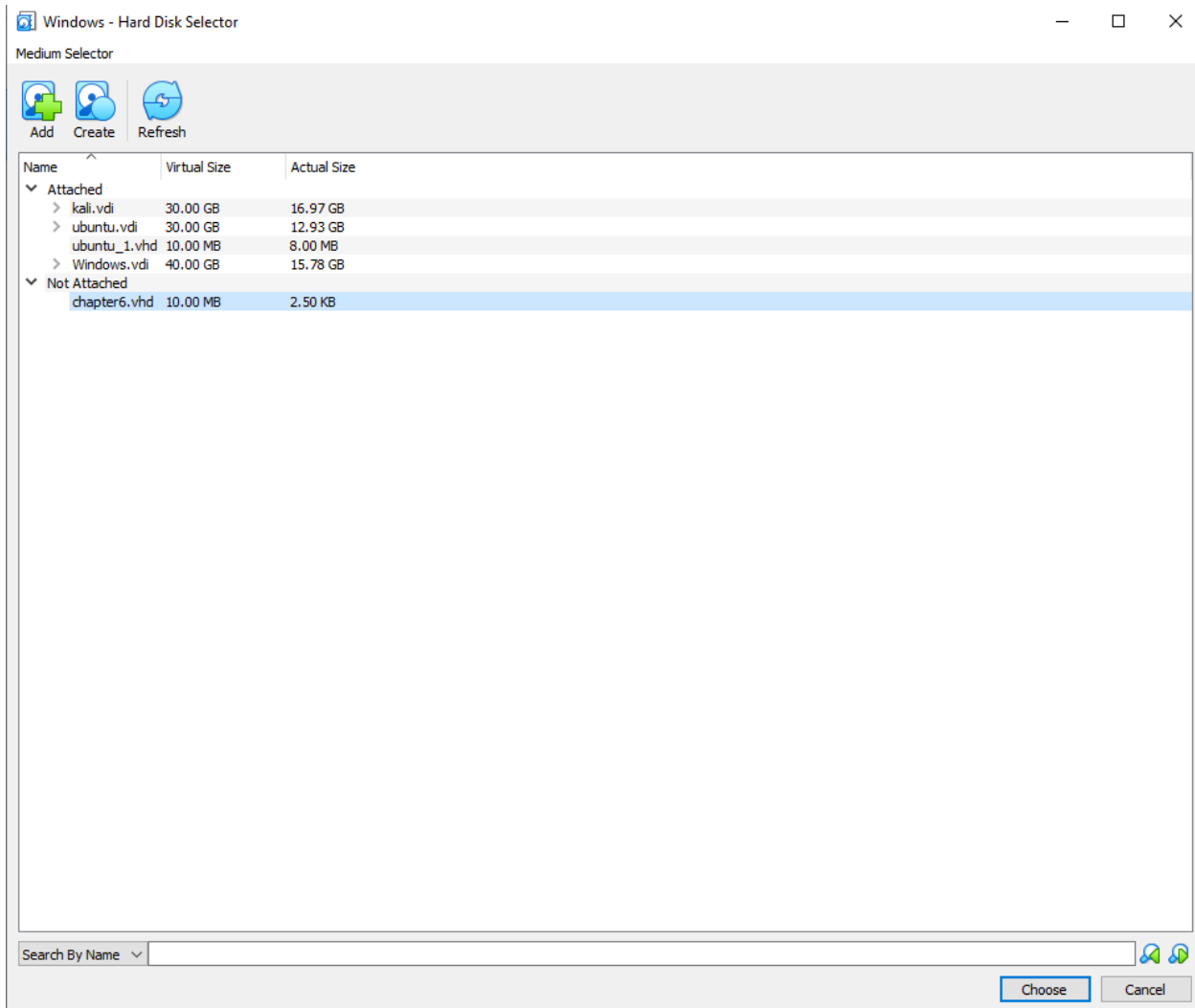
