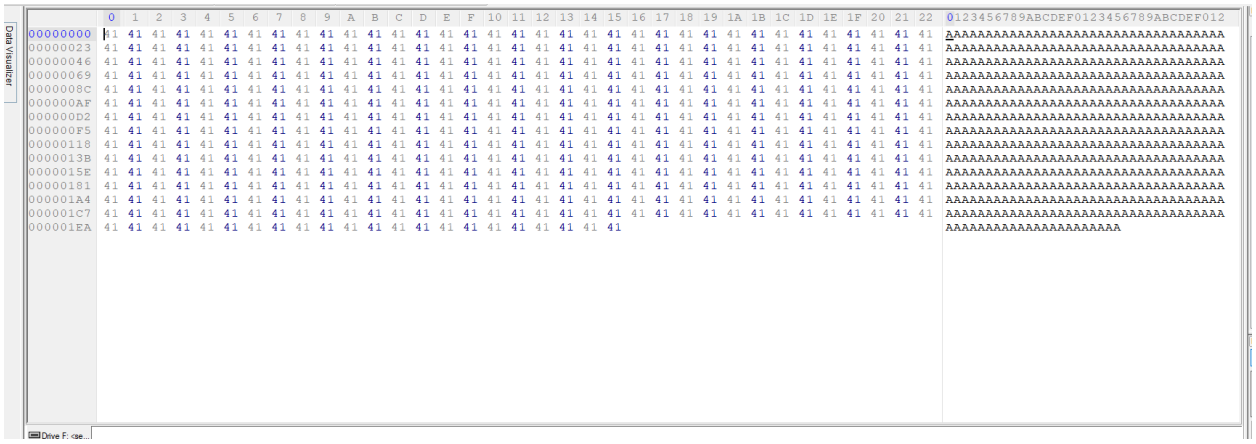
In this step, I have created a file in the new drive that was created and added 10k “A”’s to the file.



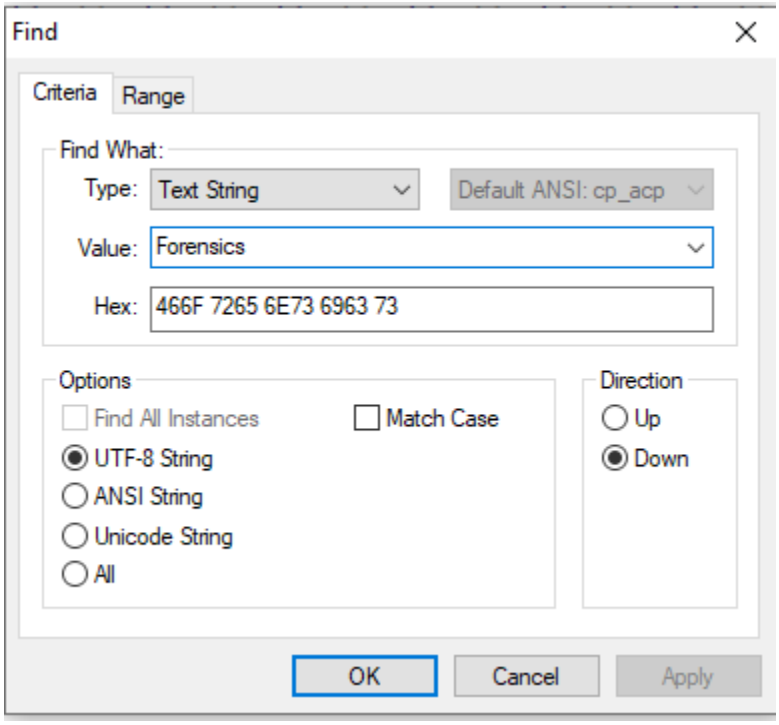
In this step, I have downloaded Hex Workshop and am running it as an admin.



