Maria Valencia

CSC 153

LAB 6

Lab 6: File Slack and Wiping

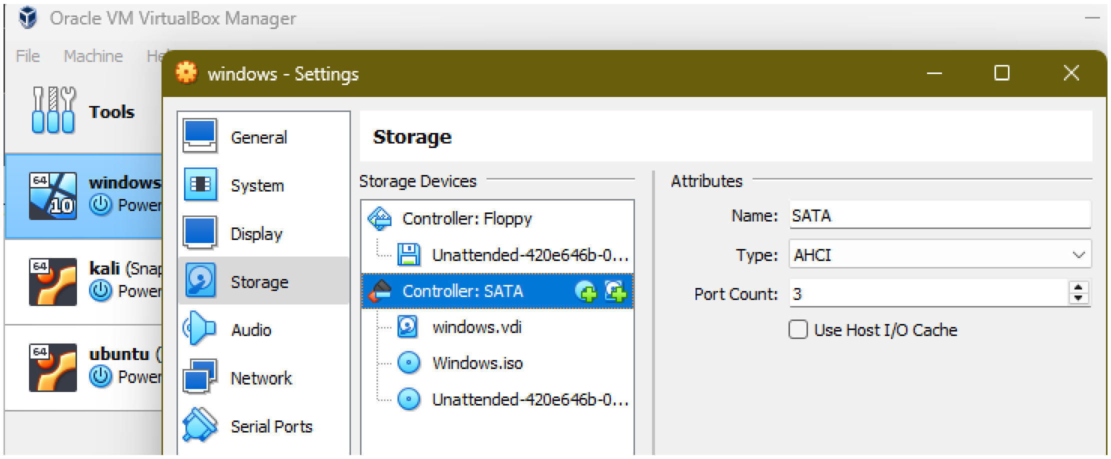
In this lab, I will complete two tasks inspired by the Hand-On Projects 6-2 and 6-3. The first task requires that I create a USB VHD and store secret data in the file slack of a sample file. The second task securely wipes that USB VHD created.

Task 1: File Slack

In this task I created a virtual device and attached it to my windows VM. The drive is used to host a file that I wrote additional data in its slack space using Hex Workshop.

Step 1: Create “USB” virtual drive

I launched the VM’s settings in VirtualBox and selected storage. Selected “Controller:SATA” within the storage Devices section and pressed the add drive button.



Storage

Storage Devices

- Controller: Floppy
  - Unattended-420e646b-0…
- Controller: SATA
  - windows.vdi
  - Windows.iso
  - Unattended-420e646b-0…

Attributes

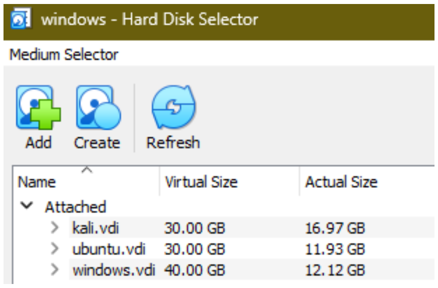
Name: SATA

Type: AHCI

Port Count: 3

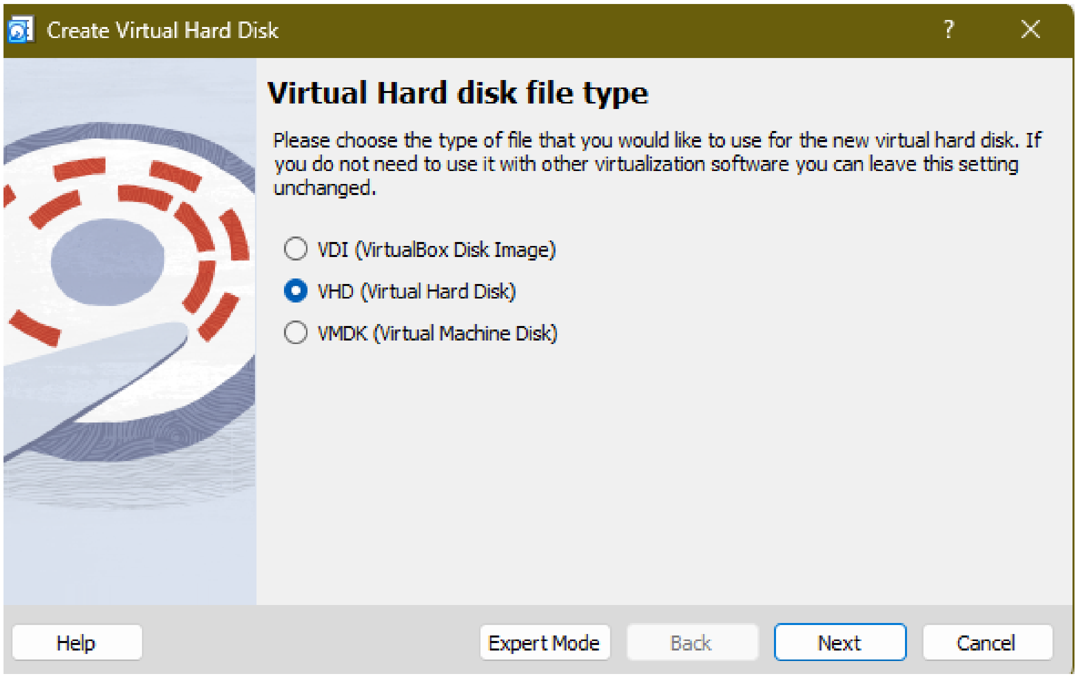
☐ Use Host I/O Cache

Selected the Create Button.



Name	Virtual Size	Actual Size
Attached		
kali.vdi	30.00 GB	16.97 GB
ubuntu.vdi	30.00 GB	11.93 GB
windows.vdi	40.00 GB	12.12 GB

Selected VHD and Next.



Virtual Hard disk file type

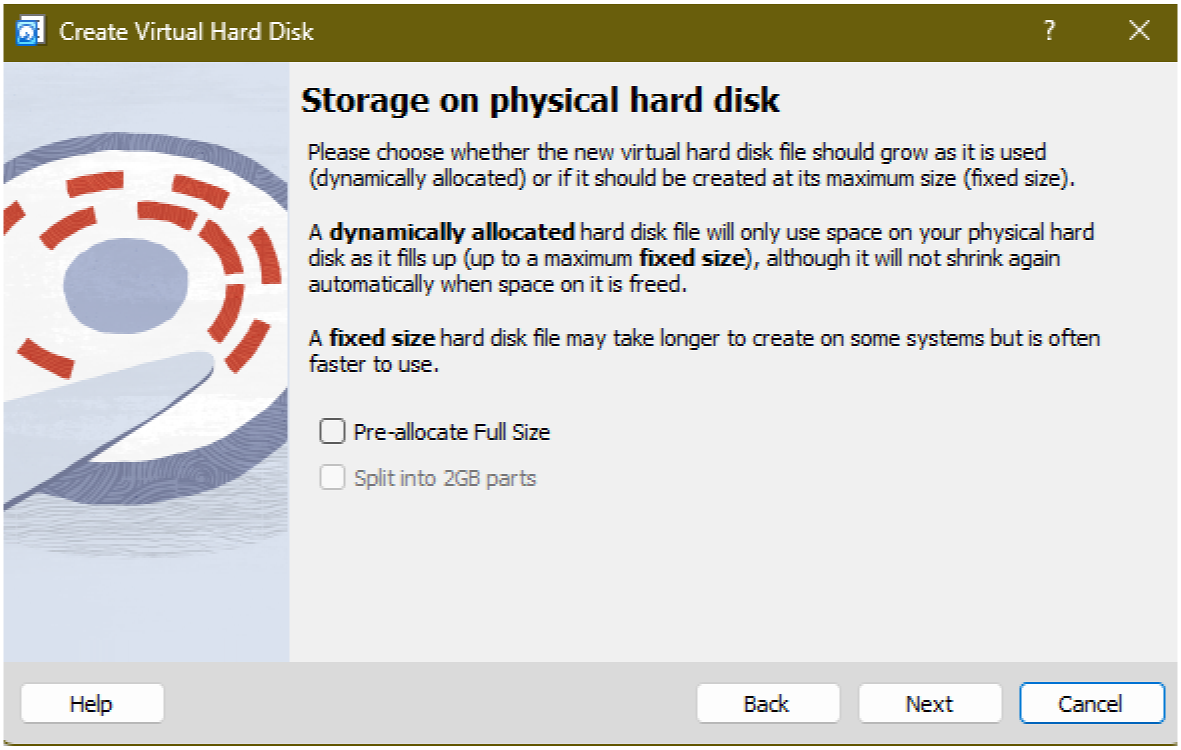
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

○ VDI (VirtualBox Disk Image)

● VHD (Virtual Hard Disk)

○ VMDK (Virtual Machine Disk)

Selected Next on the Storage on physical hard disk step.



Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

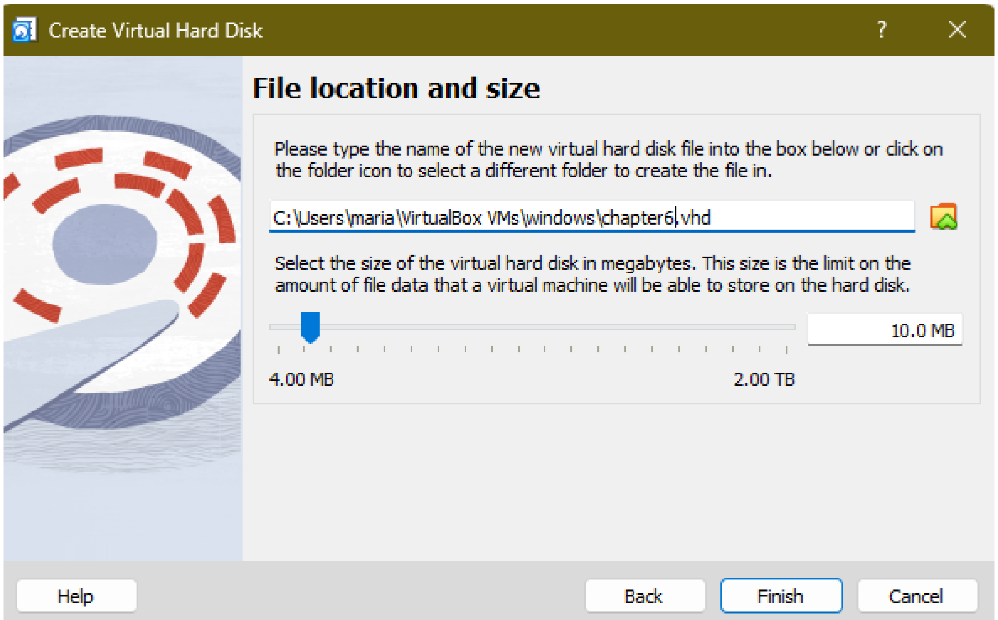
A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

☐ Pre-allocate Full Size

☐ Split into 2GB parts

I changed the file name to "chapter6.vhd" and 10MBs and pressed Finish.



