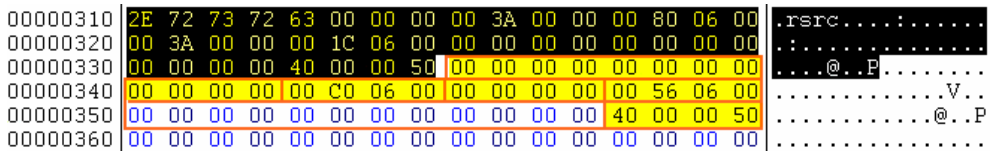
Add Section and Import Function Manually

I will discuss how you add a section to your files and also how to import function from DLL and this process useful for us in unpacking process and put unpacking information in a new section and now we will add 100h (256 bytes) to the program and the information of section occupy 40 bytes so goto the last section as follows :



The information which especially with section rsrc as follows

VirtualAddress : 00068000h

VirtualSize : 00003A00h

RawOffset : 00061C00h

RawSize : 00003A00h

RVA for virtual address for this section it 00068000h and this value it total VirtualAddress + VirtualSize for the ".reloc" section and for example if we sum it that will become like this:

00061000h + 00006108h = 00067108h

SectionAlignment = 1000h so the sum to 1000 and the result will become 00068108 and if we use nearer ,1000 the final result will become 00068000h and this value pertain the Virtual Address for the "rsrc" section so we will sum the VirtualAddress and the VirtualSze

this section to result for us VirtualAddress for the new section as follows :

00068000h + 00003A00h = 0006BA00h + 1000h = 0006CA00h

After use ,1000 the final result 0006C000h and if you notice you will

RawOffset total RwaOffset + RawSize for the previous section so the new information will become like this :

