INSIDE THE ULTIMA ONLINE CLIENT - PRE-ALPHA CLIENT LEFTOVERS, HAVING FUN WITH MENU'S

GOAL

I'm going to describe and try to understand some unused code found in the Ultima Online 2D clients (and even the Ultima Online Demo).

This article is similar to the "Pre-Alpha Client Leftovers, The Cursors" article but goes a few steps further. I will explain to you how to copy the menu from the Pre-Alpha Client to the Ultima Online Demo. I will also tell you how to look for secret menu options and what steps you can take to re-enable them. Have fun!

UTILITIES USED

<u>IDA Pro</u>, a very professional utility, definitely worth buying, Standard version is affordable <u>HxD</u>, a very neat hex editor and above all, it's free <u>Resource Hacker</u>, a free utility to fool around with a program's resources

INSIDE THE CLIENT

NOTE: the client analyzed here is version 5.0.8.3

The Ultima Online Client contains a call to the LoadMenu function at startup. The resource file does not contain a menu thus no menu will be displayed in the game window.

00536336	mov	ecx, [esp+6B4h+var 69C]
0053633A	mov	edx, GLOBAL hInstance
00536340	push	6Ah ; 1pMenuName
00536342	push	edx ; hInstance
00536343	lea	esi, [eax+ecx*2]
00536346	mov	eax, [edi]
00536348	add	esi, eax
0053634A	call	ds:LoadMenuA
00536350	mov	GLOBAL_hMenu, eax

The raises a few questions, can we add a menu and where does this menu come from in the first place?

INSIDE THE DEMO

The Ultima Online Demo contains a similar LoadMenu call:

004FCCDA push	6Ah ; 'j'	; 1pMenuName
004FCCDC mov	ecx, [ebp+var_BC]	St. Contraction and participation
004FCCE2 mov	edx, [ecx+438h]	
004FCCE8 push	edx	; hInstance
004FCCE9 call	ds:LoadMenuA	
004FCCEF mov	ecx, [ebp+var_BC]	
004FCCF5 mov	[ecx+544h], eax	

Just like in the modern client, the menu itself is missing in the resource section of the EXE.

So, whatever this menu is, it must be older than 1998 and has been removed for an unknown reason.

PRE-ALPHA

Raph Koster's website, one of the original UO designers, has posted a screenshot of the original client:

http://www.raphkoster.com/2006/06/24/random-uo-anecdote-1/

As you can see, that screenshot has a menu on it:



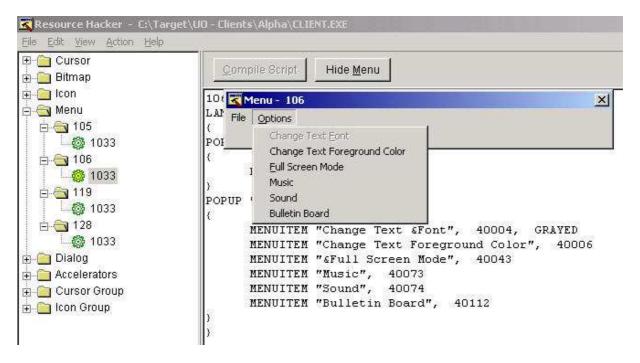
Recently, the client has become available (again) on the net, so we can delve into it and do some research.

INSIDE THE PRE-ALPHA CLIENT

As expected, the client also contains the already famous LoadMenu call:

00422483	push	6Ah	; 1pMenuName
00422485	mov	ebp, ds:LoadMenuf	1
0042248B	push	esi	; hInstance
00422480	call	ebp ; LoadMenuA	
0042248E	push	0	; 1pParam
00422490	mov	[ebx+8AFh], eax	10178 (1993 (DCL))

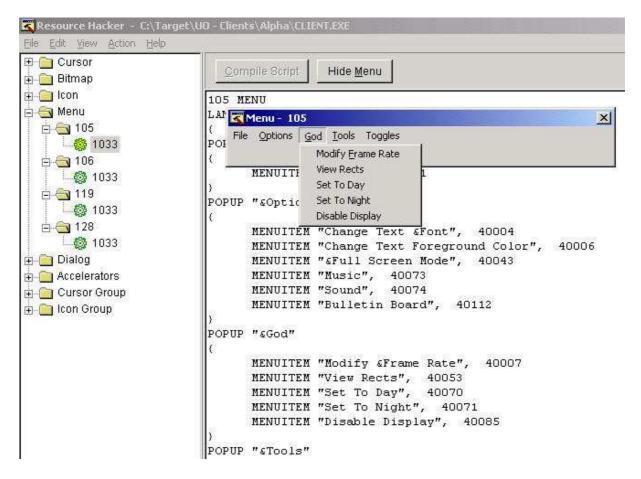
But there is a difference; the Pre-Alpha Client contains the menu lay-out as shown here (using Resource Hacker):



NOTE: 6Ah (see assembler screenshot) equals 106, 1033 is a language identifier

IS THE PRE-ALPHA CLIENT GOD?

