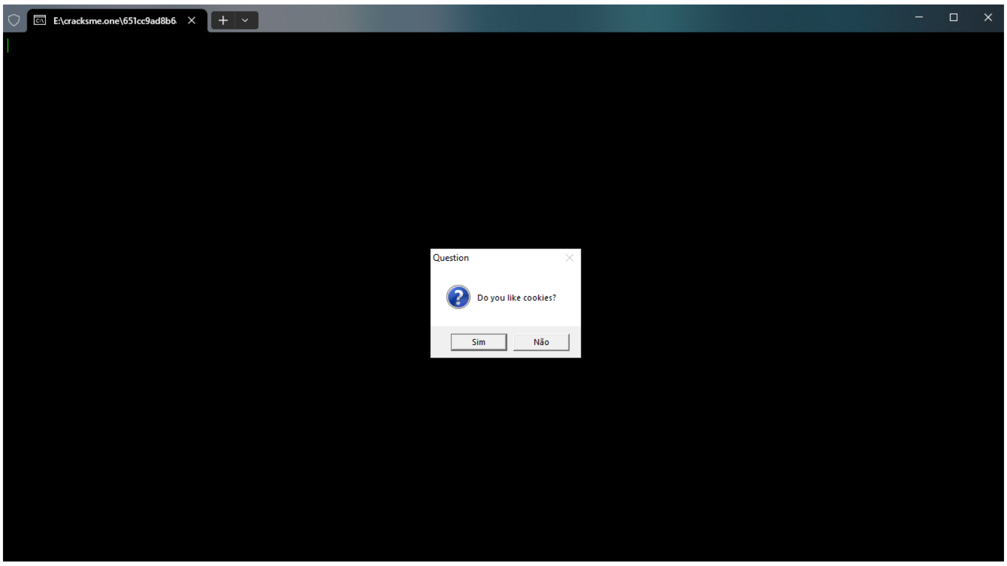
qbit32's Hidden MessageBox

<Made by: Tricta>

This is a simple crackme and you can use two methods to solve it ->

1. Reversing

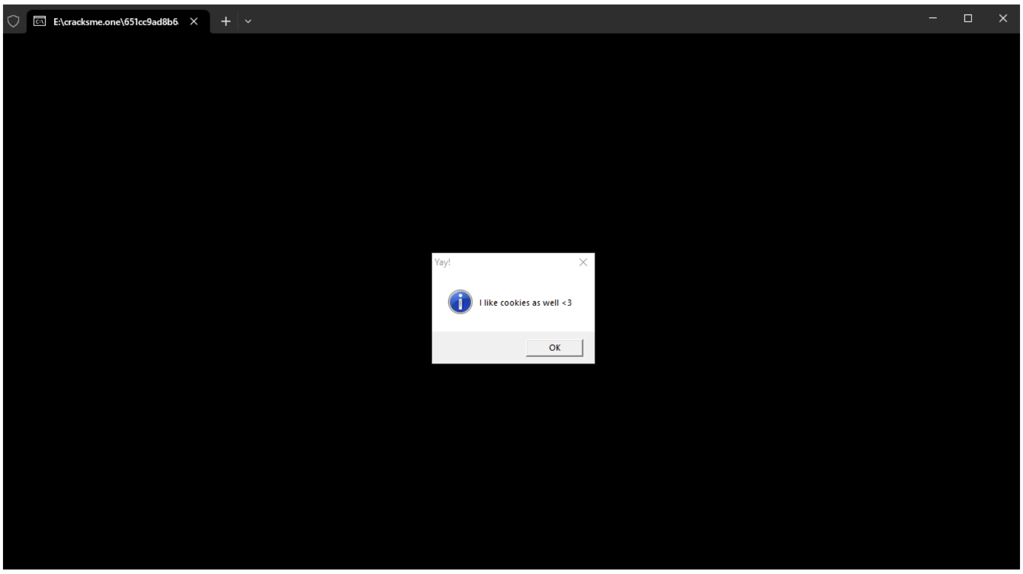
Let’s understand what it does! Running the program we obtain this screen:



Question

Do you like cookies?

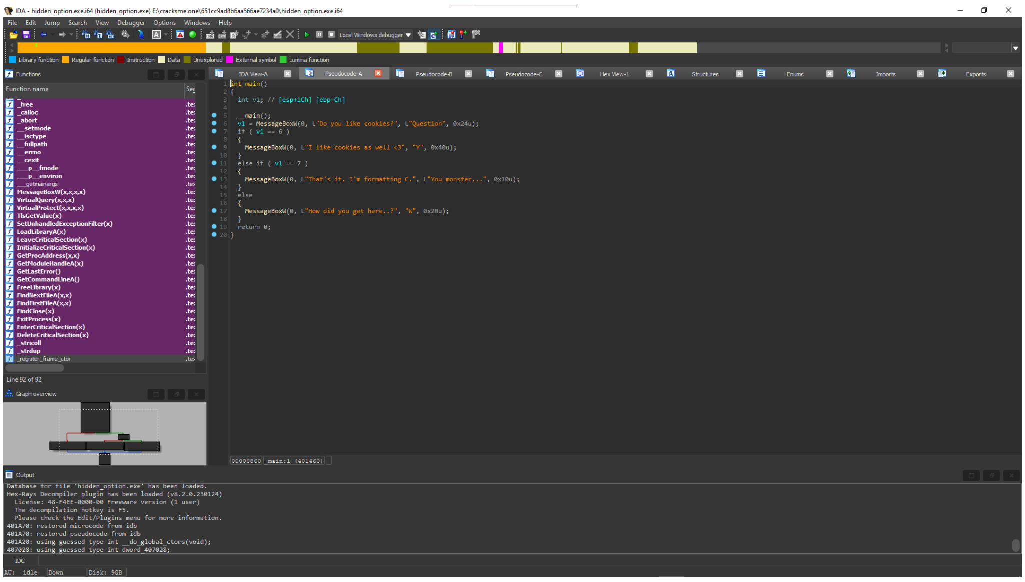
Just to see, pressing one of the two options we obtain on “yes”:



Yay!