File location and size

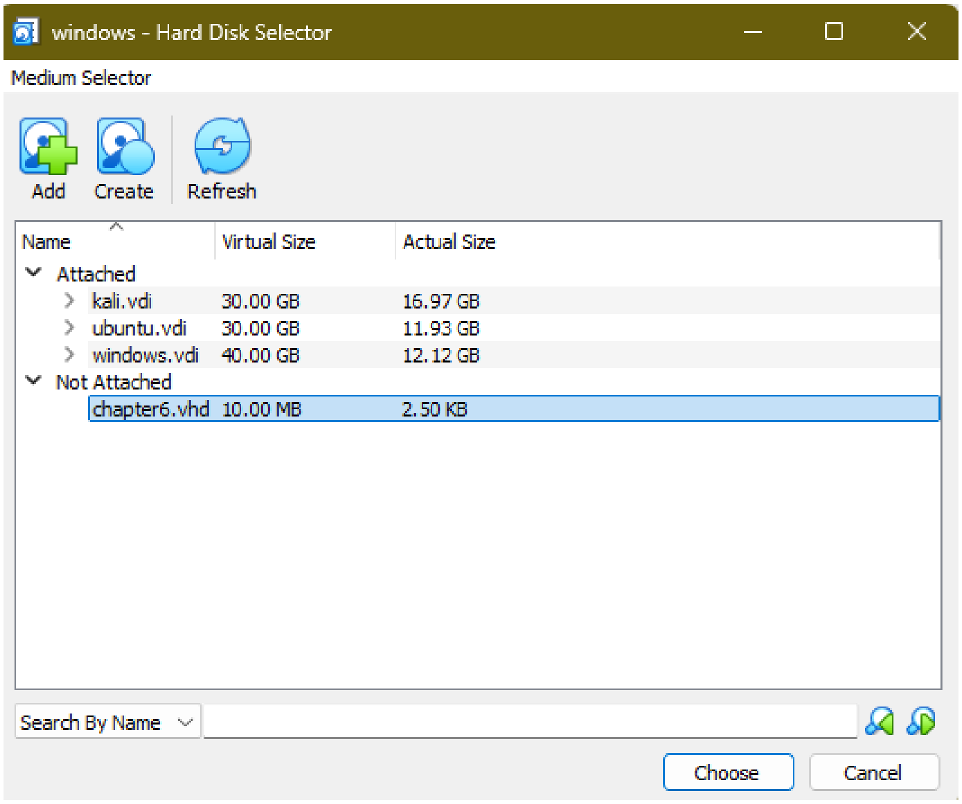
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

C:\Users\maria\VirtualBox VMs\windows\chapter6.vhd

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

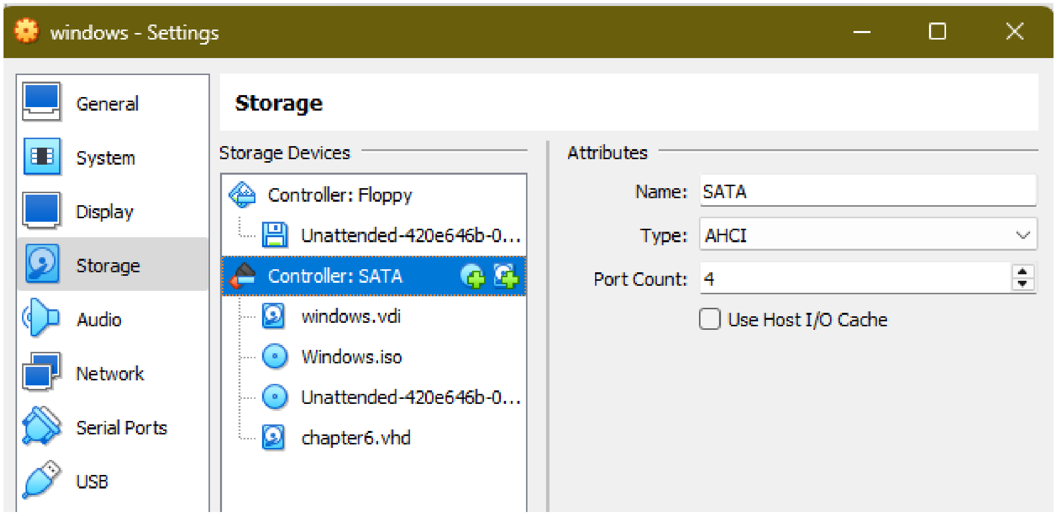
10.0 MB

I selected the chapter6.vhd under "Not Attached" and then choose.



Name	Virtual Size	Actual Size
Attached		
kali.vdi	30.00 GB	16.97 GB
ubuntu.vdi	30.00 GB	11.93 GB
windows.vdi	40.00 GB	12.12 GB
Not Attached		
chapter6.vhd	10.00 MB	2.50 KB

I observe that the drive is now attached to the VM. I pressed OK and then started the VM.



Controller: Floppy
- Unattended-420e646b-0…

Controller: SATA
- windows.vdi
- Windows.iso
- Unattended-420e646b-0…
- chapter6.vhd

Name: SATA

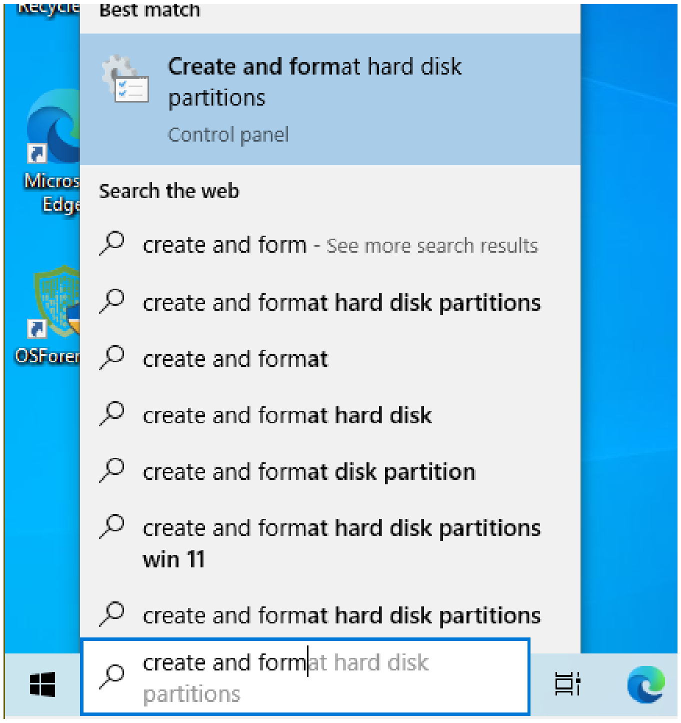
Type: AHCI

Port Count: 4

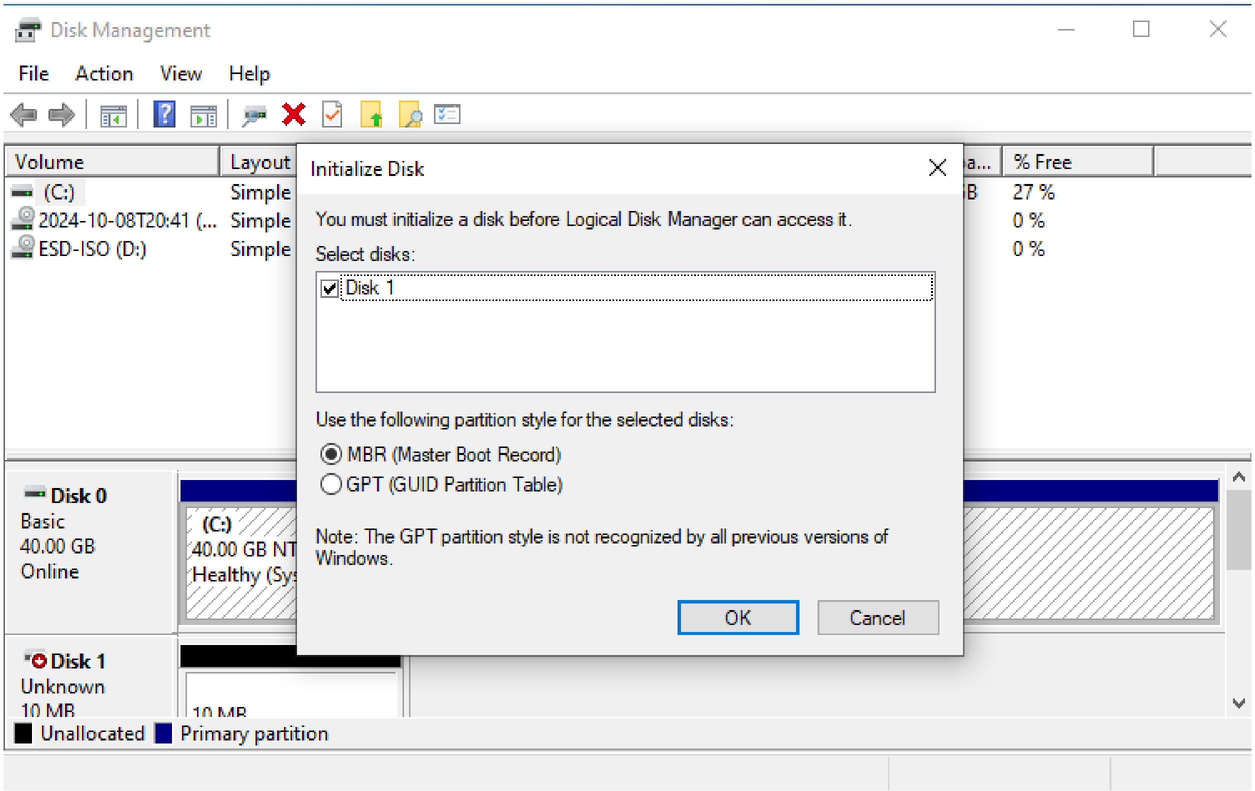
☐ Use Host I/O Cache

Step 2: Setup the "USB"

With the VHD attached and the windows VM booted, I launched the Disk Management app by searching "Create and format disk partitions".


Recycle
Micros
Edge
OSForen
Best match
Create and format hard disk partitions
Control panel
Search the web
create and form - See more search results
create and format hard disk partitions
create and format
create and format hard disk
create and format disk partition
create and format hard disk partitions win 11
create and format hard disk partitions
create and format hard disk partitions

When the Disk Management utility launched, I selected MBR and OK to the recommended prompt.



Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 1

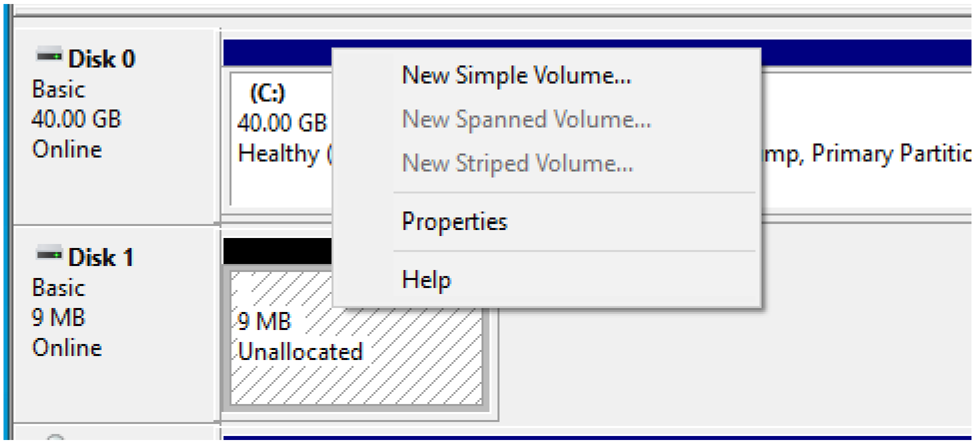
Use the following partition style for the selected disks:

● MBR (Master Boot Record)

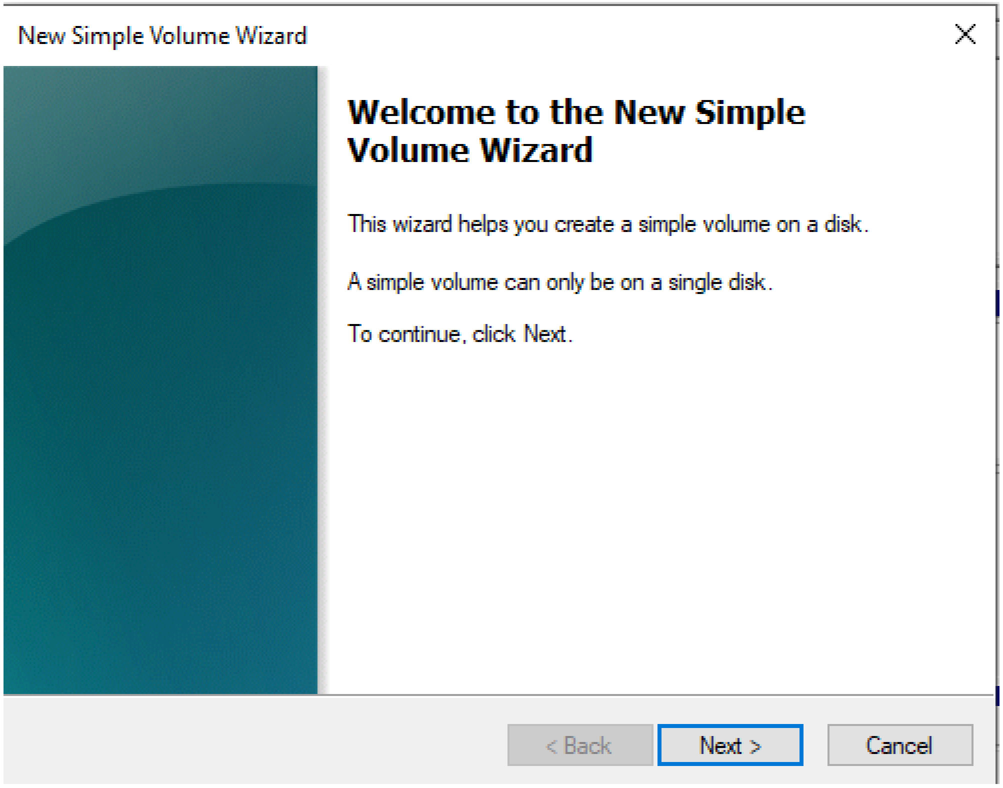
○ GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows.

With disk 1 initialized, I right clicked the drive and selected New Simple Volume from the context menu.



Selecting New Simple Volume launches the Set up wizard. I followed the wizard use default options.



New Simple Volume Wizard

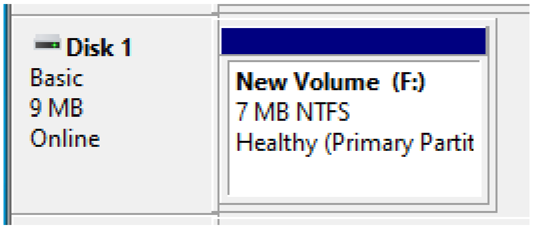
Welcome to the New Simple Volume Wizard

This wizard helps you create a simple volume on a disk.

A simple volume can only be on a single disk.

To continue, click Next.

Once Completed, it shows a 7MB NTFS volume.

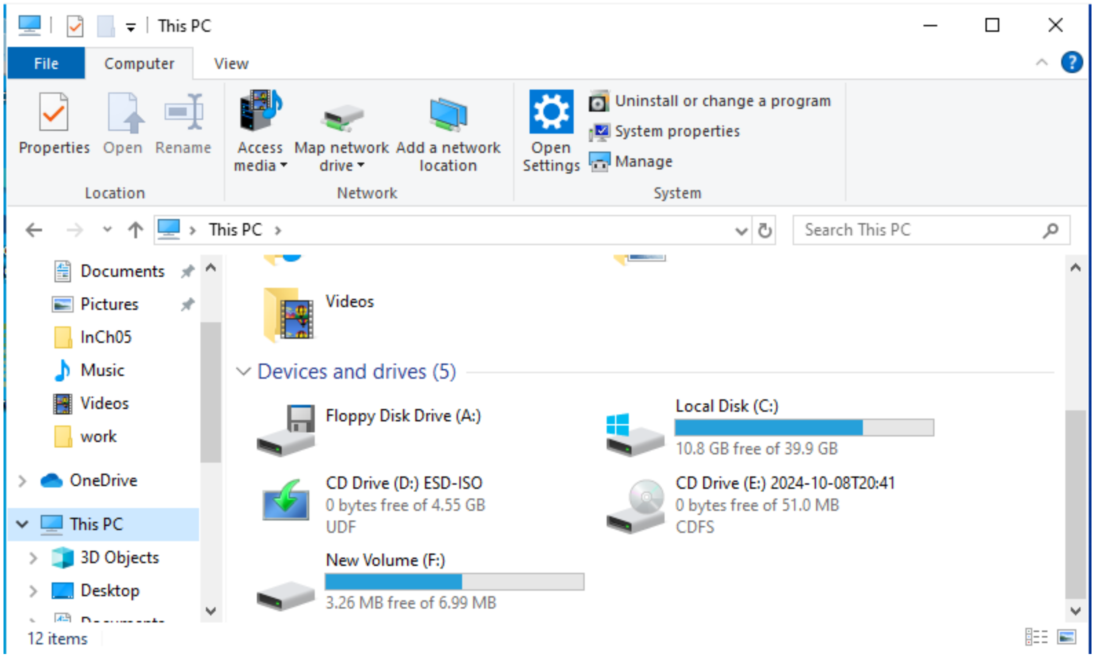


Disk 1
Basic
9 MB
Online

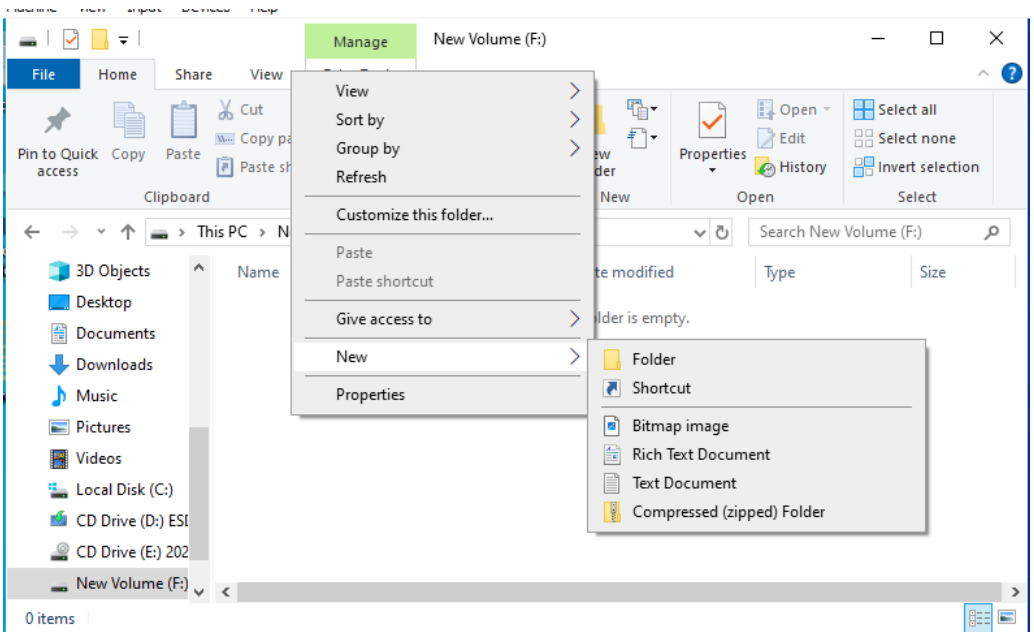
New Volume (F:)
7 MB NTFS
Healthy (Primary Partit

Step 3: Create a Test File

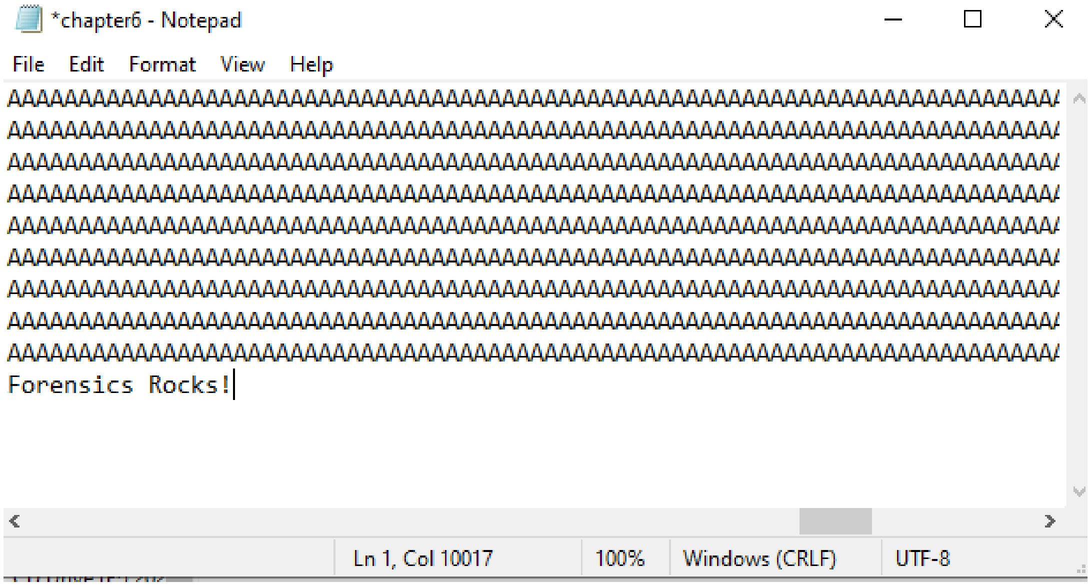
I opened File explorer and navigated to the E drive.



I right clicked in the open space drive, selected New and text document to create a new file. I named the file chapter 6.



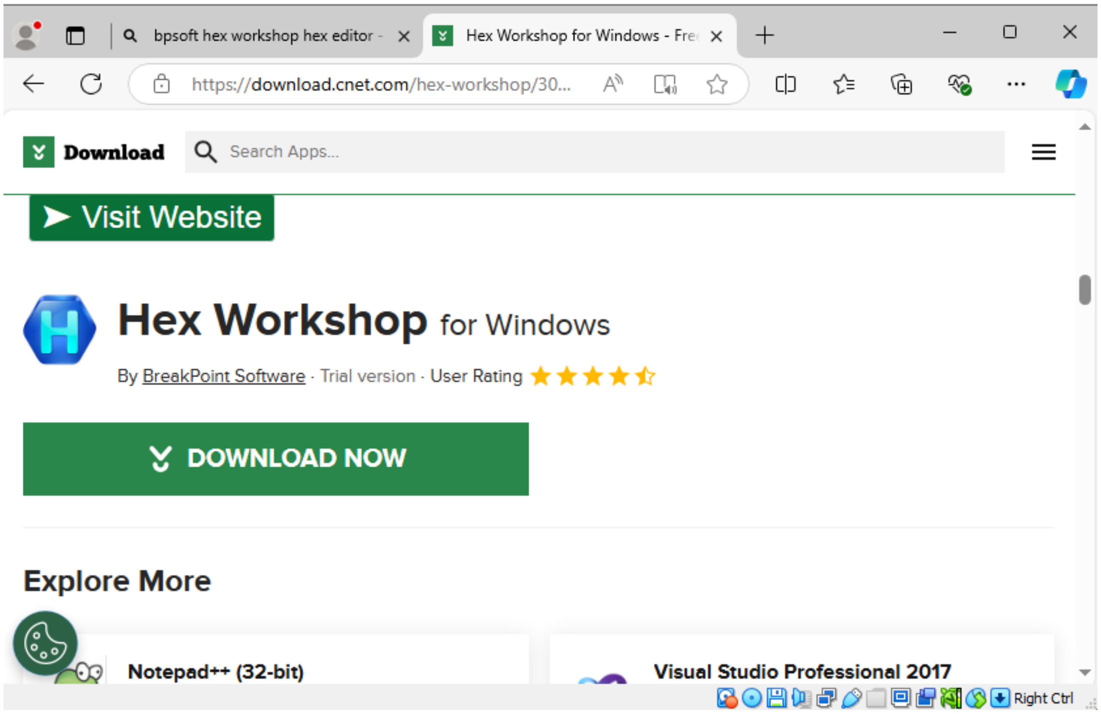
I opened the chapter6 text file and filled it with 10000 capital A’s. And the phrase “Forensics Rocks at the end. Then Save and close the text file.



