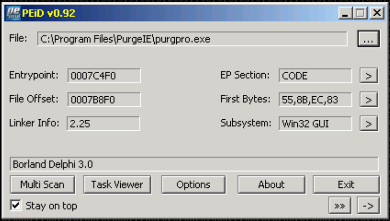
# PurgeIEPro Version 2.01 Tutorial.

| | |
|---|---|
| PurgeIEPro: | Download |
| PEiD.: | Download |
| Olly Debugger.: | Download |
| ExeScope.: | Download |
| Author.: | Kruger AR Team Member |
| Written.: | 27.06.2004 |

This tutor was made on request by.: lvhkyjr2

---

Install App, Use PEiD to Check compiler.



File: C:\Program Files\PurgeIE\purgpro.exe

Entrypoint: 0007C4F0

EP Section: CODE

File Offset: 0007B8F0

First Bytes: 55,8B,EC,83

Linker Info: 2.25

Subsystem: Win32 GUI

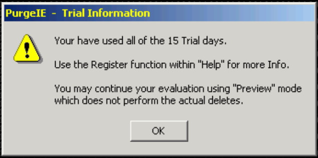
Borland Delphi 3.0

☑ Stay on top

So, Compiled in Borland Delphi 3.0

Let's move on, run app... 15 days trial.

No problem set the system clock 20 days ahead and we got this msg.:



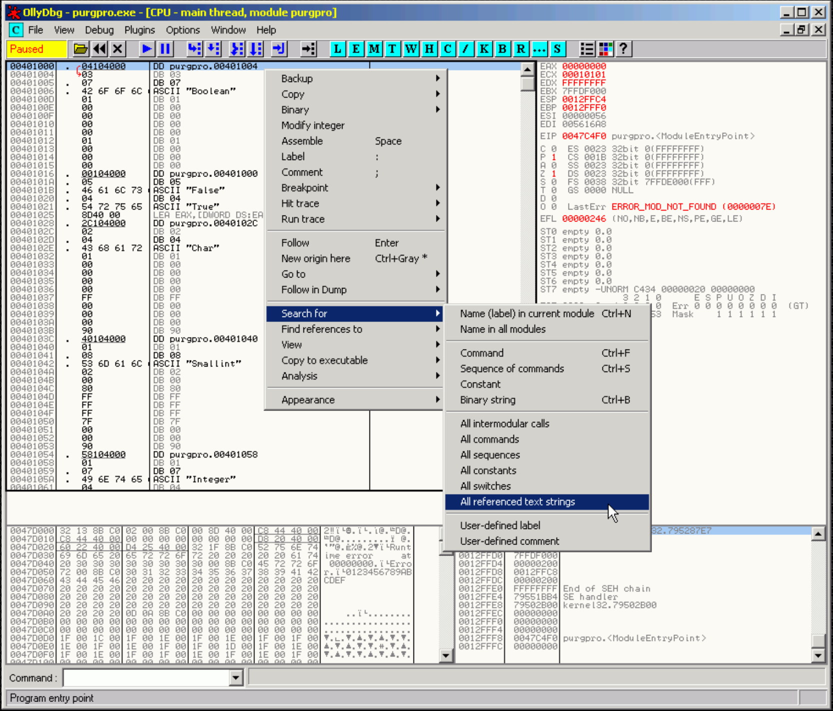
PurgeIE - Trial Information

Your have used all of the 15 Trial days.

Use the Register function within "Help" for more Info.

You may continue your evaluation using "Preview" mode which does not perform the actual deletes.

Ok, now load in Olly -> goto top -> rightclick -> and.:



```
00401000 . 04104000    DD purgpro.00401004
00401004   03          DB 03
00401005   07          DB 07
00401006 . 42 6F 6F 6C ASCII "Boolean"
0040100D   01          DB 01
00401016 . 00104000    DD purgpro.00401000
0040101A   05          DB 05
0040101B . 46 61 6C 73 ASCII "False"
00401020   04          DB 04
00401021 . 54 72 75 65 ASCII "True"
00401025   8D40 00     LEA EAX,[DWORD DS:EA
00401028 . 2C104000    DD purgpro.0040102C
0040102E . 43 68 61 72 ASCII "Char"
0040103C . 40104000    DD purgpro.00401040
00401042 . 53 6D 61 6C ASCII "Smallint"
00401054 . 58104000    DD purgpro.00401058
0040105A . 49 6E 74 65 ASCII "Integer"
```

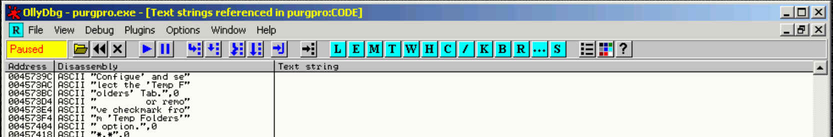
```
EAX 00000000
ECX 00010101
EDX FFFFFFFF
EBX 7FFDF000
ESP 0012FFC4
EBP 0012FFF0
ESI 00000056
EDI 005616A8
EIP 0047C4F0 purgpro.<ModuleEntryPoint>
LastErr ERROR_MOD_NOT_FOUND (0000007E)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
```

Next, On the menu line push the "R"

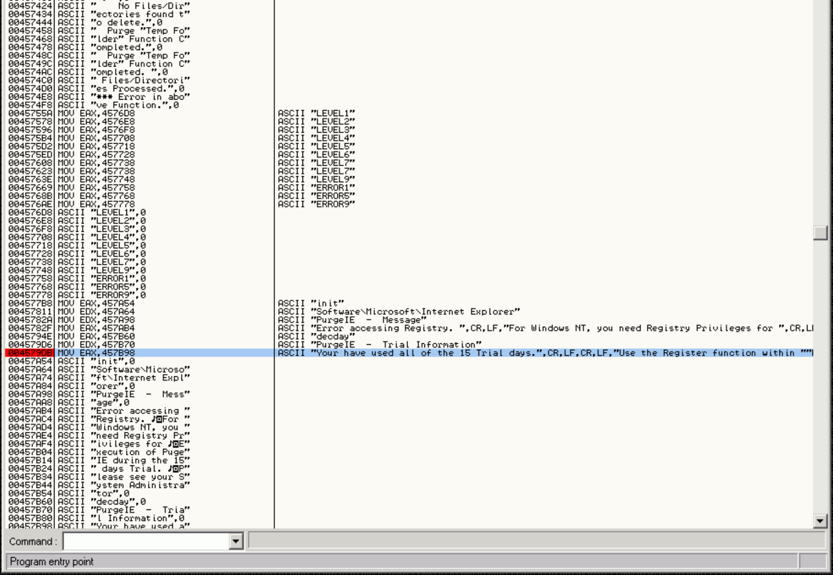
L E M T W H C / K B R ... S

Search for the text "Your have used all of the 15 Trial days."

Found it... Push F2 and "Enter"