I like cookies as well <3

Analyzing it on IDA and pressing “f5” key, we got the reversed code:


IDA - hidden_option.exe.i64 (hidden_option.exe) E:\crackme.one\651cc9ad8b6aa566ae7234a0\hidden_option.exe.i64
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
IDA View-A
Pseudocode-A
Pseudocode-B
Pseudocode-C
Hex View-1
Structures
Enums
Imports
Exports
Line 92 of 92
Graph overview
Output
IDC

```c
int main()
{
  int v1; // [esp+1Ch] [ebp-Ch]

  __main();
  v1 = MessageBoxW(0, L"Do you like cookies?", L"Question", 0x24u);
  if ( v1 == 6 )
  {
    MessageBoxW(0, L"I like cookies as well <3", "Y", 0x40u);
  }
  else if ( v1 == 7 )
  {
    MessageBoxW(0, L"That's it. I'm formatting C.", L"You monster...", 0x10u);
  }
  else
  {
    MessageBoxW(0, L"How did you get here..?", "W", 0x20u);
  }
  return 0;
}
```

```
00000860 _main:1 (401460)
```

```
Database for file 'hidden_option.exe' has been loaded.
Hex-Rays Decompiler plugin has been loaded (v8.2.0.230124)
  License: 48-F4EE-0000-00 Freeware version (1 user)
  The decompilation hotkey is F5.
  Please check the Edit/Plugins menu for more information.
401A70: restored microcode from idb
401A70: restored pseudocode from idb
401A20: using guessed type int __do_global_ctors(void);
407028: using guessed type int dword_407028;
```

```
AU:  idle   Down   Disk: 9GB
```

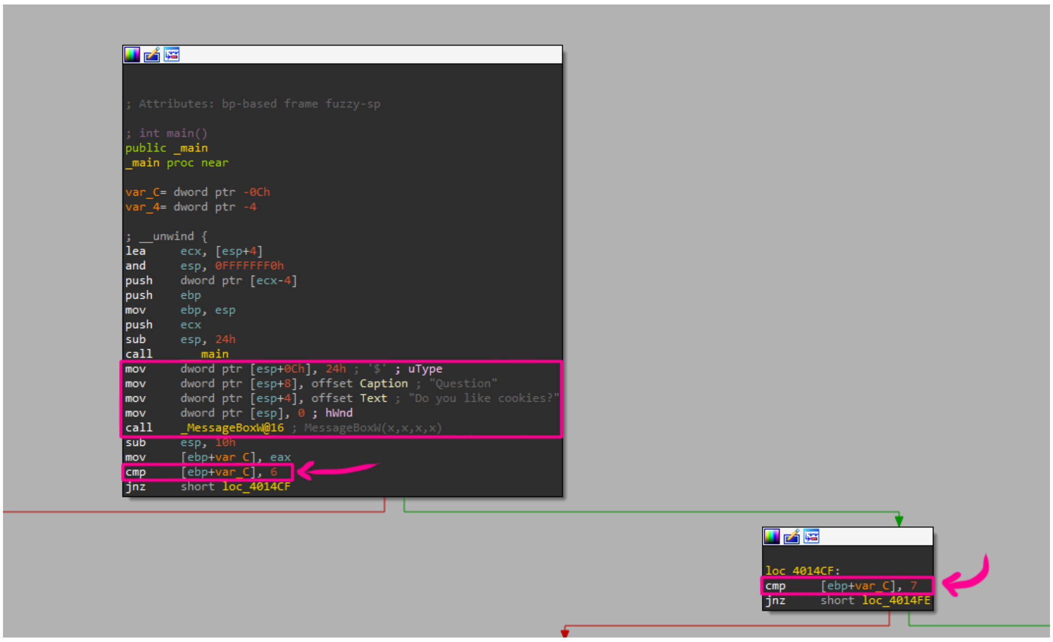
We can see the “v1” variable that is an integer and will receive the return value of the first message box that we saw on the first image.

After we enter a if statement that has 3 possibilities of answers, the first we saw was when we pressed the “yes” button.

If you press the “no” button you will enter the “else if” scope that shows the message: “That's it. I'm formatting C.”, so what we need to solve the crackme is enter on the “else” scope, in other words, not pressing one of the only two buttons :\

2. First method

I solved the challenge on this method by the first time, Let’s go to the assembly code:



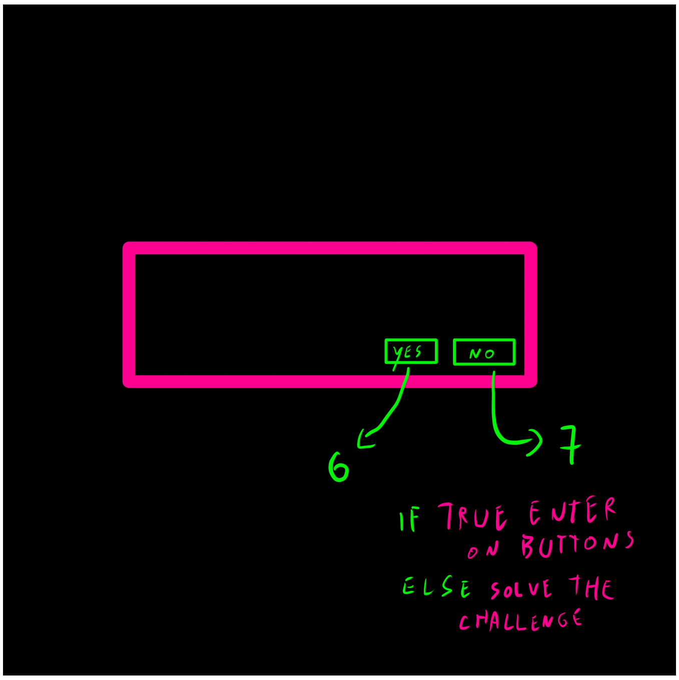
```
; Attributes: bp-based frame fuzzy-sp

; int main()
public _main
_main proc near

var_C= dword ptr -0Ch
var_4= dword ptr -4

; __unwind {
lea     ecx, [esp+4]
and     esp, 0FFFFFFF0h
push    dword ptr [ecx-4]
push    ebp
mov     ebp, esp
push    ecx
sub     esp, 24h
call    ___main
mov     dword ptr [esp+0Ch], 24h ; '$' ; uType
mov     dword ptr [esp+8], offset Caption ; "Question"
mov     dword ptr [esp+4], offset Text ; "Do you like cookies?"
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
mov     [ebp+var_C], eax
cmp     [ebp+var_C], 6
jnz     short loc_4014CF
```

```
loc_4014CF:
cmp     [ebp+var_C], 7
jnz     short loc_4014FE
```

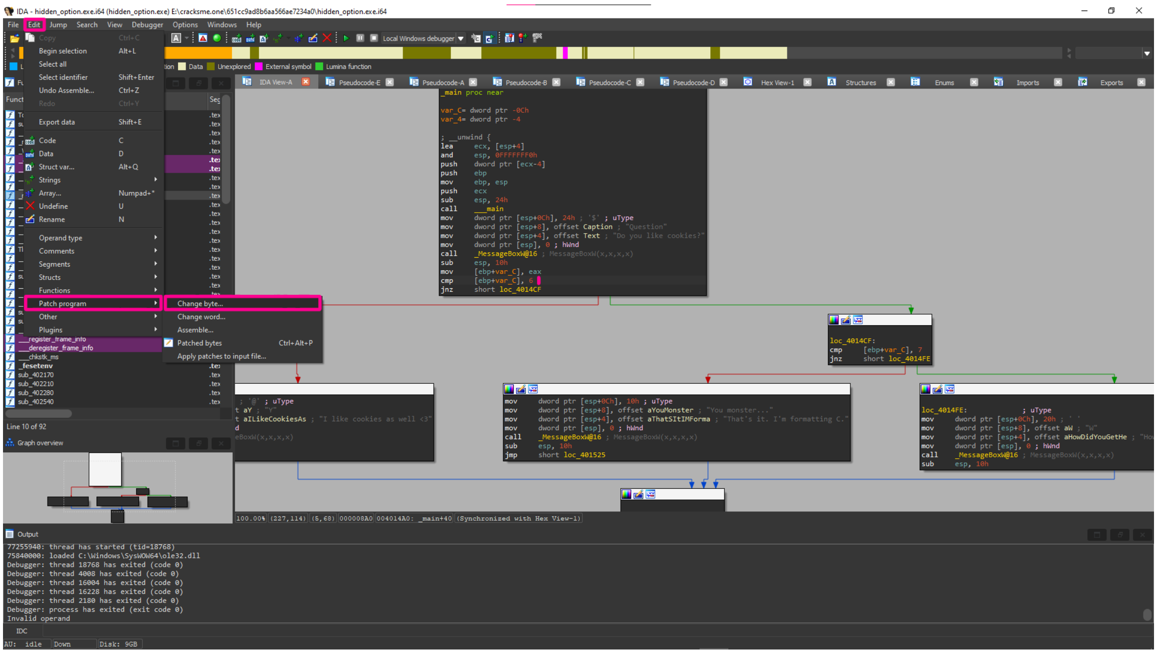
After the main function initialize we can see the 4 parameters and the message box function call, and going down a little bit we see the compare instruction between some value that is on the memory and the 6, so we can deduce two things:

1. var_c is the “same” variable of v1
2. this compare is our first condition of if statement

Soon after, we can see other compare instruction between our variable and the 7, the same value of “else if”, if to solve the challenge we need the else we can change these values to what the message box doesn't have. Let’s draw to be more cleary:



Click on the lines that do the compare instruction and on IDA click on *Edit->Patch Program->Change byte:*



```
_main proc near

var_C= dword ptr -0Ch
var_4= dword ptr -4

; __unwind {
lea     ecx, [esp+4]
and     esp, 0FFFFFFF0h
push    dword ptr [ecx-4]
push    ebp
mov     ebp, esp
push    ecx
sub     esp, 24h
call    ___main
mov     dword ptr [esp+0Ch], 24h ; '$' ; uType
mov     dword ptr [esp+8], offset Caption ; "Question"
mov     dword ptr [esp+4], offset Text ; "Do you like cookies?"
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
mov     [ebp+var_C], eax
cmp     [ebp+var_C], 6
jnz     short loc_4014CF
```

```
loc_4014CF:
cmp     [ebp+var_C], 7
jnz     short loc_4014FE
```

```
; '@' ; uType
t aY ; "Y"
t aILikeCookiesAs ; "I like cookies as well <3"
d
eBoxW(x,x,x,x)
```

```
mov     dword ptr [esp+0Ch], 10h ; uType
mov     dword ptr [esp+8], offset aYouMonster ; "You monster..."
mov     dword ptr [esp+4], offset aThatSItIMForma ; "That's it. I'm formatting C."
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
jmp     short loc_401525
```