There is another difference; the Pre-Alpha Client contains a GOD menu too, with ID 105 (69h):



Let's investigate if the Pre-Alpha Client supports (handles/can execute) this GOD menu.

When dealing with menus you need to investigate the WindowProc function and look for WM_COMMAND handling:

00424052 LOCAL	HandleWMCOMMAND:	; CODE XREF: FUNC WindowProc+6Ftj
00424052	mov	ebx, [esp+158h+wParam]
00424059	mov	eax, ebx
0042405B	and	eax, OFFFFh
00424060	sub	eax, 40001
00424065	cmp	eax, 73h ; switch 116 cases
00424068	ja	loc_424517 ; default
00424068	28	; jumptable 00424076 cases 1,2,4,0
0042406E	xor	ecx, ecx
00424070	mov	cl, ds:byte_42458C[eax]
00424076	jmp	ds: <mark>off_42<mark>4560</mark>[ecx*4] ; switch jump</mark>

00424560 off 424560	dd	offset 1	oc 42407	7D, off	set lo	oc 424098, offset loc 4240A9
00424560				;	DATA	XREF: FUNC WindowProc+4661r
00424560	dd	offset 1	oc_4240	A, off	set l	oc_424236, offset loc_424292 ;
00424560	dd	offset 1	DC_4240)A, off	set l	oc_4242EE, offset loc_42431E
00424560	dd	offset 1	oc 42436	AA, off	set Ll	OCAL_HandleWMCOMMAND_DoNothing
0042458C byte_42458C	db	0,	ØAh,	ØAh,	1	18
0042458C					DATA	XREF: FUNC_WindowProc+4601r
00424580	db	ØAh,	2,	ØAh,	ØAh	; indirect table for switch st
00424580	db	OAh,	OAh,	ØAh,	ØAh	
00424580	db	ØAh,	ØAh,	ØAh,	ØAh	
0042458C	db	ØAh,	ØAh,	ØAh,	ØAh	
00424580	db	OAh,	ØAh,	ØAh,	ØAh	
00424580	db	ØAh,	ØAh,	ØAh,	ØAh	
00424580	db	ØAh,	ØAh,	ØAh,	ØAh	
0042458C	db	ØAh,	ØAh,	ØAh,	ØAh	
00424580	db	OAh,	ØAh,	ØAh,	ØAh	
00424580	db	OAh,	OAh,	3,	ØAh	
00424580	db	ØAh,	ØAh,	0Ah,	ØAh	

A jump-table is used (see the previous screenshot), so we need to look at this table:

Most resource ID's will default to the eleventh (0Ah+ 1) handler, this handler will jump directly to DefWindowProc. This means nothing else happens for those menu options, they are unhandled!

This is a screenshot of the handler going to DefWindowProc:

00424517	LOCAL_HandleWMCOMMA	ND_DoNothing:	; CODE XREF: FUNC_WindowProc+458†j
00424517			; FUNC_WindowProc+4661j
00424517			; DATA XREF:
00424517	mov	esi, [esp	+158h+hWnd] ; default
00424517			; jumptable 00424076 cases 1,2,4,6-41,
0042451E	jmp	short L00	AL_GoDoDefWindowProc
00424520	•		
00424520			
00424520	loc_424520:		; CODE XREF: FUNC_WindowProc+3E21j
00424520	mov	esi, [es	+158h+hWnd]
00424527	jmp	short loo	424530
00424529	;		T
00424529			
00424529	LOCAL_GoDoDefWindow	Proc:	; CODE XREF: FUNC_WindowProc+35 [†] j
00424529			; FUNC_WindowProc+3271j
00424529	mov	ebp, [esp	+158h+1Param]
00424530			
00424530	loc 424530:		; CODE XREF: FUNC WindowProc+8E21j
00424530			; FUNC_WindowProc+9051j
00424530	pus	h ebp	; 1Param
00424531	pus	h ebx	; wParam
00424532	pus	h edi	; Msg
00424533	pus	h esi	; hWnd
00424534	cal	l ds:DefWin	IdowProcA

ANSWER

The Pre-Alpha Client is not GOD but the available GOD menu at least gives us insight in what the Pre-Alpha GOD client was capable of during the early development in 1996.