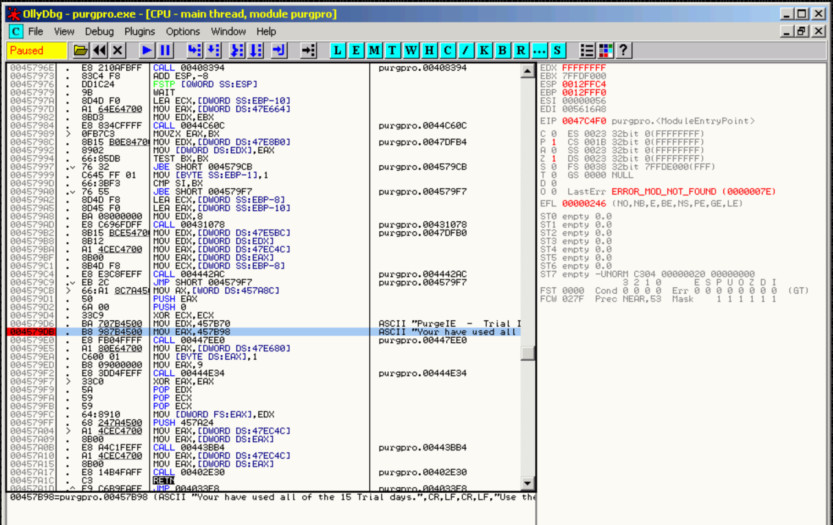

OllyDbg - purgpro.exe - [Text strings referenced in purgpro:CODE]
R File View Debug Plugins Options Window Help
Paused
L E M T W H C / K B R ... S
Address Disassembly Text string

```
0045739C ASCII "Configue' and se"
004573AC ASCII "lect the 'Temp F"
004573BC ASCII "olders' Tab.",0
004573D4 ASCII "        or remo"
004573E4 ASCII "ve checkmark fro"
004573F4 ASCII "m 'Temp Folders'"
00457404 ASCII " option.",0
00457418 ASCII "*.*",0
```



```
00457424|ASCII "    No Files/Dir"
00457434|ASCII "ectories found t"
00457444|ASCII "o delete.",0
00457458|ASCII "  Purge "Temp Fo"
00457468|ASCII "lder" Function C"
00457478|ASCII "ompleted.",0
0045748C|ASCII "  Purge "Temp Fo"
0045749C|ASCII "lder" Function C"
004574AC|ASCII "ompleted. ",0
004574C0|ASCII " Files/Directori"
004574D0|ASCII "es Processed.",0
004574E8|ASCII "*** Error in abo"
004574F8|ASCII "ve Function.",0
0045755A|MOV EAX,4576D8              |ASCII "LEVEL1"
00457578|MOV EAX,4576E8              |ASCII "LEVEL2"
00457596|MOV EAX,4576F8              |ASCII "LEVEL3"
004575B4|MOV EAX,457708              |ASCII "LEVEL4"
004575D2|MOV EAX,457718              |ASCII "LEVEL5"
004575ED|MOV EAX,457728              |ASCII "LEVEL6"
00457608|MOV EAX,457738              |ASCII "LEVEL7"
00457623|MOV EAX,457738              |ASCII "LEVEL7"
0045763E|MOV EAX,457748              |ASCII "LEVEL9"
00457669|MOV EAX,457758              |ASCII "ERROR1"
0045768B|MOV EAX,457768              |ASCII "ERROR5"
004576AE|MOV EAX,457778              |ASCII "ERROR9"
004576D8|ASCII "LEVEL1",0
004576E8|ASCII "LEVEL2",0
004576F8|ASCII "LEVEL3",0
00457708|ASCII "LEVEL4",0
00457718|ASCII "LEVEL5",0
00457728|ASCII "LEVEL6",0
00457738|ASCII "LEVEL7",0
00457748|ASCII "LEVEL9",0
00457758|ASCII "ERROR1",0
00457768|ASCII "ERROR5",0
00457778|ASCII "ERROR9",0
004577B8|MOV EAX,457A54              |ASCII "init"
00457811|MOV EDX,457A64              |ASCII "Software\Microsoft\Internet Explorer"
0045782A|MOV EDX,457A98              |ASCII "PurgeIE  -  Message"
0045782F|MOV EAX,457AB4              |ASCII "Error accessing Registry. ",CR,LF,"For Windows NT, you need Registry Privileges for ",CR,LI
0045794E|MOV EAX,457B60              |ASCII "decday"
004579D6|MOV EDX,457B70              |ASCII "PurgeIE  -  Trial Information"
004579DB|MOV EAX,457B98              |ASCII "Your have used all of the 15 Trial days.",CR,LF,CR,LF,"Use the Register function within ""I
00457A54|ASCII "init",0
00457A64|ASCII "Software\Microso"
00457A74|ASCII "ft\Internet Expl"
00457A84|ASCII "orer",0
00457A98|ASCII "PurgeIE  -  Mess"
00457AA8|ASCII "age",0
00457AB4|ASCII "Error accessing "
00457AC4|ASCII "Registry. ♪◘For "
00457AD4|ASCII "Windows NT, you "
00457AE4|ASCII "need Registry Pr"
00457AF4|ASCII "ivileges for ♪◘E"
00457B04|ASCII "xecution of Puge"
00457B14|ASCII "IE during the 15"
00457B24|ASCII " days Trial. ♪◘P"
00457B34|ASCII "lease see your S"
00457B44|ASCII "ystem Administra"
00457B54|ASCII "tor",0
00457B60|ASCII "decday",0
00457B70|ASCII "PurgeIE  -  Tria"
00457B80|ASCII "l Information",0
00457B98|ASCII "Your have used a"
```

**We are back in the CPU Window...**



OllyDbg - purgpro.exe - [CPU - main thread, module purgpro]
C File View Debug Plugins Options Window Help
Paused
L E M T W H C / K B R ... S
?

```
0045796E   .  E8 210AFBFF    CALL 00408394                      purgpro.00408394
00457973   .  83C4 F8        ADD ESP,-8
00457976   .  DD1C24         FSTP [QWORD SS:ESP]
00457979   .  9B             WAIT
0045797A   .  8D4D F0        LEA ECX,[DWORD SS:EBP-10]
0045797D   .  A1 64E64700    MOV EAX,[DWORD DS:47E664]
00457982   .  8BD3           MOV EDX,EBX
00457984   .  E8 834CFFFF    CALL 0044C60C                      purgpro.0044C60C
00457989   >  0FB7C3         MOVZX EAX,BX
0045798C   .  8B15 B0E8470   MOV EDX,[DWORD DS:47E8B0]          purgpro.0047DFB4
00457992   .  8902           MOV [DWORD DS:EDX],EAX
00457994   .  66:85DB        TEST BX,BX
00457997   .v 76 32          JBE SHORT 004579CB                 purgpro.004579CB
00457999   .  C645 FF 01     MOV [BYTE SS:EBP-1],1
0045799D   .  66:3BF3        CMP SI,BX
004579A0   .v 76 55          JBE SHORT 004579F7                 purgpro.004579F7
004579A2   .  8D4D F8        LEA ECX,[DWORD SS:EBP-8]
004579A5   .  8D45 F0        LEA EAX,[DWORD SS:EBP-10]
004579A8   .  BA 08000000    MOV EDX,8
004579AD   .  E8 C696FDFF    CALL 00431078                      purgpro.00431078
004579B2   .  8B15 BCE5470   MOV EDX,[DWORD DS:47E5BC]          purgpro.0047DFB0
004579B8   .  8B12           MOV EDX,[DWORD DS:EDX]
004579BA   .  A1 4CEC4700    MOV EAX,[DWORD DS:47EC4C]
004579BF   .  8B00           MOV EAX,[DWORD DS:EAX]
004579C1   .  8B4D F8        MOV ECX,[DWORD SS:EBP-8]
004579C4   .  E8 E3C8FEFF    CALL 004442AC                      purgpro.004442AC
004579C9   .v EB 2C          JMP SHORT 004579F7                 purgpro.004579F7
004579CB   >  66:A1 8C7A45   MOV AX,[WORD DS:457A8C]
004579D1   .  50             PUSH EAX
004579D2   .  6A 00          PUSH 0
004579D4   .  33C9           XOR ECX,ECX
004579D6   .  BA 707B4500    MOV EDX,457B70                     ASCII "PurgeIE  -  Trial I
004579DB   .  B8 987B4500    MOV EAX,457B98                     ASCII "Your have used all
004579E0   .  E8 FB04FFFF    CALL 00447EE0                      purgpro.00447EE0
004579E5   .  A1 80E64700    MOV EAX,[DWORD DS:47E680]
004579EA   .  C600 01        MOV [BYTE DS:EAX],1
004579ED   .  B8 09000000    MOV EAX,9
004579F2   .  E8 3DD4FEFF    CALL 00444E34                      purgpro.00444E34
004579F7   >  33C0           XOR EAX,EAX
004579F9   .  5A             POP EDX
004579FA   .  59             POP ECX
004579FB   .  59             POP ECX
004579FC   .  64:8910        MOV [DWORD FS:EAX],EDX
004579FF   .  68 247A4500    PUSH 457A24
00457A04   >  A1 4CEC4700    MOV EAX,[DWORD DS:47EC4C]
00457A09   .  8B00           MOV EAX,[DWORD DS:EAX]
00457A0B   .  E8 A4C1FEFF    CALL 00443BB4                      purgpro.00443BB4
00457A10   .  A1 4CEC4700    MOV EAX,[DWORD DS:47EC4C]
00457A15   .  8B00           MOV EAX,[DWORD DS:EAX]
00457A17   .  E8 14B4FAFF    CALL 00402E30                      purgpro.00402E30
00457A1C   .  C3             RETN
00457A1D   .^ E9 C6B9FAFF    JMP 004033E8                       purgpro.004033E8
00457B98=purgpro.00457B98 (ASCII "Your have used all of the 15 Trial days.",CR,LF,CR,LF,"Use the
```

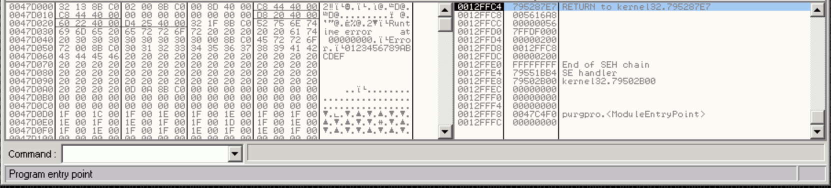
```
EDX FFFFFFFF
EBX 7FFDF000
ESP 0012FFC4
EBP 0012FFF0
ESI 00000056
EDI 005616A8

EIP 0047C4F0 purgpro.<ModuleEntryPoint>

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 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_MOD_NOT_FOUND (0000007E)

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

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty -UNORM C304 00000020 00000000
               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
```



```
0047D000 32 13 8B C0 02 00 8B C0 00 8D 40 00 C8 44 40 00 2‼ï└☻.ï└.ì@.╚D@.
0047D010 C8 44 40 00 00 00 00 00 00 00 00 00 D8 20 40 00 ╚D@.........ï @.
0047D020 60 22 40 00 D4 25 40 00 32 1F 8B C0 52 75 6E 74 `"@.È%@.2▼ï└Runt
0047D030 69 6D 65 20 65 72 72 6F 72 20 20 20 20 20 61 74 ime error     at
0047D040 20 30 30 30 30 30 30 30 30 00 8B C0 45 72 72 6F  00000000.ï└Erro
0047D050 72 00 8B C0 30 31 32 33 34 35 36 37 38 39 41 42 r.ï└0123456789AB
0047D060 43 44 45 46 20 20 20 20 20 20 20 20 20 20 20 20 CDEF
0047D070 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D080 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D090 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D0A0 20 20 20 20 0D 0A 8B C0 00 00 00 00 00 00 00 00     ..ï└........
0047D0B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0047D0C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0047D0D0 1F 00 1C 00 1F 00 1E 00 1F 00 1E 00 1F 00 1F 00 ▼.∟.▼.▲.▼.▲.▼.▼.
0047D0E0 1E 00 1F 00 1E 00 1F 00 1F 00 1D 00 1F 00 1E 00 ▲.▼.▲.▼.▼.#.▼.▲.
0047D0F0 1F 00 1E 00 1F 00 1F 00 1E 00 1F 00 1E 00 1F 00 ▼.▲.▼.▼.▲.▼.▲.▼.
```

```
0012FFC4 795287E7 RETURN to kernel32.795287E7
0012FFC8 005616A8
0012FFCC 00000056
0012FFD0 7FFDF000
0012FFD4 00000200
0012FFD8 0012FFC8
0012FFDC 00000200
0012FFE0 FFFFFFFF End of SEH chain
0012FFE4 79551BB4 SE handler
0012FFE8 79502B00 kernel32.79502B00
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
0012FFF8 0047C4F0 purgpro.<ModuleEntryPoint>
0012FFFC 00000000
```