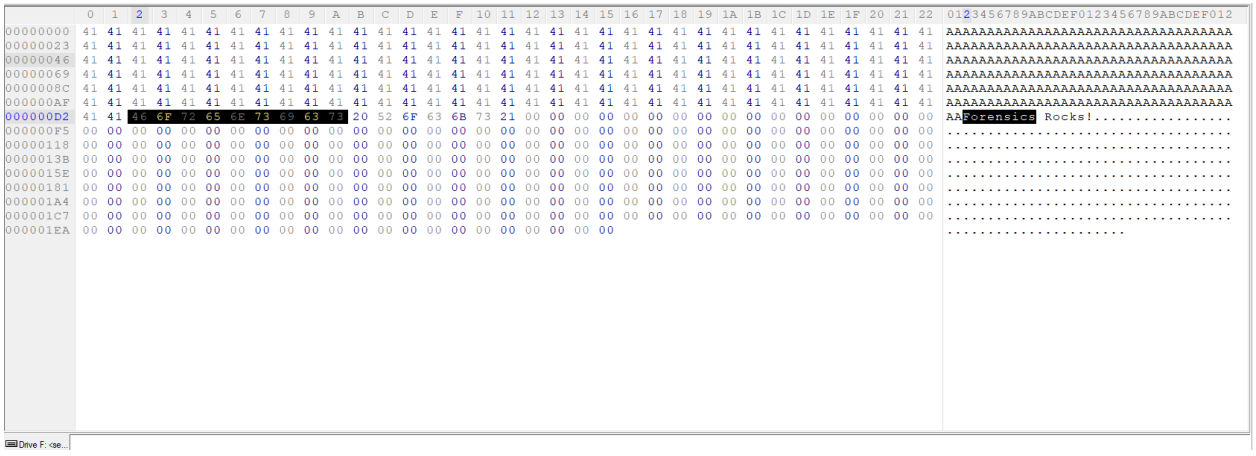
In this step, I have loaded the new drive to Hex Workshop.



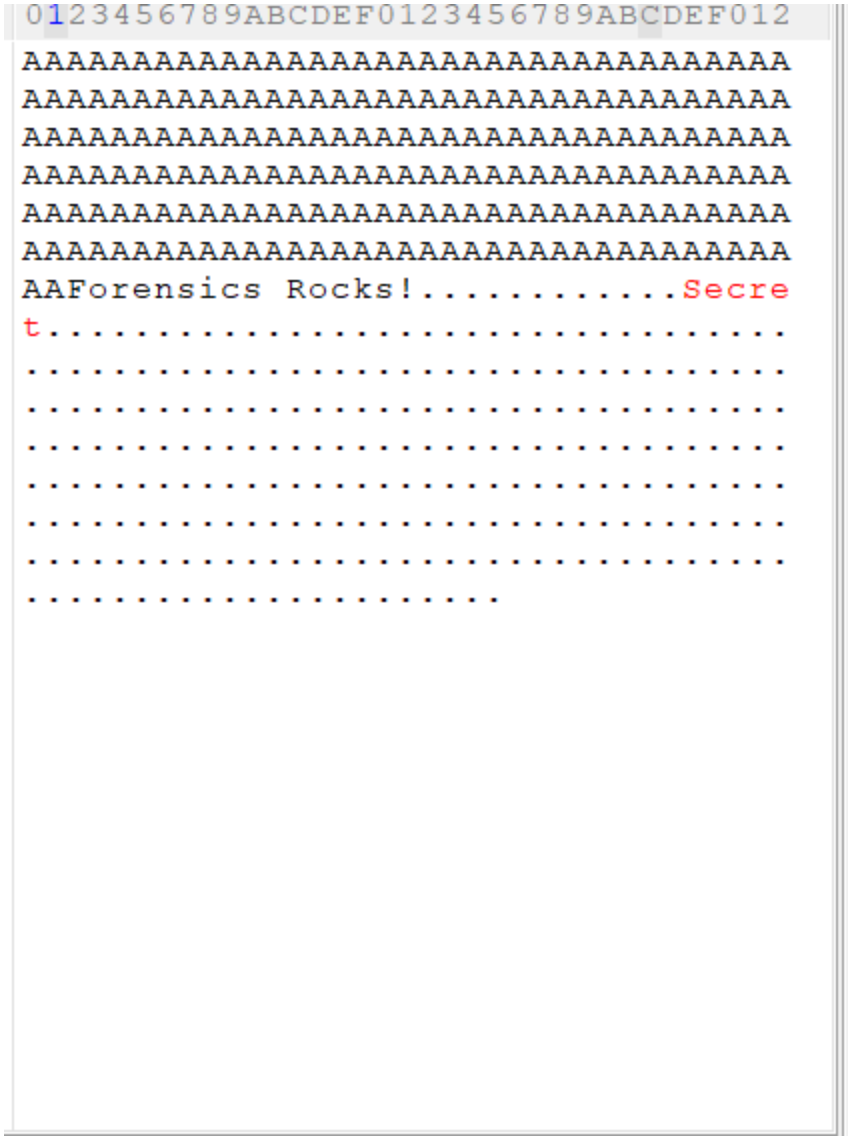
In this step, I have navigate to the sector with all the A's.