INSIDE THE GOD CLIENT

The leaked GOD client from the year 2000 also contains multiple menus and a few LoadMenu calls:

Dire	T.,	Address	Text	t	
<u>լ, լ</u> Սթ	р	sub_42EAF0+77	call	ds:LoadMenuA	30 ja
<u>Li</u> Up	P	sub_42EAF0+E4	call	ds:LoadMenuA	
<u>լ, վ</u> Սթ	р	sub_5E3270+83	call	ds:LoadMenuA	
L <u>LL</u> Up	P	sub_64CBF0+D8	call	ds:LoadMenuA	
L <u>ul</u> Up	P	sub_64CBF0+FF	call	ds:LoadMenuA	
Up Up	1	sub_42EAF0+77	call	ds:LoadMenuA	
Lt Up	E	sub_42EAF0+E4	call	ds:LoadMenuA	
L <u>ul</u> Up	ſ	sub_5E3270+83	call	ds:LoadMenuA	
Up Up	r.	sub_64CBF0+D8	call	ds:LoadMenuA	
L <u>ul</u> Up	r	sub_64CBF0+FF	call	ds:LoadMenuA	
Lul Up	ſ	.text:00658526	jmp	ds:LoadMenuA	

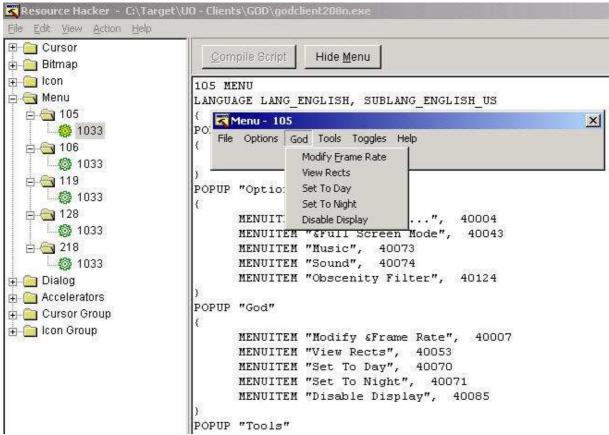
Two menus are the same as we saw in the Pre-Alpha Client, namely menu 69h and 6Ah. I'll provide two screenshots of the actual code loading them.

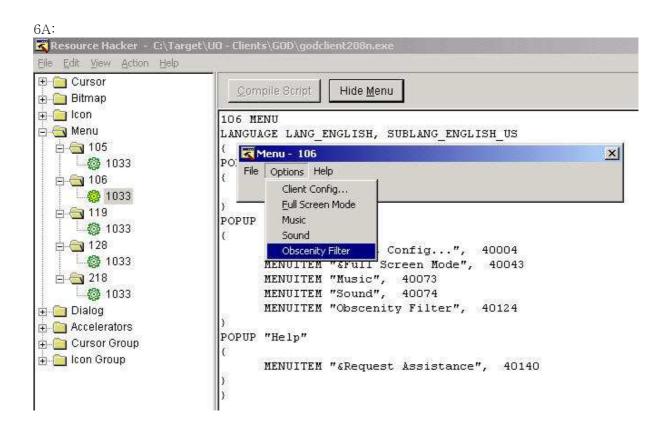
69h: 0042EB5E 0042EB60 0042EB66 0042EB67 0042EB6D	push mov push call mov	69h ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+hMenu], eax
6Ah: 0042EBCB 0042EBCD 0042EBD3 0042EBD4 0042EBDA	push mov push call mov	<pre>6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+hMenu], eax</pre>

It's logical that a GOD client would load the GOD menu (69h). It's interesting to note that the menu identifiers from 1996 are still used in the year 2000. This means the client is clearly a continuation of the original pre-alpha client.

Screenshots of the GOD menu and the Normal menu using Resource Hacker:

69h:





LOADMENU (GOD MODE ON/OFF)