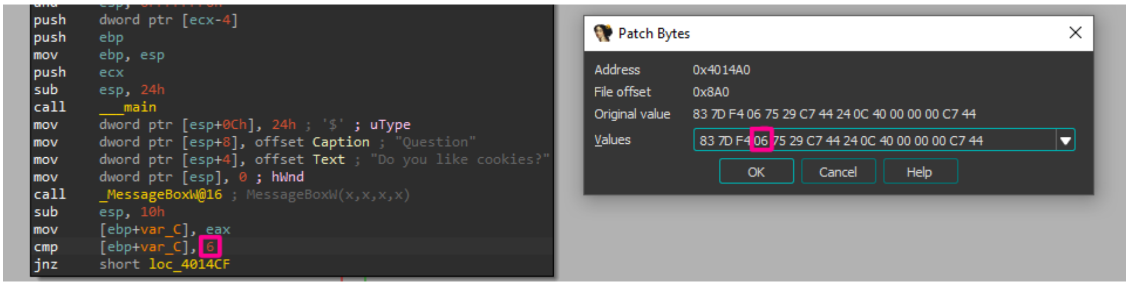
```
loc_4014FE:             ; uType
mov     dword ptr [esp+0Ch], 20h ; ' '
mov     dword ptr [esp+8], offset aW ; "W"
mov     dword ptr [esp+4], offset aHowDidYouGetHe ; "Ho
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
```

```
100.00% (227,114) (5,68) 000008A0 004014A0: _main+40 (Synchronized with Hex View-1)
```

```
77255940: thread has started (tid=18768)
75840000: loaded C:\Windows\SysWOW64\ole32.dll
Debugger: thread 18768 has exited (code 0)
Debugger: thread 4008 has exited (code 0)
Debugger: thread 16004 has exited (code 0)
Debugger: thread 16228 has exited (code 0)
Debugger: thread 2180 has exited (code 0)
Debugger: process has exited (exit code 0)
Invalid operand
```

```
AU:  idle   Down   Disk: 9GB
```

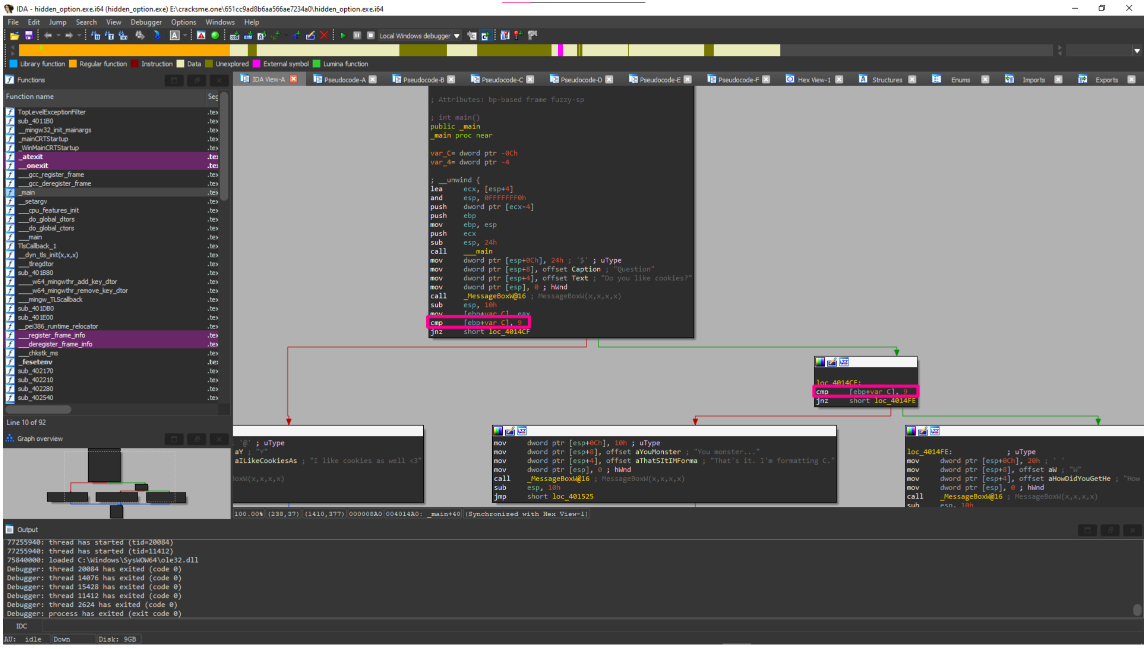
Now find the value of the comparessing of the if statement and change it for other value different of 6 or 7:



```
push    dword ptr [ecx-4]
push    ebp
mov     ebp, esp
push    ecx
sub     esp, 24h
call    ___main
mov     dword ptr [esp+0Ch], 24h ; '$' ; uType
mov     dword ptr [esp+8], offset Caption ; "Question"
mov     dword ptr [esp+4], offset Text ; "Do you like cookies?"
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
mov     [ebp+var_C], eax
cmp     [ebp+var_C], 6
jnz     short loc_4014CF
```

Address 0x4014A0
File offset 0x8A0
Original value 83 7D F4 06 75 29 C7 44 24 0C 40 00 00 00 C7 44
Values 83 7D F4 06 75 29 C7 44 24 0C 40 00 00 00 C7 44

Now your assembly will be like that:



```
; Attributes: bp-based frame fuzzy-sp

; int main()
public _main
_main proc near

var_C= dword ptr -0Ch
var_4= dword ptr -4

; __unwind {
lea     ecx, [esp+4]
and     esp, 0FFFFFFF0h
push    dword ptr [ecx-4]
push    ebp
mov     ebp, esp
push    ecx
sub     esp, 24h
call    ___main
mov     dword ptr [esp+0Ch], 24h ; '$' ; uType
mov     dword ptr [esp+8], offset Caption ; "Question"
mov     dword ptr [esp+4], offset Text ; "Do you like cookies?"
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
mov     [ebp+var_C], eax
cmp     [ebp+var_C], 9
jnz     short loc_4014CF
```

```
loc_4014CF:
cmp     [ebp+var_C], 9
jnz     short loc_4014FE
```

