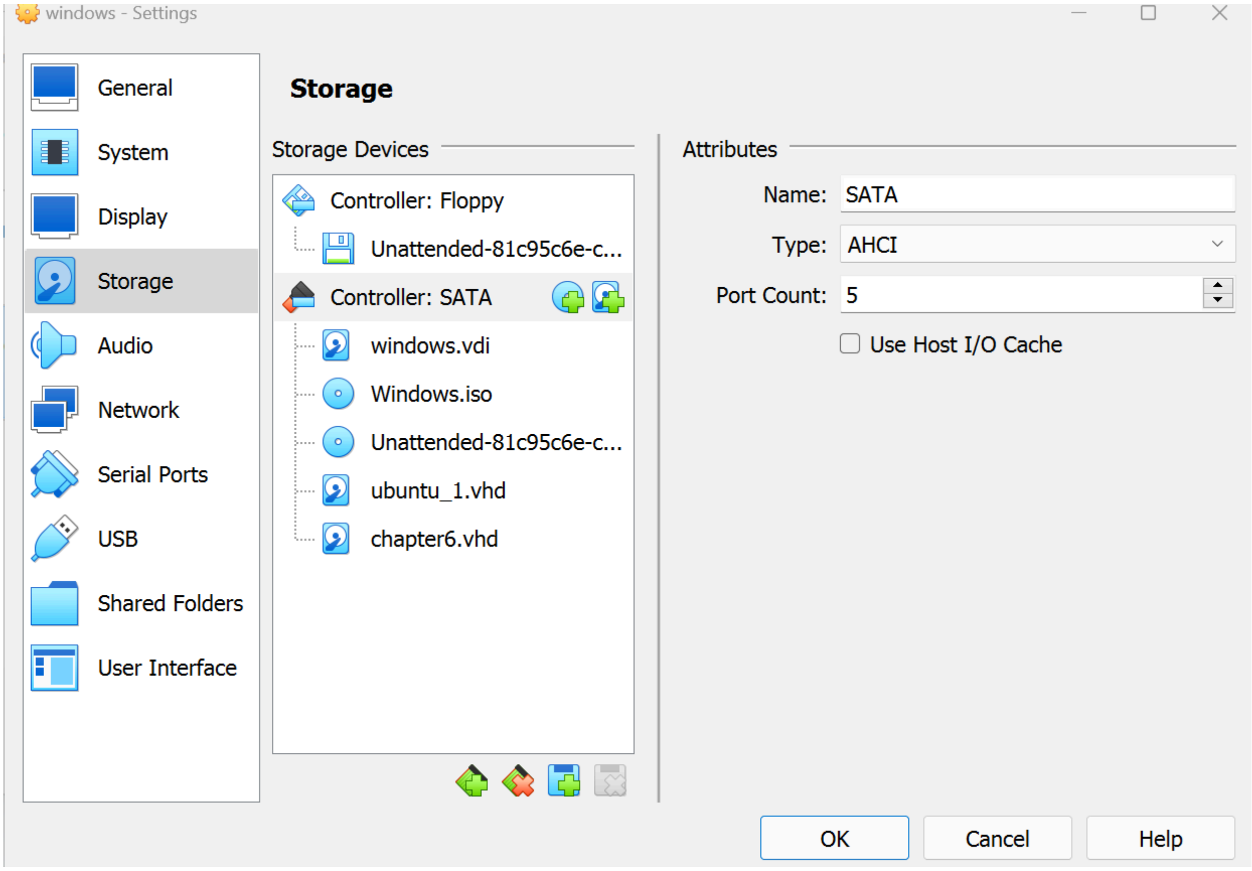
Task 1: File Slack

Step 1: Create USB virtual Drive


windows - Settings

Storage

Storage Devices

- Controller: Floppy
  - Unattended-81c95c6e-c...
- Controller: SATA
  - windows.vdi
  - Windows.iso
  - Unattended-81c95c6e-c...
  - ubuntu_1.vhd
  - chapter6.vhd