0042EB21		mov	ecx, [ebp+VAR_FlagGOD]
0042EB24		and	ecx, OFFh
0042EB2A 0042EB2C		test jz	ecx, ecx Local Godoff
0042EB32		12	
	LOCAL GODon:		
0042EB32	Loone_doooni	cmp	dword 85D6E4, 0
0042EB39		jz	short loc 42EB5E
0042EB3B		mov	dword 85D6E4, 8
0042EB45		спр	dword_852140, 0
0042EB4C		jz	short loc_42EB59
0042EB4E		MOV	ecx, dword_B52140
0042EB54		call	sub_404F11
0042EB59	1 LOEDE0.		- 0005 V055
	1oc_42EB59:	0.11	; CODE XREF: sub_42EAF0+5CTj
0042EB59 0042EB5E		call	sub_403E72
	1oc 42EB5E:		; CODE XREF: sub 42EAF0+491j
0042EB5E	100_4220521	push	69h ; 1pMenuName
0042EB60		mov	edx, GLOBAL_hInstance
0042EB66		push	edx ; hInstance
0042EB67		call	ds:LoadMenuA
0042EB6D		MOV	[ebp+VAR_hMenuLoaded], eax
0042EB70		cmp	dword_18A3FB4, 0
0042EB77		jnz	short loc_42EB8D
0042EB79		mov	eax, [ebp+VAR_hMenuLoaded]
0042EB7C		push	eax ; hMenu
0042EB7D		MOV	ecx, dword_18A4B84
0042EB83 0042EB86		nush	edx, [ecx+4] edx ; hWnd
0042EB87		call	ds:SetNenu
0042EB8D			
	1oc 42EB8D:		; CODE XREF: sub_42EAF0+871j
0042EB8D	en den en e	cmp	GLOBAL_hMenu, 0
0042EB94		jz	short LOCAL_DoNotDestroyMenu69
0042EB96		MOV	eax, GLOBAL_hMenu
0042EB9B		push	eax ; hMenu
0042EB9C		call	ds:DestroyMenu
0042EBA2			
	LOCAL_DoNotDest		
0042EBA2		MOV	ecx, [ebp+VAR_hMenuLoaded]
0042EBA5 0042EBAB		nuch	GLOBAL_hMenu, ecx offset aGodModeIsNowOn ; "God mode is now on."
0042EBB0		push	3
0042EBB2		push	0
0042EBB4		call	sub 409B3D
0042EBB9		add	esp, OCh
0042EBBC		call	sub 408E13
0042EBC1		call	sub 4019E2
0042EBC1 0042EBC6			sub_4019E2 LOCAL_GoReturn
		call	
0042EBC6 0042EBCB 0042EBCB	an Unicedentificationen and	call	LOCAL_GoReturn
0042EBC6 0042EBCB 0042EBCB 0042EBCB 0042EBCB	; LOCAL_GODoff:	call jmp	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C [†] j
0042EBC6 0042EBCB 0042EBCB 0042EBCB 0042EBCB 0042EBCB	an Unicedentificationen and	call jmp push	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C [†] j 6Ah ; 1pMenuName
0042EBC6 0042EBCB 0042EBCB 0042EBCB 0042EBCB 0042EBCB 0042EBCB	an Unicedentificationen and	call jmp push mov	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; IpMenuName edx, GLOBAL_hInstance
8042EBC6 8042EBCB 8042EBCB 8042EBCB 8042EBCB 8042EBCB 8042EBCB 8042EBC3	an Unicedentificationen and	call jmp push mov push	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance
0042EBC6 0042EBCB 0042EBCB 0042EBCB 0042EBCB 0042EBCB 0042EBCD 0042EBD3 0042EBD3 0042EBD4	an Unicedentificationen and	call jmp push mov push call	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; IpMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA
8042EBC6 8042EBCB 8042EBCB 8042EBCB 8042EBCB 8042EBCB 8042EBCB 8042EBC3	an Unicedentificationen and	call jmp push mov push call mov	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C [†] j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+VAR_hMenuLoaded], eax
9042EBC6 9042EBCB 9042EBCB 9042EBCB 9042EBCB 9042EBCB 9042EBCD 9042EBD3 9042EBD4 9042EBD4	an Unicedentificationen and	call jmp push mov push call mov cmp	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0
9042EBC6 9042EBCB 9042EBCB 9042EBCB 9042EBCB 9042EBCB 9042EBCD 9042EBD3 9042EBD4 9042EBDA 9042EBDA	an Unicedentificationen and	call jmp push mov push call mov	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C [†] j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+VAR_hMenuLoaded], eax
0042EBC6 0042EBCB 0042EBCB 0042EBCB 0042EBCB 0042EBCB 0042EBD3 0042EBD4 0042EBD4 0042EBD4 0042EBD4	an Unicedentificationen and	call jmp push mov push call mov cmp jnz	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+VAR_hMenuLoaded], eax dword_10A3FB4, 0 short loc_42EBFA
0042EBC6 0042EBC8 0042EBC8 0042EBC8 0042EBC8 0042EBC8 0042EBC9 0042EBD4 0042EBD4 0042EBD4 0042EBD4 0042EBE9 0042EBE9 0042EBE9	an Unicedentificationen and	call jmp push mov push call mov cmp jnz mov push mov	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadHenuA [ebp+URR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+URR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84
0042E8C6 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8D3 0042E8D3 0042E8D3 0042E8D4 0042E8D4 0042E8E4 0042E8E4 0042E8E4 0042E8E4 0042E8E8	an Unicedentificationen and	call jmp push mov push call mov cmp jnz mov push mov push	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4]