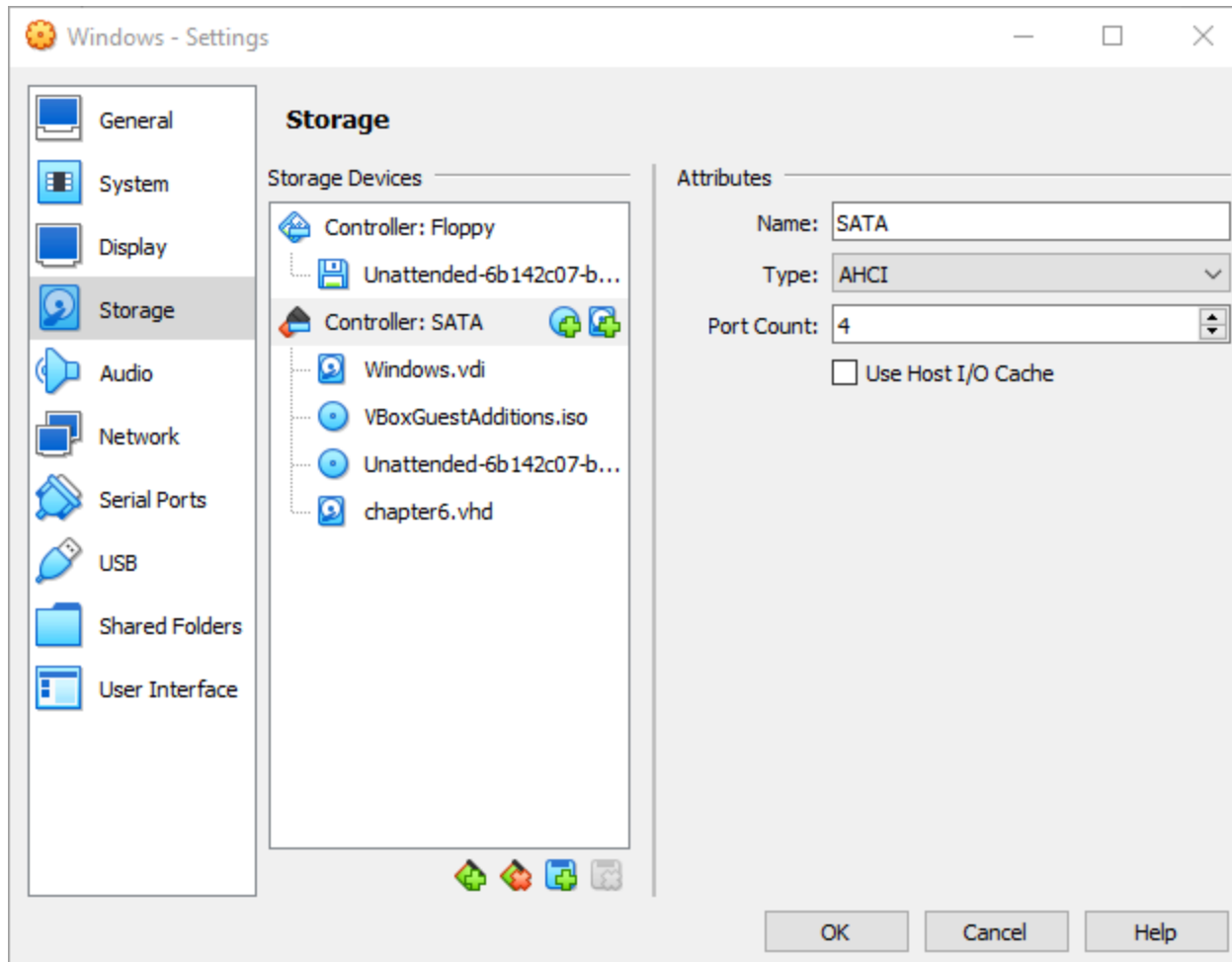