Attributes

Name: SATA

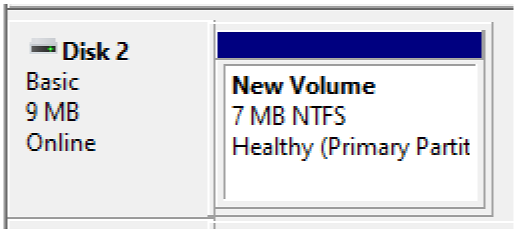
Type: AHCI

Port Count: 5

☐ Use Host I/O Cache

Successful creation of virtual USB and attached it to the Windows VM.

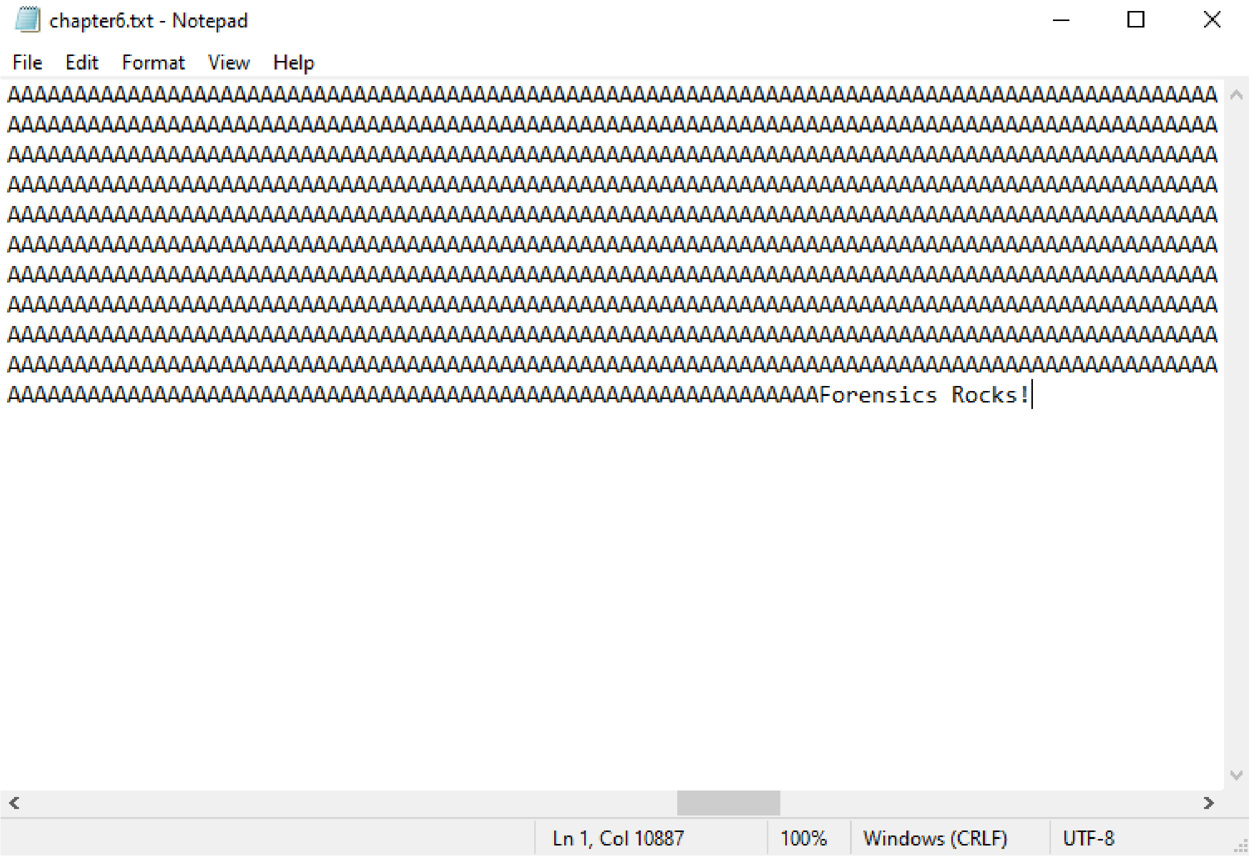
Step 2: Setup the USB


Disk 2
Basic
9 MB
Online

New Volume
7 MB NTFS
Healthy (Primary Partit

Successfully allocated memory and partitions to the USB drive.