Program entry point

**Now, have a look up in Code to see if we find anything...**

**If you have problems with finding the counter, try to put some brakes up in code load and push F7/F8...**

**Hint.: See the txt "decday"**

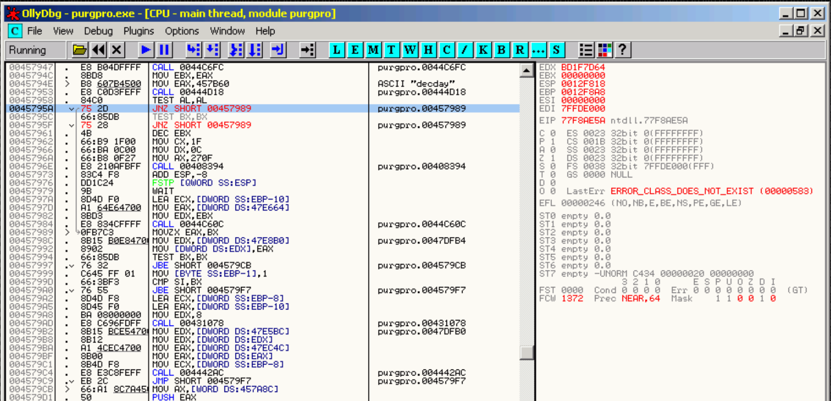
```
0045795A /74 2D JE SHORT 00457989 ; purgpro.00457989
0045795C |66:85DB TEST BX,BX
0045795F |76 28 JBE SHORT 00457989 ; purgpro.00457989
00457961 . |4B DEC EBX
00457962 . |66:B9 1F00 MOV CX,1F
00457966 . |66:BA 0C00 MOV DX,0C
0045796A . |66:B8 0F27 MOV AX,270F
0045796E . |E8 210AFBFF CALL 00408394 ;
purgpro.00408394
00457973 . |83C4 F8 ADD ESP,-8
00457976 . |DD1C24 FSTP [QWORD SS:ESP]
00457979 . |9B WAIT
0045797A . |8D4D F0 LEA ECX,[DWORD SS:EBP-10]
0045797D . |A1 64E64700 MOV EAX,[DWORD DS:47E664]
00457982 . |8BD3 MOV EDX,EBX
00457984 . |E8 834CFFFF CALL 0044C60C ;
purgpro.0044C60C
00457989 > \0FB7C3 MOVZX EAX,BX
```

**0045795A /74 2D JE SHORT 00457989 ; purgpro.00457989**
**0045795C |66:85DB TEST BX,BX**
**0045795F |76 28 JBE SHORT 00457989 ; purgpro.00457989**

**Hmm....... First if JE we goto .00457989  JE = Jump if equal (=)**

**Next if JBE we goto .00457989  JBE = Jump if Below or Equal (>=)**

**We change the Code to make the counter a little better... ;-)**



OllyDbg - purgpro.exe - [CPU - main thread, module purgpro]

C File View Debug Plugins Options Window Help
Running
L E M T W H C / K B R ... S ?

```
00457947  .  E8 B04DFFFF   CALL 0044C6FC                    purgpro.0044C6FC
0045794C  .  8BD8          MOV EBX,EAX
0045794E  >  B8 607B4500   MOV EAX,457B60                   ASCII "decday"
00457953  .  E8 C0D3FEFF   CALL 00444D18                    purgpro.00444D18
00457958  .  84C0          TEST AL,AL
0045795A  v  75 2D         JNZ SHORT 00457989               purgpro.00457989
0045795C     66:85DB       TEST BX,BX
0045795F  v  75 28         JNZ SHORT 00457989               purgpro.00457989
00457961  .  4B            DEC EBX
00457962  .  66:B9 1F00    MOV CX,1F
00457966  .  66:BA 0C00    MOV DX,0C
0045796A  .  66:B8 0F27    MOV AX,270F
0045796E  .  E8 210AFBFF   CALL 00408394                    purgpro.00408394
00457973  .  83C4 F8       ADD ESP,-8
00457976  .  DD1C24        FSTP [QWORD SS:ESP]
00457979  .  9B            WAIT
0045797A  .  8D4D F0       LEA ECX,[DWORD SS:EBP-10]
0045797D  .  A1 64E64700   MOV EAX,[DWORD DS:47E664]
00457982  .  8BD3          MOV EDX,EBX
00457984  .  E8 834CFFFF   CALL 0044C60C                    purgpro.0044C60C
00457989  >  0FB7C3        MOVZX EAX,BX
0045798C  .  8B15 B0E8470  MOV EDX,[DWORD DS:47E8B0]        purgpro.0047DFB4
00457992  .  8902          MOV [DWORD DS:EDX],EAX
00457994  .  66:85DB       TEST BX,BX
00457997  .v 76 32         JBE SHORT 004579CB               purgpro.004579CB
00457999  .  C645 FF 01    MOV [BYTE SS:EBP-1],1
0045799D  .  66:3BF3       CMP SI,BX
004579A0  .v 76 55         JBE SHORT 004579F7               purgpro.004579F7
004579A2  .  8D4D F8       LEA ECX,[DWORD SS:EBP-8]
004579A5  .  8D45 F0       LEA EAX,[DWORD SS:EBP-10]
004579A8  .  BA 08000000   MOV EDX,8
004579AD  .  E8 C696FDFF   CALL 00431078                    purgpro.00431078
004579B2  .  8B15 BCE5470  MOV EDX,[DWORD DS:47E5BC]        purgpro.0047DFB0
004579B8  .  8B12          MOV EDX,[DWORD DS:EDX]
004579BA  .  A1 4CEC4700   MOV EAX,[DWORD DS:47EC4C]
004579BF  .  8B00          MOV EAX,[DWORD DS:EAX]
004579C1  .  8B4D F8       MOV ECX,[DWORD SS:EBP-8]
004579C4  .  E8 E3C8FEFF   CALL 004442AC                    purgpro.004442AC
004579C9  .v EB 2C         JMP SHORT 004579F7               purgpro.004579F7
004579CB  >  66:A1 8C7A45  MOV AX,[WORD DS:457A8C]
004579D1  .  50            PUSH EAX
```

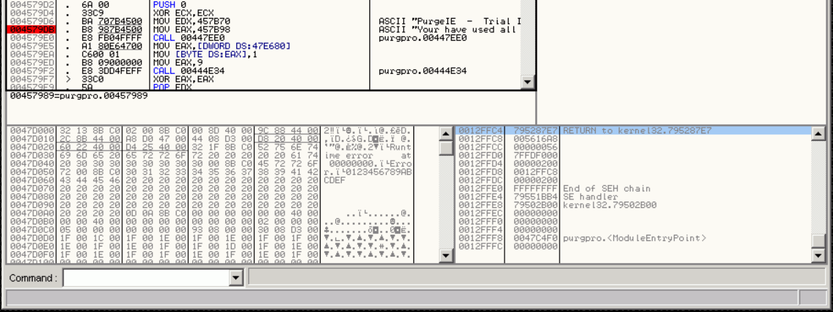
```
EDX BD1F7D64
EBX 00000000
ESP 0012F818
EBP 0012F8A8
ESI 00000000
EDI 7FFDE000

EIP 77F8AE5A ntdll.77F8AE5A

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 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_CLASS_DOES_NOT_EXIST (00000583)

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

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty -UNORM C434 00000020 00000000
               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 1372  Prec NEAR,64  Mask    1 1 0 0 1 0
```