0042EBC6 0042EBC8 0042EBC8 0042EBC8 0042EBC8 0042EBC8 0042EBC8 0042EBD3 0042EBD4 0042EBD4 0042EBD4 0042EBE4 0042EBE6 0042EBE9 0042EBF0 0042EBF3	an Unicedentificationen and	call jmp push call mov cmp jnz mov push mov push mov push	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd
0042E8C6 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8D3 0042E8D3 0042E8D3 0042E8D4 0042E8D0 0042E8E4 0042E8E9 0042E8E9 0042E8F3 0042E8F4	an Unicedentificationen and	call jmp push mov push call mov cmp jnz mov push mov push	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4]
0042E8C6 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8D3 0042E8D3 0042E8D3 0042E8D4 0042E8D0 0042E8E4 0042E8E4 0042E8E4 0042E8F6 0042E8F4 0042E8F4	LOCAL_GODOFF:	call jmp push call mov cmp jnz mov push mov push mov push	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadHenuA [ebp+VAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+VAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4884 edx, [ecx+4] edx] ; hWnd ds:SetHenu
9042E8C6 9042E8C8 9042E8C8 9042E8C8 9042E8C8 9042E8C9 9042E8D3 9042E8D4 9042E8D4 9042E8D4 9042E8D4 9042E85 9042E85 9042E85 9042E85 9042E85 9042E85 9042E85	an Unicedentificationen and	call jmp push mov push call mov push mov push call	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd
0042E8C6 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8D3 0042E8D3 0042E8D3 0042E8D4 0042E8D0 0042E8E4 0042E8E4 0042E8E4 0042E8F6 0042E8F4 0042E8F4	LOCAL_GODOFF:	call jmp push mov push call mov mov mov mov mov mov mov sush call cmp	<pre>LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx] ; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j</pre>
0042E8C6 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8D3 0042E8D3 0042E8D3 0042E8D4 0042E8D4 0042E8B9 0042E8E9 0042E8E9 0042E8F3 0042E8F4 0042E8FA 0042E8FA	LOCAL_GODOFF:	call jmp push mov push call mov push mov push call	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadHenuA [ebp+URR_hMenuLoaded], eax dword_1803FB4, 0 short loc_42EBFA eax, [ebp+URR_hMenuLoaded] eax ; hMenu ecx, dword_1804B84 edx, [ecx+4] edx] ; hWnd ds:SetNenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0
0042E8C6 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8D3 0042E8D3 0042E8D3 0042E8D4 0042E8D4 0042E8E4 0042E8E4 0042E8F4 0042E8F4 0042E8F4 0042E8FA 0042E8FA 0042E8FA 0042E8FA	LOCAL_GODOFF:	call jmp push mov push call mov cmp jnz mov push call call cmp jz	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadHenuA [ebp+VAR_hMenuLoaded], eax dword_18A3F84, 0 short loc_42EBFA eax, [ebp+VAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4884 edx, [ecx+4] edx] ; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F4 [†] j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A
0042EBC6 0042EBCB 0042EBCB 0042EBCB 0042EBCB 0042EBCB 0042EBD3 0042EBD4 0042EBD4 0042EBD4 0042EBE4 0042EBE4 0042EBE9 0042EBF4 0042EBF4 0042EBF4 0042EBFA 0042EBFA 0042EBFA 0042EBFA 0042EBFA 0042EC01 0042EC08 0042EC08	LOCAL_GODOFF:	call jmp push mov push call mov push mov push call cmp jz mov	<pre>LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax, GLOBAL_hMenu</pre>
9042E8C6 9042E8C8 9042E8C8 9042E8C8 9042E8C8 9042E8C9 9042E8D3 9042E8D4 9042E8D4 9042E8D4 9042E8D4 9042E859 9042E859 9042E853 9042E853 9042E854 9042E854 9042E850 9042EC95 9042EC05	LOCAL_GODoff: 10c_42EBFA:	call jmp push mov push call mov push mov push call cmp jz mov push call	<pre>LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hMenu ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu</pre>
0042EBC6 0042EBC8 0042EBC8 0042EBC8 0042EBC8 0042EBC9 0042EBD3 0042EBD4 0042EBD4 0042EBD4 0042EBD4 0042EBE9 0042EBE9 0042EBF9 0042EBF3 0042EBF3 0042EBF4 0042EBFA 0042EBFA 0042EBFA 0042EC03 0042EC08 0042EC0F	LOCAL_GODOFF:	call jmp push mov push call mov push call cmp jz mov push call cmp zall cmp	<pre>LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetMenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONOtDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111j</pre>