Step 3: Create a Test File

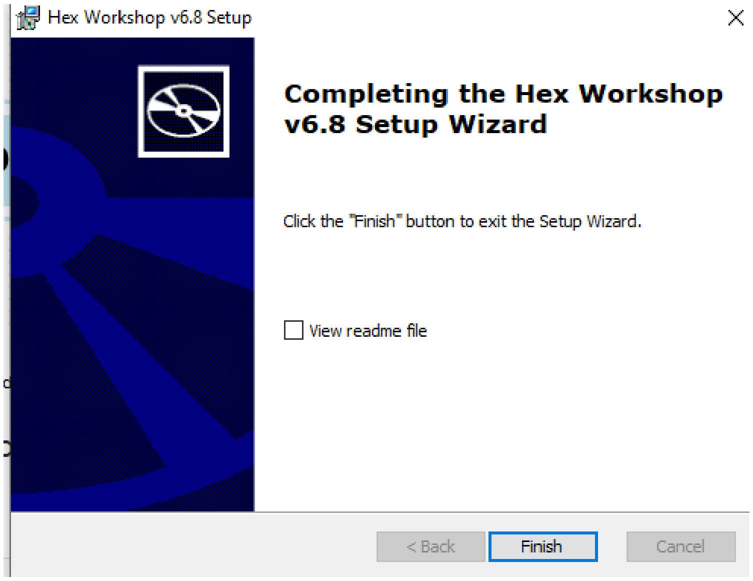


```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAForensics Rocks!
```

Ln 1, Col 10887 | 100% | Windows (CRLF) | UTF-8

Successfully created the text file with 10,000 A’s and “Forensics Rocks!” at the end.

Step 4: Install Hex Workshop



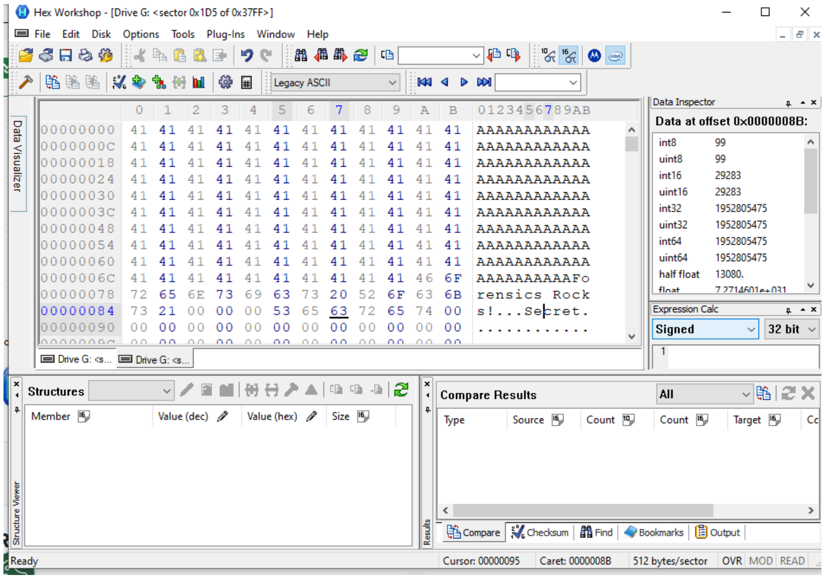
Completing the Hex Workshop v6.8 Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

☐ View readme file

Successful install of Hex Workshop and restarted the VM.