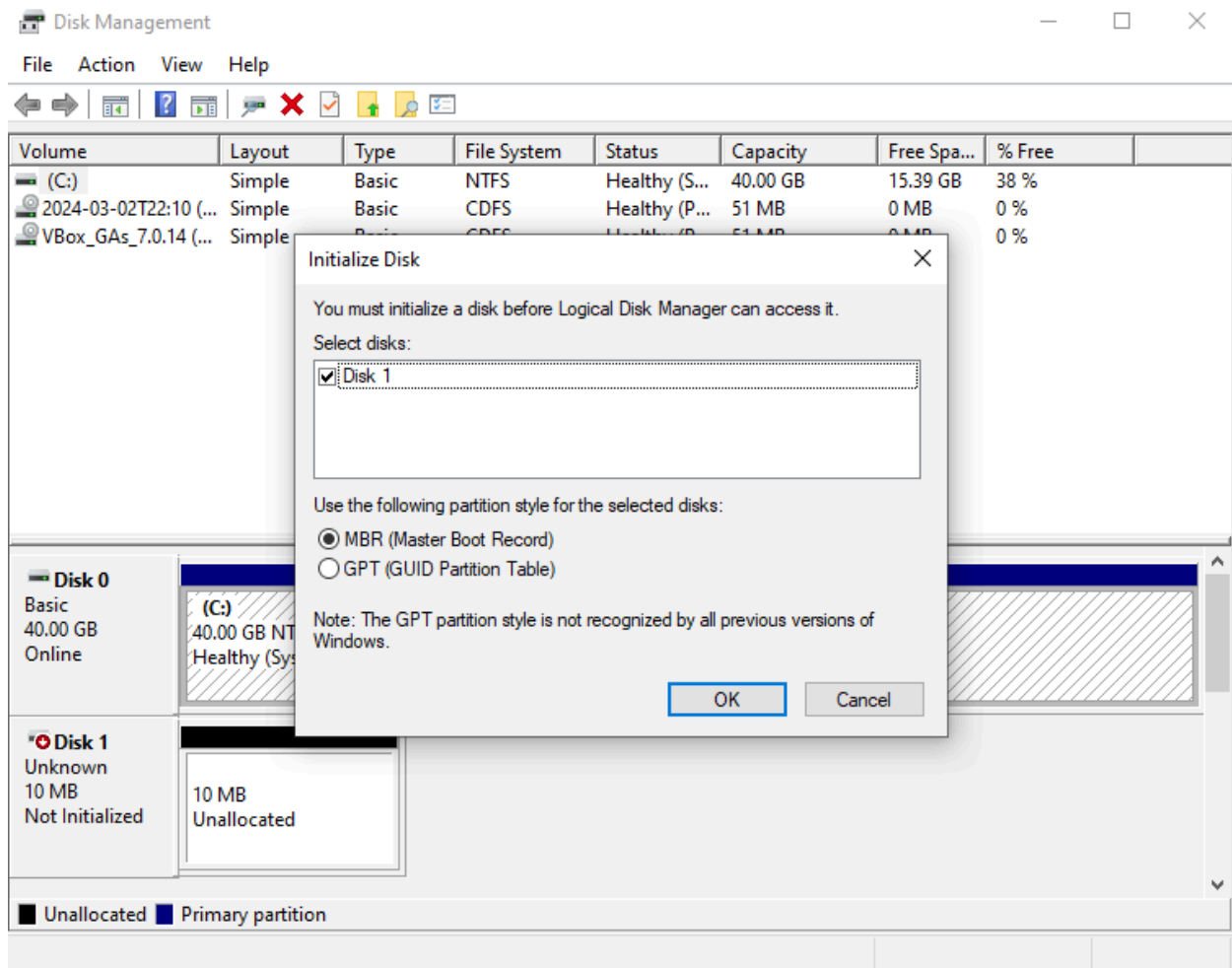
## Task 1:



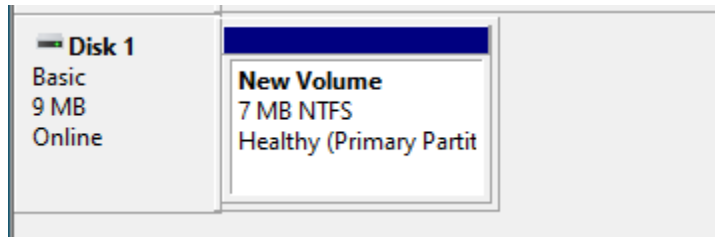
In this step, I have created a new virtual hard disk for my Windows VM and I am about to attach it to the VM.



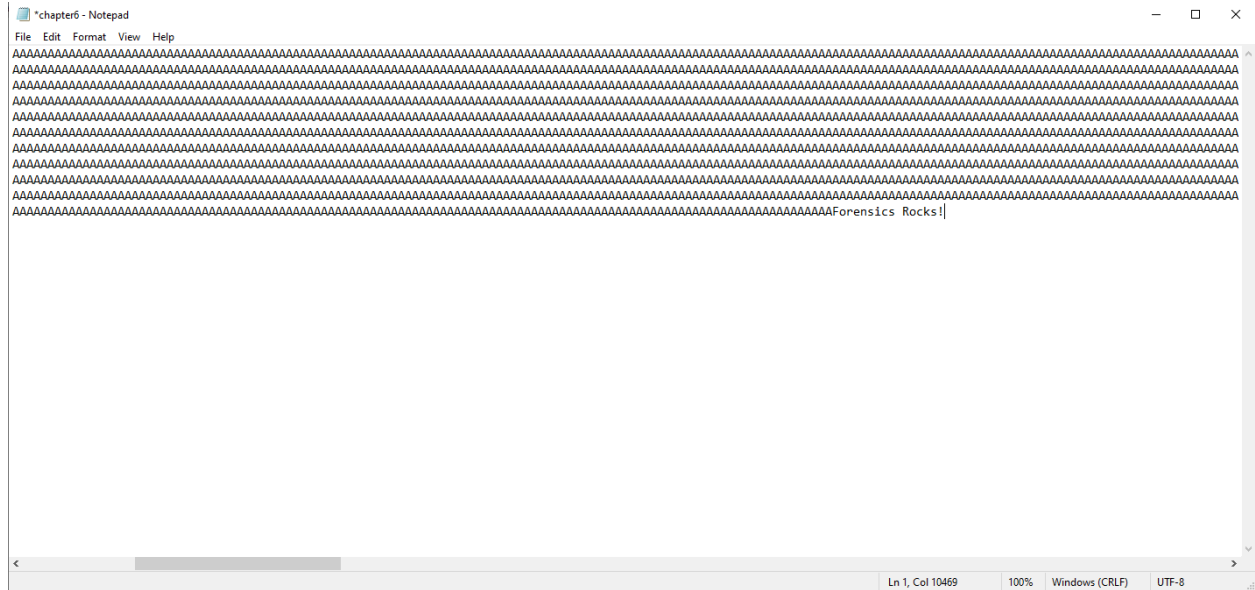
The VHD is attached to the Windows VM.



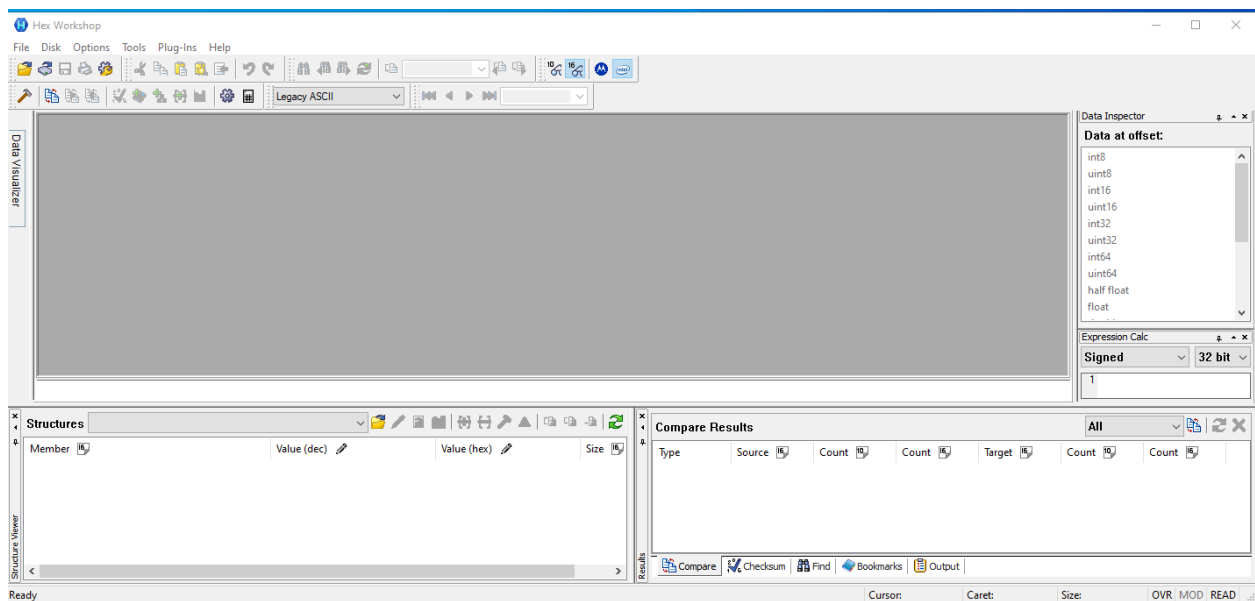
In this step, I am in the Windows VM and have opened the Disk Management Utility and am initializing disk 1.