0042E8C6 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C9 0042E8D3 0042E8D3 0042E8D4 0042E8D4 0042E8D4 0042E8E9 0042E8E9 0042E8F3 0042E8F3 0042E8F4 0042E8FA 0042E8FA 0042E8FA 0042E8FA 0042E8FA 0042E8FA 0042E8FA 0042E67 0042EC09 0042EC0F	LOCAL_GODoff: 10c_42EBFA:	call jmp push mov call mov cmp jnz mov push call call cmp jz mov push call call	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadHenuA [ebp+URR_hMenuLoaded], eax dword_1803F04, 0 short loc_42EBFA eax, [ebp+URR_hMenuLoaded] eax ; hMenu ecx, dword_180AB84 edx, [ecx+4] edx [; hWnd ds:SetNenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONOtDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111j ecx, [ebp+UAR_hMenuLoaded]
9042E8C6 9042E8C8 9042E8C8 9042E8C8 9042E8C8 9042E8C9 9042E8D3 9042E8D4 9042E8D4 9042E8D4 9042E8D4 9042E859 9042E859 9042E856 9042E856 9042E856 9042E856 9042E856 9042E856 9042E605 9042EC05 9042EC05 9042EC05	LOCAL_GODoff: 10c_42EBFA:	call jmp push mov push call mov push call cmp jz mov push call call cmp jz mov push call	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadHenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4884 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax ; hMenu eax ; hMenu ds:DestroyMenu
0042EBC6 0042EBCB 0042EBCB 0042EBCB 0042EBCB 0042EBCD 0042EBD3 0042EBD4 0042EBD4 0042EBD4 0042EBD4 0042EBD9 0042EBE9 0042EBF9 0042EBF9 0042EBF3 0042EBF4 0042EBF4 0042EBF4 0042EBF4 0042EBF0 0042EC0F 0042EC0F 0042EC0F 0042EC0F 0042EC0F 0042EC12 0042EC12	LOCAL_GODOFF:	call jmp push mov push call mov push call cmp jz mov push call cmp jz mov push call	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadHenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx] ; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111j ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodHodelsNowOf; "God mode is now off."
0042E8C6 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8D3 0042E8D3 0042E8D4 0042E8D4 0042E8D4 0042E8E9 0042E8E9 0042E8F3 0042E8F3 0042E8F3 0042E8F4 0042E8F4 0042E8F3 0042E8F3 0042E8F3 0042E8F3 0042E8F3 0042EC3 0042EC3 0042EC09 0042EC09 0042EC09 0042EC09 0042EC07 0042EC18 0042EC18	LOCAL_GODOFF:	call jmp push mov call call mov push call cmp jz mov push call call cmp jz mov push call call mov push push push push push push	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_1803F04, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_1804B04 edx, [ecx+4] edx [; hWnd ds:SetNenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONOtDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111 ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModelsNowOf; "God mode is now off."
0042EBC6 0042EBCB 0042EBCB 0042EBCB 0042EBCB 0042EBCD 0042EBD3 0042EBD4 0042EBD4 0042EBD4 0042EBD4 0042EBD9 0042EBE9 0042EBF9 0042EBF9 0042EBF3 0042EBF4 0042EBF4 0042EBF4 0042EBF4 0042EBF0 0042EC0F 0042EC0F 0042EC0F 0042EC0F 0042EC0F 0042EC12 0042EC12	LOCAL_GODOFF:	call jmp push mov push call mov push call cmp jz mov push call cmp jz mov push call	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111 ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeIsNowOf; "God mode is now off." 3
9042E8C6 9042E8C8 9042E8C8 9042E8C8 9042E8C8 9042E8C9 9042E8D3 9042E8D4 9042E8D4 9042E8D4 9042E8D4 9042E854 9042E856 9042E856 9042E856 9042E856 9042E856 9042E856 9042E605 9042EC05 9042EC05 9042EC05 9042EC12 9042EC12	LOCAL_GODOFF:	call jmp push mov push call mov push mov push call cmp jz mov push call call call call push call	<pre>LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hMenu ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; ; CODE XREF: sub_42EAF0+1111j ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeIsNowOF ; "God mode is now off." 3 0] sub_409B3D</pre>
0042E8C6 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C9 0042E8D3 0042E8D3 0042E8D4 0042E8D4 0042E8D4 0042E8E4 0042E8E9 0042E8F3 0042E8F3 0042E8F4 0042E8F4 0042E8F4 0042E8F4 0042E8F6 0042E8F6 0042EC05 0042EC05 0042EC07 0042EC07 0042EC18 0042EC18 0042EC18 0042EC18 0042EC18 0042EC18 0042EC18	LOCAL_GODOFF:	call jmp push mov push call cmp jnz mov push call cmp jz mov push call call cmp push call	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111 ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeIsNowOf; "God mode is now off." 3