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Forensics Rocks!
```

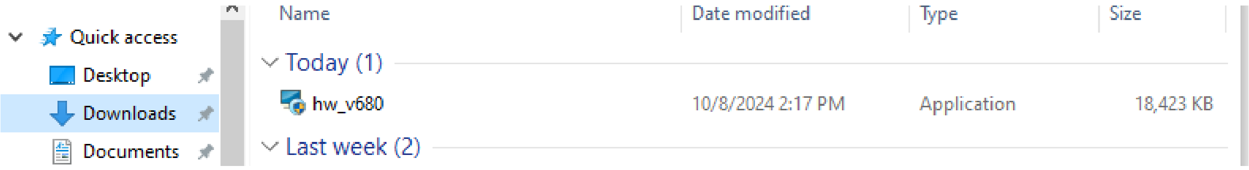
Step 4: Install Hex Workshop

I opened a web browser and navigated to http://www.bpsoft.com/downloads/ and downloaded the latest version of Hex Workshop Hex Editor. (this was unavailable so I found a work-around)



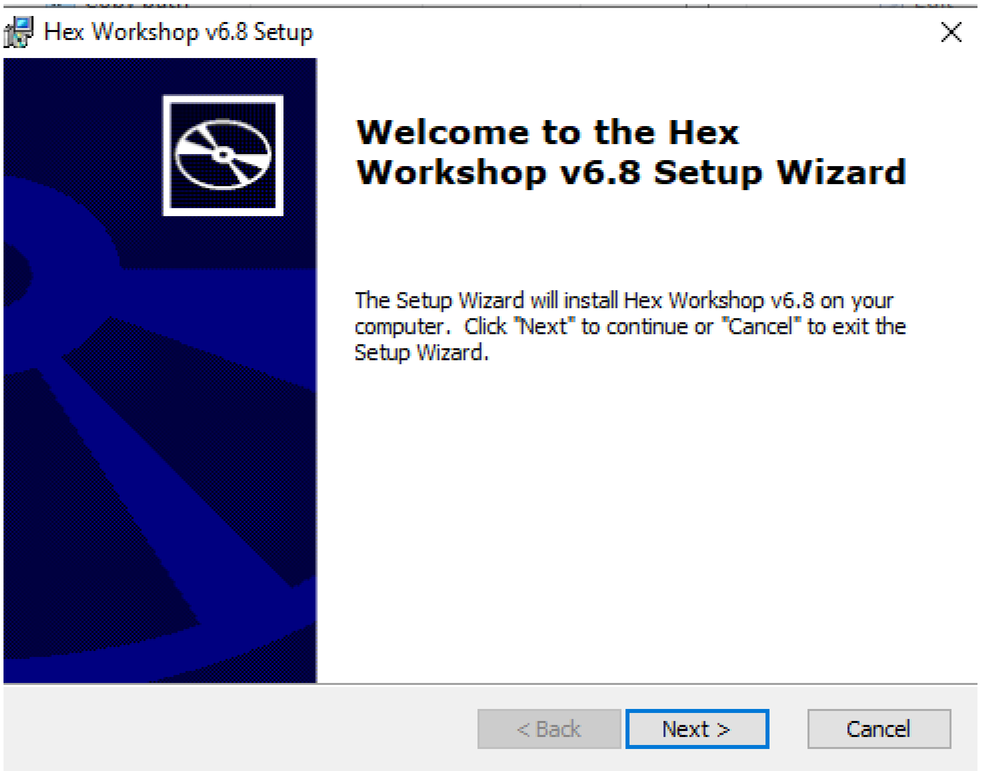
bpsoft hex workshop hex editor -
Hex Workshop for Windows - Fre
https://download.cnet.com/hex-workshop/30...
Download
Search Apps...
Visit Website
Hex Workshop for Windows
By BreakPoint Software · Trial version · User Rating
DOWNLOAD NOW
Explore More
Notepad++ (32-bit)
Visual Studio Professional 2017
Right Ctrl

Once it was downloaded, I went to my downloads folder and double clicked it to start the installation process. I accepted the UAC prompts.



Name	Date modified	Type	Size
hw_v680	10/8/2024 2:17 PM	Application	18,423 KB

Select next when the Hex Workshop installation wizard launches. Allow any older versions to be removed, accept the license agreement, and use the Typical setup type, then install. After a few seconds the installation should be complete. Select Finish and then reboot the Windows VM.

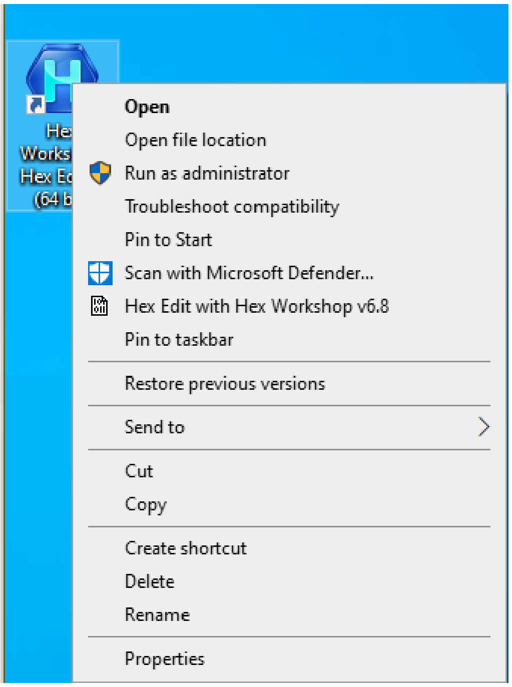


Welcome to the Hex Workshop v6.8 Setup Wizard

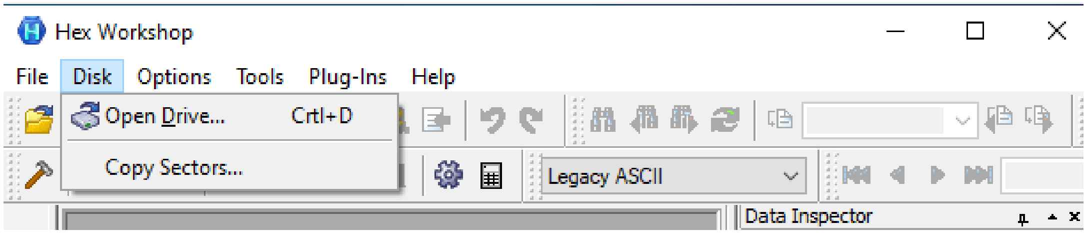
The Setup Wizard will install Hex Workshop v6.8 on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Step 5: Hide data in Slack Space

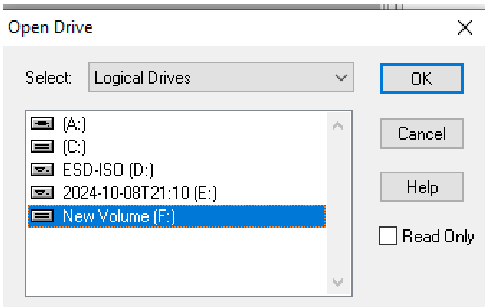
After the windows VM rebooted, I right-clicked the Hex Workshop Icon and ran as administrator to launch the application.



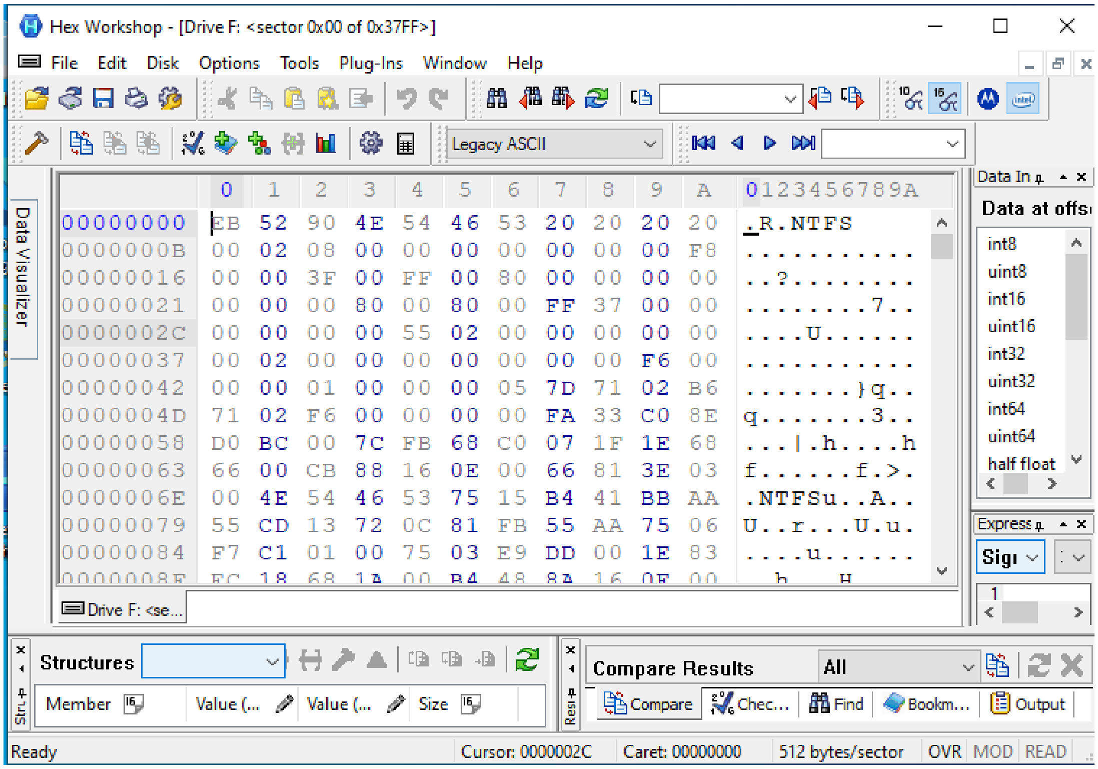
I opened the VHD/USB drive by selecting disk and then “Open Drive”.



I chose the “New Volume (E:)” and pressed OK.



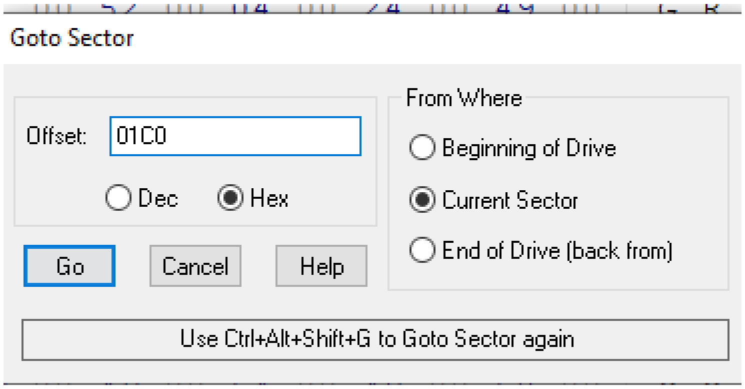
I observed the drives hexadecimal space is loaded with ASCII representation on the right column.