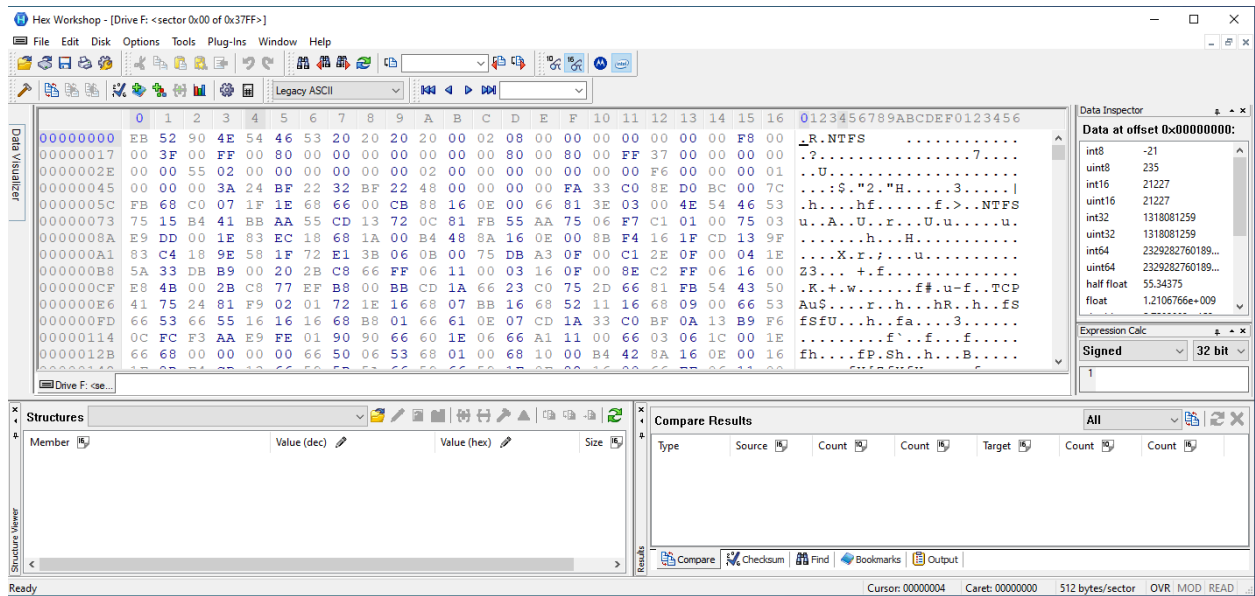
In this step, I have created a partition for Disk 1.



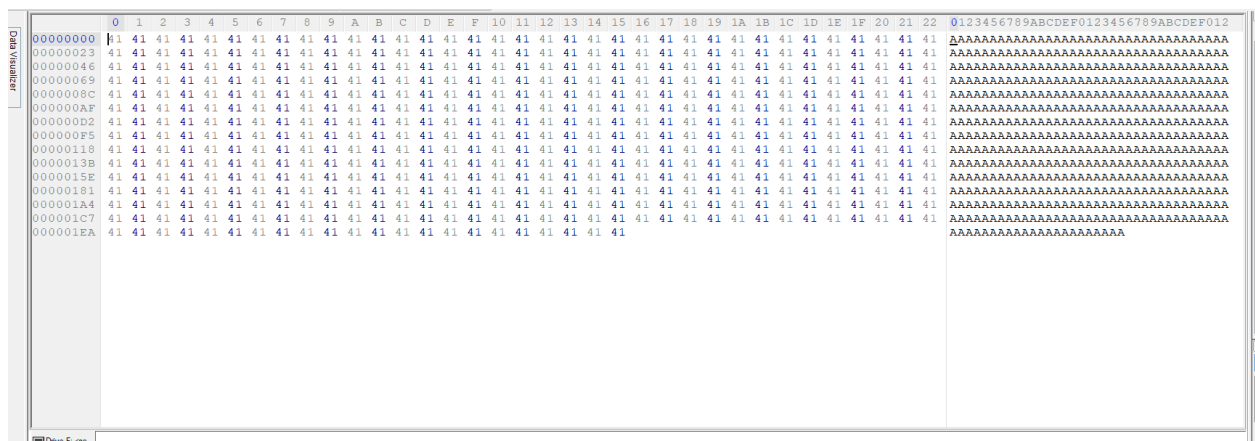
In this step, I have created a file in the new drive that was created and added 10k “A”s to the file.



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.