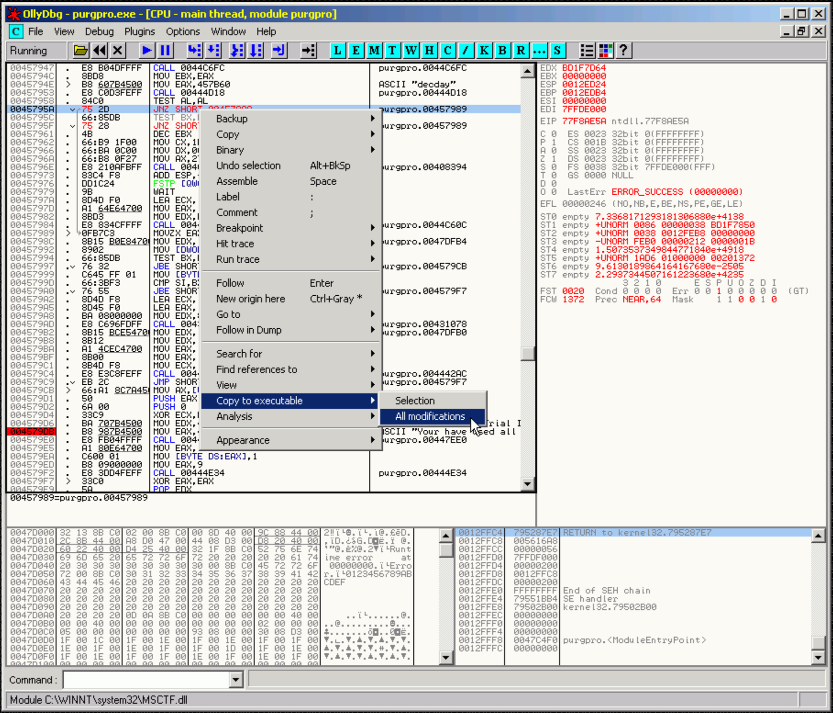


```
004579D2  .  6A 00          PUSH 0
004579D4  .  33C9           XOR ECX,ECX
004579D6  .  BA 707B4500    MOV EDX,457B70                  ASCII "PurgeIE  -  Trial I
004579DB  .  B8 987B4500    MOV EAX,457B98                  ASCII "Your have used all
004579E0  .  E8 FB04FFFF    CALL 00447EE0                   purgpro.00447EE0
004579E5  .  A1 80E64700    MOV EAX,[DWORD DS:47E680]
004579EA  .  C600 01        MOV [BYTE DS:EAX],1
004579ED  .  B8 09000000    MOV EAX,9
004579F2  .  E8 3DD4FEFF    CALL 00444E34                   purgpro.00444E34
004579F7  >  33C0           XOR EAX,EAX
004579F9  .  5A             POP EDX
00457989=purgpro.00457989
```

```
0047D000 32 13 8B C0 02 00 8B C0 00 8D 40 00 9C 88 44 00 2‼ï└@.ï└.ì@.£èD.
0047D010 2C 8B 44 00 A8 D0 47 00 44 08 D3 00 D8 20 40 00 ,ïD.¿ðG.D◘Ë.ï @.
0047D020 60 22 40 00 D4 25 40 00 32 1F 8B C0 52 75 6E 74 `"@.È%@.2▼ï└Runt
0047D030 69 6D 65 20 65 72 72 6F 72 20 20 20 20 20 61 74 ime error     at
0047D040 20 30 30 30 30 30 30 30 30 00 8B C0 45 72 72 6F  00000000.ï└Erro
0047D050 72 00 8B C0 30 31 32 33 34 35 36 37 38 39 41 42 r.ï└0123456789AB
0047D060 43 44 45 46 20 20 20 20 20 20 20 20 20 20 20 20 CDEF
0047D070 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D080 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D090 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D0A0 20 20 20 20 0D 0A 8B C0 00 00 00 00 00 00 40 00     ..ï└......@.
0047D0B0 00 00 40 00 00 00 00 00 00 00 00 00 02 00 00 00 ..@.........☻...
0047D0C0 05 00 00 00 00 00 00 00 93 08 00 00 30 08 D3 00 ♣.......ô◘..0◘Ë.
0047D0D0 1F 00 1C 00 1F 00 1E 00 1F 00 1E 00 1F 00 1F 00 ▼.∟.▼.▲.▼.▲.▼.▼.
0047D0E0 1E 00 1F 00 1E 00 1F 00 1F 00 1D 00 1F 00 1E 00 ▲.▼.▲.▼.▼.↔.▼.▲.
0047D0F0 1F 00 1E 00 1F 00 1F 00 1E 00 1F 00 1E 00 1F 00 ▼.▲.▼.▼.▲.▼.▲.▼.
```

```
0012FFC4   795287E7  RETURN to kernel32.795287E7
0012FFC8   005616A8
0012FFCC   00000056
0012FFD0   7FFDF000
0012FFD4   00000200
0012FFD8   0012FFC8
0012FFDC   00000200
0012FFE0   FFFFFFFF  End of SEH chain
0012FFE4   79551BB4  SE handler
0012FFE8   79502B00  kernel32.79502B00
0012FFEC   00000000
0012FFF0   00000000
0012FFF4   00000000
0012FFF8   0047C4F0  purgpro.<ModuleEntryPoint>
0012FFFC   00000000
```

Time to save changes.:



```
00457947  .  E8 B04DFFFF    CALL 0044C6FC                   purgpro.0044C6FC
0045794C  .  8BD8           MOV EBX,EAX
0045794E  >  B8 607B4500    MOV EAX,457B60                  ASCII "decday"
00457953  .  E8 C0D3FEFF    CALL 00444D18                   purgpro.00444D18
00457958  .  84C0           TEST AL,AL
0045795A  v  75 2D          JNZ SHORT                       purgpro.00457989
0045795C     66:85DB        TEST BX,
0045795F  v  75 28          JNZ SHORT                       urgpro.00457989
00457961  .  4B             DEC EBX
00457962  .  66:B9 1F00     MOV CX,1
00457966  .  66:BA 0C00     MOV DX,0
0045796A  .  66:B8 0F27     MOV AX,2
0045796E  .  E8 210AFBFF    CALL 004                        urgpro.00408394
00457973  .  83C4 F8        ADD ESP,
00457976  .  DD1C24         FSTP [QW
00457979  .  9B             WAIT
0045797A  .  8D4D F0        LEA ECX,
0045797D  .  A1 64E64700    MOV EAX,
00457982  .  8BD3           MOV EDX,
00457984  .  E8 834CFFFF    CALL 004                        urgpro.0044C60C
00457989  >  0FB7C3         MOVZX EA
0045798C  .  8B15 B0E8470   MOV EDX,                        urgpro.0047DFB4
00457992  .  8902           MOV [DWO
00457994  .  66:85DB        TEST BX,
00457997  .v 76 32          JBE SHOR                        urgpro.004579CB
00457999  .  C645 FF 01     MOV [BYT
0045799D  .  66:3BF3        CMP SI,B
004579A0  .v 76 55          JBE SHOR                        urgpro.004579F7
004579A2  .  8D4D F8        LEA ECX,
004579A5  .  8D45 F0        LEA EAX,
004579A8  .  BA 08000000    MOV EDX,
004579AD  .  E8 C696FDFF    CALL 004                        urgpro.00431078
004579B2  .  8B15 BCE5470   MOV EDX,                        urgpro.0047DFB0
004579B8  .  8B12           MOV EDX,
004579BA  .  A1 4CEC4700    MOV EAX,
004579BF  .  8B00           MOV EAX,
004579C1  .  8B4D F8        MOV ECX,
004579C4  .  E8 E3C8FEFF    CALL 004                        urgpro.004442AC
004579C9  .v EB 2C          JMP SHOR                        urgpro.004579F7
004579CB  >  66:A1 8C7A45   MOV AX,[
004579D1  .  50             PUSH EAX
004579D2  .  6A 00          PUSH 0
004579D4  .  33C9           XOR ECX,
004579D6  .  BA 707B4500    MOV EDX,                        rial I
004579DB  .  B8 987B4500    MOV EAX,                        SCII "Your have  sed all
004579E0  .  E8 FB04FFFF    CALL 004                        urgpro.00447EE0
004579E5  .  A1 80E64700    MOV EAX,
004579EA  .  C600 01        MOV [BYTE DS:EAX],1
004579ED  .  B8 09000000    MOV EAX,9
004579F2  .  E8 3DD4FEFF    CALL 00444E34                   purgpro.00444E34
004579F7  >  33C0           XOR EAX,EAX
004579F9  .  5A             POP EDX
00457989=purgpro.00457989
```

```
EDX BD1F7D64
EBX 00000000
ESP 0012ED24
EBP 0012EDB4
ESI 00000000
EDI 7FFDE000

EIP 77F8AE5A ntdll.77F8AE5A

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 0038 32bit 7FFDE000(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 7.3368171293181306880e+4138
ST1 empty +UNORM 0086 00000038 BD1F7850
ST2 empty +UNORM 0038 0012FEB8 00000000
ST3 empty -UNORM FEB0 00000212 0000001B
ST4 empty 1.5073537349844771840e+4918
ST5 empty +UNORM 1AD6 01000000 00201372
ST6 empty 9.6130189864164167680e-2505
ST7 empty 2.2937344507161223680e+4235
               3 2 1 0      E S P U O Z D I
FST 0020  Cond 0 0 0 0  Err 0 0 1 0 0 0 0 0  (GT)
FCW 1372  Prec NEAR,64  Mask    1 1 0 0 1 0
```

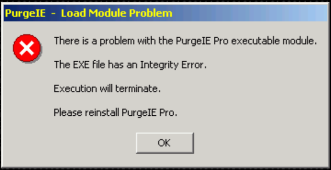
```
0047D000 32 13 8B C0 02 00 8B C0 00 8D 40 00 9C 88 44 00 2‼ï└@.ï└.ì@.£èD.
0047D010 2C 8B 44 00 A8 D0 47 00 44 08 D3 00 D8 20 40 00 ,ïD.¿ðG.D◘Ë.ï @.
0047D020 60 22 40 00 D4 25 40 00 32 1F 8B C0 52 75 6E 74 `"@.È%@.2▼ï└Runt
0047D030 69 6D 65 20 65 72 72 6F 72 20 20 20 20 20 61 74 ime error     at
0047D040 20 30 30 30 30 30 30 30 30 00 8B C0 45 72 72 6F  00000000.ï└Erro
0047D050 72 00 8B C0 30 31 32 33 34 35 36 37 38 39 41 42 r.ï└0123456789AB
0047D060 43 44 45 46 20 20 20 20 20 20 20 20 20 20 20 20 CDEF
0047D070 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D080 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D090 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D0A0 20 20 20 20 0D 0A 8B C0 00 00 00 00 00 00 40 00     ..ï└......@.
0047D0B0 00 00 40 00 00 00 00 00 00 00 00 00 02 00 00 00 ..@.........☻...
0047D0C0 05 00 00 00 00 00 00 00 93 08 00 00 30 08 D3 00 ♣.......ô◘..0◘Ë.
0047D0D0 1F 00 1C 00 1F 00 1E 00 1F 00 1E 00 1F 00 1F 00 ▼.∟.▼.▲.▼.▲.▼.▼.
0047D0E0 1E 00 1F 00 1E 00 1F 00 1F 00 1D 00 1F 00 1E 00 ▲.▼.▲.▼.▼.↔.▼.▲.
0047D0F0 1F 00 1E 00 1F 00 1F 00 1E 00 1F 00 1E 00 1F 00 ▼.▲.▼.▼.▲.▼.▲.▼.
```

```
0012FFC4   795287E7  RETURN to kernel32.795287E7
0012FFC8   005616A8
0012FFCC   00000056
0012FFD0   7FFDF000
0012FFD4   00000200
0012FFD8   0012FFC8
0012FFDC   00000200
0012FFE0   FFFFFFFF  End of SEH chain
0012FFE4   79551BB4  SE handler
0012FFE8   79502B00  kernel32.79502B00
0012FFEC   00000000
0012FFF0   00000000
0012FFF4   00000000
0012FFF8   0047C4F0  purgpro.<ModuleEntryPoint>
0012FFFC   00000000
```

```
Module C:\WINNT\system32\MSCTF.dll
```

Done. Run the saved file...

