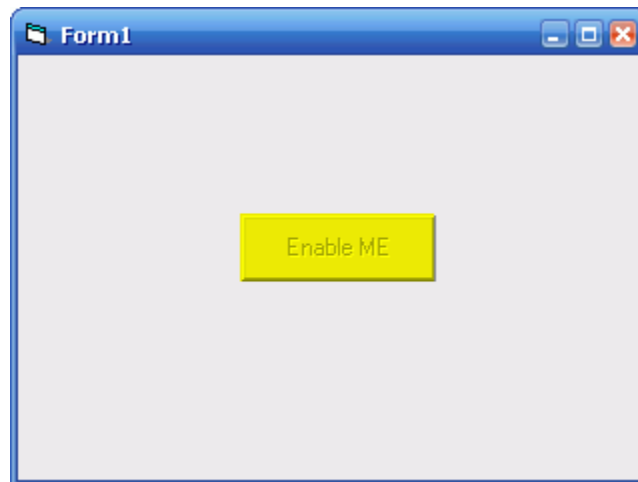


Some Tricks About VB Programs

Some people thinking crack the visual basic programs it difficult but in the truth not difficult and through cracking many of visual basic programs accumulation for me some experience in cracking this quality of programs and let's start with the first example "Example1" as follows :

Example 1



The pervious form contain one command but disabled therefore load this file in OllyDbg then Goto the "All InterModular Call" to see this :

00401AFA	CALL	DWORD	PTR	DS: [<&MSVBVM60.#595>]	MSVBVM60.rtcMsgBox
00401181	CALL	<JMP.&MSVBVM60.#100>			MSVBVM60.ThunRTMain
00401BF0	CALL	DWORD	PTR	DS: [<&MSVBVM60.__vbaFree0	MSVBVM60.__vbaFreeObj
00401C03	CALL	DWORD	PTR	DS: [<&MSVBVM60.__vbaFree0	MSVBVM60.__vbaFreeObj
00401B12	CALL	DWORD	PTR	DS: [<&MSVBVM60.__vbaFreeV	MSVBVM60.__vbaFreeVarList
00401B37	CALL	DWORD	PTR	DS: [<&MSVBVM60.__vbaFreeV	MSVBVM60.__vbaFreeVarList
00401BE7	CALL	DWORD	PTR	DS: [<&MSVBVM60.__vbaHresv	MSVBVM60.__vbaHresultCheckObj
00401BC3	CALL	DWORD	PTR	DS: [<&MSVBVM60.__vbaObjSe	MSVBVM60.__vbaObjSet
00401AE3	CALL	DWORD	PTR	DS: [<&MSVBVM60.__vbaVarD	MSVBVM60.__vbaVarDup

This Pervious function is very important and it meaning the object position from where her position Enable or Disable so press double click to go the address as follows :

00401BC3	.	FF15	20104000	CALL	DWORD	PTR	DS: [<&MSVBVM60.__vbaObjSet>	
00401BC9	.	8BF0		MOV	ESI	EAX		
00401BCB	.	57		PUSH	EDI			
00401BCC	.	56		PUSH	ESI			
00401BCD	.	8B0E		MOV	ECX	DWORD	PTR	DS: [ESI]
00401BCF	.	FF91	8C000000	CALL	DWORD	PTR	DS: [ECX+8C]	
00401BD5	.	3BC7		CMP	EAX	EDI		
00401BD7	.	DBE2		FCLEX				

As you show in the pervious form this instruction call the value for this command to become disabled and this value [ECX+8C] it constant but the register may be differ so NOP this instruction or change it to JMP as you see in this form :

```

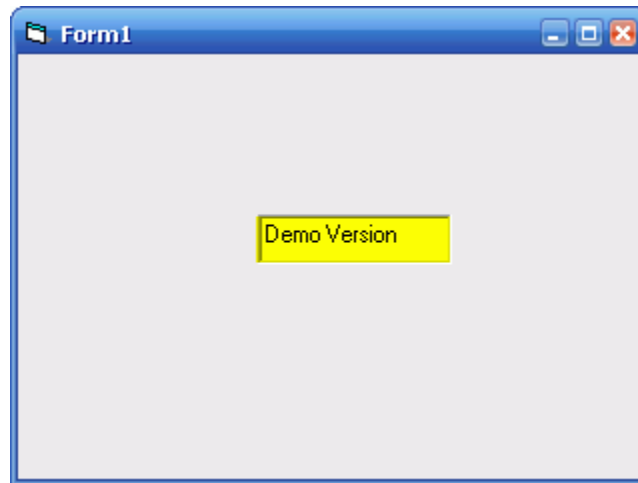
00401BC3 . FF15 20104000 CALL DWORD PTR DS:[<&MSVBVM60.__vbaObjSet>]
00401BC9 . 8BF0          MOV ESI,EAX
00401BCB . 57           PUSH EDI
00401BCC . 56           PUSH ESI
00401BCD . 8B0E        MOV ECX,DWORD PTR DS:[ESI]
00401BCF . E9 01000000 JMP 00401BD5
00401BD4 . 90          NOP
00401BD5 . 3BC7        CMP EAX,EDI