```
           0  1  2  3  4  5  6  7  8  9  A   0123456789A
00000000  EB 52 90 4E 54 46 53 20 20 20 20   .R.NTFS
0000000B  00 02 08 00 00 00 00 00 00 00 F8   ...........
00000016  00 00 3F 00 FF 00 80 00 00 00 00   ..?........
00000021  00 00 00 80 00 80 00 FF 37 00 00   ........7..
0000002C  00 00 00 00 55 02 00 00 00 00 00   ....U......
00000037  00 02 00 00 00 00 00 00 00 F6 00   ...........
00000042  00 00 01 00 00 00 05 7D 71 02 B6   .......}q..
0000004D  71 02 F6 00 00 00 00 FA 33 C0 8E   q.......3..
00000058  D0 BC 00 7C FB 68 C0 07 1F 1E 68   ...|.h....h
00000063  66 00 CB 88 16 0E 00 66 81 3E 03   f......f.>.
0000006E  00 4E 54 46 53 75 15 B4 41 BB AA   .NTFSu..A..
00000079  55 CD 13 72 0C 81 FB 55 AA 75 06   U..r...U.u.
00000084  F7 C1 01 00 75 03 E9 DD 00 1E 83   ....u......
0000008F  FC 18 68 1A 00 B4 48 8A 16 0F 00     h    H
```

Ready | Cursor: 0000002C | Caret: 00000000 | 512 bytes/sector | OVR | MOD | READ

Pressing the blue right triangle will load the next sector in the drive. Alternatively, press “Alt+Dn” to go to the next sector as a shortcut key. Cycle through the sectors until you find the sector filled with “A”s which may be 100s of sectors away from the 1st sector of the drive.


Goto Sector

Offset: 01C0

○ Dec ● Hex

From Where

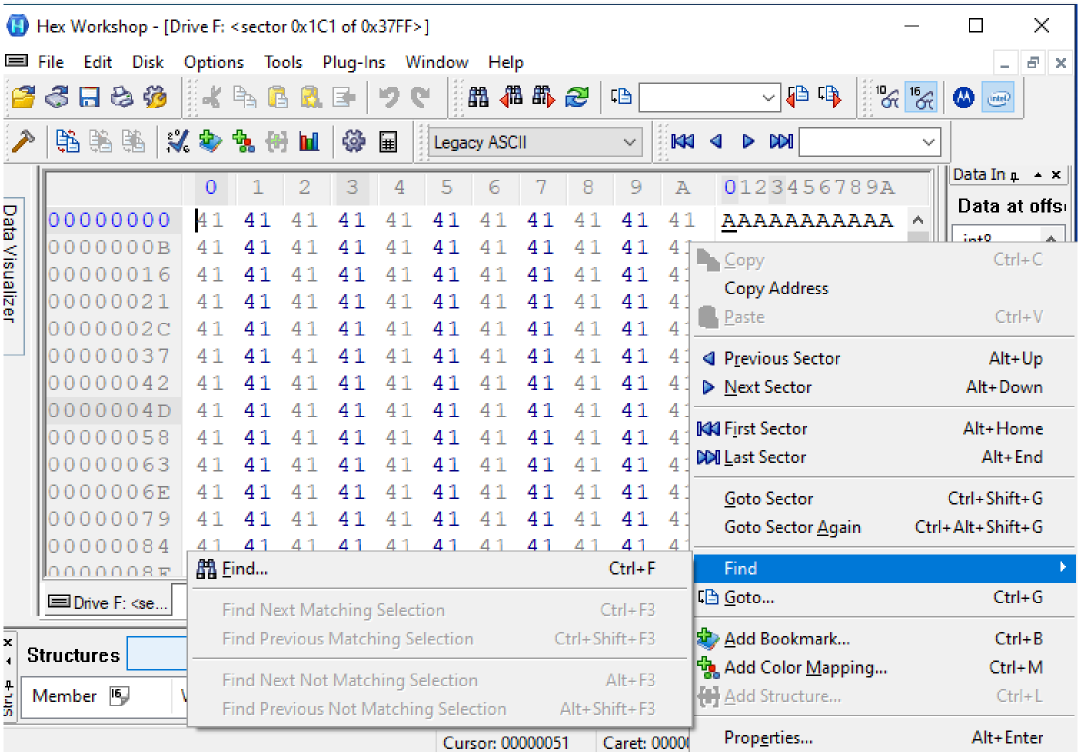
○ Beginning of Drive

● Current Sector

○ End of Drive (back from)

Use Ctrl+Alt+Shift+G to Goto Sector again

I right-clicked the ASCII section, selected find and find again to open the search window.

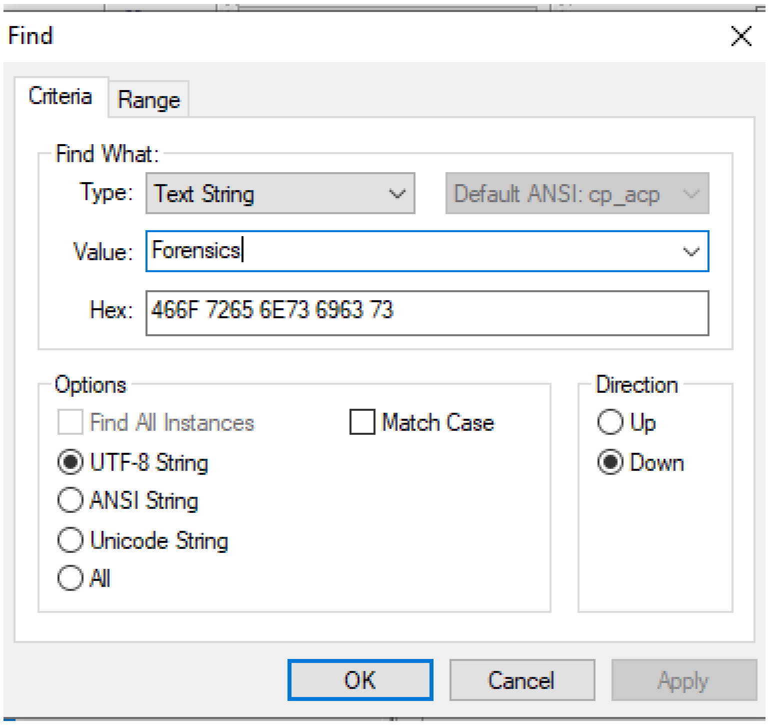


Hex Workshop - [Drive F: <sector 0x1C1 of 0x37FF>]

```
          0  1  2  3  4  5  6  7  8  9  A   0123456789A
00000000  41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAA
0000000B  41 41 41 41 41 41 41 41 41 41 4
00000016  41 41 41 41 41 41 41 41 41 41 4
00000021  41 41 41 41 41 41 41 41 41 41 4
0000002C  41 41 41 41 41 41 41 41 41 41 4
00000037  41 41 41 41 41 41 41 41 41 41 4
00000042  41 41 41 41 41 41 41 41 41 41 4
0000004D  41 41 41 41 41 41 41 41 41 41 4
00000058  41 41 41 41 41 41 41 41 41 41 4
00000063  41 41 41 41 41 41 41 41 41 41 4
0000006E  41 41 41 41 41 41 41 41 41 41 4
00000079  41 41 41 41 41 41 41 41 41 41 4
00000084  41 41 41 41 41 41 41 41 41 4
```

Cursor: 00000051 Caret: 0000

I enter “Forensics” in the value and pressed OK to search for Forensics.



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

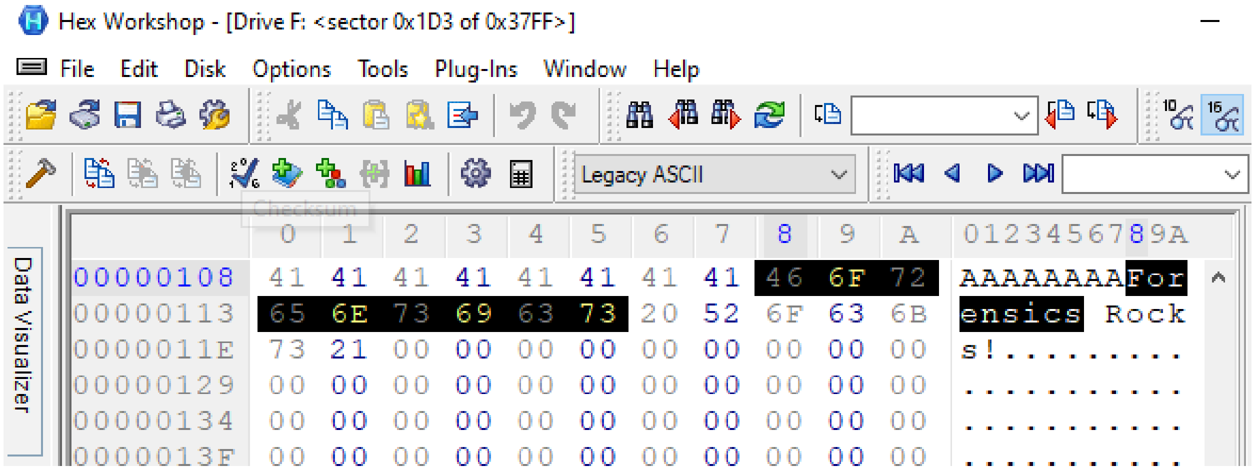
○ All

Direction

○ Up

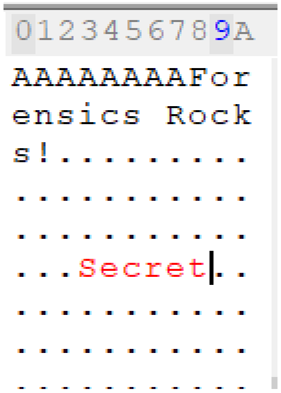
● Down

The file should have some empty bytes after “Forensics Rocks!” as highlighted in the following screenshot. This empty space is called file slack, where the content of the file does not completely feel the sector of the drive it resides in.

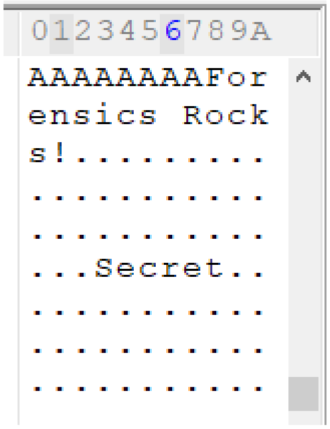