Run app, (Not with Olly!) And We get this msg.:



**PurgeIE - Load Module Problem**

There is a problem with the PurgeIE Pro executable module.

The EXE file has an Integrity Error.

Execution will terminate.

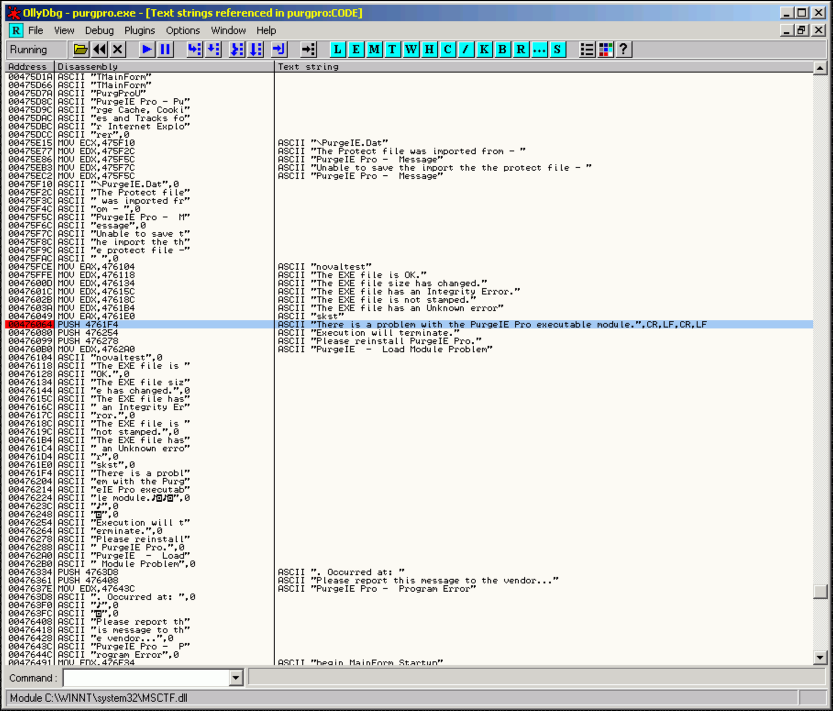
Please reinstall PurgeIE Pro.

Shit, file got a CRC Check... Let's kill it.

Push The "R" Button.:

L E M T W H C / K B R ... S

Search for the text "There is a problem with the PurgeIE Pro executable module."



**OllyDbg - purgpro.exe - [Text strings referenced in purgpro:CODE]**

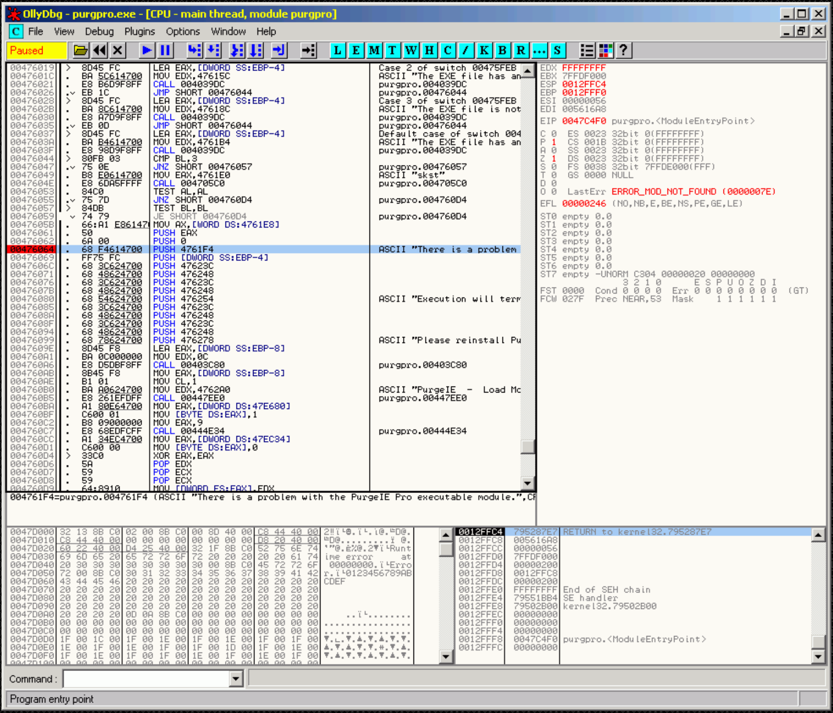
R File View Debug Plugins Options Window Help
Running
L E M T W H C / K B R ... S
?

```
Address  Disassembly                     Text string
00475D1A ASCII "TMainForm"
00475D66 ASCII "TMainForm"
00475D7A ASCII "PurgProU"
00475D8C ASCII "PurgeIE Pro - Pu"
00475D9C ASCII "rge Cache, Cooki"
00475DAC ASCII "es and Tracks fo"
00475DBC ASCII "r Internet Explo"
00475DCC ASCII "rer",0
00475E15 MOV ECX,475F10                  ASCII "\PurgeIE.Dat"
00475E77 MOV EDX,475F2C                  ASCII "The Protect file was imported from - "
00475E86 MOV EDX,475F5C                  ASCII "PurgeIE Pro -  Message"
00475EB3 MOV EDX,475F7C                  ASCII "Unable to save the import the the protect file - "
00475EC2 MOV EDX,475F5C                  ASCII "PurgeIE Pro -  Message"
00475F10 ASCII "\PurgeIE.Dat",0
00475F2C ASCII "The Protect file"
00475F3C ASCII " was imported fr"
00475F4C ASCII "om - ",0
00475F5C ASCII "PurgeIE Pro -  M"
00475F6C ASCII "essage",0
00475F7C ASCII "Unable to save t"
00475F8C ASCII "he import the th"
00475F9C ASCII "e protect file -"
00475FAC ASCII " ",0
00475FCE MOV EAX,476104                  ASCII "novaltest"
00475FFE MOV EDX,476118                  ASCII "The EXE file is OK."
0047600D MOV EDX,476134                  ASCII "The EXE file size has changed."
0047601C MOV EDX,47615C                  ASCII "The EXE file has an Integrity Error."
0047602B MOV EDX,47618C                  ASCII "The EXE file is not stamped."
0047603A MOV EDX,4761B4                  ASCII "The EXE file has an Unknown error"
00476049 MOV EAX,4761E0                  ASCII "skst"
00476064 PUSH 4761F4                     ASCII "There is a problem with the PurgeIE Pro executable module.",CR,LF,CR,LF
00476080 PUSH 476254                     ASCII "Execution will terminate."
00476099 PUSH 476278                     ASCII "Please reinstall PurgeIE Pro."
004760B0 MOV EDX,4762A0                  ASCII "PurgeIE  -  Load Module Problem"
00476104 ASCII "novaltest",0
00476118 ASCII "The EXE file is "
00476128 ASCII "OK.",0
00476134 ASCII "The EXE file siz"
00476144 ASCII "e has changed.",0
0047615C ASCII "The EXE file has"
0047616C ASCII " an Integrity Er"
0047617C ASCII "ror.",0
0047618C ASCII "The EXE file is "
0047619C ASCII "not stamped.",0
004761B4 ASCII "The EXE file has"
004761C4 ASCII " an Unknown erro"
004761D4 ASCII "r",0
004761E0 ASCII "skst",0
004761F4 ASCII "There is a probl"
00476204 ASCII "em with the Purg"
00476214 ASCII "eIE Pro executab"
00476224 ASCII "le module.♪◘♪◘",0
0047623C ASCII "♪",0
00476248 ASCII "◘",0
00476254 ASCII "Execution will t"
00476264 ASCII "erminate.",0
00476278 ASCII "Please reinstall"
00476288 ASCII " PurgeIE Pro.",0
004762A0 ASCII "PurgeIE  -  Load"
004762B0 ASCII " Module Problem",0
00476334 PUSH 4763D8                     ASCII ". Occurred at: "
00476361 PUSH 476408                     ASCII "Please report this message to the vendor..."
0047637E MOV EDX,47643C                  ASCII "PurgeIE Pro -  Program Error"
004763D8 ASCII ". Occurred at: ",0
004763F0 ASCII "♪",0
004763FC ASCII "◘",0
00476408 ASCII "Please report th"
00476418 ASCII "is message to th"
00476428 ASCII "e vendor...",0
0047643C ASCII "PurgeIE Pro -  P"
0047644C ASCII "rogram Error",0
00476491 MOV EDX,476F34                  ASCII "begin MainForm Startup"
```

Module C:\WINNT\system32\MSCTF.dll

F2 + "Enter"

Back to CPU Window again.