Step 5: Hide Data in Slack Space



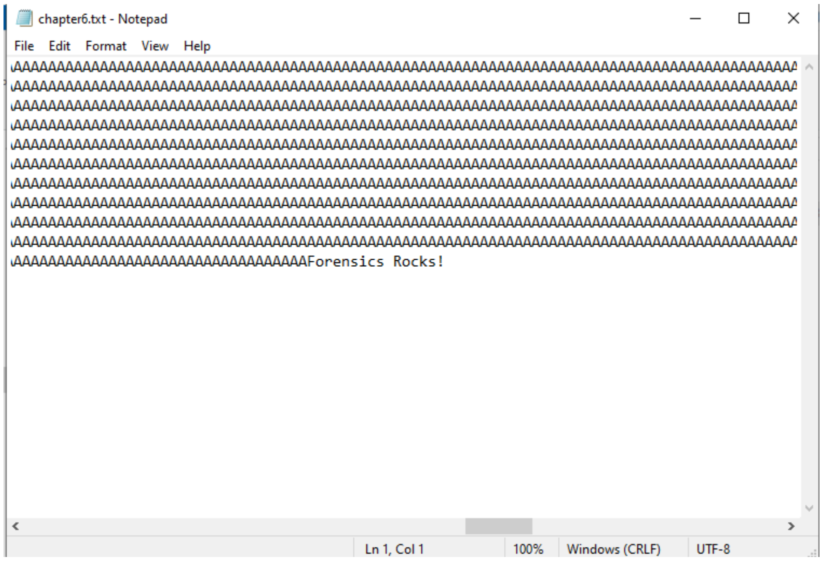
```
          0  1  2  3  4  5  6  7  8  9  A  B  0123456789AB
00000000 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAA
0000000C 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAA
00000018 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAA
00000024 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAA
00000030 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAA
0000003C 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAA
00000048 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAA
00000054 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAA
00000060 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAA
0000006C 41 41 41 41 41 41 41 41 41 41 46 6F  AAAAAAAAAAFo
00000078 72 65 6E 73 69 63 73 20 52 6F 63 6B  rensics Rock
00000084 73 21 00 00 00 53 65 63 72 65 74 00  s!...Secret.
00000090 00 00 00 00 00 00 00 00 00 00 00 00  ............
```

Data Inspector
Data at offset 0x0000008B:

int8	99
uint8	99
int16	29283
uint16	29283
int32	1952805475
uint32	1952805475
int64	1952805475
uint64	1952805475
half float	13080.
float	7.2714601e+031