VirtualAddress : 0006C000h ---→ 00 C0 06 00

VirtualSize : 100h ---→ 00 01 00 00

RawOffset : 00065600h ---→ 00 56 06 00

RawSize : 100h ---→ 00 01 00 00

Characteristics : E00000060 ---→ 60 00 00 E0

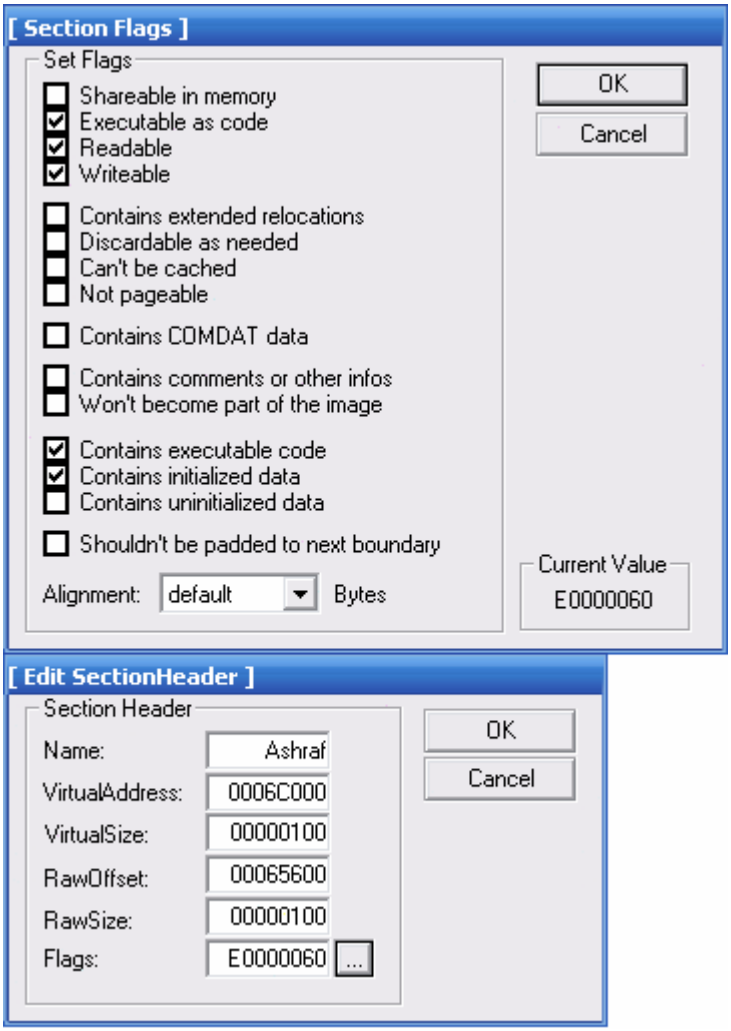
You will put the previous information in Hex Workshop as follows :

```
00000330 00 00 00 00 40 00 00 50 41 73 68 72 61 66 00 00 ....@..PAshraf..
00000340 00 01 00 00 00 C0 06 00 00 01 00 00 00 56 06 00 .............V..
00000350 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 E0 ............`...
00000360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

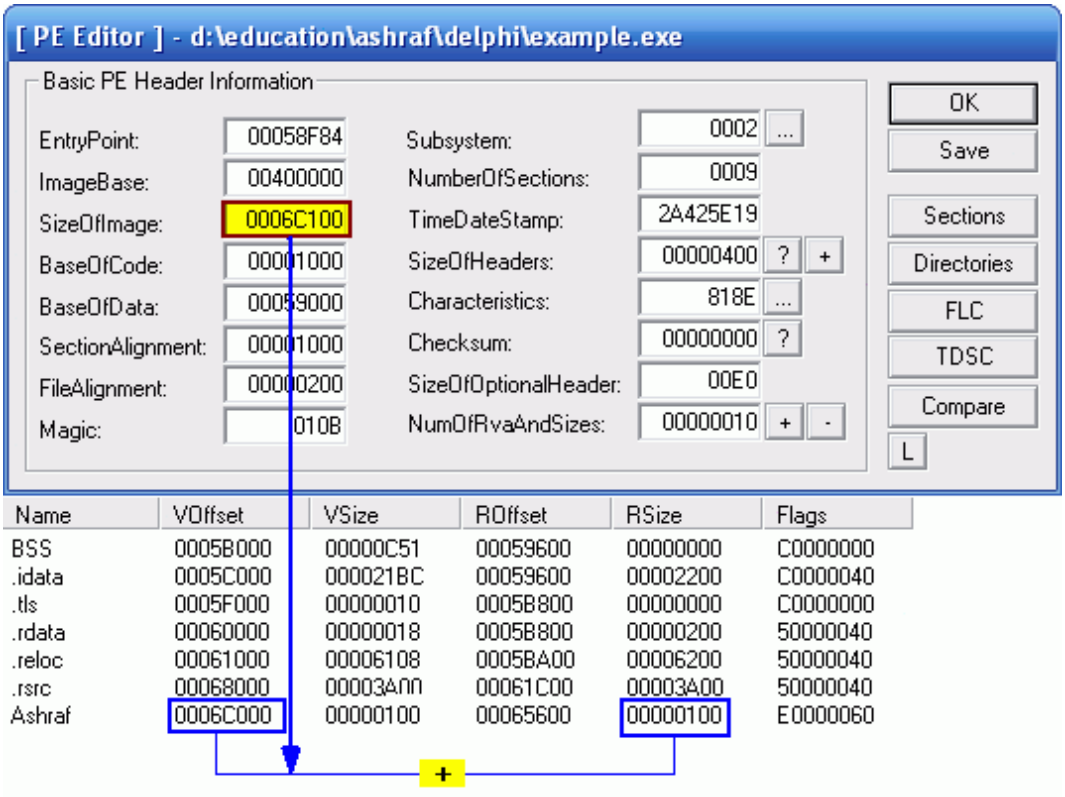
Then paste 256 bytes end the file and change NumberOfSection to number 9 and if you browse sections of program you will see that :

Name	VOffset	VSize	ROffset	RSize	Flags
CODE	00001000	00057FCC	00000400	00058000	60000020
DATA	00059000	0000111C	00058400	00001200	C0000040
BSS	0005B000	00000C51	00059600	00000000	C0000000
.idata	0005C000	000021BC	00059600	00002200	C0000040
.tls	0005F000	00000010	0005B800	00000000	C0000000
.rdata	00060000	00000018	0005B800	00000200	50000040
.reloc	00061000	00006108	0005BA00	00006200	50000040
.rsrc	00068000	00003A00	00061C00	00003A00	50000040
Ashraf	0006C000	00000100	00065600	00000100	E0000060

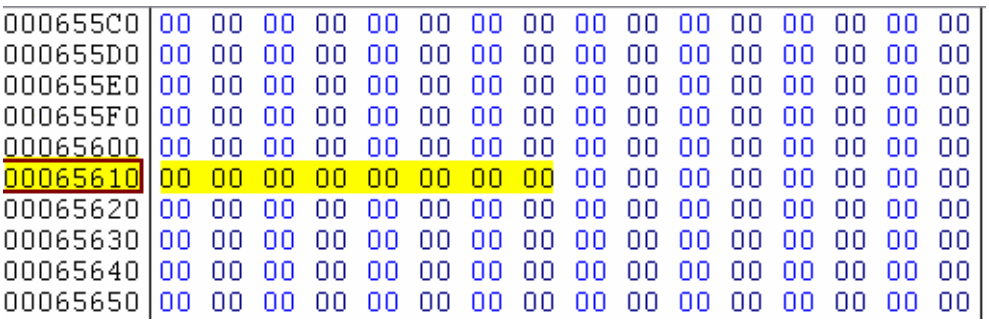