```
          0  1  2  3  4  5  6  7  8  9  A   0123456789A
00000108 41 41 41 41 41 41 41 41 46 6F 72   AAAAAAAAFor
00000113 65 6E 73 69 63 73 20 52 6F 63 6B   ensics Rock
0000011E 73 21 00 00 00 00 00 00 00 00 00   s!.........
00000129 00 00 00 00 00 00 00 00 00 00 00   ...........
00000134 00 00 00 00 00 00 00 00 00 00 00   ...........
0000013F 00 00 00 00 00 00 00 00 00 00 00   ...........
```

Click somewhere in the file slack space, with at least 5 characters of space to the right, and type the word “Secret”. Observe the lettering is red, which indicates an unsaved change. Then save the file by pressing “Ctrl S”, the save icon on the menu bar, or File -> Save. After saving the lettering becomes a black font.

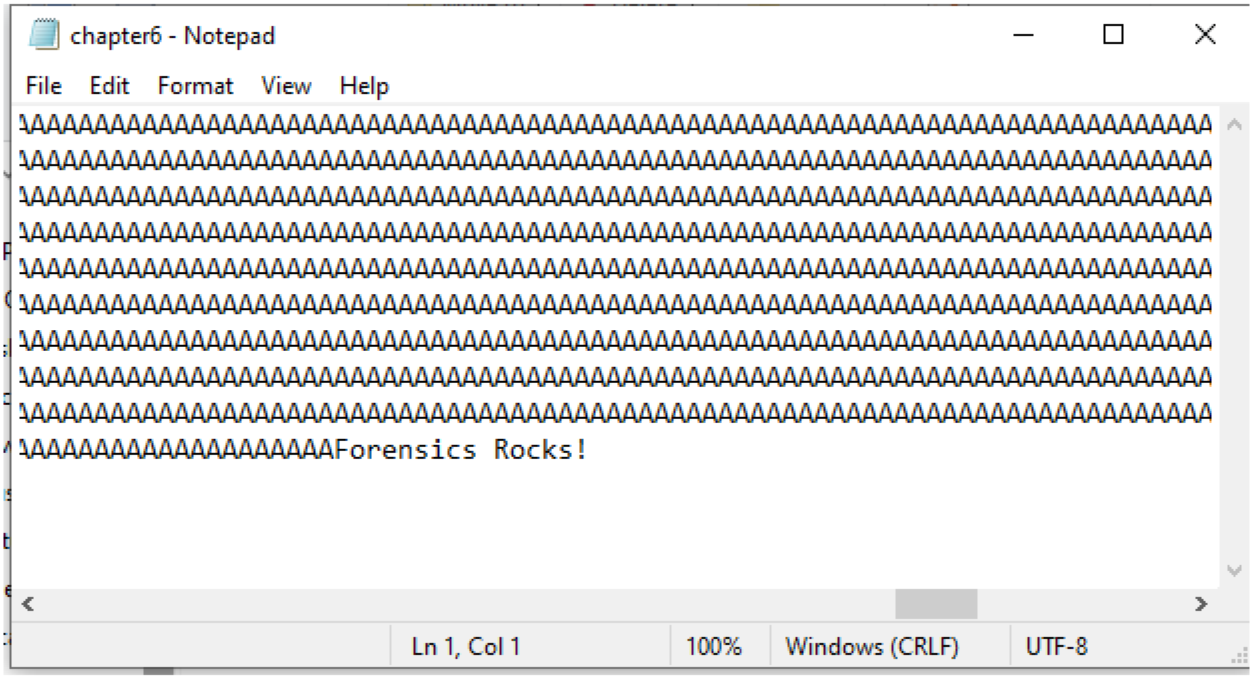


```
0123456789A
AAAAAAAAFor
ensics Rock
s!.........
...........
...........
...Secret..
...........
...........
...........
```