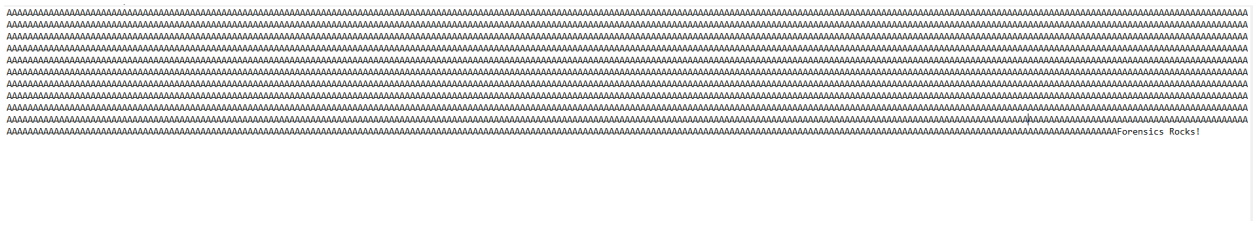
In this step, I am searching for the string "Forensics".



"Forensics" has been found.

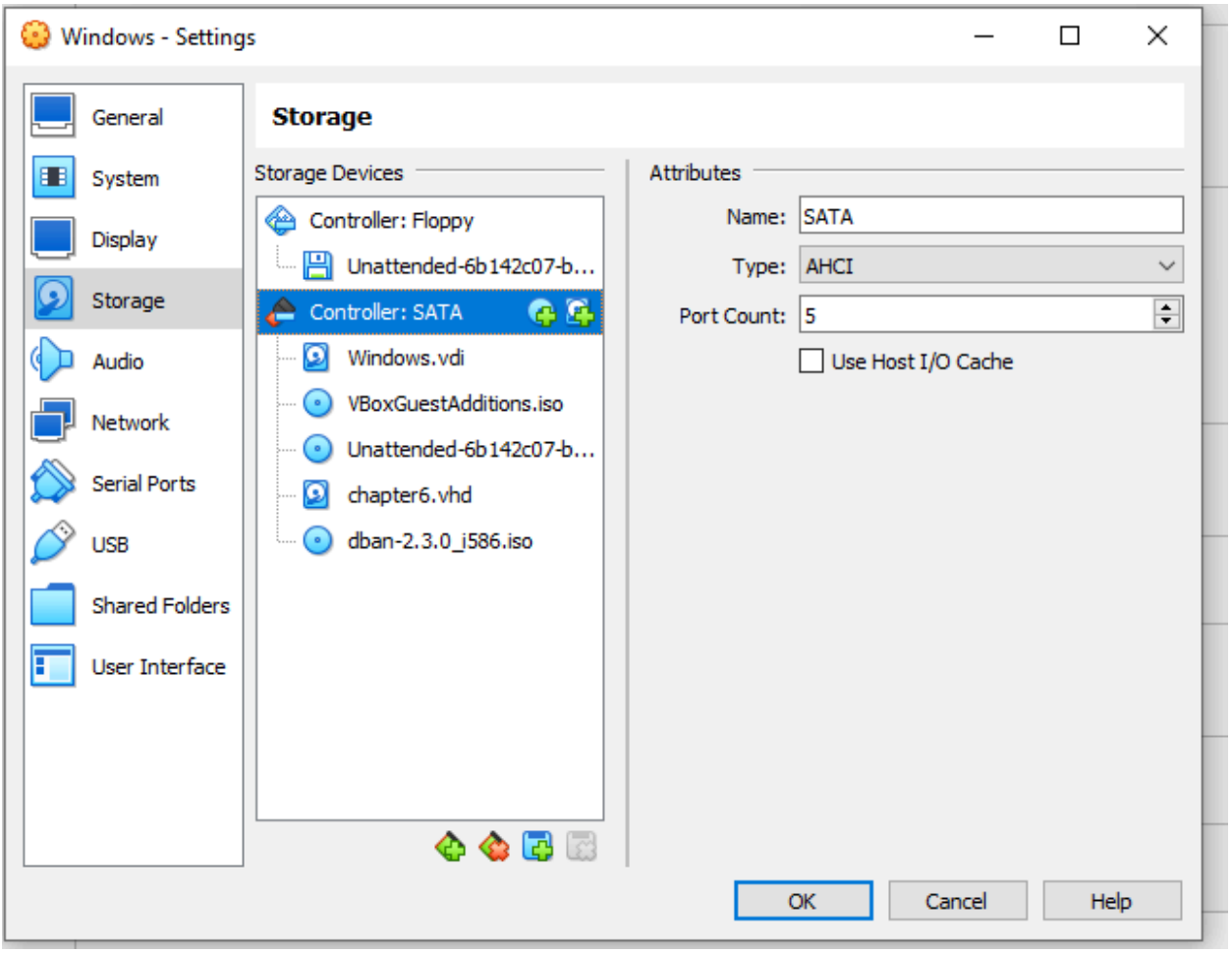


In this step, I am adding the string “Secret” to the file slack space.