The previous form indicate to the new section which created and if we browse the information which pertain it you will see that :



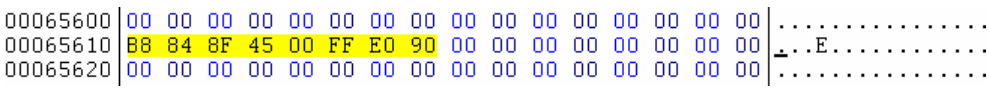
SizeOfImage it total VirtualAddress and RawSize like this :



Goto the RawOffset this :



Add this values :



The previous values mean it :

MOV EAX, 00458F84

JMP EAX

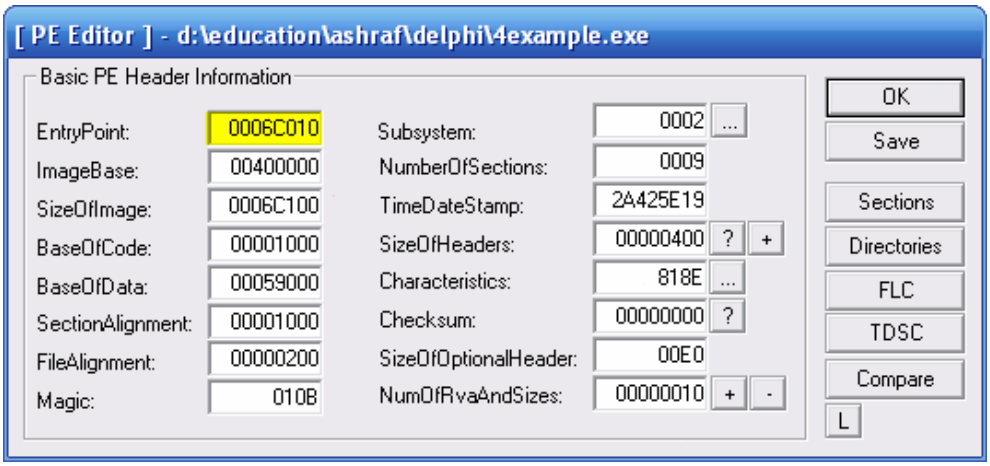
Save it and convert the RawOffset to VA with this :

VA = RawOffset +(V.OffsetOfSection + R.OffsetOfSection) + ImageBase

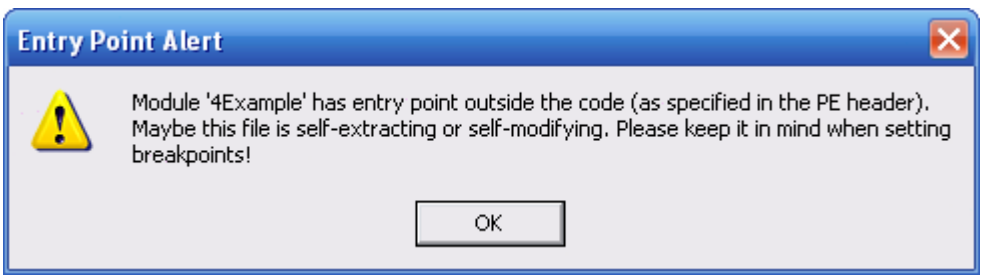
VA = 0046C010 and convert to RAV with this

RVA = VA – ImageBase

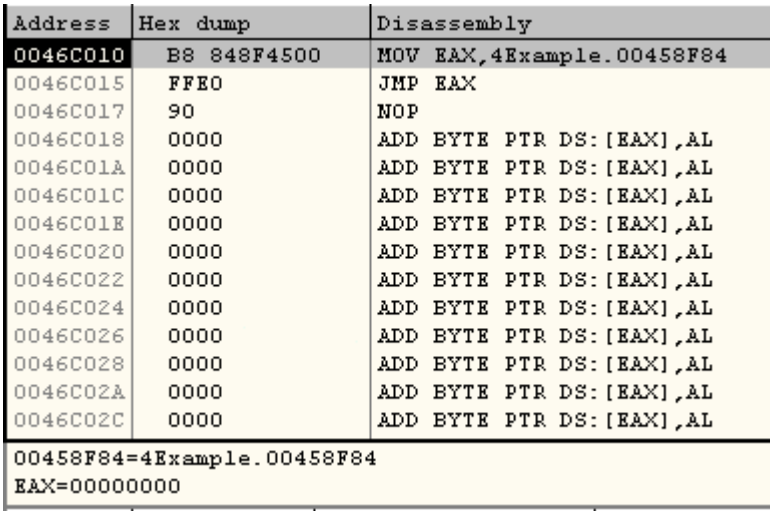
0006C010 = 0046C010 – 00400000 and put it in EP address like this :



Load the program into ollydbg to see this message :



The pervious tell you the Entry Point it not in the section CODE but it in another section anyway press OK to see this form :



Address	Hex dump	Disassembly
0046C010	B8 848F4500	MOV EAX,4Example.00458F84
0046C015	FFE0	JMP EAX
0046C017	90	NOP
0046C018	0000	ADD BYTE PTR DS:[EAX],AL
0046C01A	0000	ADD BYTE PTR DS:[EAX],AL
0046C01C	0000	ADD BYTE PTR DS:[EAX],AL
0046C01E	0000	ADD BYTE PTR DS:[EAX],AL
0046C020	0000	ADD BYTE PTR DS:[EAX],AL
0046C022	0000	ADD BYTE PTR DS:[EAX],AL
0046C024	0000	ADD BYTE PTR DS:[EAX],AL
0046C026	0000	ADD BYTE PTR DS:[EAX],AL
0046C028	0000	ADD BYTE PTR DS:[EAX],AL
0046C02A	0000	ADD BYTE PTR DS:[EAX],AL
0046C02C	0000	ADD BYTE PTR DS:[EAX],AL