```
0123456789A
AAAAAAAAFor
ensics Rock
s!.........
...........
...........
...Secret..
...........
...........
...........
```

Close Hex Workshop and open the chapter6.txt file. Navigate to the end of the last line where the “Forensics Rocks!” phrase is located. Observe the word “Secret” is not there!



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAForensics Rocks!
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

Step 6: File Slack Explanation

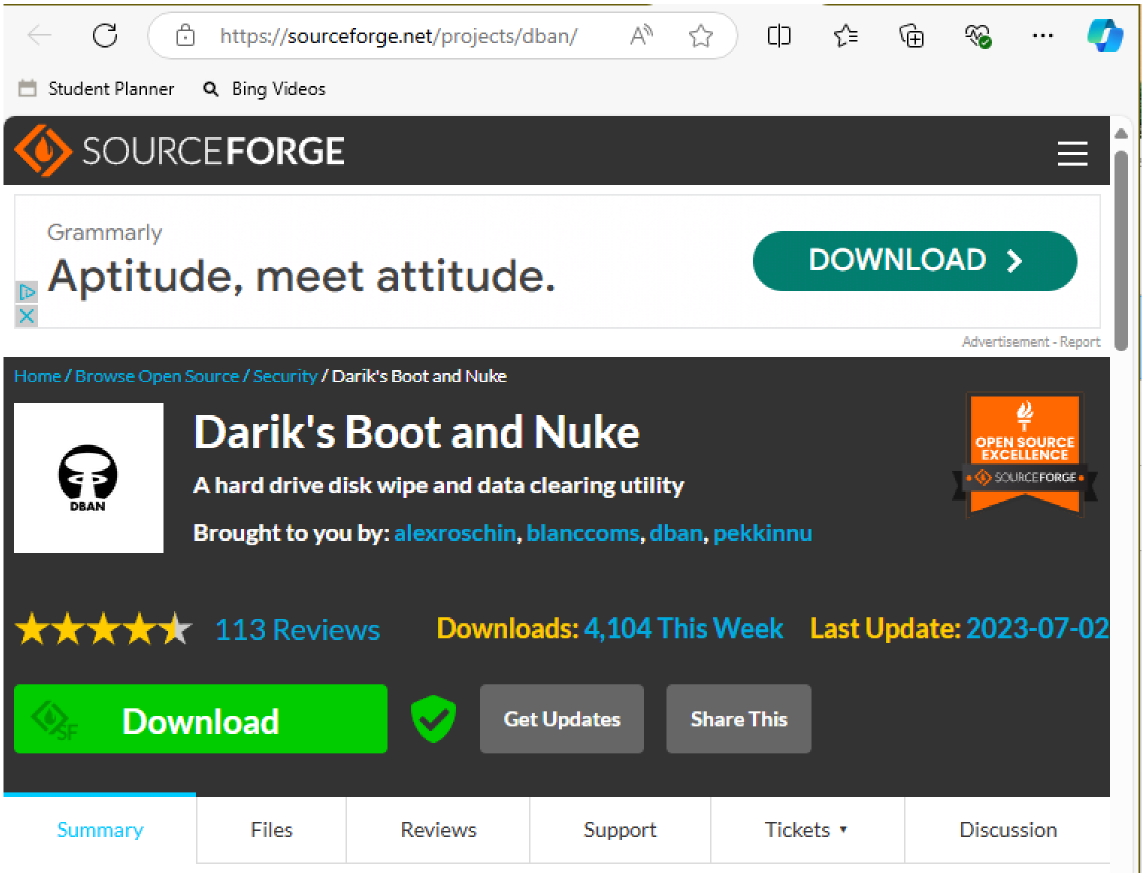
“Secret” was not represented in the chapter6 txt file because when we first created and saved the chapter6 text file, we did not have it there. Since we added it on the hex editor and saved it on the hex editor, it will show up there and not the text file because the hex editor can build upon a text file but the text file itself cannot be changed within the hex editor. We can hide data this way because if there is something we do not want on the text file itself, we can add it on the hex editor where you will only be able to see it on there. So, if you sell your computer, you won't have to worry about sensitive information on the text files.

Task 2: Secure Wipe

In this task , I installed DBAN disk wiping utility and secure the “USB” drive created in the previous task.

Step1: Download and Setup DBAN

From my host machine, I navigate to https://sourceforge.net/projects/dban/ and download the ISO.



Home / Browse Open Source / Security / Darik's Boot and Nuke

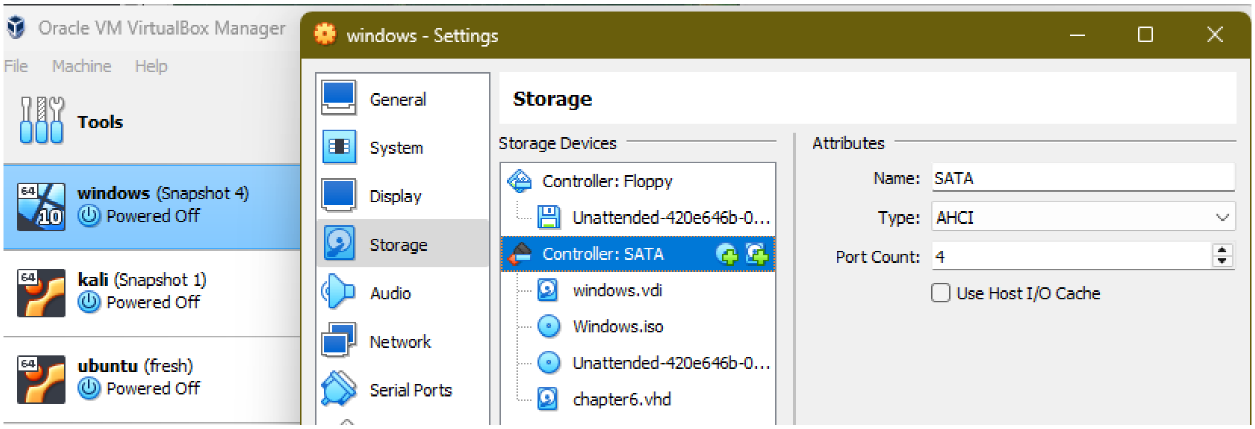
Darik's Boot and Nuke

A hard drive disk wipe and data clearing utility

Brought to you by: alexroschin, blanccoms, dban, pekkinnu

113 Reviews Downloads: 4,104 This Week Last Update: 2023-07-02

Now on your windows VM settings in virtual box, navigat eto storage. Select controller: SATA and press the add optical drive.



Storage

Storage Devices

- Controller: Floppy
  - Unattended-420e646b-0...
- Controller: SATA
  - windows.vdi
  - Windows.iso
  - Unattended-420e646b-0...
  - chapter6.vhd

Attributes

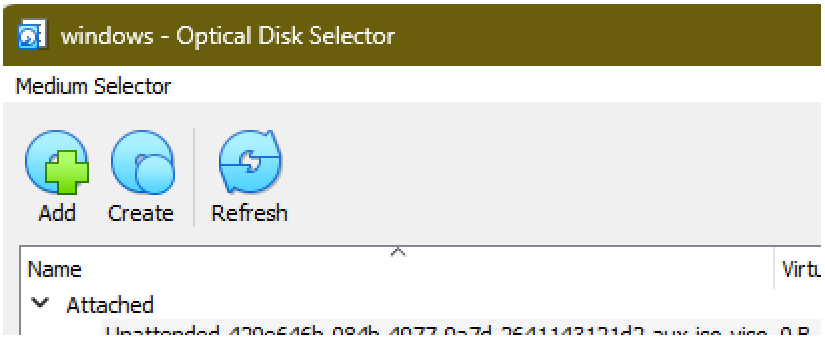
Name: SATA

Type: AHCI

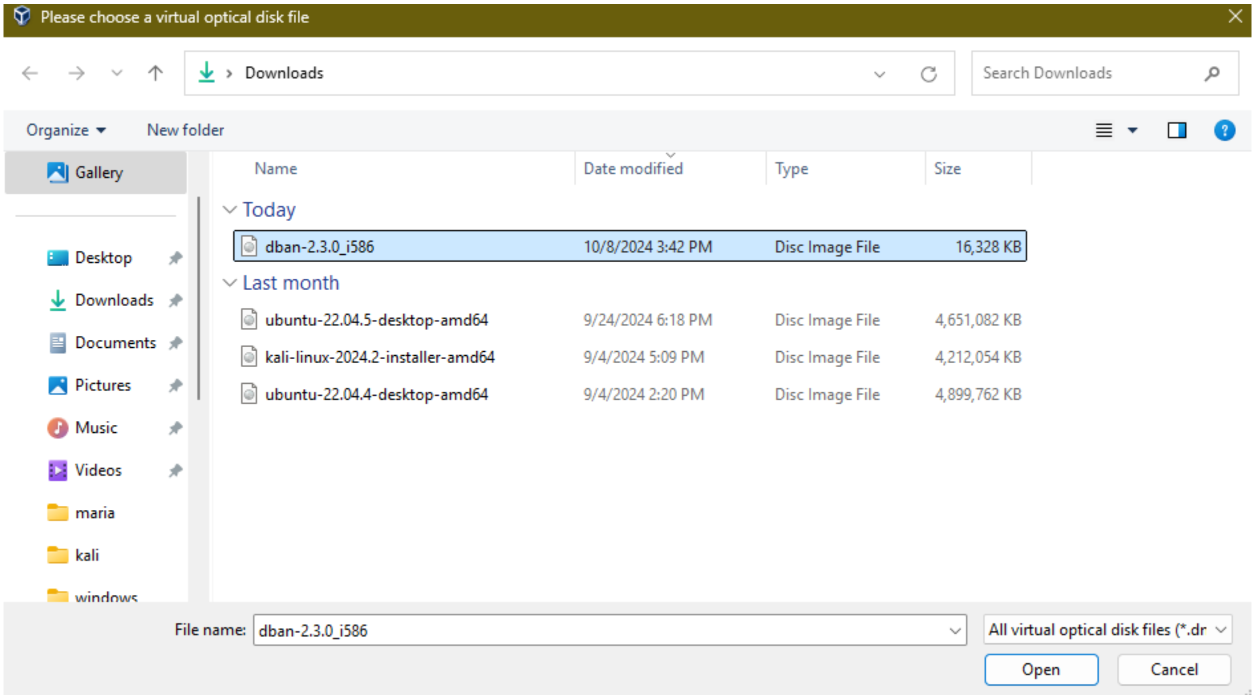
Port Count: 4

□ Use Host I/O Cache

I pressed the Add button in the optical disk selector window.



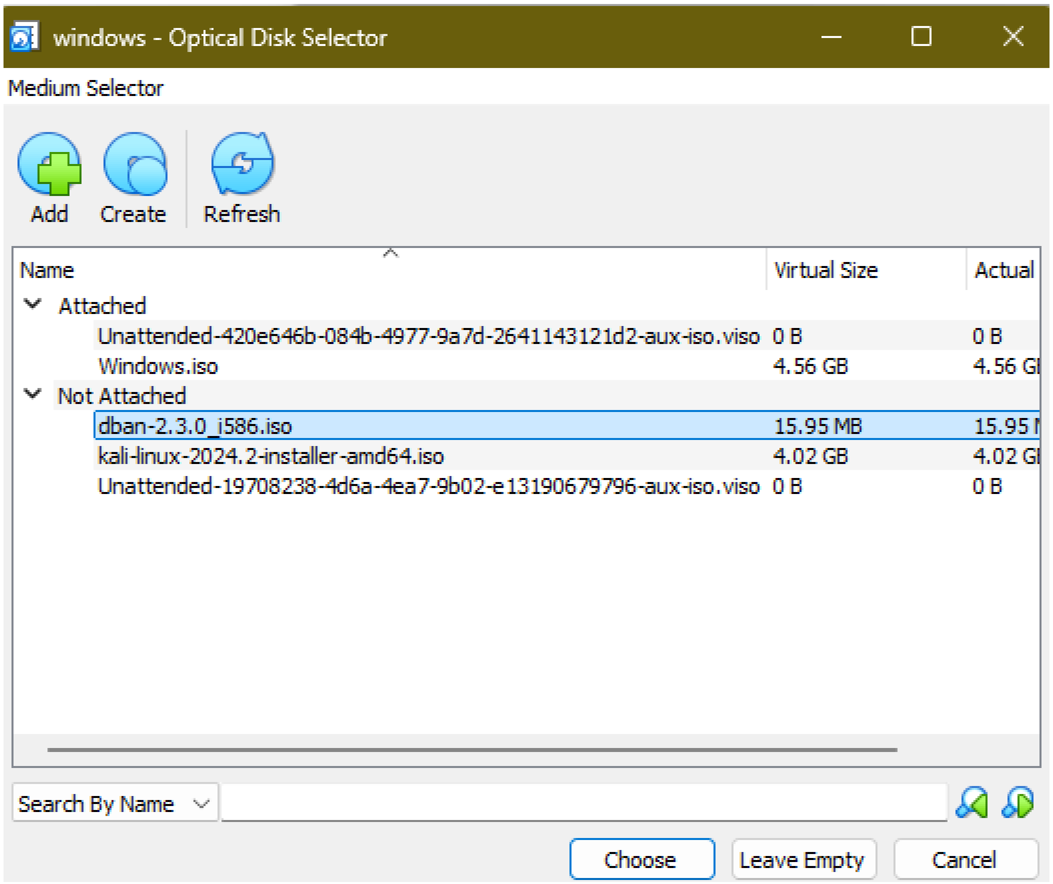
I navigated to my downloads folder where the DBAN ISO file is located. Selected the ISO and pressed open.



Name	Date modified	Type	Size
Today			
dban-2.3.0_i586	10/8/2024 3:42 PM	Disc Image File	16,328 KB
Last month			
ubuntu-22.04.5-desktop-amd64	9/24/2024 6:18 PM	Disc Image File	4,651,082 KB
kali-linux-2024.2-installer-amd64	9/4/2024 5:09 PM	Disc Image File	4,212,054 KB
ubuntu-22.04.4-desktop-amd64	9/4/2024 2:20 PM	Disc Image File	4,899,762 KB

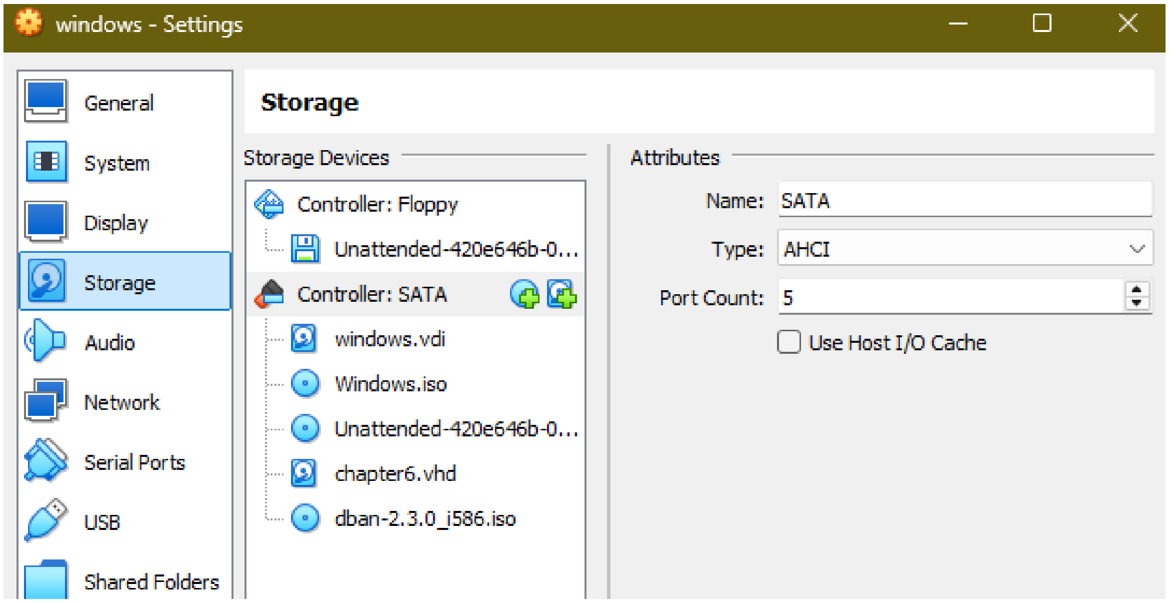
File name: dban-2.3.0_i586

Th ISO appears in the Not Attached section of the optical disk selector windows. I selected it and pressed choose.



Name	Virtual Size	Actual
Attached		
Unattended-420e646b-084b-4977-9a7d-2641143121d2-aux-iso.viso	0 B	0 B
Windows.iso	4.56 GB	4.56 G
Not Attached		
dban-2.3.0_i586.iso	15.95 MB	15.95 M
kali-linux-2024.2-installer-amd64.iso	4.02 GB	4.02 G
Unattended-19708238-4d6a-4ea7-9b02-e13190679796-aux-iso.viso	0 B	0 B

The DBAN ISO now appears in the storage devices section.



Storage

Storage Devices

- Controller: Floppy
  - Unattended-420e646b-0...
- Controller: SATA
  - windows.vdi
  - Windows.iso
  - Unattended-420e646b-0...
  - chapter6.vhd
  - dban-2.3.0_i586.iso

Attributes

Name: SATA

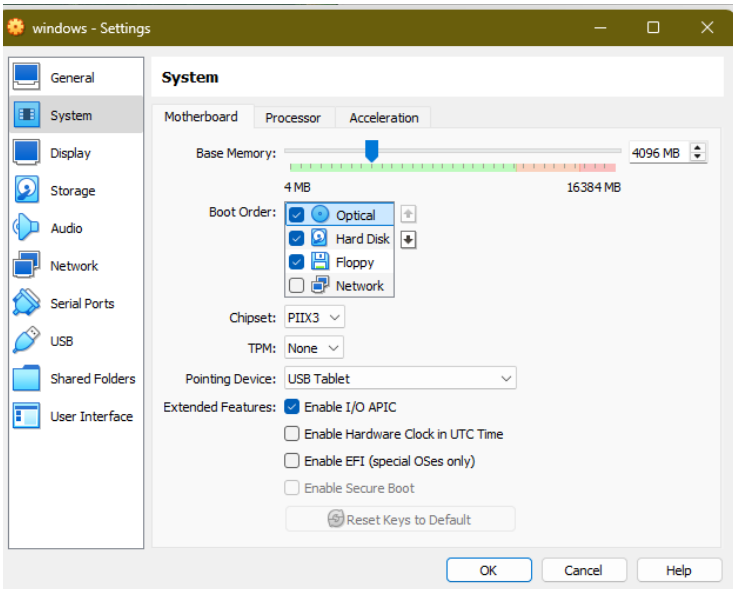
Type: AHCI

Port Count: 5

□ Use Host I/O Cache

Step 2: Boot to the DBAN ISO

With the VirtualBox VM settings open, I selected System and then chose “Optical” from the Boot Order section. I pressed the up-arrow icon to move Optical to the first position (top of the list). Then pressed OK.



System

Base Memory: 4096 MB

4 MB 16384 MB

Boot Order:
☑ Optical
☑ Hard Disk
☑ Floppy
☐ Network

Chipset: PIIX3

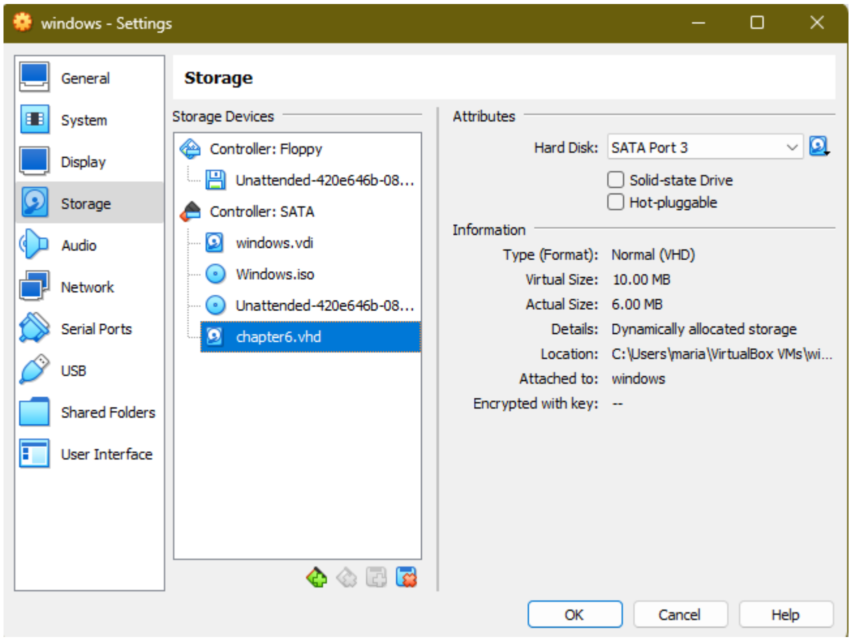
TPM: None

Pointing Device: USB Tablet

Extended Features: ☑ Enable I/O APIC
☐ Enable Hardware Clock in UTC Time
☐ Enable EFI (special OSes only)
☐ Enable Secure Boot
Reset Keys to Default

DBAN was booted.

I closed the windows VM by selecting “Power Off” and then OK. With the VM powered down, I returned to the VirtualBox Windows VM settings, selecting Storage adn then removing the DBAN ISO attachment.



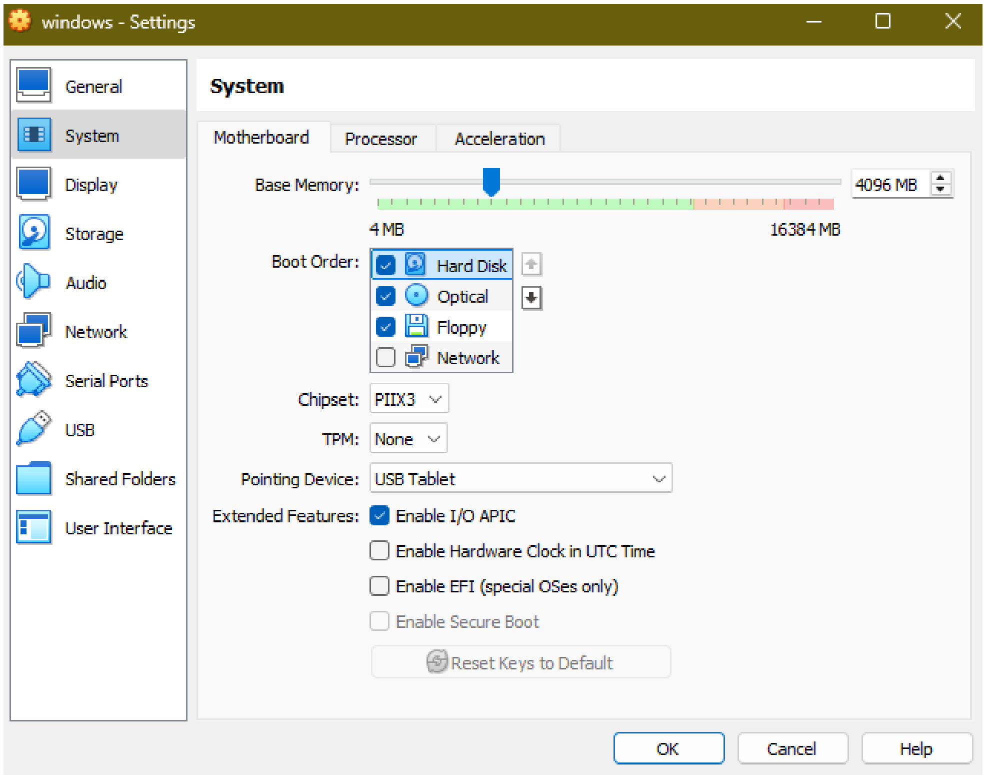
Storage

Storage Devices
Controller: Floppy
Unattended-420e646b-08...
Controller: SATA
windows.vdi
Windows.iso
Unattended-420e646b-08...
chapter6.vhd

Attributes
Hard Disk: SATA Port 3
☐ Solid-state Drive
☐ Hot-pluggable

Information
Type (Format): Normal (VHD)
Virtual Size: 10.00 MB
Actual Size: 6.00 MB
Details: Dynamically allocated storage
Location: C:\Users\maria\VirtualBox VMs\wi...
Attached to: windows
Encrypted with key: --

I then navigate to the windows VM settings for system and change the boot order back to having a hard disk at the top of the list.



windows - Settings

System

Motherboard | Processor | Acceleration

Base Memory: 4096 MB (4 MB – 16384 MB)

Boot Order:
☑ Hard Disk
☑ Optical
☑ Floppy
□ Network

Chipset: PIIX3

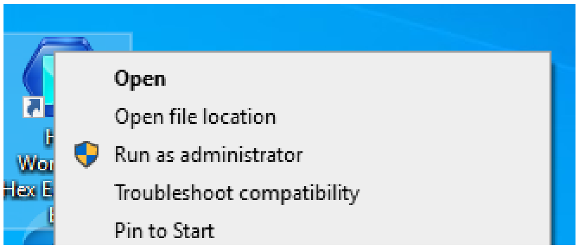
TPM: None

Pointing Device: USB Tablet

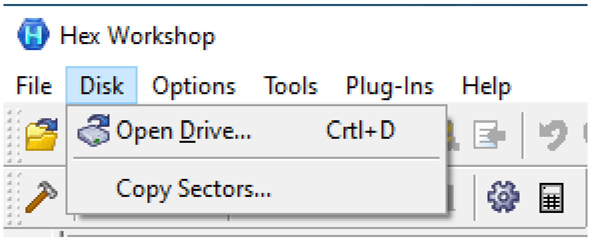
Extended Features:
☑ Enable I/O APIC
□ Enable Hardware Clock in UTC Time
□ Enable EFI (special OSes only)
□ Enable Secure Boot

Step 3: Investigate the drive

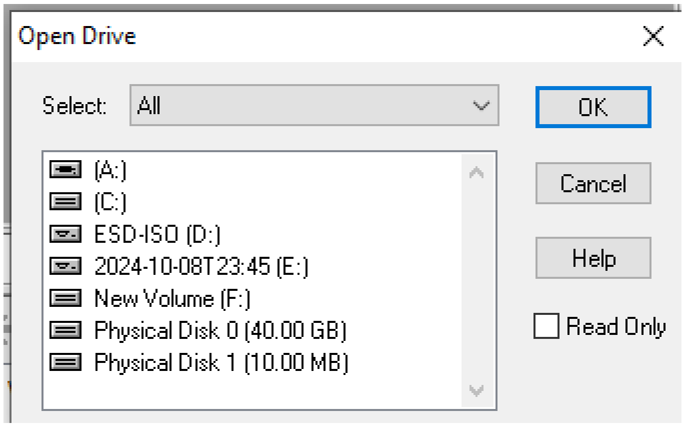
With the Windows VM started, I right clicked the Hex Workshop shortcut and ran as administrator.



I load the USB drive by navigating to Disk and Open Drive.



I select the 10MB drive and press OK.

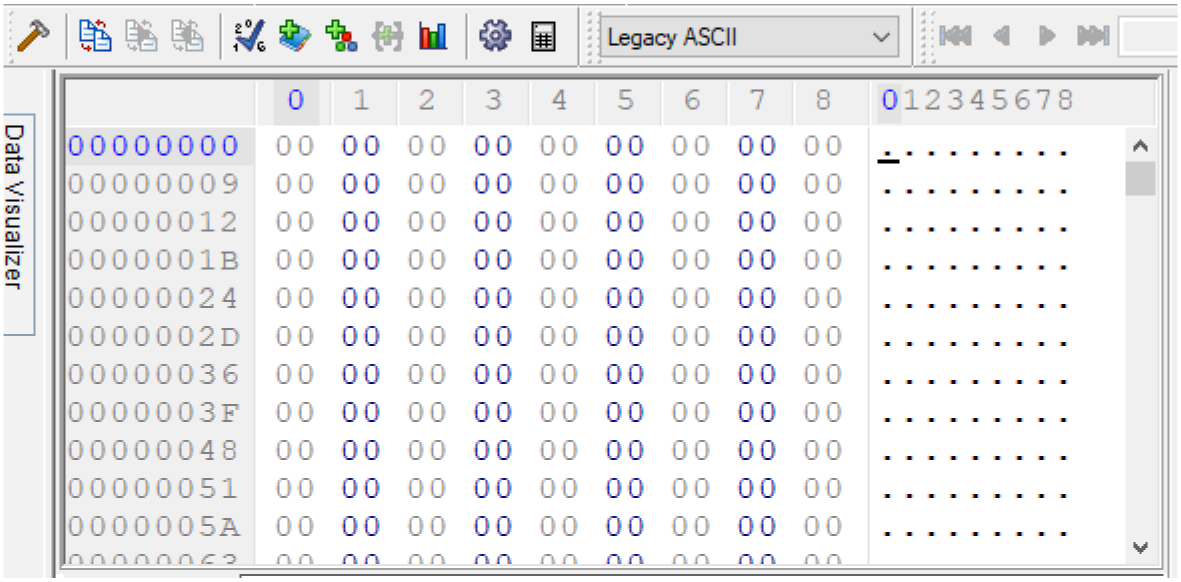


Select: All

- (A:)
- (C:)
- ESD-ISO (D:)
- 2024-10-08T23:45 (E:)
- New Volume (F:)
- Physical Disk 0 (40.00 GB)
- Physical Disk 1 (10.00 MB)

□ Read Only

I observe all sectors have no data!