Find

Criteria Range

Find What:

Type: Text String Default ANSI: cp\_acp

Value: Forensics

Hex: 466F 7265 6E73 6963 73

Options

☐ Find All Instances ☐ Match Case

☒ UTF-8 String

☐ ANSI String

☐ Unicode String

☐ All

Direction

☐ Up

☒ Down

OK Cancel Apply

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

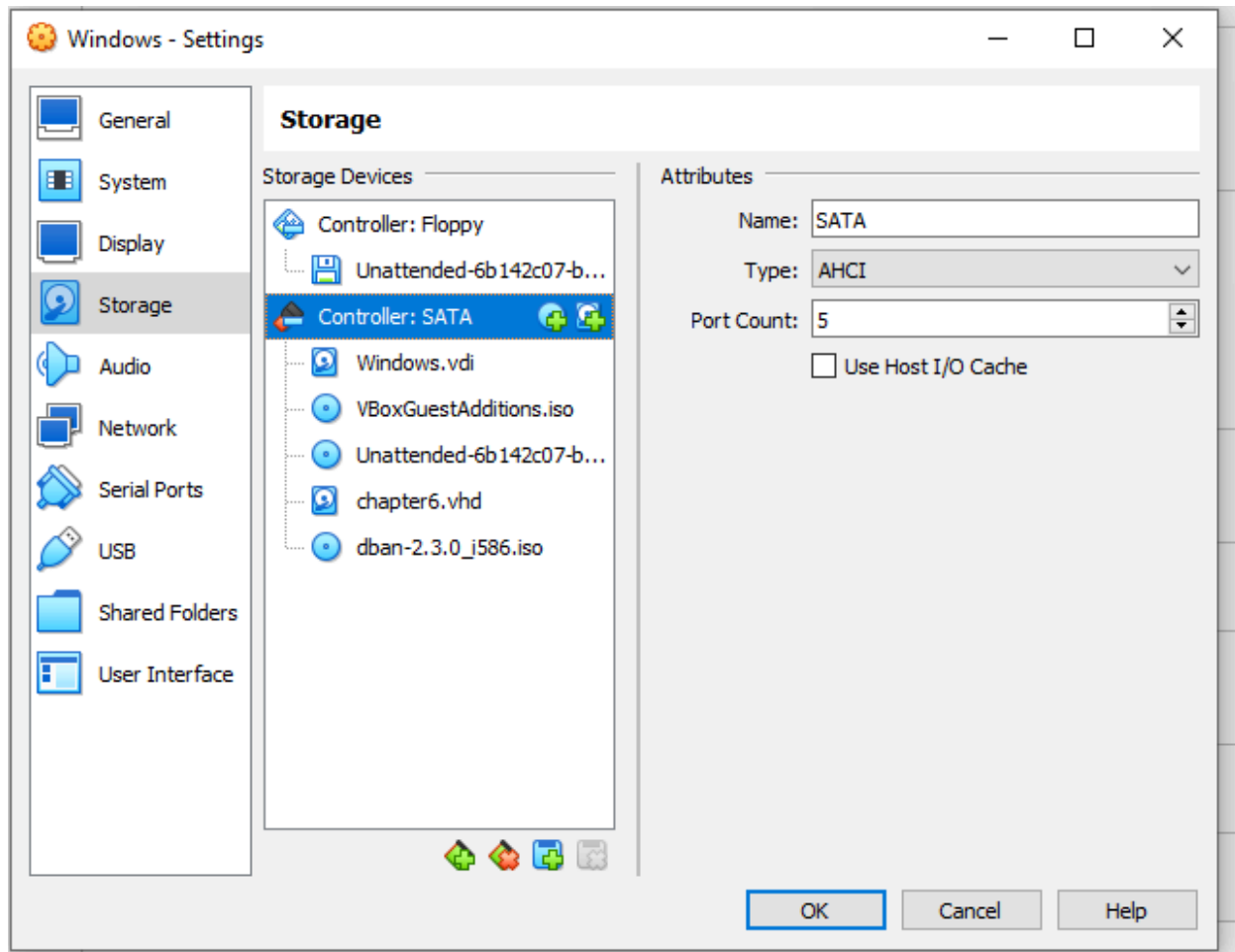
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	20	21	22	0123456789ABCDEF0123456789ABCDEF012
00000000	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00000023	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00000046	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
00000069	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0000008C	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
000000AF	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
000000D2	41	41	46	6F	72	65	6E	73	69	63	73	20	52	6F	63	6B	73	21	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	AAForensics Rocks!.....
000000F5	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000118	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
0000013B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
0000015E	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
00000181	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000001A4	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000001C7	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	
000001EA	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....	

Drive F - cse

“Forensics” has been found.