00458F84=4Example.00458F84
EAX=00000000

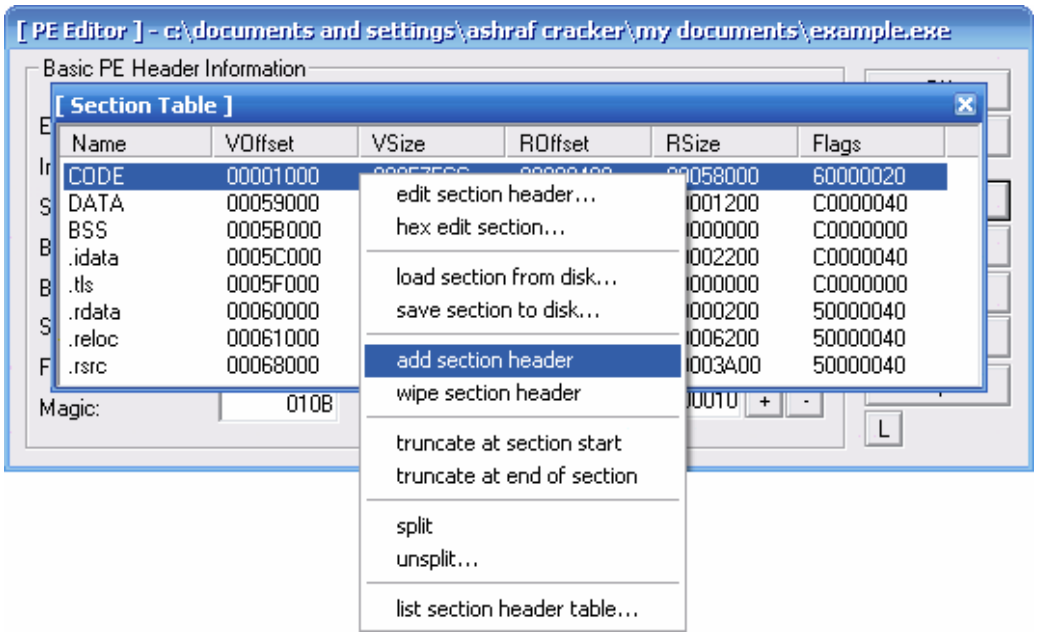
Now we will talking about how to import a function from DLL.Import Table contain of structure as IMAGE_IMPORT_DESCRIPTOR and in this program we found 13 table and if we need to import a function we will increase the number of tables to 14 and we will must execute this steps to creating this values :

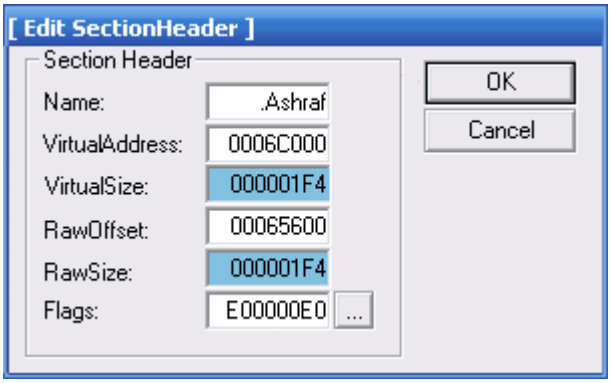
1- move the tables from the exist place to another place.
2- Change the value of directory to the new address.
3- Add the function which you want to add it.
4- Add the information which indicate to the new function to the new import.
5- Change the EP to new EP which we add the instructions to it.

The real place of import table it :

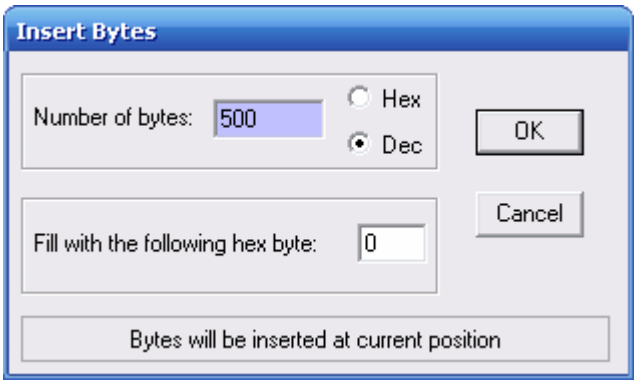
```
000595E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ........
000595F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ........
00059600 00 00 00 00 00 00 00 00 00 00 00 00 40 C7 05 00 ........
00059610 04 C1 05 00 00 00 00 00 00 00 00 00 00 00 00 00 ........
00059620 20 CA 05 00 AC C1 05 00 00 00 00 00 00 00 00 00  .......
00059630 00 00 00 00 66 CA 05 00 C0 C1 05 00 00 00 00 00 ....f...
00059640 00 00 00 00 00 00 00 00 A6 CA 05 00 D0 C1 05 00 ........
00059650 00 00 00 00 00 00 00 00 00 00 00 00 EE CA 05 00 ........