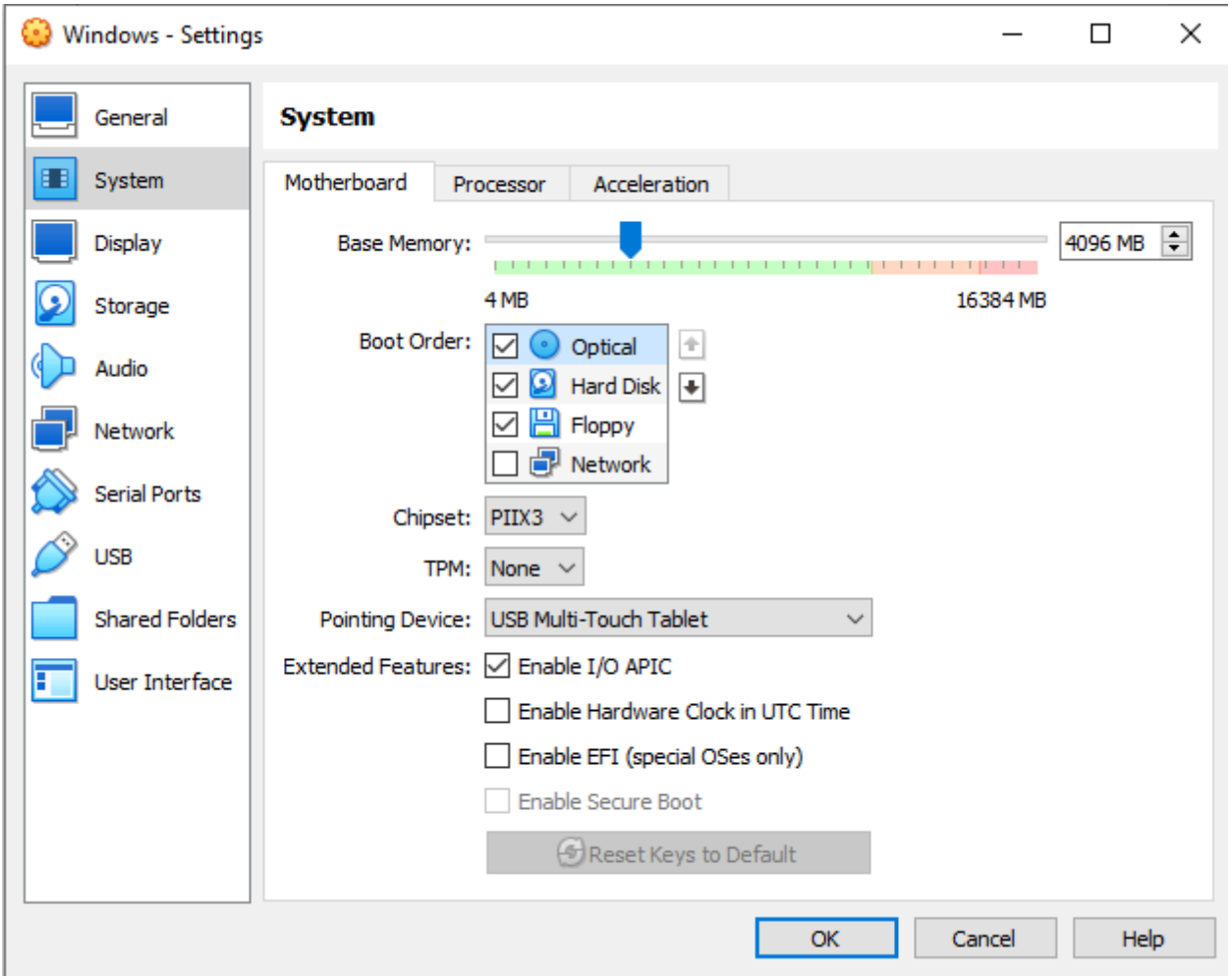


Now in the chapter6.txt file, “Secrets" is not shown because since it is stored in the file slack space, it is not in the allocated space for