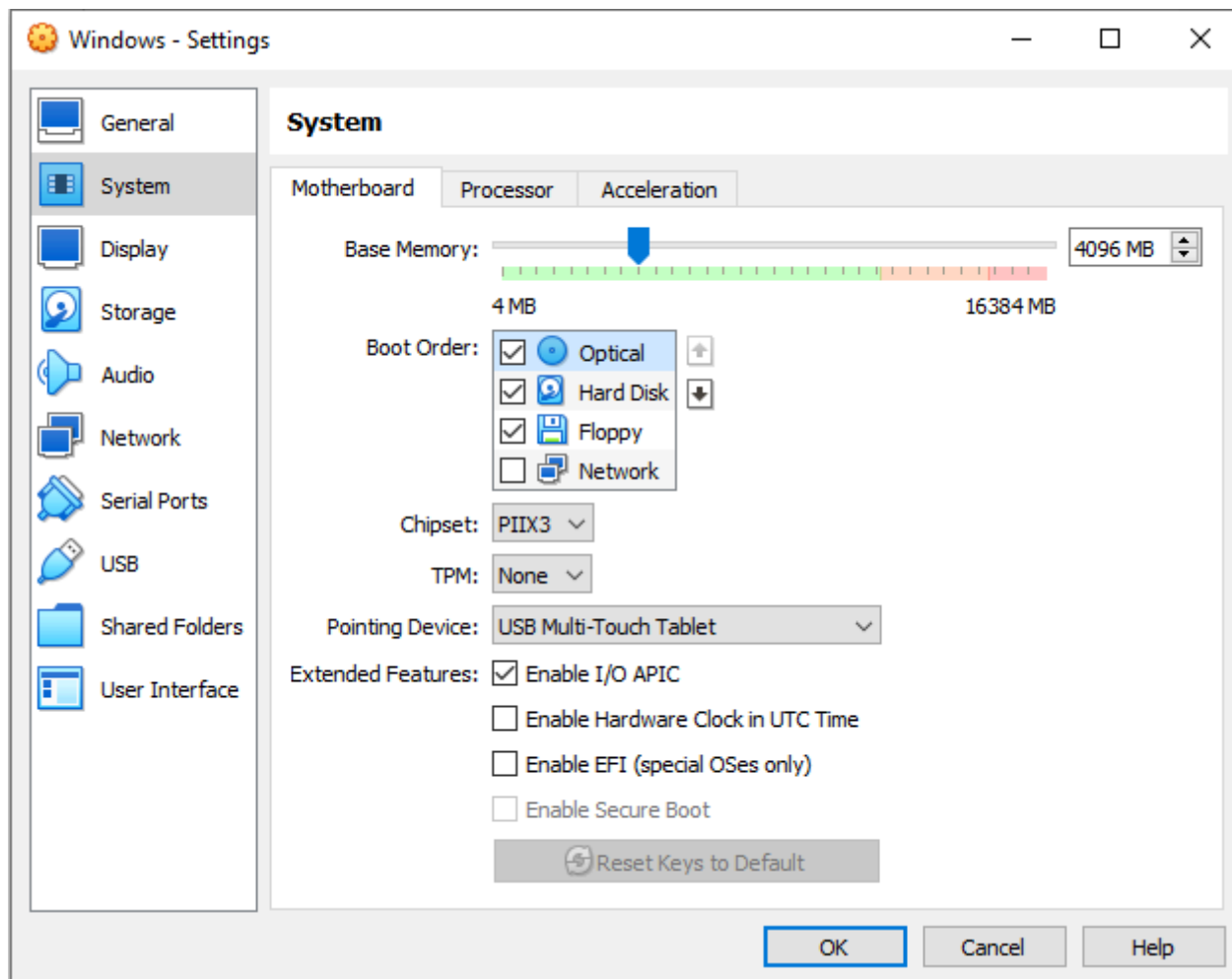
[illegible][illegible]

### 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.

## Darik's Boot and Nuke

**Warning:** This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose. In no event shall the software authors or contributors be liable for any damages arising from the use of this software. This software is provided "as is".

<http://www.dban.org/>

- \* Press the F2 key to learn about DBAN.
- \* Press the F3 key for a list of quick commands.
- \* Press the F4 key to read the RAID disclaimer.
- \* Press the ENTER key to start DBAN in interactive mode.
- \* Enter autonuke at this prompt to start DBAN in automatic mode.

boot:

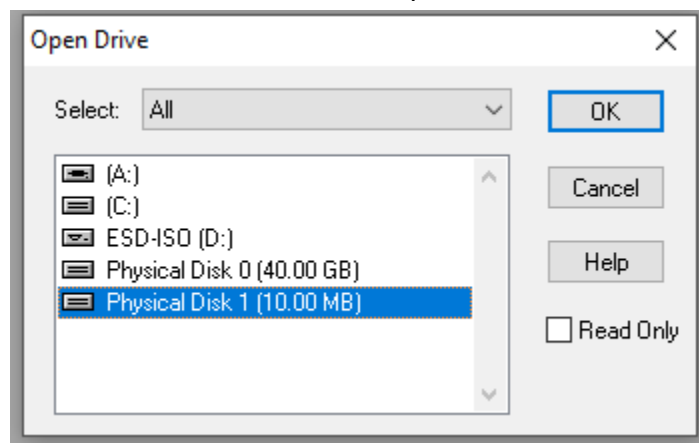
In this step, I have DBAN booted.