00059660 E0 C1 05 00 00 00 00 00 00 00 00 00 00 00 00 00 ........
00059670 3A CB 05 00 F4 C1 05 00 00 00 00 00 00 00 00 00 :.......
00059680 00 00 00 00 7A CB 05 00 04 C2 05 00 00 00 00 00 ....z...
00059690 00 00 00 00 00 00 00 00 64 CF 05 00 F4 C2 05 00 ........
000596A0 00 00 00 00 00 00 00 00 00 00 00 00 E0 D3 05 00 ........
000596B0 FC C3 05 00 00 00 00 00 00 00 00 00 00 00 00 00 ........
000596C0 1E DE 05 00 80 C6 05 00 00 00 00 00 00 00 00 00 ........
000596D0 00 00 00 00 34 DE 05 00 88 C6 05 00 00 00 00 00 ....4...
000596E0 00 00 00 00 00 00 00 00 C4 DF 05 00 E4 C6 05 00 ........
000596F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ........
00059700 00 00 00 00 4E C7 05 00 66 C7 05 00 7E C7 05 00 ....N...
```

The previous tables we need to move it to another place nad you don't find a place in this Section (.idata) to paste it so we will create new section by using LORDPE as follows :

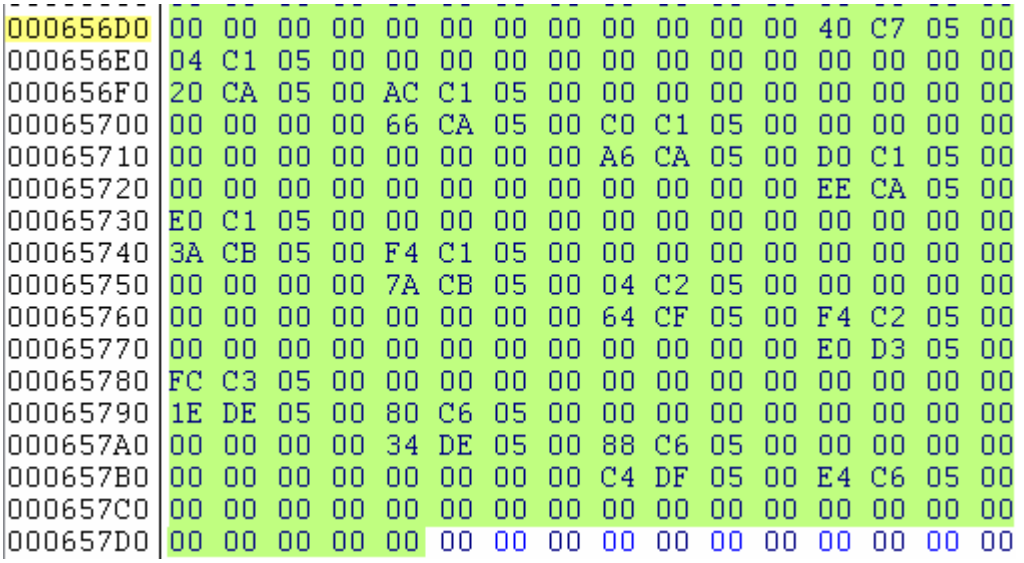




We add the size of section only and run the Hex Workshop to add the size as follows :



Copy the previous tables to this place :



000656D0	00	00	00	00	00	00	00	00	00	00	00	00	40	C7	05	00
000656E0	04	C1	05	00	00	00	00	00	00	00	00	00	00	00	00	00
000656F0	20	CA	05	00	AC	C1	05	00	00	00	00	00	00	00	00	00
00065700	00	00	00	00	66	CA	05	00	C0	C1	05	00	00	00	00	00
00065710	00	00	00	00	00	00	00	00	A6	CA	05	00	D0	C1	05	00