OllyDbg - purgpro.exe - [CPU - main thread, module purgpro]

```
00476019  > 8D45 FC        LEA EAX,[DWORD SS:EBP-4]       Case 2 of switch 00475FEB
0047601C  . BA 5C614700    MOV EDX,47615C                 ASCII "The EXE file has an
00476021  . E8 B6D9F8FF    CALL 004039DC                  purgpro.004039DC
00476026  .v EB 1C         JMP SHORT 00476044             purgpro.00476044
00476028  > 8D45 FC        LEA EAX,[DWORD SS:EBP-4]       Case 3 of switch 00475FEB
0047602B  . BA 8C614700    MOV EDX,47618C                 ASCII "The EXE file is not
00476030  . E8 A7D9F8FF    CALL 004039DC                  purgpro.004039DC
00476035  .v EB 0D         JMP SHORT 00476044             purgpro.00476044
00476037  > 8D45 FC        LEA EAX,[DWORD SS:EBP-4]       Default case of switch 004
0047603A  . BA B4614700    MOV EDX,4761B4                 ASCII "The EXE file has an
0047603F  . E8 98D9F8FF    CALL 004039DC                  purgpro.004039DC
00476044  > 80FB 03        CMP BL,3
00476047  .v 75 0E         JNZ SHORT 00476057             purgpro.00476057
00476049  . B8 E0614700    MOV EAX,4761E0                 ASCII "skst"
0047604E  . E8 6DA5FFFF    CALL 004705C0                  purgpro.004705C0
00476053  . 84C0           TEST AL,AL
00476055  .v 75 7D         JNZ SHORT 004760D4             purgpro.004760D4
00476057  > 84DB           TEST BL,BL
00476059   v 74 79         JE SHORT 004760D4              purgpro.004760D4
0047605B  . 66:A1 E86147(  MOV AX,[WORD DS:4761E8]
00476061  . 50             PUSH EAX
00476062  . 6A 00          PUSH 0
00476064  . 68 F4614700    PUSH 4761F4                    ASCII "There is a problem
00476069  . FF75 FC        PUSH [DWORD SS:EBP-4]
0047606C  . 68 3C624700    PUSH 47623C
00476071  . 68 48624700    PUSH 476248
00476076  . 68 3C624700    PUSH 47623C
0047607B  . 68 48624700    PUSH 476248
00476080  . 68 54624700    PUSH 476254                    ASCII "Execution will term
00476085  . 68 3C624700    PUSH 47623C
0047608A  . 68 48624700    PUSH 476248
0047608F  . 68 3C624700    PUSH 47623C
00476094  . 68 48624700    PUSH 476248
00476099  . 68 78624700    PUSH 476278                    ASCII "Please reinstall Pu
0047609E  . 8D45 F8        LEA EAX,[DWORD SS:EBP-8]
004760A1  . BA 0C000000    MOV EDX,0C
004760A6  . E8 D5DBF8FF    CALL 00403C80                  purgpro.00403C80
004760AB  . 8B45 F8        MOV EAX,[DWORD SS:EBP-8]
004760AE  . B1 01          MOV CL,1
004760B0  . BA A0624700    MOV EDX,4762A0                 ASCII "PurgeIE  -  Load Mc
004760B5  . E8 261EFDFF    CALL 00447EE0                  purgpro.00447EE0
004760BA  . A1 80E64700    MOV EAX,[DWORD DS:47E680]
004760BF  . C600 01        MOV [BYTE DS:EAX],1
004760C2  . B8 09000000    MOV EAX,9
004760C7  . E8 68EDFCFF    CALL 00444E34                  purgpro.00444E34
004760CC  . A1 34EC4700    MOV EAX,[DWORD DS:47EC34]
004760D1  . C600 00        MOV [BYTE DS:EAX],0
004760D4  > 33C0           XOR EAX,EAX
004760D6  . 5A             POP EDX
004760D7  . 59             POP ECX
004760D8  . 59             POP ECX
004760D9  . 64:8910        MOV [DWORD FS:EAX],EDX
004761F4=purgpro.004761F4 (ASCII "There is a problem with the PurgeIE Pro executable module.",CR
```

```
EDX FFFFFFFF
EBX 7FFDF000
ESP 0012FFC4
EBP 0012FFF0
ESI 00000056
EDI 005616A8

EIP 0047C4F0 purgpro.<ModuleEntryPoint>

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 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_MOD_NOT_FOUND (0000007E)

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

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty -UNORM C304 00000020 00000000
               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
```

```
0047D000 32 13 8B C0 02 00 8B C0 00 8D 40 00 C8 44 40 00  2‼ï└@.ï└.ì@.└D@.
0047D010 C8 44 40 00 00 00 00 00 00 00 00 00 D8 20 40 00  └D@.........ï @.
0047D020 60 22 40 00 D4 25 40 00 32 1F 8B C0 52 75 6E 74  `"@.È%@.2▼ï└Runt
0047D030 69 6D 65 20 65 72 72 6F 72 20 20 20 20 20 61 74  ime error     at
0047D040 20 30 30 30 30 30 30 30 30 00 8B C0 45 72 72 6F   00000000.ï└Erro
0047D050 72 00 8B C0 30 31 32 33 34 35 36 37 38 39 41 42  r.ï└0123456789AB
0047D060 43 44 45 46 20 20 20 20 20 20 20 20 20 20 20 20  CDEF
0047D070 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D080 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D090 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D0A0 20 20 20 20 0D 0A 8B C0 00 00 00 00 00 00 00 00      ..ï└........
0047D0B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0047D0C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0047D0D0 1F 00 1C 00 1F 00 1E 00 1F 00 1E 00 1F 00 1F 00  ▼.∟.▼.▲.▼.▲.▼.▼.
0047D0E0 1E 00 1F 00 1E 00 1F 00 1F 00 1D 00 1F 00 1E 00  ▲.▼.▲.▼.▼.#.▼.▲.
0047D0F0 1F 00 1E 00 1F 00 1F 00 1E 00 1F 00 1E 00 1F 00  ▼.▲.▼.▼.▲.▼.▲.▼.
```

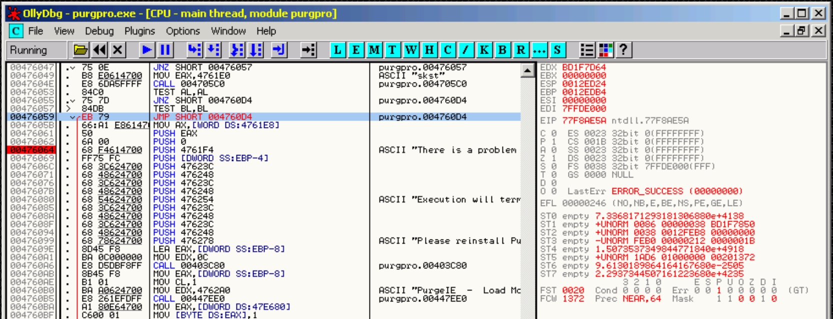
```
0012FFC4   795287E7  RETURN to kernel32.795287E7
0012FFC8   005616A8
0012FFCC   00000056
0012FFD0   7FFDF000
0012FFD4   00000200
0012FFD8   0012FFC8
0012FFDC   00000200
0012FFE0   FFFFFFFF  End of SEH chain
0012FFE4   79551BB4  SE handler
0012FFE8   79502B00  kernel32.79502B00
0012FFEC   00000000
0012FFF0   00000000
0012FFF4   00000000
0012FFF8   0047C4F0  purgpro.<ModuleEntryPoint>
0012FFFC   00000000
```

Program entry point

Easy, see the jump.:

00476059 |74 79 JE SHORT 004760D4 ; purgpro.004760D4

Let's jump all the time.:


OllyDbg - purgpro.exe - [CPU - main thread, module purgpro]

```
00476047  .v 75 0E         JNZ SHORT 00476057             purgpro.00476057
00476049  . B8 E0614700    MOV EAX,4761E0                 ASCII "skst"
0047604E  . E8 6DA5FFFF    CALL 004705C0                  purgpro.004705C0
00476053  . 84C0           TEST AL,AL
00476055  .v 75 7D         JNZ SHORT 004760D4             purgpro.004760D4
00476057  > 84DB           TEST BL,BL
00476059   v EB 79         JMP SHORT 004760D4             purgpro.004760D4
0047605B  . 66:A1 E86147(  MOV AX,[WORD DS:4761E8]
00476061  . 50             PUSH EAX
00476062  . 6A 00          PUSH 0
00476064  . 68 F4614700    PUSH 4761F4                    ASCII "There is a problem
00476069  . FF75 FC        PUSH [DWORD SS:EBP-4]
0047606C  . 68 3C624700    PUSH 47623C
00476071  . 68 48624700    PUSH 476248
00476076  . 68 3C624700    PUSH 47623C
0047607B  . 68 48624700    PUSH 476248
00476080  . 68 54624700    PUSH 476254                    ASCII "Execution will term
00476085  . 68 3C624700    PUSH 47623C
0047608A  . 68 48624700    PUSH 476248
0047608F  . 68 3C624700    PUSH 47623C
00476094  . 68 48624700    PUSH 476248
00476099  . 68 78624700    PUSH 476278                    ASCII "Please reinstall Pu
0047609E  . 8D45 F8        LEA EAX,[DWORD SS:EBP-8]
004760A1  . BA 0C000000    MOV EDX,0C
004760A6  . E8 D5DBF8FF    CALL 00403C80                  purgpro.00403C80
004760AB  . 8B45 F8        MOV EAX,[DWORD SS:EBP-8]
004760AE  . B1 01          MOV CL,1
004760B0  . BA A0624700    MOV EDX,4762A0                 ASCII "PurgeIE  -  Load Mc
004760B5  . E8 261EFDFF    CALL 00447EE0                  purgpro.00447EE0
004760BA  . A1 80E64700    MOV EAX,[DWORD DS:47E680]
004760BF  . C600 01        MOV [BYTE DS:EAX],1
```