Darik's Boot and Nuke 2.3.0	
Options	Statistics
Entropy: Linux Kernel (urandom)	Runtime:
PRNG: Mersenne Twister (mt19937ar-cok)	Remaining:
Method: DoD Short	Load Averages:
Verify: Last Pass	Throughput:
Rounds: 1	Errors:
Disks and Partitions	
▶ [wipe] ATA Disk VBox HARDDISK 1.0 10MiB (10MB) VB4888c420-554d010b	
[ ] ATA Disk VBox HARDDISK 1.0 40GiB (42GB) VBe58c293e-551f1c03	
P-PRNG M-Method H-Hexify R-Rounds L-Up V-Down Space-Select F10-Start	

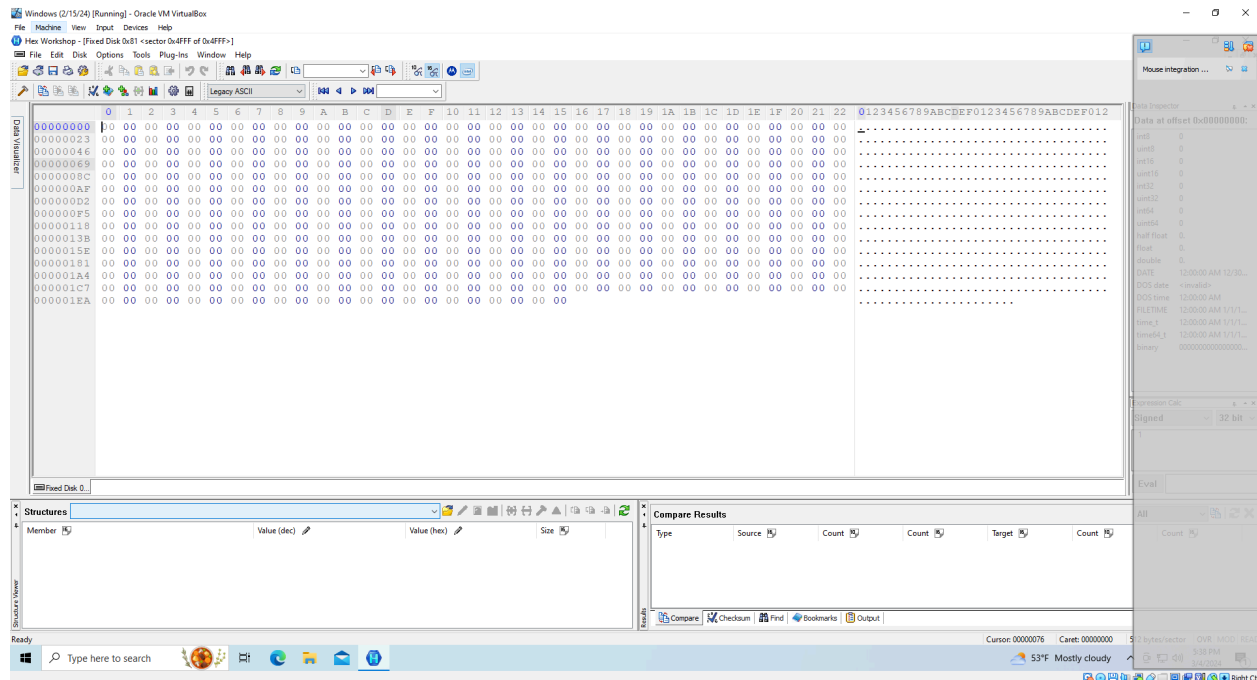
In this step, I have selected the correct drive.

```
DBAN succeeded.  
All selected disks have been wiped.  
Hardware clock operation start date: Mon Mar 04 17:33:25 2024  
Hardware clock operation finish date: Mon Mar 04 17:35:16 2024  
  
* pass ATA Disk VBox HARDDISK 1.0 10MiB (10MB) VB4888c420-554d010b  
  
USB stick(s) not detected. Unable to save logs..  
Press any key to continue...
```

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-Fill 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.