our chapter6.txt file. This leads to our computer only outputting the information that is stored in the allocated space for that file.

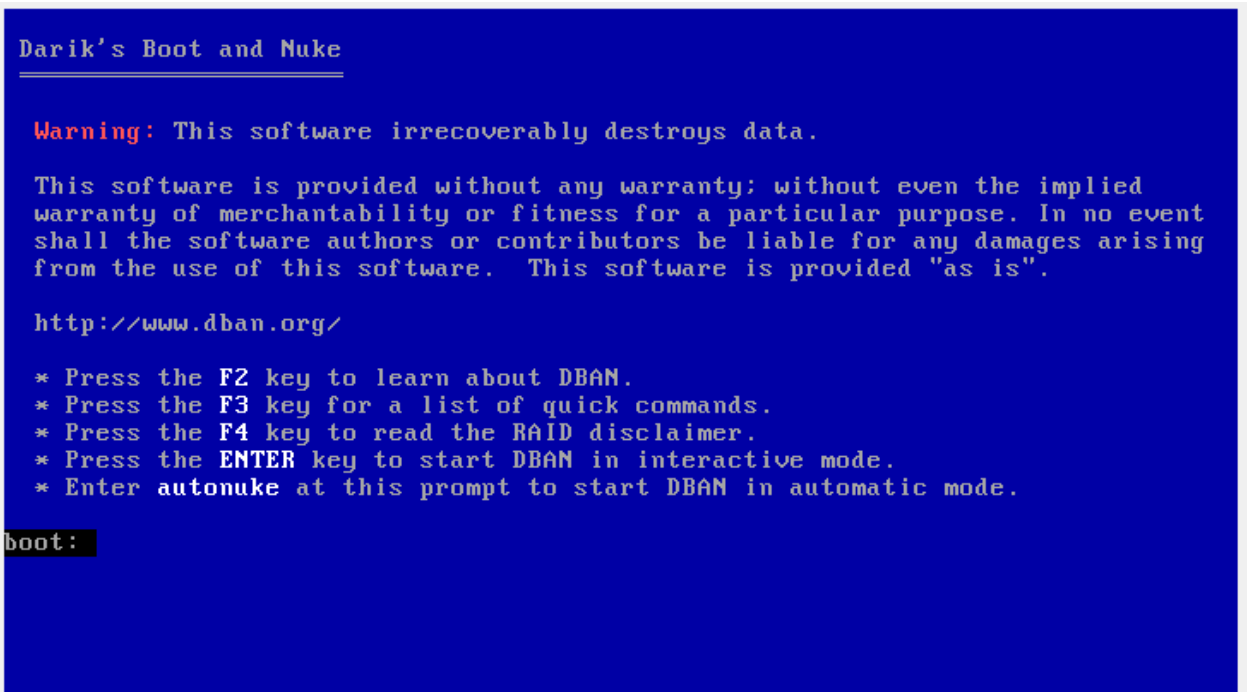
Task 2:



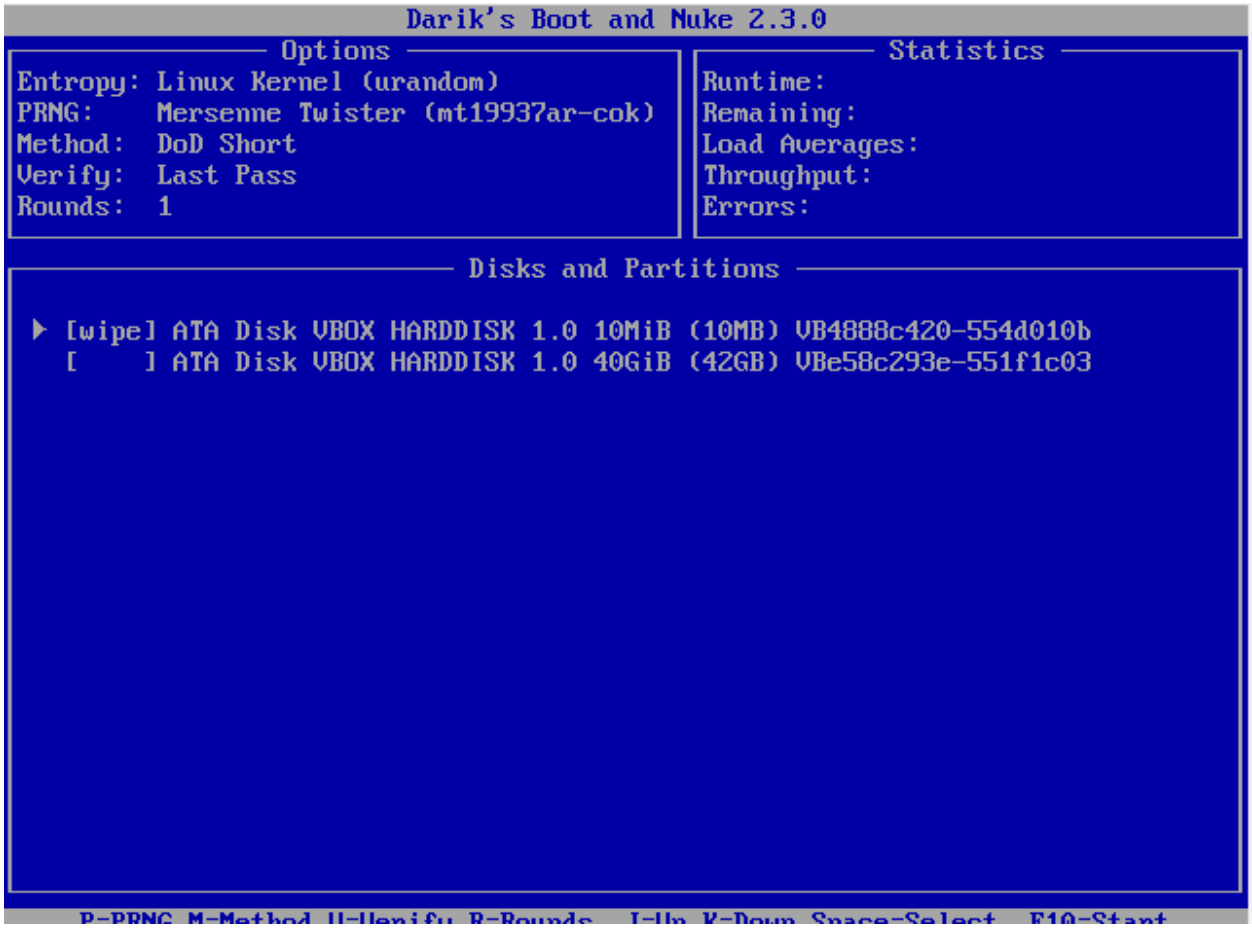
In this step, I have downloaded the DBAN ISO to my host machine and have added it to my Windows VM.