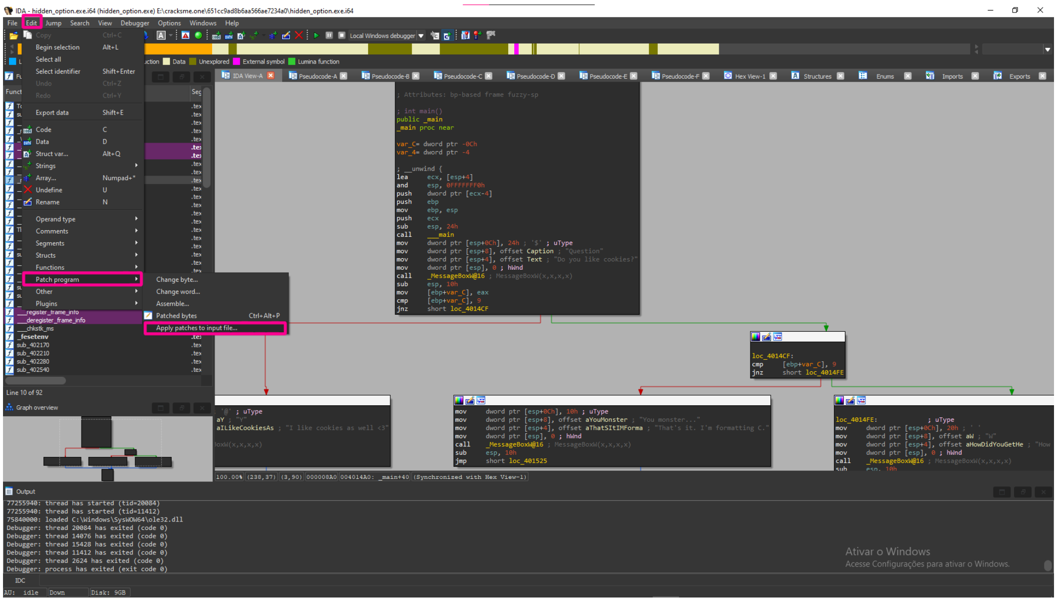
```
mov     dword ptr [esp+0Ch], 10h ; uType
mov     dword ptr [esp+8], offset aYouMonster ; "You monster..."
mov     dword ptr [esp+4], offset aThatSItIMForma ; "That's it. I'm formatting C."
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
jmp     short loc_401525
```

```
loc_4014FE:                 ; uType
mov     dword ptr [esp+0Ch], 20h ; ' '
mov     dword ptr [esp+8], offset aW ; "W"
mov     dword ptr [esp+4], offset aHowDidYouGetHe ; "How
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
```

```
100.00% (238,37) (1410,377) 000008A0 004014A0: _main+40 (Synchronized with Hex View-1)
```

```
77255940: thread has started (tid=20084)
77255940: thread has started (tid=11412)
75840000: loaded C:\Windows\SysWOW64\ole32.dll
Debugger: thread 20084 has exited (code 0)
Debugger: thread 14076 has exited (code 0)
Debugger: thread 15428 has exited (code 0)
Debugger: thread 11412 has exited (code 0)
Debugger: thread 2624 has exited (code 0)
Debugger: process has exited (exit code 0)
```

And you just need to apply the patch on *Edit->Patch Program->Apply patches to input field…* and after that run your program:



```
; Attributes: bp-based frame fuzzy-sp

; int main()
public _main
_main proc near

var_C= dword ptr -0Ch
var_4= dword ptr -4

; __unwind {
lea     ecx, [esp+4]
and     esp, 0FFFFFFF0h
push    dword ptr [ecx-4]
push    ebp
mov     ebp, esp
push    ecx
sub     esp, 24h
call    ___main
mov     dword ptr [esp+0Ch], 24h ; '$' ; uType
mov     dword ptr [esp+8], offset Caption ; "Question"
mov     dword ptr [esp+4], offset Text ; "Do you like cookies?"
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
mov     [ebp+var_C], eax
cmp     [ebp+var_C], 9
jnz     short loc_4014CF
```

```
loc_4014CF:
cmp     [ebp+var_C], 9
jnz     short loc_4014FE
```

```
'@' ; uType
aY ; "Y"
aILikeCookiesAs ; "I like cookies as well <3"

oxW(x,x,x,x)
```