00065720	00	00	00	00	00	00	00	00	00	00	00	00	EE	CA	05	00
00065730	E0	C1	05	00	00	00	00	00	00	00	00	00	00	00	00	00
00065740	3A	CB	05	00	F4	C1	05	00	00	00	00	00	00	00	00	00
00065750	00	00	00	00	7A	CB	05	00	04	C2	05	00	00	00	00	00
00065760	00	00	00	00	00	00	00	00	64	CF	05	00	F4	C2	05	00
00065770	00	00	00	00	00	00	00	00	00	00	00	00	E0	D3	05	00
00065780	FC	C3	05	00	00	00	00	00	00	00	00	00	00	00	00	00
00065790	1E	DE	05	00	80	C6	05	00	00	00	00	00	00	00	00	00
000657A0	00	00	00	00	34	DE	05	00	88	C6	05	00	00	00	00	00
000657B0	00	00	00	00	00	00	00	00	C4	DF	05	00	E4	C6	05	00
000657C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000657D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

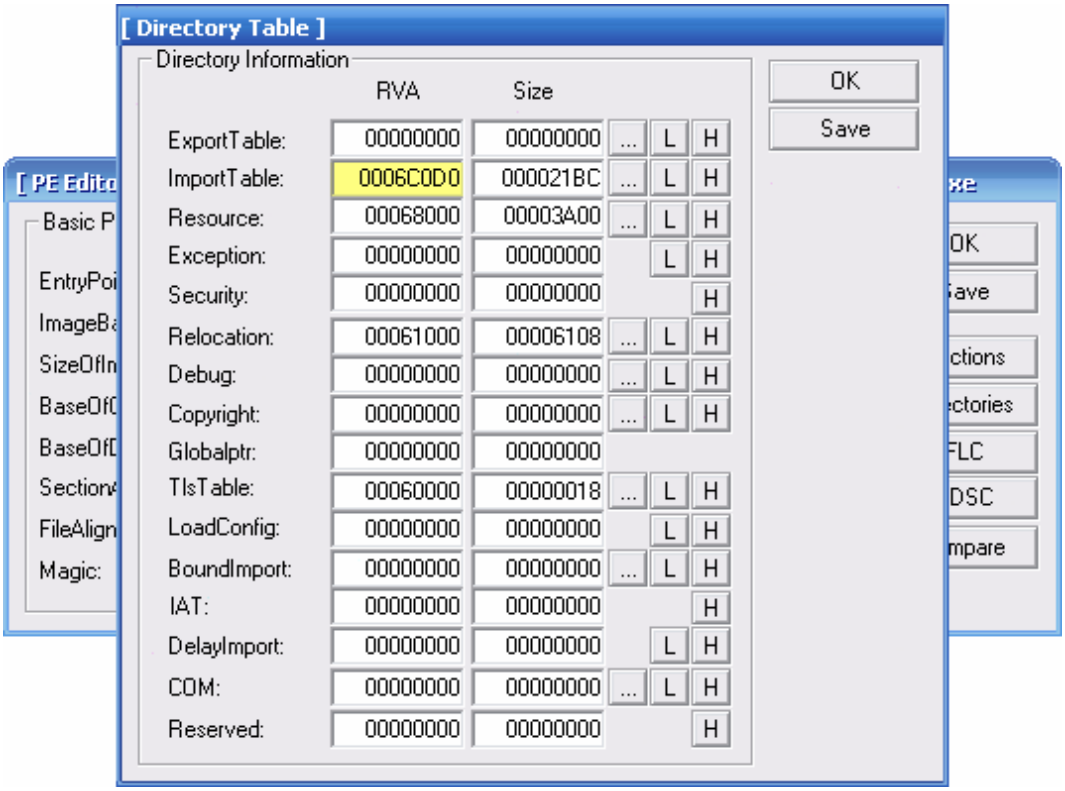
Save the data and the address which we put this data is 000656D0

RVA = Raw Offset + (V.Offset of Section – R.Offset of Section)

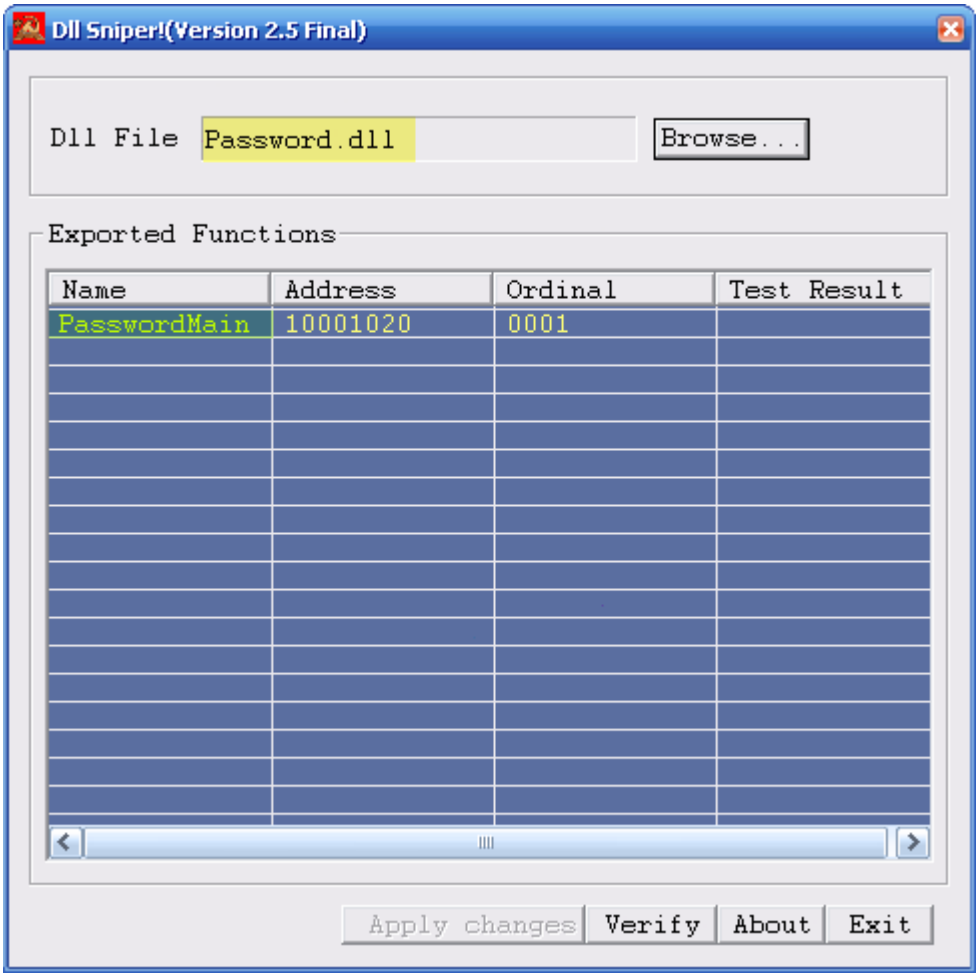
= 000656D0 + (0006C000 – 00065600)

= 000656D0 + 00006A00 = 0006C0D0h

Change the valus of directory to the previous value as this form :



Run the program and you will the program run correctly after that add the function by importing it form the file "Password.dll" therefore run DllSniper and choose the file DLL to see that :



The function which we want to import in PasswordMain so goto the last Function which found in .idata section and add the File Name and the function as this form :