```

then you will see the command become enable

Example 2

When you run the example 2 you will see this form :



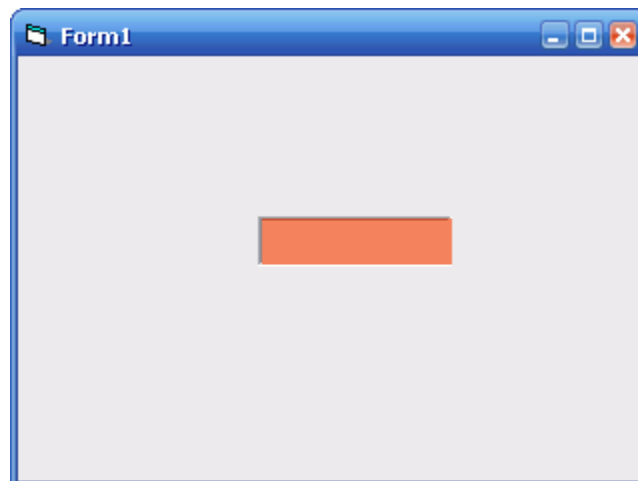
We want to erase the text "Demo Version" so goto the vbaObjSet as follows :

```

00401A53 . FF15 18104000 CALL DWORD PTR DS:[<&MSVBVM60.__vbaObjSet>]
00401A59 . 8BF0          MOV ESI,EAX
00401A5B . 68 BC164000  PUSH 004016BC
00401A60 . 56           PUSH ESI
00401A61 . 8B0E        MOV ECX,DWORD PTR DS:[ESI]
00401A63 . FF91 A4000000 CALL DWORD PTR DS:[ECX+A4]
00401A69 . 3BC7        CMP EAX,EDI

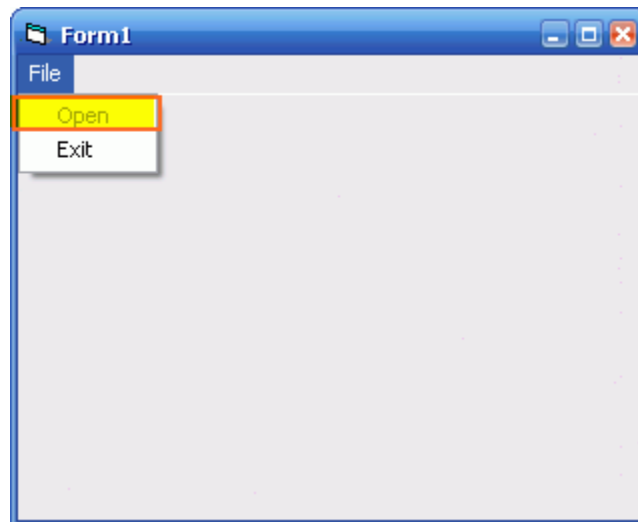
```

As you see in the pervious form the value "A4" it constant and you will find this value when you see a string into Textbox so NOP This instruction and run it to see this :



Example 3

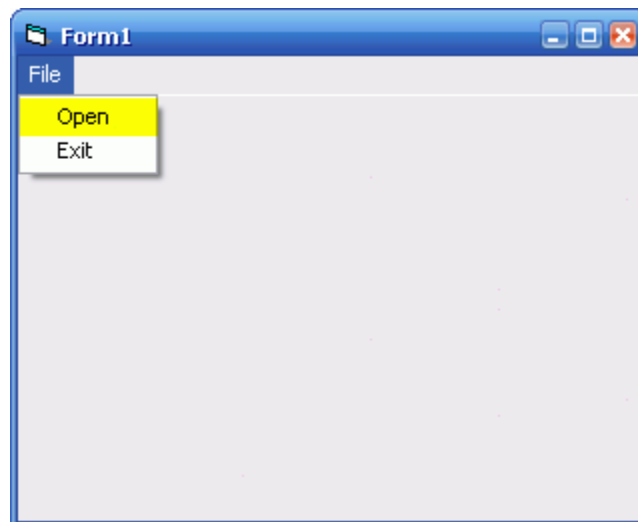
This example show menu contain object disabled as follows :



Then we goto automatically to the function VbaObjSet as follows :