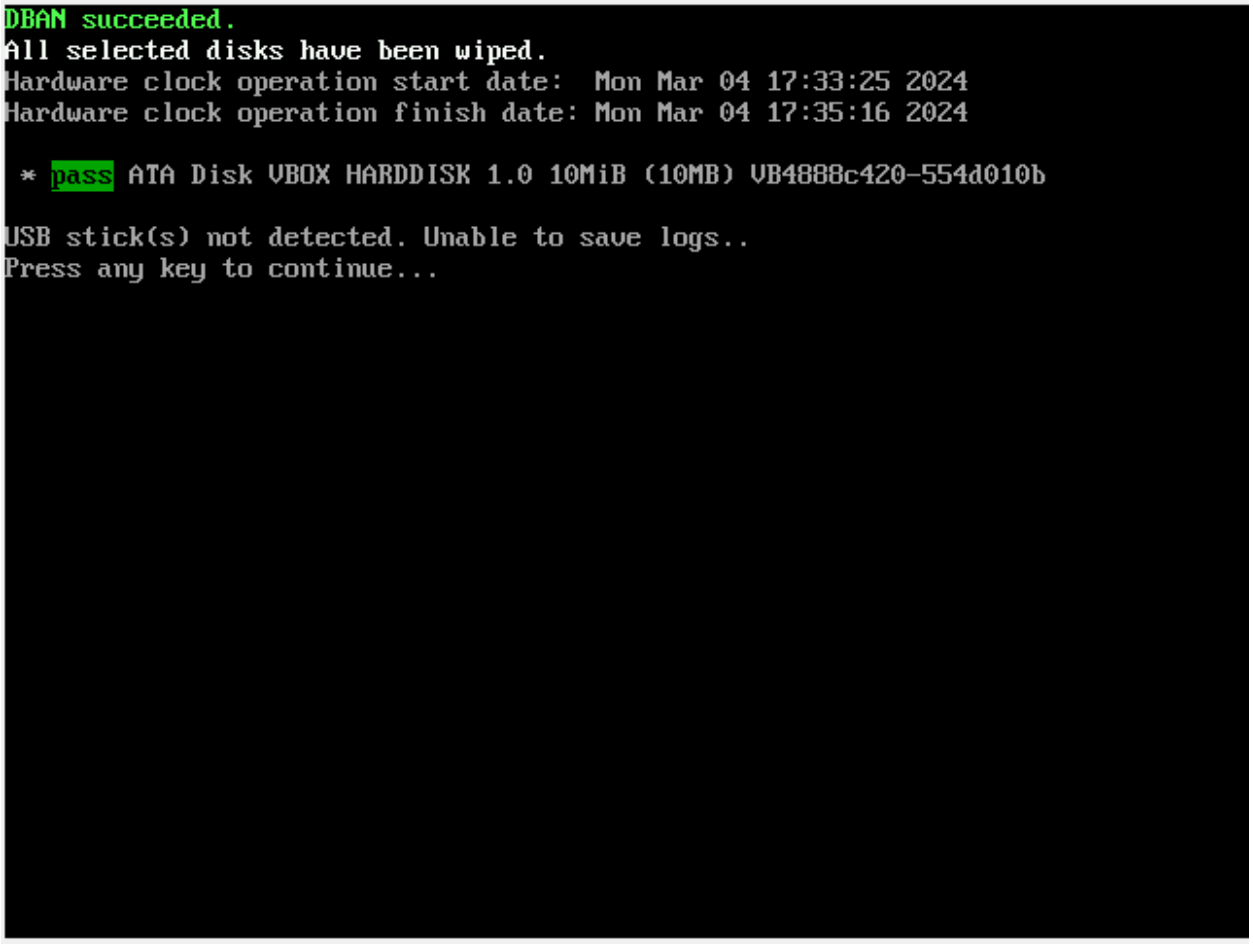
In this step, I have moved the Optical disk to the top of the boot order.