0042EBC6 0042EBC8 0042EBC8 0042EBC8 0042EBC8 0042EBC9 0042EBD3 0042EBD4 0042EBD4 0042EBD9 0042EBD9 0042EBE9 0042EBF9 0042EBF3 0042EBF3 0042EBF3 0042EBF3 0042EBF4 0042EBF3 0042EC0F 0042EC0F 0042EC0F 0042EC0F 0042EC0F 0042EC10 0042EC11 0042EC11 0042EC11 0042EC10	LOCAL_GODOFF:	call jmp push mov call call mov push call cmp jz mov push call call call call comp jz mov push call call call mov push call add	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_180AFB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_180AB84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONOtDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111j ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModelsNowOf; "God mode is now off." 3 0] sub_409B3D esp, 0Ch
0042EBC6 0042EBC8 0042EBC8 0042EBC8 0042EBC8 0042EBC9 0042EBD3 0042EBD4 0042EBD4 0042EBD4 0042EBD9 0042EBD9 0042EBE9 0042EBF4 0042EBF4 0042EBF4 0042EBFA 0042EBFA 0042EBFA 0042EC09 0042EC11 0042EC11 0042EC11 0042EC21 0042EC21 0042EC23 0042EC30	LOCAL_GODOFF:	call jmp push mov push call mov push call cmp jz mov push call call call call call call call cal	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadHenuA [ebp+VAR_hMenuLoaded], eax dword_1803F04, 0 short loc_42EBFA eax, [ebp+VAR_hMenuLoaded] eax ; hMenu ecx, dword_1804B84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONOtDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111j ecx, [ebp+VAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModelsNowOf; "God mode is now off." 3 0] sub_409B3D esp, 0Ch [ebp+var_10], 1 edx, [ebp+var_10] edx
9042EBC6 9042EBC8 9042EBC8 9042EBC8 9042EBC8 9042EBC9 9042EBD3 9042EBD4 9042EBD4 9042EBD4 9042EBF4 9042EBF4 9042EBF6 9042EBF6 9042EBFA 9042EBFA 9042EBFA 9042EBFA 9042EC09 9042EC09 9042EC09 9042EC09 9042EC07 9042EC07 9042EC07 9042EC12 9042EC12 9042EC11 9042EC11 9042EC11 9042EC11 9042EC11 9042EC11 9042EC11 9042EC11 9042EC11 9042EC11 9042EC21 9042EC21 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC3 9042EC3	LOCAL_GODOFF:	call jmp push mov push call mov push call cmp jz mov push call call cmp jz mov push call call call call cmp jz mov push call call call call call call call cal	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; ; CODE XREF: sub_42EAF0+1111j ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeIsNowOf; "God mode is now off." 3 0] sub_409B3D esp, 0Ch [ebp+var_10], 1 edx, [ebp+var_10]
9042E8C6 9042E8C8 9042E8C8 9042E8C8 9042E8C8 9042E8C9 9042E8D3 9042E8D4 9042E8D4 9042E8D4 9042E8D4 9042E8F4 9042E8F3 9042E8F3 9042E8F4 9042E8F4 9042E8F4 9042E8F4 9042E8F4 9042E8F6 9042E8F6 9042EC05 9042EC05 9042EC05 9042EC07 9042EC18 9042EC18 9042EC18 9042EC18 9042EC18 9042EC18 9042EC18 9042EC29 9042EC29 9042EC29 9042EC29 9042EC29 9042EC29 9042EC39	LOCAL_GODOFF:	call jmp push mov push call mov push call cmp jz mov push call call cmp jz mov push call call call cmp jz mov push call call call call call call call cal	LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; ; CODE XREF: sub_42EAF0+1111j ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeIsNowOf; "God mode is now off." 3 0] sub_409B3D esp, 0Ch [ebp+uar_10], 1 edx, [ebp+uar_10] edx offset dword_141BB78 sub_4094854
0042E8C6 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C9 0042E8C9 0042E8D3 0042E8D4 0042E8D4 0042E8D4 0042E8D4 0042E8D9 0042E8B7 0042E8F3 0042E8F3 0042E8F3 0042E8F4 0042E8F4 0042E8F4 0042E8F6 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC11 0042EC11 0042EC11 0042EC11 0042EC21 0042EC21 0042EC21 0042EC23 0042EC30 0042EC30 0042EC30 0042EC38	LOCAL_GODOFF:	call jmp push mov call call mov push call cmp jz mov push call call royMenu6 mov push call royMenu6 mov push call call call add mov	LUCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadHenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetMenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONOtDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111j ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeISNowOF ; "God mode is now off." 3 9] sub_409B3D esp, 0Ch [ebp+var_10], 1 edx, [ebp+var_10] edx offset dword_141BB78 sub_404854 esp, 8