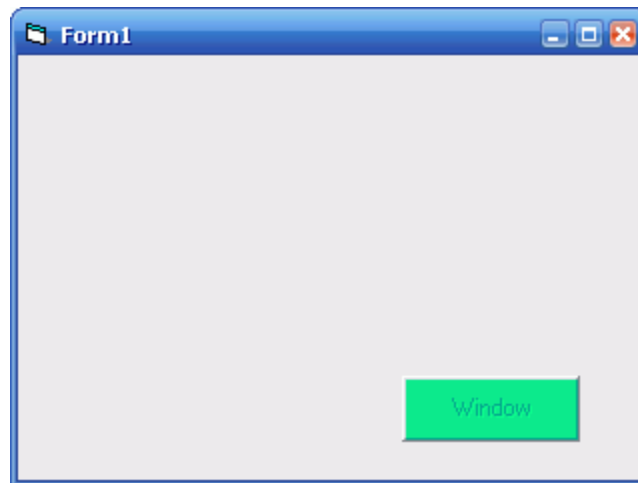
```
00401BC3 . FF15 20104000 CALL DWORD PTR DS:[<&MSVBM60.__vbaObjSet>]
00401BC9 . 8BFO          MOV ESI,EAX
00401BCB . 57           PUSH EDI
00401BCC . 56           PUSH ESI
00401BCD . 8B0E          MOV ECX,DWORD PTR DS:[ESI]
00401BCF . FF51 74      CALL DWORD PTR DS:[ECX+74]
00401BD2 . 3BC7          CMP EAX,EDI
```

As you see in the pervious form the value "74" it constant and you will find this value when you see menu it disabled so NOP This instruction and run it to see this :



Example 4

This example contain a command like this :



but we want to knowing properties this command and we will se this by using Hex Workshop so run it and search about this Caption "Window" to see this :

```
6C0C 0000 4603 FF01 2A00 0000 0108 0043 6F6D 6D61 6E64 3100 0401 0600 |1...F...*.....Command1.....
5769 6E64 6F77 0004 400B 6009 3705 EF01 0800 1100 00FF 0204 5000 0000 |Window...@...7.....P...
```

This value it means :

Name of object = Command 1

Object. Caption = Window

Object. Left = 400B->0B40 = 2880

(The value 400Bh in Little Endian Format will become 0B40h and if you convert this to Decimal then become 2880)

Object. Top = 6009->0960 = 2400

Object. Width = 3705->0537 = 1335

Object. Height = EF01->01EF = 495

Object. Enabled = False

The value 0800 after reverse it become 0008 and 00 it the value of command disabled and if change it to 08FF you will see this command become enabled and I want to clear the object value as follows "

```
00 PictureBox
01 Label
02 Textbox
03 Frame
04 Command Button
05 Checkbox
06 Option Button
07 ComboBox
08 ListBox
0B Timer
0D Form
```

Example 5

If you load this example in the Hex Workshop then you will see this form :

```
00 2F 01 00 00 3E 00 00 00 00 05 00 46 6F 72 6D | ./...>.....Form
31 00 0D 01 05 00 46 6F 72 6D 31 00 19 01 00 42 | 1.█...Form1...B
00 23 FF FF FF FF 24 05 00 46 6F 72 6D 31 00 35 | .#....$.Form1.5
3C 00 00 00 68 01 00 00 48 12 00 00 6C 0C 00 00 | <...h...H...l...
46 03 FF 01 23 00 00 00 05 08 00 50 69 63 74 75 | F...#.....Pictu
72 65 31 00 00 05 20 0D 68 01 57 03 EF 01 12 04 | rel1.█. .h.W.....
00 1A 01 00 42 00 FF 03 26 00 00 00 04 06 00 43 | ....B...&.....C
68 65 63 6B 31 00 05 01 06 00 41 73 68 72 61 66 | heck1.█...Ashraf
00 05 C0 03 78 00 CF 03 EF 01 12 03 00 FF 03 27 | ....x.....'
00 00 00 03 07 00 4F 70 74 69 6F 6E 31 00 06 01 | .....Option1.█.
06 00 61 73 68 72 61 66 00 05 58 02 70 08 BF 04 | ..ashraf..X.p...
EF 01 12 02 00 FF 03 25 00 00 00 02 05 00 54 65 | .....%.....Te
78 74 31 00 02 04 30 0C A0 05 57 03 EF 01 0B 06 | xt1.█.0...W.....
00 61 73 68 72 61 66 00 12 01 00 FF 03 2A 00 00 | .ashraf.....*...
00 01 08 00 43 6F 6D 6D 61 6E 64 31 00 04 01 06 | ....Command1.█..
00 57 69 6E 64 6F 77 00 04 40 0B 60 09 37 05 EF | .Window..@.`.7..
01 08 00 11 00 00 FF 03 26 00 00 00 06 06 00 4C | .....&.....L
61 62 65 6C 31 00 01 01 06 00 41 73 68 72 61 66 | abel1.█...Ashraf
00 05 D0 02 B0 04 47 04 67 02 12 05 00 FF 02 04 | .....G.g.....
```

As you see every object showing the equal value to it and with this I'm finished from this tricks and I hope in making clear about this important tricks and how to crack it.