```
          0  1  2  3  4  5  6  7  8   012345678
00000000  00 00 00 00 00 00 00 00 00  .........
00000009  00 00 00 00 00 00 00 00 00  .........
00000012  00 00 00 00 00 00 00 00 00  .........
0000001B  00 00 00 00 00 00 00 00 00  .........
00000024  00 00 00 00 00 00 00 00 00  .........
0000002D  00 00 00 00 00 00 00 00 00  .........
00000036  00 00 00 00 00 00 00 00 00  .........
0000003F  00 00 00 00 00 00 00 00 00  .........
00000048  00 00 00 00 00 00 00 00 00  .........
00000051  00 00 00 00 00 00 00 00 00  .........
0000005A  00 00 00 00 00 00 00 00 00  .........
00000063  00 00 00 00 00 00 00 00 00
```

Step 4: Research DBAN methods

Another method is the DoD 7-pass which overwrites data seven times: three passes of overwriting with different patterns followed by a verification pass. There's also the Gutmann Method which performs 35 passes of overwriting with a specific sequence of random and predefined patterns. Finally, there is the random data pass which overwrites the drive with random data in just a single pass. I believe from these three the most secure would be the DoD 7 pass since there's three passes of overwriting with different patterns followed by a verification pass and it is quicker than the Gutmann Method.