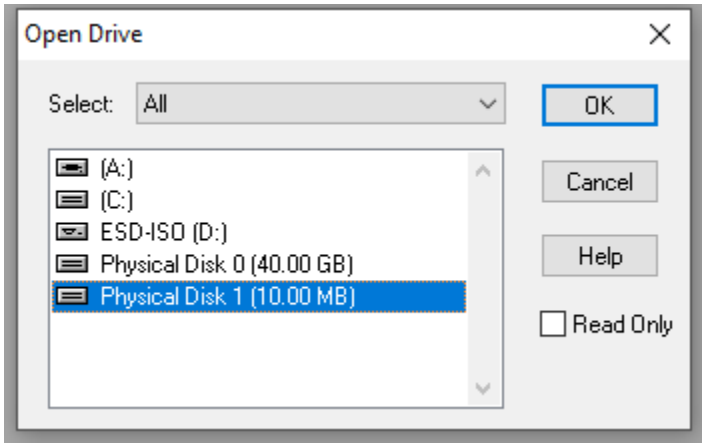
In this step, I have DBAN booted.



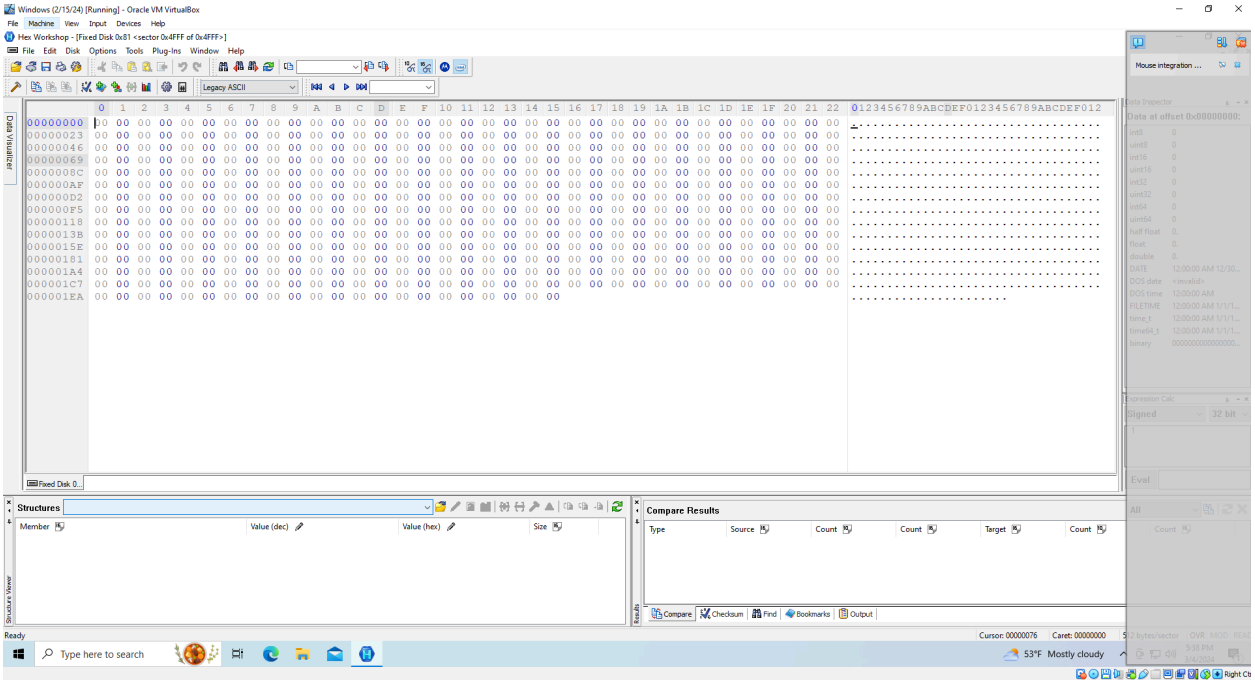
In this step, I have selected the correct drive.



The selected drive has been wiped.



In this step, I have loaded back the Windows VM and am running Hex Workshop as an admin. I am going to open the drive that was just wiped.



The sectors are empty, meaning that DBAN has worked.

Other methods we could have used instead of DoD are Random Data Overwrite, Zero-Fill and the Gutmann Method. The Random Data Overwrite involves overwriting the entire hard drive with random data patterns multiple times. The Zero-Fil method involves overwriting the entire hard drive with zeros once. The Gutmann method involves overwriting the hard drive 35 times with various patterns. The Gutmann method is the most secure out of the 3 since it goes over the hard drive 35 times, overwriting its data every time.