Expression Calc
Signed 32 bit
1

Cursor: 00000095 Caret: 0000008B 512 bytes/sector



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAForensics Rocks!
```

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

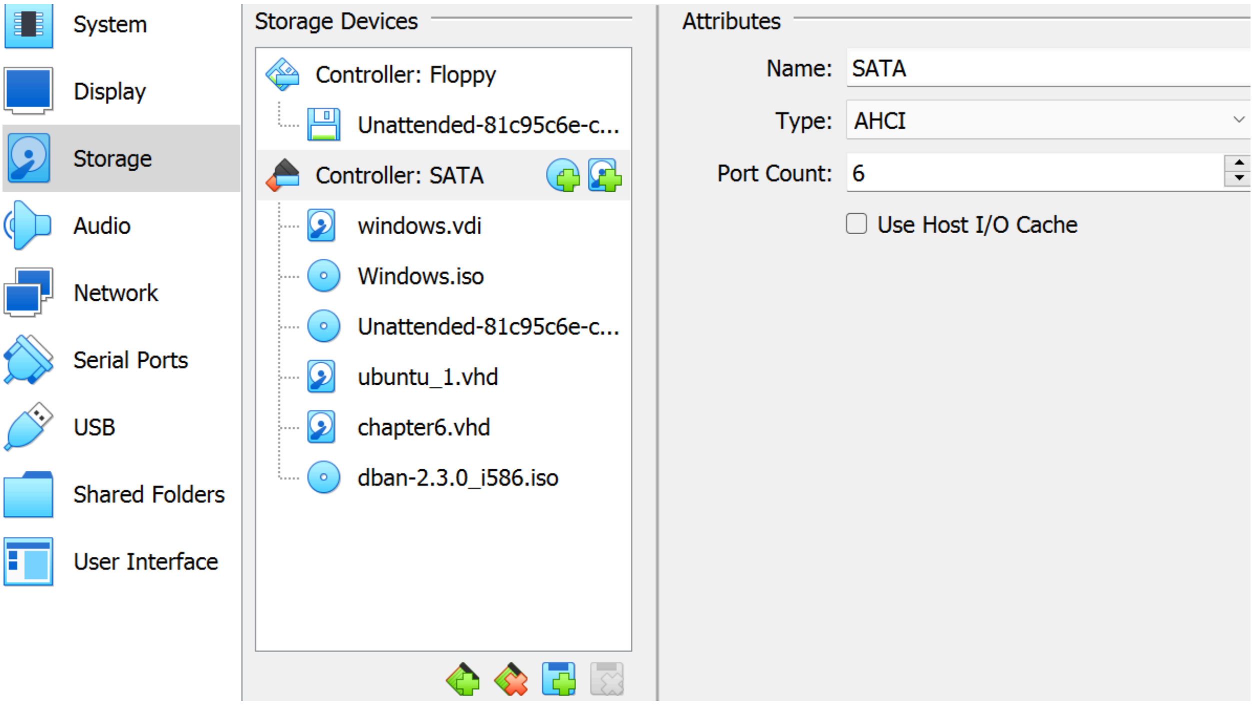
Successfully hid data in the text file.

Step 6: Explanation

This works by utilizing the difference in space between the size of the file and the size of memory that was allocated for it. In this in-between, data can be hidden and not appear in the original file since this space is unused.