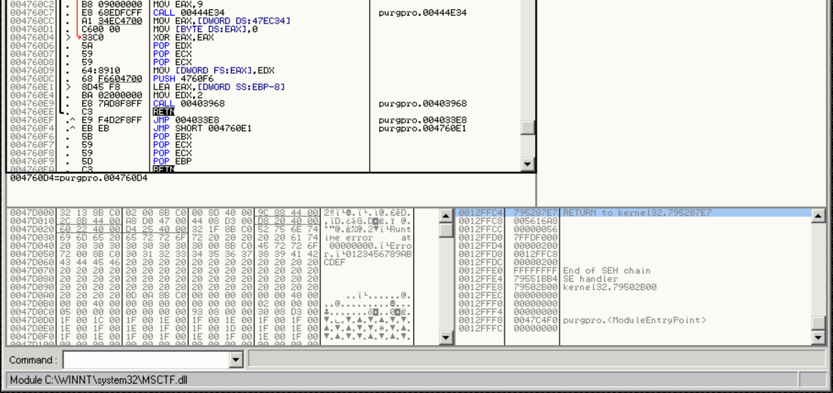
```
EDX BD1F7D64
EBX 00000000
ESP 0012ED24
EBP 0012EDB4
ESI 00000000
EDI 7FFDE000

EIP 77F8AE5A ntdll.77F8AE5A

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 0038 32bit 7FFDE000(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 7.3368171293181306880e+4138
ST1 empty +UNORM 0086 00000038 BD1F7850
ST2 empty +UNORM 0038 0012FEB8 00000000
ST3 empty -UNORM FEB0 00000212 0000001B
ST4 empty 1.5073537349844771840e+4918
ST5 empty +UNORM 1AD6 01000000 00201372
ST6 empty 9.6130189864164167680e-2505
ST7 empty 2.2937344507161223680e+4235
               3 2 1 0      E S P U O Z D I
FST 0020  Cond 0 0 0 0  Err 0 0 1 0 0 0 0 0  (GT)
FCW 1372  Prec NEAR,64  Mask    1 1 0 0 1 0
```



```
004760C2  .  B8 09000000    MOV EAX,9
004760C7  .  E8 68EDFCFF    CALL 00444E34                         purgpro.00444E34
004760CC  .  A1 34EC4700    MOV EAX,[DWORD DS:47EC34]
004760D1  .  C600 00        MOV [BYTE DS:EAX],0
004760D4  >  33C0           XOR EAX,EAX
004760D6  .  5A             POP EDX
004760D7  .  59             POP ECX
004760D8  .  59             POP ECX
004760D9  .  64:8910        MOV [DWORD FS:EAX],EDX
004760DC  .  68 F6604700    PUSH 4760F6
004760E1  >  8D45 F8        LEA EAX,[DWORD SS:EBP-8]
004760E4  .  BA 02000000    MOV EDX,2
004760E9  .  E8 7AD8F8FF    CALL 00403968                         purgpro.00403968
004760EE  .  C3             RETN
004760EF  .^ E9 F4D2F8FF    JMP 004033E8                          purgpro.004033E8
004760F4  .^ EB EB          JMP SHORT 004760E1                    purgpro.004760E1
004760F6  .  5B             POP EBX
004760F7  .  59             POP ECX
004760F8  .  59             POP ECX
004760F9  .  5D             POP EBP
004760FA  .  C3             RETN
004760D4=purgpro.004760D4
```

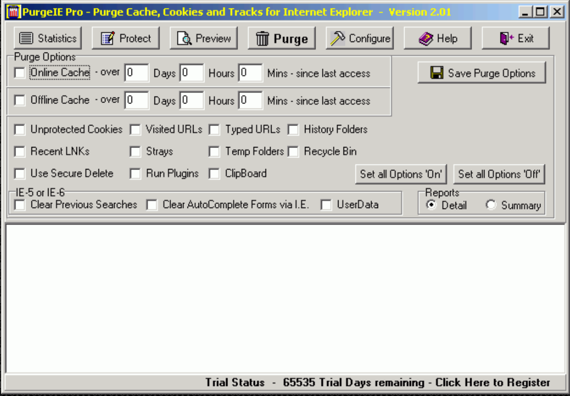
```
0047D000  32 13 8B C0 02 00 8B C0 00 8D 40 00 9C 88 44 00  2‼ï└@.ï└.ì@.£èD.
0047D010  2C 8B 44 00 A8 D0 47 00 44 08 D3 00 D8 20 40 00  ,ïD.¿ÐG.D◘Ë.Ï @.
0047D020  60 22 40 00 D4 25 40 00 32 1F 8B C0 52 75 6E 74  `"@.È%@.2▼ï└Runt
0047D030  69 6D 65 20 65 72 72 6F 72 20 20 20 20 20 61 74  ime error     at
0047D040  20 30 30 30 30 30 30 30 30 00 8B C0 45 72 72 6F   00000000.ï└Erro
0047D050  72 00 8B C0 30 31 32 33 34 35 36 37 38 39 41 42  r.ï└0123456789AB
0047D060  43 44 45 46 20 20 20 20 20 20 20 20 20 20 20 20  CDEF
0047D070  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D080  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D090  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0047D0A0  20 20 20 20 0D 0A 8B C0 00 00 00 00 00 00 40 00      ..ï└......@.
0047D0B0  00 00 40 00 00 00 00 00 00 00 00 00 02 00 00 00  ..@.........☻...
0047D0C0  05 00 00 00 00 00 00 00 93 08 00 00 30 08 D3 00  ♣.......ô◘..0◘Ë.
0047D0D0  1F 00 1C 00 1F 00 1E 00 1F 00 1E 00 1F 00 1F 00  ▼.∟.▼.▲.▼.▲.▼.▼.
0047D0E0  1E 00 1F 00 1E 00 1F 00 1F 00 1D 00 1F 00 1E 00  ▲.▼.▲.▼.▼.↔.▼.▲.
0047D0F0  1F 00 1E 00 1F 00 1F 00 1E 00 1F 00 1E 00 1F 00  ▼.▲.▼.▼.▲.▼.▲.▼.
```

```
0012FFC4   795287E7  RETURN to kernel32.795287E7
0012FFC8   005616A8
0012FFCC   00000056
0012FFD0   7FFDF000
0012FFD4   00000200
0012FFD8   0012FFC8
0012FFDC   00000200
0012FFE0   FFFFFFFF  End of SEH chain
0012FFE4   79551BB4  SE handler
0012FFE8   79502B00  kernel32.79502B00
0012FFEC   00000000
0012FFF0   00000000
0012FFF4   00000000
0012FFF8   0047C4F0  purgpro.<ModuleEntryPoint>
0012FFFC   00000000
```

Module C:\WINNT\system32\MSCTF.dll

Good old story, let's save file again.

Now, try to run it...



PurgeIE Pro - Purge Cache, Cookies and Tracks for Internet Explorer - Version 2.01

Purge Options

☐ Online Cache - over 0 Days 0 Hours 0 Mins - since last access

☐ Offline Cache - over 0 Days 0 Hours 0 Mins - since last access

☐ Unprotected Cookies ☐ Visited URLs ☐ Typed URLs ☐ History Folders

☐ Recent LNKs ☐ Strays ☐ Temp Folders ☐ Recycle Bin

☐ Use Secure Delete ☐ Run Plugins ☐ ClipBoard

IE-5 or IE-6

☐ Clear Previous Searches ☐ Clear AutoComplete Forms via I.E. ☐ UserData

Reports

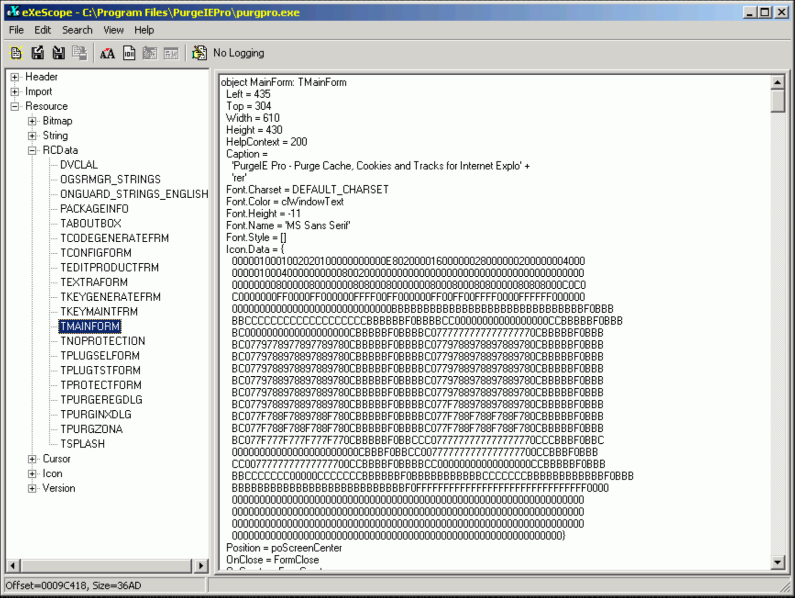
● Detail ○ Summary

Trial Status - 65535 Trial Days remaining - Click Here to Register

Now, the only thing that looks strange is the bottom of the program.

Load file in ExeScope.