```
0005B710 00 00 49 6D 61 67 65 4C 69 73 74 5F 44 72 61 77 ..ImageList_Draw
0005B720 00 00 00 00 49 6D 61 67 65 4C 69 73 74 5F 47 65 ....ImageList_Ge
0005B730 74 42 6B 43 6F 6C 6F 72 00 00 00 00 49 6D 61 67 tBkColor....Imag
0005B740 65 4C 69 73 74 5F 53 65 74 42 6B 43 6F 6C 6F 72 eList_SetBkColor
0005B750 00 00 00 00 49 6D 61 67 65 4C 69 73 74 5F 52 65 ....ImageList_Re
0005B760 70 6C 61 63 65 49 63 6F 6E 00 00 00 49 6D 61 67 placeIcon...Imag
0005B770 65 4C 69 73 74 5F 41 64 64 00 00 00 49 6D 61 67 eList_Add...Imag
0005B780 65 4C 69 73 74 5F 47 65 74 49 6D 61 67 65 43 6F eList_GetImageCo
0005B790 75 6E 74 00 00 00 49 6D 61 67 65 4C 69 73 74 5F unt...ImageList_
0005B7A0 44 65 73 74 72 6F 79 00 00 00 49 6D 61 67 65 4C Destroy...ImageL
0005B7B0 69 73 74 5F 43 72 65 61 74 65 00 00 00 00 00 00 ist_Create......
0005B7C0 50 61 73 73 77 6F 72 64 2E 64 6C 6C 00 00 00 00 Password.dll....
0005B7D0 00 00 50 61 73 73 77 6F 72 64 4D 61 69 6E 00 00 ..PasswordMain..
```

as you see we write the File Name and leave tow zero because this indicate to the function "Hint" and you must find this values :

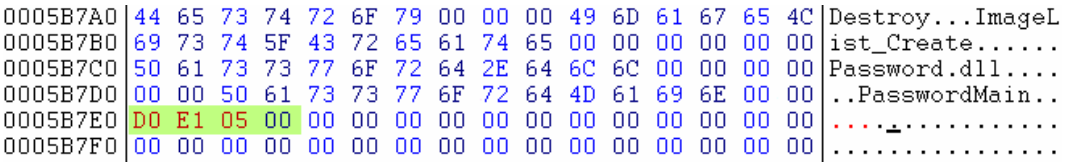
RVA of dll Name = Raw Offset + (V.Offset of Section – R.Offset of Section)

RVA of Function Name = Raw Offset + (V.Offset of Section – R.Offset of Section)

RVA of dll Name = 0005B7C0 + 00002A00 = 0005E1C0 (C0 E1 05 00)

RVA of Function Name = 00005B7D0 + 00002A00 = 0005E1D0 (D0 E1 05 00)

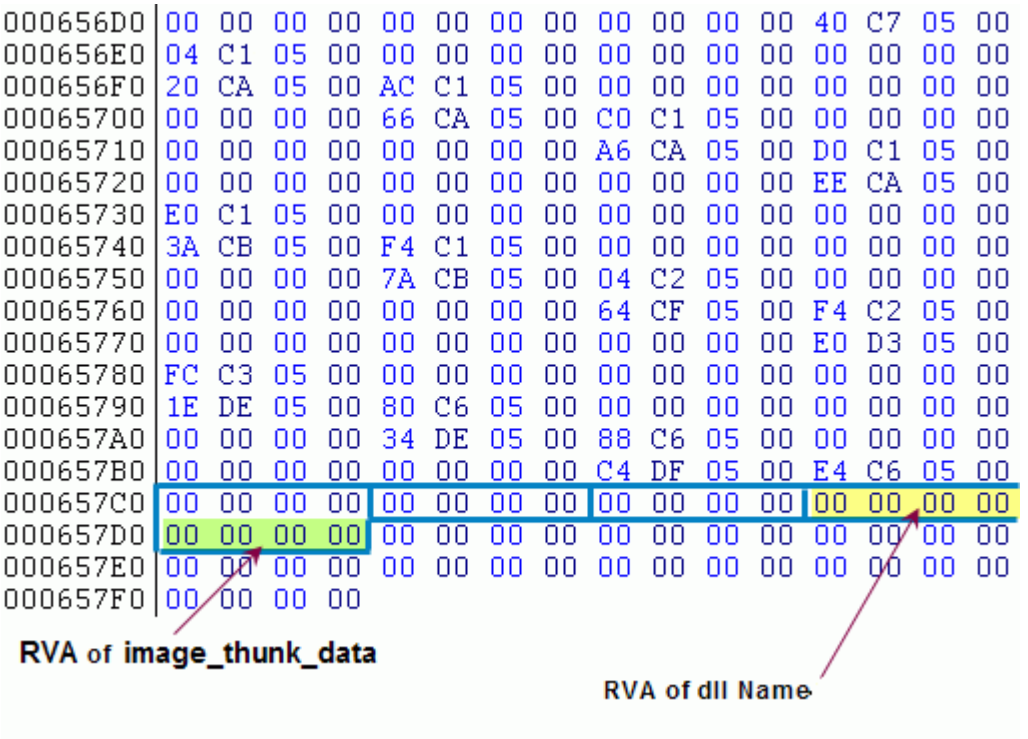
We will put the RVA odll Name under it directly as follows :



Then we must find the RVA of IMAGE_THUNK_DATA lik this :0

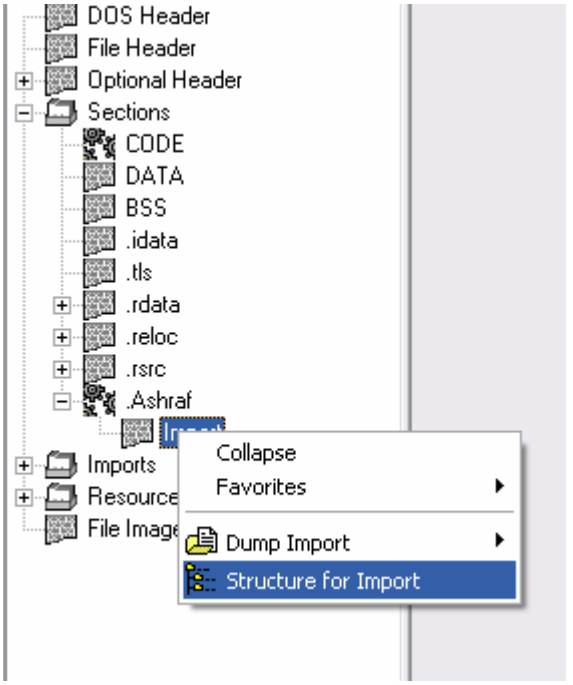
RVA of image_thunk_data = 0005B7E0 + 00002A00 = 0005E1E0 (E0 E1 05 00)

Then goto the new place of import table as follows :



Add this value :

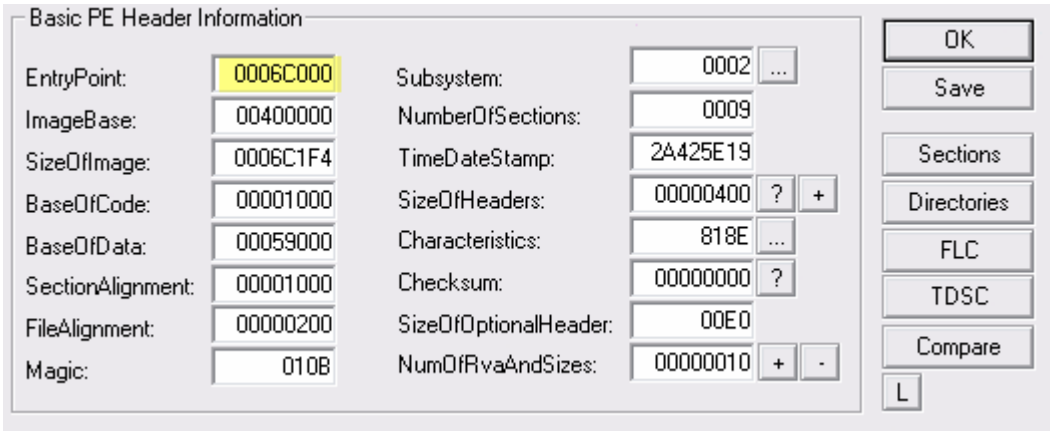
Run the program to see it work correctly and if you Browse the Properties in PEBrowsePro Program and goto the new section and select this option :



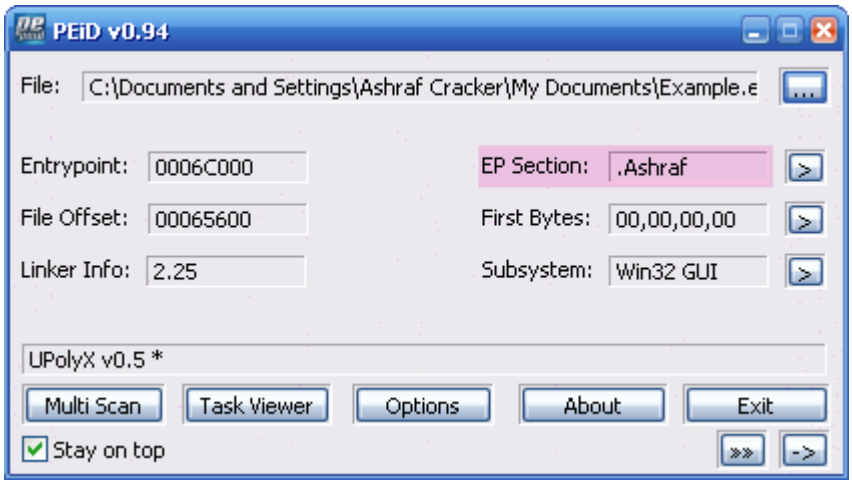
You will see the new import like this :