Task 2: Secure Wipe

Step 1: Download DBAN



Storage Devices

- Controller: Floppy
  - Unattended-81c95c6e-c...
- Controller: SATA
  - windows.vdi
  - Windows.iso
  - Unattended-81c95c6e-c...
  - ubuntu_1.vhd
  - chapter6.vhd
  - dban-2.3.0_i586.iso

Attributes

Name: SATA

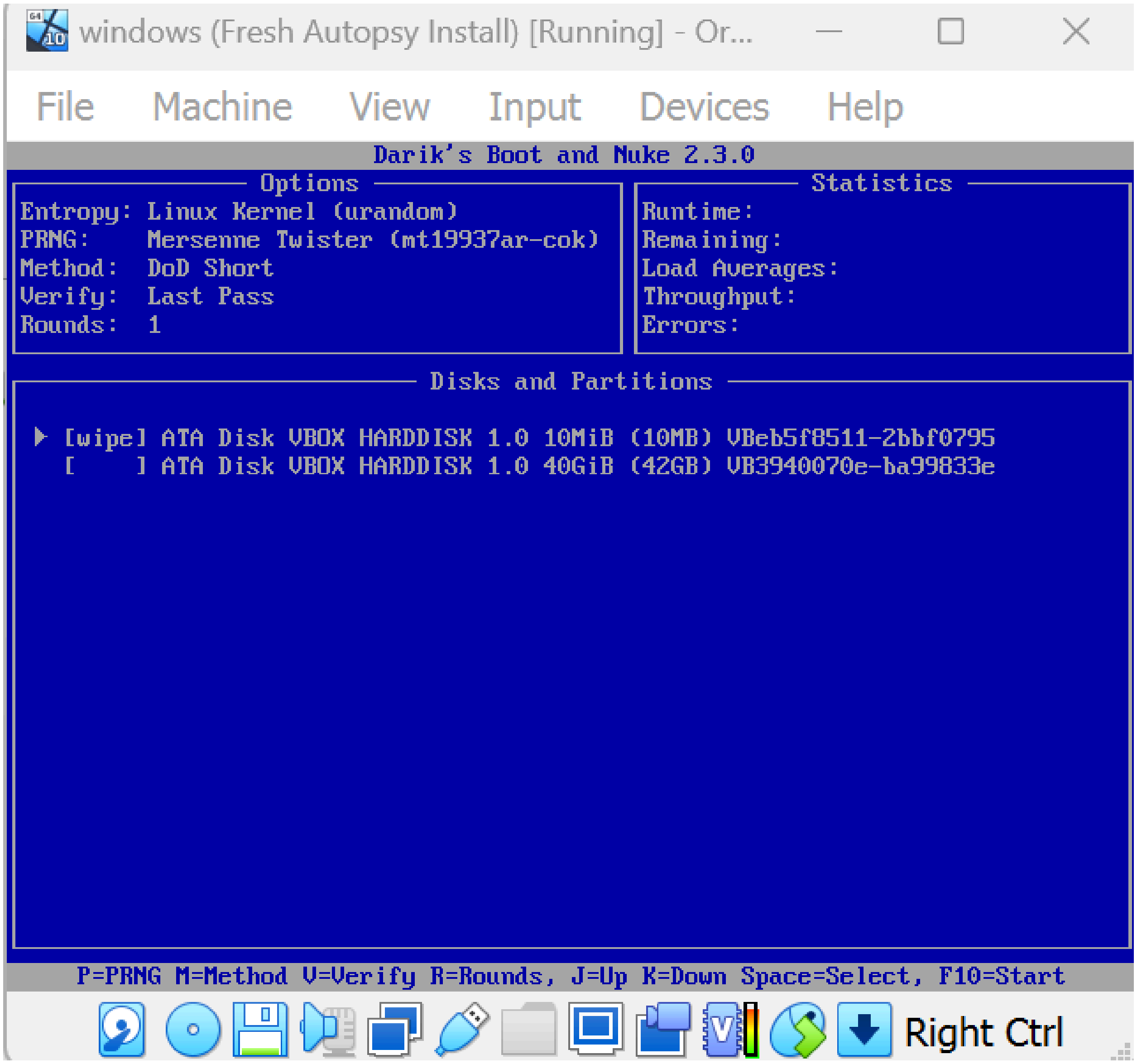
Type: AHCI

Port Count: 6

□ Use Host I/O Cache

Successfully attached DBAN ISO.

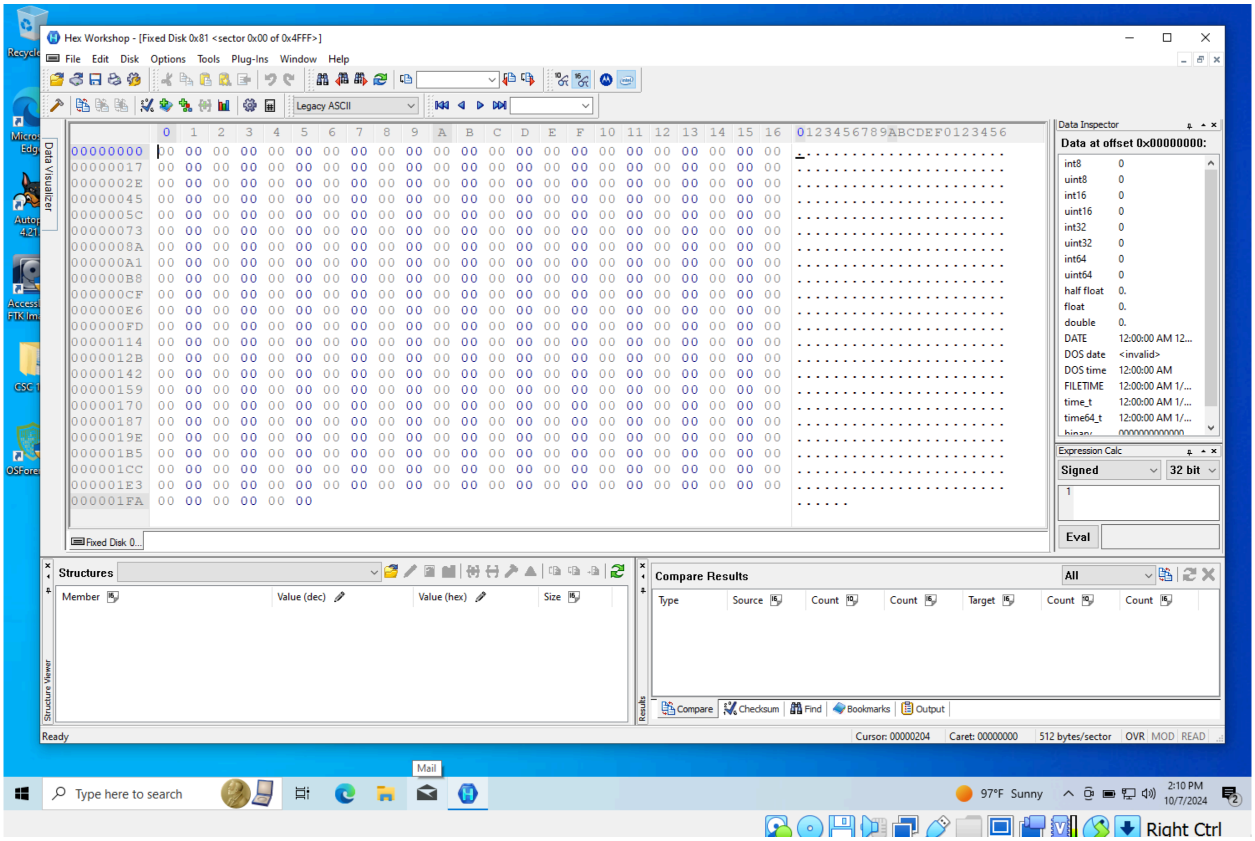
Step 2: Boot to the DBAN ISO