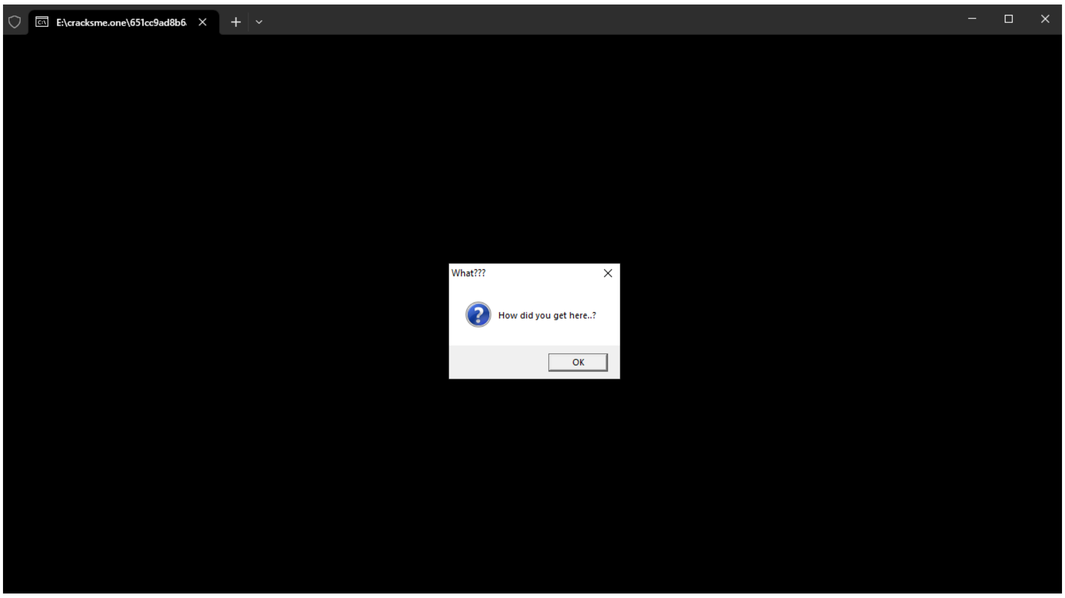
```
mov     dword ptr [esp+0Ch], 10h ; uType
mov     dword ptr [esp+8], offset aYouMonster ; "You monster..."
mov     dword ptr [esp+4], offset aThatSItIMForma ; "That's it. I'm formatting C."
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
jmp     short loc_401525
```

```
loc_4014FE:             ; uType
mov     dword ptr [esp+0Ch], 20h ; ' '
mov     dword ptr [esp+8], offset aW ; "W"
mov     dword ptr [esp+4], offset aHowDidYouGetHe ; "How
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
```

```
100.00% (238,37) (3,90) 000008A0 004014A0: _main+40 (Synchronized with Hex View-1)
```

```
77255940: thread has started (tid=20084)
77255940: thread has started (tid=11412)
75840000: loaded C:\Windows\SysWOW64\ole32.dll
Debugger: thread 20084 has exited (code 0)
Debugger: thread 14076 has exited (code 0)
Debugger: thread 15428 has exited (code 0)
Debugger: thread 11412 has exited (code 0)
Debugger: thread 2624 has exited (code 0)
Debugger: process has exited (exit code 0)
```

```
AU:  idle   Down   Disk: 9GB
```

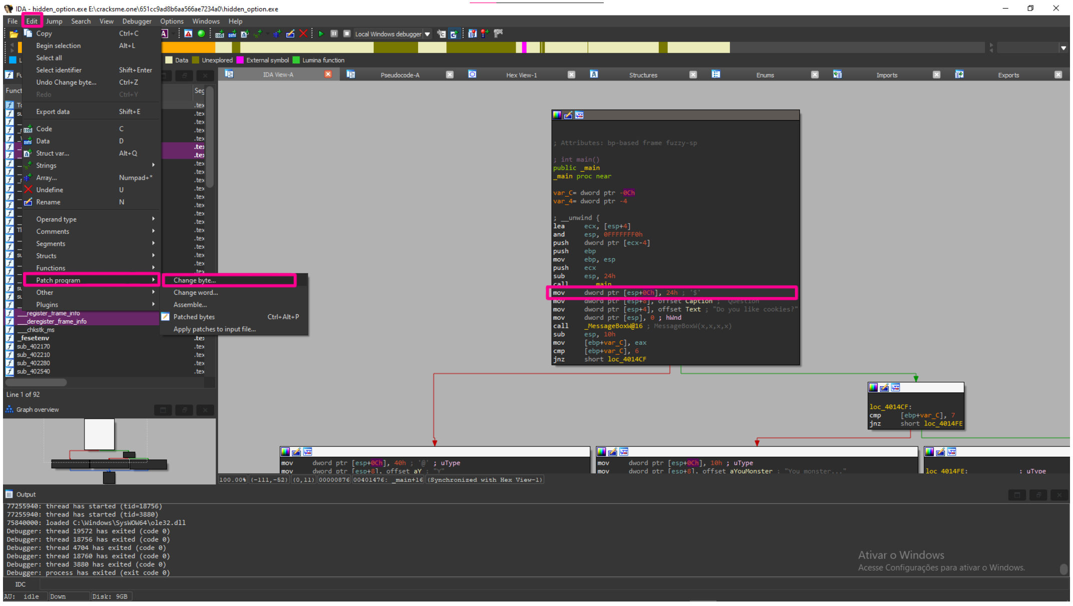


What???

How did you get here..?

2. Second method

The second method is just add one more button on the message box click on the line showed in the image below, this is the parameter of message box that changes the buttons and the icon, and click on *Edit->Patch Program->Change byte:*