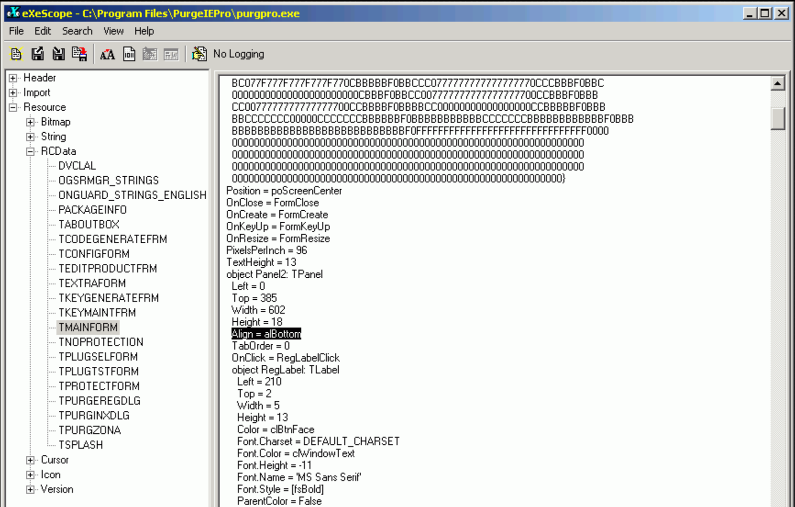
Open "TMAINFORM"



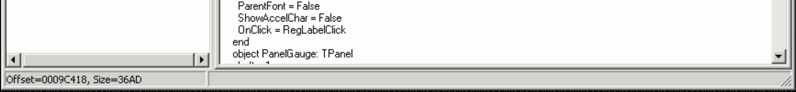
```
object MainForm: TMainForm
  Left = 435
  Top = 304
  Width = 610
  Height = 430
  HelpContext = 200
  Caption =
    'PurgeIE Pro - Purge Cache, Cookies and Tracks for Internet Explo' +
    'rer'
  Font.Charset = DEFAULT_CHARSET
  Font.Color = clWindowText
  Font.Height = -11
  Font.Name = 'MS Sans Serif'
  Font.Style = []
  Icon.Data = {
    0000010001002020100000000000E80200001600000028000000200000004000
    0000010004000000000080020000000000000000000000000000000000000000
    000000008000008000000080800080000000800080008080000080808000C0C0
    C0000000FF0000FF000000FFFF00FF000000FF00FF00FFFF0000FFFFFF000000
    00000000000000000000000000000000BBBBBBBBBBBBBBBBBBBBBBBBBBBF0BBB
    BBCCCCCCCCCCCCCCCCCCCBBBBBBF0BBBBCC00000000000000000CCBBBBBF0BBB
    BC0000000000000000000CBBBBBF0BBBBC0777777777777777770CBBBBBF0BBB
    BC0779778977897789780CBBBBBF0BBBBC0779788978897889780CBBBBBF0BBB
    BC0779788978897889780CBBBBBF0BBBBC0779788978897889780CBBBBBF0BBB
    BC0779788978897889780CBBBBBF0BBBBC0779788978897889780CBBBBBF0BBB
    BC0779788978897889780CBBBBBF0BBBBC0779788978897889780CBBBBBF0BBB
    BC0779788978897889780CBBBBBF0BBBBC0779788978897889780CBBBBBF0BBB
    BC0779788978897889780CBBBBBF0BBBBC077F788978897889780CBBBBBF0BBB
    BC077F788F7889788F780CBBBBBF0BBBBC077F788F788F788F780CBBBBBF0BBB
    BC077F788F788F788F780CBBBBBF0BBBBC077F788F788F788F780CBBBBBF0BBB
    BC077F777F777F777F770CBBBBBF0BBCCC0777777777777777770CCCBBBF0BBC
    00000000000000000000000CBBBF0BBCC0077777777777777777700CCBBBF0BBB
    CC007777777777777777700CCBBBBF0BBBBCC0000000000000000CCBBBBBF0BBB
    BBCCCCCCC00000CCCCCCCBBBBBBF0BBBBBBBBBBBCCCCCCCBBBBBBBBBBBBF0BBB
    BBBBBBBBBBBBBBBBBBBBBBBBBBBBF0FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000000000000000000000000000}
  Position = poScreenCenter
  OnClose = FormClose
```

Offset=0009C418, Size=36AD

**Browse Down in code...**



```
    BC077F777F777F777F770CBBBBBF0BBCCC0777777777777777770CCCBBBF0BBC
    00000000000000000000000CBBBF0BBCC0077777777777777777700CCBBBF0BBB
    CC007777777777777777700CCBBBBF0BBBBCC0000000000000000CCBBBBBF0BBB
    BBCCCCCCC00000CCCCCCCBBBBBBF0BBBBBBBBBBBCCCCCCCBBBBBBBBBBBBF0BBB
    BBBBBBBBBBBBBBBBBBBBBBBBBBBBF0FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    0000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000000000000000000000000000}
  Position = poScreenCenter
  OnClose = FormClose
  OnCreate = FormCreate
  OnKeyUp = FormKeyUp
  OnResize = FormResize
  PixelsPerInch = 96
  TextHeight = 13
  object Panel2: TPanel
    Left = 0
    Top = 385
    Width = 602
    Height = 18
    Align = alBottom
    TabOrder = 0
    OnClick = RegLabelClick
    object RegLabel: TLabel
      Left = 210
      Top = 2
      Width = 5
      Height = 13
      Color = clBtnFace
      Font.Charset = DEFAULT_CHARSET
      Font.Color = clWindowText
      Font.Height = -11
      Font.Name = 'MS Sans Serif'
      Font.Style = [fsBold]
      ParentColor = False
```

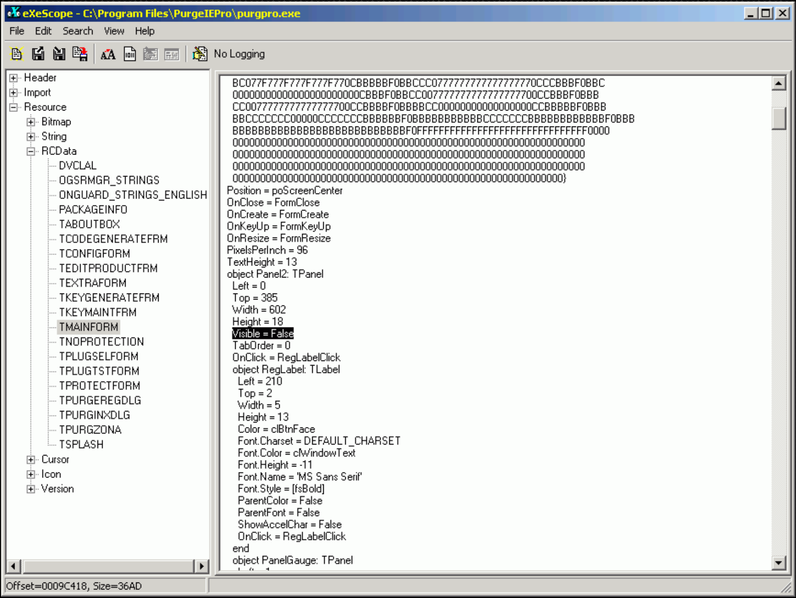


```
  ParentFont = False
  ShowAccelChar = False
  OnClick = RegLabelClick
end
object PanelGauge: TPanel
```

Offset=0009C418, Size=36AD

**This is the Code that we can change without destroying/changing filesize.**

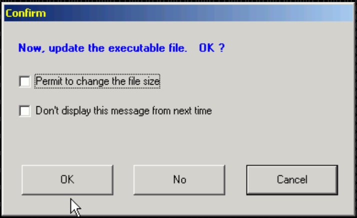
**Just change text to "Visible = False"**



```
  BC077F777F777F777F770CBBBBBF0BBCCC07777777777777777770CCCBBBF0BBC
  0000000000000000000000CBBBF0BBCC007777777777777777700CCBBBF0BBB
  CC007777777777777777700CCBBBBF0BBBBCC00000000000000000CCBBBBBF0BBB
  BBCCCCCCC00000CCCCCCCBBBBBBF0BBBBBBBBBBBCCCCCCCBBBBBBBBBBBBF0BBB
  BBBBBBBBBBBBBBBBBBBBBBBBBBBBF0FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0000
  0000000000000000000000000000000000000000000000000000000000000000
  0000000000000000000000000000000000000000000000000000000000000000
  0000000000000000000000000000000000000000000000000000000000000000
  000000000000000000000000000000000000000000000000000000000000}
Position = poScreenCenter
OnClose = FormClose
OnCreate = FormCreate
OnKeyUp = FormKeyUp
OnResize = FormResize
PixelsPerInch = 96
TextHeight = 13
object Panel2: TPanel
  Left = 0
  Top = 385
  Width = 602
  Height = 18
  Visible = False
  TabOrder = 0
  OnClick = RegLabelClick
  object RegLabel: TLabel
    Left = 210
    Top = 2
    Width = 5
    Height = 13
    Color = clBtnFace
    Font.Charset = DEFAULT_CHARSET
    Font.Color = clWindowText
    Font.Height = -11
    Font.Name = 'MS Sans Serif'
    Font.Style = [fsBold]
    ParentColor = False
    ParentFont = False
    ShowAccelChar = False
    OnClick = RegLabelClick
  end
  object PanelGauge: TPanel
```

Offset=0009C418, Size=36AD

**Now, save file.:**



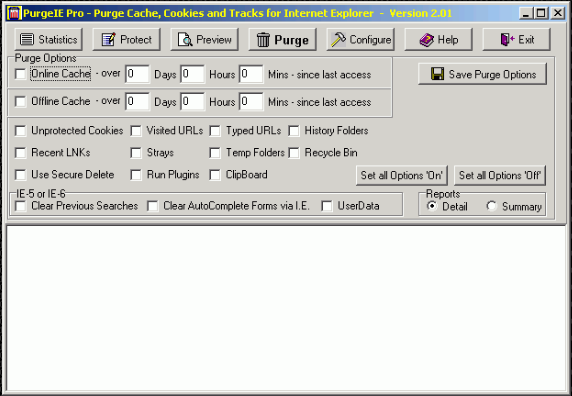
Confirm

**Now, update the executable file.  OK ?**

☐ Permit to change the file size

☐ Don't display this message from next time

**Done?, run app.**



Purge Options

☐ Online Cache - over 0 Days 0 Hours 0 Mins - since last access

☐ Offline Cache - over 0 Days 0 Hours 0 Mins - since last access

☐ Unprotected Cookies ☐ Visited URLs ☐ Typed URLs ☐ History Folders

☐ Recent LNKs ☐ Strays ☐ Temp Folders ☐ Recycle Bin

☐ Use Secure Delete ☐ Run Plugins ☐ ClipBoard

IE-5 or IE-6

☐ Clear Previous Searches ☐ Clear AutoComplete Forms via I.E. ☐ UserData

Reports

● Detail ○ Summary

**Enjoy!**
**That's all 4 now!**
**Remember if you use the application then buy it!**

**SHOUTZ AND GREETZ:**
**To all Members of AR Team, and the creator of Olly!**