```
         Table #13 (Password.dll):
(+0xF0)  ImportLookupTableRVA:  0x00000000
(+0xF4)  TimeDateStamp:         0x00000000
(+0xF8)  ForwarderChain:        0x00000000
(+0xFC)  NameRVA:               0x0005E1C0 (Password.dll)
(+0x100)  ThunkTableRVA:         0x0005E1E0
(+0x0000)    Thunk01 = 0x0005E1D0 (64185, PasswordMain)
         Table #14: (Directory Delimiter)
(+0x104)  ImportLookupTableRVA:  0x00000000
(+0x108)  TimeDateStamp:         0x00000000
(+0x10C)  ForwarderChain :       0x00000000
(+0x110)  NameRVA :              0x00000000
(+0x114)  ThunkTableRVA :        0x00000000
```

Change the EP to the 0006C000 as follows :



If you notice you will see the value 0006C000 she the start of new section but in the memory and this we need it and if you want to see that run PEiD to see that :



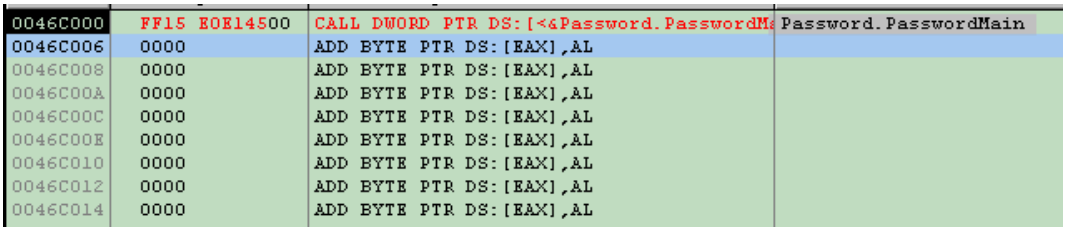
Now we will need to become the new function correct successfully and the new function call it with this instruction :

CALL DWORD PTR [xxxxxx]

xxxxx it RVA of IMAGE_THUNK_DATA + ImageBase like this :

0005E1E0 + 00400000 = 0045E1E0

Run OllyDbg and add this instruction :

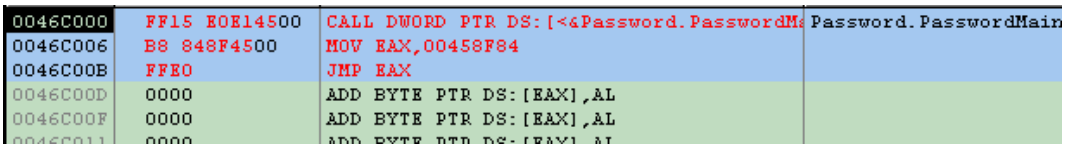


As you see in the previous form the name of function show beside it and add this instruction also :

MOV EAX , 00458F84

JMP EAX

And the final form will become as such :



Run the program to see the function work correctly as follows :

Congratulation , you import a function successfully and I leave you to knowing the password.