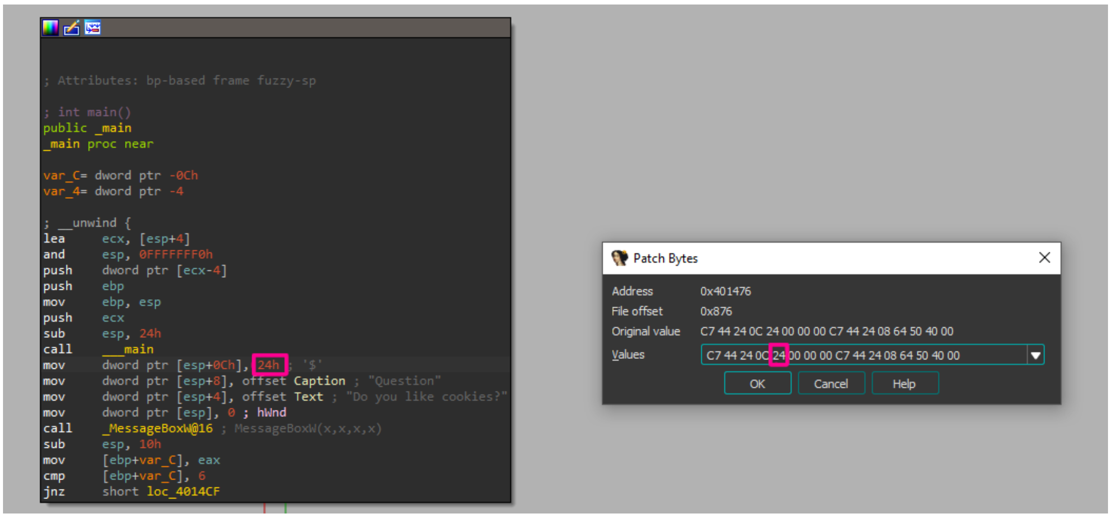
```
; Attributes: bp-based frame fuzzy-sp

; int main()
public _main
_main proc near

var_C= dword ptr -0Ch
var_4= dword ptr -4

; __unwind {
lea     ecx, [esp+4]
and     esp, 0FFFFFFF0h
push    dword ptr [ecx-4]
push    ebp
mov     ebp, esp
push    ecx
sub     esp, 24h
call    ___main
mov     dword ptr [esp+0Ch], 24h ; '$'
mov     dword ptr [esp+8], offset Caption ; "Question"
mov     dword ptr [esp+4], offset Text ; "Do you like cookies?"
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
mov     [ebp+var_C], eax
cmp     [ebp+var_C], 6
jnz     short loc_4014CF
```

```
100.00% (-111,-52) (0,11) 00000876 00401476: _main+16 (Synchronized with Hex View-1)
```

```
77255940: thread has started (tid=18756)
77255940: thread has started (tid=3880)
75840000: loaded C:\Windows\SysWOW64\ole32.dll
Debugger: thread 19572 has exited (code 0)
Debugger: thread 18756 has exited (code 0)
Debugger: thread 4704 has exited (code 0)
Debugger: thread 18760 has exited (code 0)
Debugger: thread 3880 has exited (code 0)
Debugger: process has exited (exit code 0)
```

```
AU:  idle   Down   Disk: 9GB
```

After that, go on the second 24h value and change for other value that correspond a button value, you can check on the win32 documentation if needed -> I chose the 02h value ;)



```
; Attributes: bp-based frame fuzzy-sp

; int main()
public _main
_main proc near

var_C= dword ptr -0Ch
var_4= dword ptr -4

; __unwind {
lea     ecx, [esp+4]
and     esp, 0FFFFFFF0h
push    dword ptr [ecx-4]
push    ebp
mov     ebp, esp
push    ecx
sub     esp, 24h
call    ___main
mov     dword ptr [esp+0Ch], 24h ; '$'
mov     dword ptr [esp+8], offset Caption ; "Question"
mov     dword ptr [esp+4], offset Text ; "Do you like cookies?"
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
mov     [ebp+var_C], eax
cmp     [ebp+var_C], 6
jnz     short loc_4014CF
```

Patch Bytes

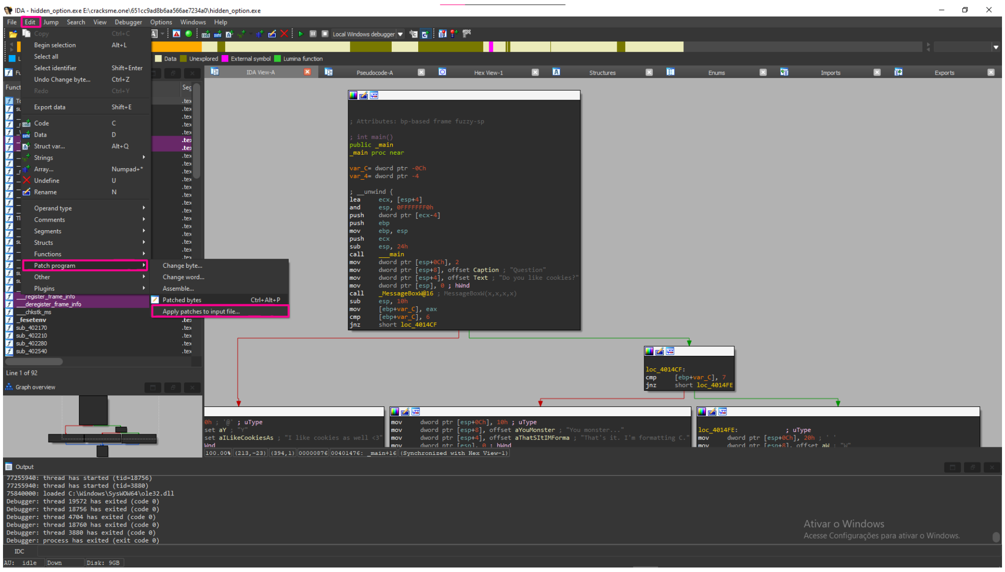
Address 0x401476

File offset 0x876

Original value C7 44 24 0C 24 00 00 00 C7 44 24 08 64 50 40 00

Values C7 44 24 0C 24 00 00 00 C7 44 24 08 64 50 40 00

Now you go on *Edit->Patch Program->Apply patches to input field…* After that you're done:



```
; Attributes: bp-based frame fuzzy-sp

; int main()
public _main
_main proc near

var_C= dword ptr -0Ch
var_4= dword ptr -4

; __unwind {
lea     ecx, [esp+4]
and     esp, 0FFFFFFF0h
push    dword ptr [ecx-4]
push    ebp
mov     ebp, esp
push    ecx
sub     esp, 24h
call    ___main
mov     dword ptr [esp+0Ch], 2
mov     dword ptr [esp+8], offset Caption ; "Question"
mov     dword ptr [esp+4], offset Text ; "Do you like cookies?"
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxW@16 ; MessageBoxW(x,x,x,x)
sub     esp, 10h
mov     [ebp+var_C], eax
cmp     [ebp+var_C], 6
jnz     short loc_4014CF
```

```
loc_4014CF:
cmp     [ebp+var_C], 7
jnz     short loc_4014FE
```

```
0h ; '@' ; uType
set aY ; "Y"
set aILikeCookiesAs ; "I like cookies as well <3"
Wnd
```