```
                         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) VBeb5f8511-2bbf0795
   [    ] ATA Disk VBOX HARDDISK 1.0 40GiB (42GB) VB3940070e-ba99833e

 P=PRNG M=Method V=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start
```

Successful restoration to original settings after booting DBAN ISO on the Windows VM.

Step 3: Investigate the Drive



Hex Workshop - [Fixed Disk 0x81 <sector 0x00 of 0x4FFF>]

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13 14 15 16  0123456789ABCDEF0123456
00000000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
00000017  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
0000002E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
00000045  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
0000005C  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
00000073  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
0000008A  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
000000A1  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
000000B8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
000000CF  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
000000E6  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
000000FD  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
00000114  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
0000012B  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
00000142  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
00000159  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
00000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
00000187  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
0000019E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
000001B5  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
000001CC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
000001E3  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......................
000001FA  00 00 00 00 00 00                                                     ......
```

Data at offset 0x00000000:

```
int8        0
uint8       0
int16       0
uint16      0
int32       0
uint32      0
int64       0
uint64      0
half float  0.
float       0.
double      0.
DATE        12:00:00 AM 12...
DOS date    <invalid>
DOS time    12:00:00 AM
FILETIME    12:00:00 AM 1/...
time_t      12:00:00 AM 1/...
time64_t    12:00:00 AM 1/...
binary      00000000000
```

```
Ready    Cursor: 00000204    Caret: 00000000    512 bytes/sector    OVR  MOD  READ
```

Verified the successful wiping of data on the virtual USB.

Step 4: Research DBAN Methods

Other DBAN methods:
Gutmann: This sanitization method writes a random character over the data up to 35 times. As a result, this method takes longer than others because of the redundancy of rewriting bytes with garbage data.

Write Zero: Passes through the data once and writes a zero. Usually, this method doesn't include verification.

PRNG: This method writes pseudo-random data over the contents of the disk. Supposedly, this is better than Write Zero and is just as fast.

Of the three methods, I would say PRNG is the best because it doesn't take as long as Gutmann and is better than Write Zero while still maintaining its speed and effectiveness.

Sources:
https://security.stackexchange.com/questions/117724/what-is-the-difference-between-the-different-wiping-methods-used-by-dban

https://www.lifewire.com/how-to-erase-a-hard-drive-using-dban-2619148