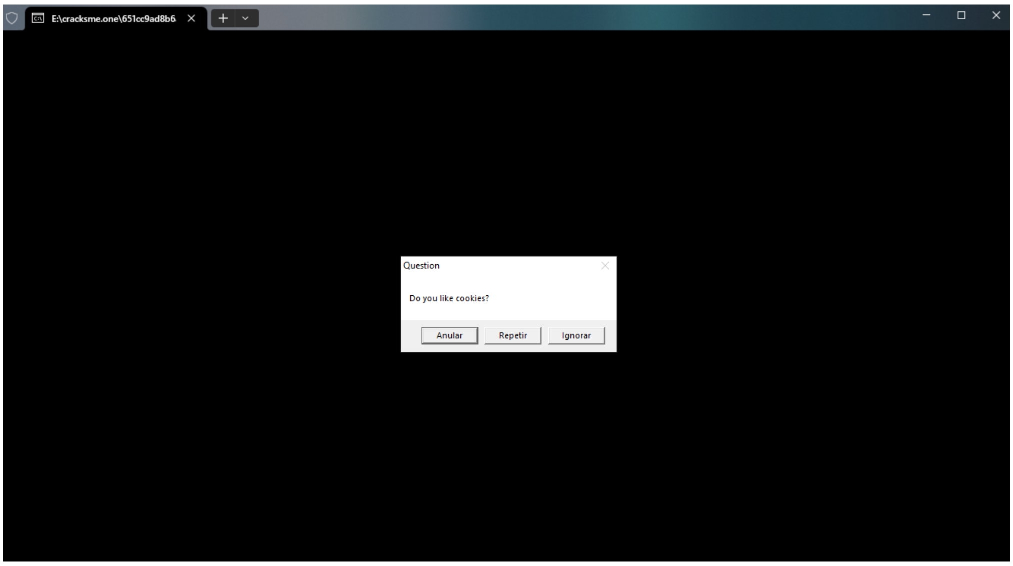
```
mov     dword ptr [esp+0Ch], 10h ; uType
mov     dword ptr [esp+8], offset aYouMonster ; "You monster..."
mov     dword ptr [esp+4], offset aThatSItIMForma ; "That's it. I'm formatting C."
mov     dword ptr [esp], 0 ; hWnd
```

```
loc_4014FE:              ; uType
mov     dword ptr [esp+0Ch], 20h ; ' '
mov     dword ptr [esp+8], offset aW ; "W"
```

```
100.00% (213,-23) (394,1) 00000876 00401476: _main+16 (Synchronized with Hex View-1)
```

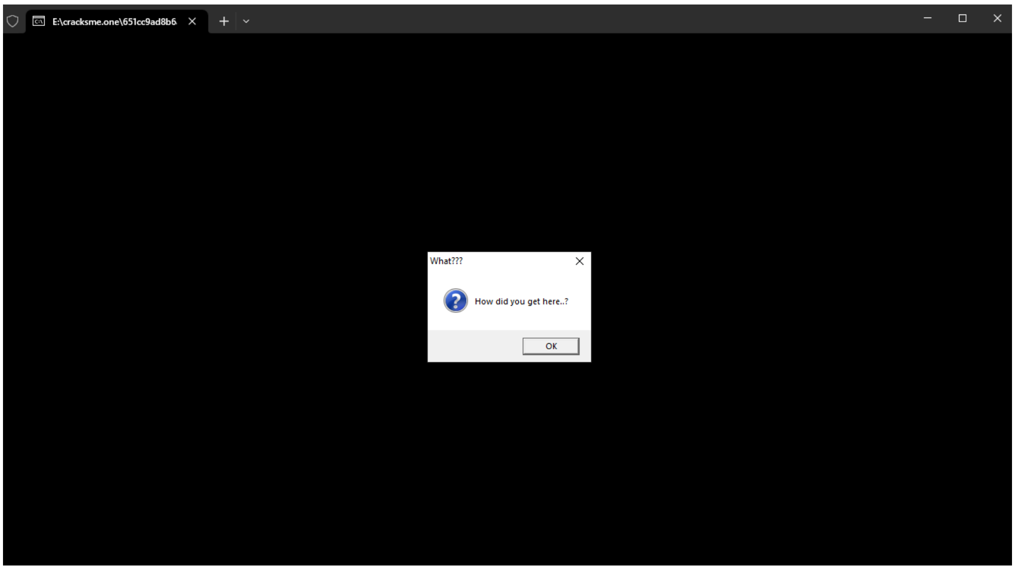
```
77255940: thread has started (tid=18756)
77255940: thread has started (tid=3880)
75840000: loaded C:\Windows\SysWOW64\ole32.dll
Debugger: thread 19572 has exited (code 0)
Debugger: thread 18756 has exited (code 0)
Debugger: thread 4704 has exited (code 0)
Debugger: thread 18760 has exited (code 0)
Debugger: thread 3880 has exited (code 0)
Debugger: process has exited (exit code 0)
```

```
AU:  idle   Down   Disk: 9GB
```



Question

Do you like cookies?



What???

How did you get here..?