9042E8C6 9042E8C8 9042E8C8 9042E8C8 9042E8C8 9042E8C9 9042E8D3 9042E8D4 9042E8D4 9042E8D4 9042E8D4 9042E8F4 9042E8F6 9042E8F6 9042E8F6 9042E8FA 9042E8FA 9042E8FA 9042E8FA 9042E8FA 9042EC09 9042EC09 9042EC09 9042EC09 9042EC07 9042EC12 9042EC12 9042EC11 9042EC11 9042EC11 9042EC11 9042EC11 9042EC11 9042EC21 9042EC11 9042EC21 9042EC21 9042EC21 9042EC23 9042EC33 9042EC33 9042EC34	LOCAL_GODOFF:	call jmp push mov push call mov push call cmp jz mov push call call call call call call call cal	LUCGL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetNenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short locAL_DONotDestroyMenu6A eax, GLOBAL_hMenu eax ; hNenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111j ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeIsNowOf ; "God mode is now off." 3 0] sub_489B3D esp, 0Ch [ebp+var_10], 1 edx, [ebp+var_10] edx offset dword_141BB78 sub_484854 esp, 8 eax, 0FFh
0042EBC6 0042EBC8 0042EBC8 0042EBC8 0042EBC8 0042EBC9 0042EBD3 0042EBD3 0042EBD4 0042EBD4 0042EB4 0042EBF4 0042EBF3 0042EBF3 0042EBF3 0042EBF4 0042EBF4 0042EBF4 0042EBF4 0042EBF6 0042EC05 0042EC05 0042EC05 0042EC05 0042EC15 0042EC18 0042EC18 0042EC18 0042EC18 0042EC18 0042EC18 0042EC20 0042EC30 0042EC30 0042EC30	LOCAL_GODOFF:	call jmp push mov push call mov push call cmp jz mov push call cmp jz mov push call call cmp jz mov push call call coyHenu6 mov push call add add test	<pre>LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; ; CODE XREF: sub_42EAF0+f4111j ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeIsNowOf; "God mode is now off." 3 0] sub_409B3D esp, 0Ch [ebp+uar_10], 1 edx, [ebp+uar_10] edx offset dword_141BB78 sub_404854 esp, 8 eax, 0FFh eax, eax</pre>
0042E8C6 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C8 0042E8C9 0042E8D3 0042E8D3 0042E8D4 0042E8D4 0042E8E9 0042E8E9 0042E8E9 0042E8F3 0042E8F3 0042E8F3 0042E8F4 0042E8F4 0042E8F4 0042E8F6 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC09 0042EC19 0042EC19 0042EC19 0042EC19 0042EC19 0042EC19 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC20 0042EC30 000	LOCAL_GODOFF:	call jmp push mov push call mov push call cmp jz mov push call call royMenu6 mov push call royMenu6 mov push call call call call mov push call call mov push call call mov push call call so push call call mov push call call mov push call call mov push call call so push call call mov push call call so push call call so push call so push call call so push call so push call call so push call call so push call so so push call so push call so so push call so so push call so push call so so push call so push call so so push call so so so so so so so so so so so so so	<pre>LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadHenuA [ebp+VAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+VAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONOtDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+F41j ecx, [ebp+VAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeIsNowOf ; "God mode is now off." 3 0 [sub_409B3D esp, 0Ch [ebp+var_10] edx offset dword_141BB78 sub_404854 esp, 8 eax, eax short LOCAL_GOREturn</pre>
9042E8C8 9042E8C8 9042E8C8 9042E8C8 9042E8C8 9042E8C9 9042E8D3 9042E8D4 9042E8D4 9042E8D4 9042E8D4 9042E8F4 9042E8F6 9042E8F6 9042E8F6 9042E8FA 9042E8FA 9042E8FA 9042E8FA 9042E8FA 9042EC99 9042EC09 9042EC09 9042EC09 9042EC07 9042EC10 9042EC12 9042EC12 9042EC10 9042EC10 9042EC10 9042EC10 9042EC10 9042EC10 9042EC10 9042EC11 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC20 9042EC3 9042EC3 9042EC3 9042EC3 9042EC3 9042EC41 9042EC41	LOCAL_GODOFF:	call jmp push mov push call mov push call cmp jz mov push call cmp jz mov push call call cmp jz mov push call call coyHenu6 mov push call add and test	<pre>LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; ; CODE XREF: sub_42EAF0+1111j ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeIsNowOf; "God mode is now off." 3 0] sub_409B3D esp, 0Ch [ebp+uar_10], 1 edx, [ebp+uar_10] edx offset dword_141BB78 sub_404854 esp, 8 eax, 0FFh eax, eax</pre>
9042EBC6 9042EBC8 9042EBC8 9042EBC8 9042EBC8 9042EBC9 9042EBD3 9042EBD4 9042EBD4 9042EBD4 9042EBC9 9042EBF4 9042EBF6 9042EBF3 9042EBF3 9042EBF4 9042EBF4 9042EBF4 9042EBF6 9042EC05 9042EC05 9042EC05 9042EC07 9042EC07 9042EC07 9042EC07 9042EC12 9042EC18 9042EC18 9042EC18 9042EC19 9042EC209 9042EC21 9042EC21 9042EC21 9042EC21 9042EC21 9042EC21 9042EC21 9042EC21 9042EC23 9042EC39 9042EC39 9042EC34 9042EC48 9042EC48	LOCAL_GODoff: loc_42EBFA: LOCAL_DoNotDest	call jmp push mov push call mov push call cmp jz mov push call call royMenu6 mov push call royMenu6 mov push call call call call mov push call call mov push call call mov push call call so push call call mov push call call mov push call call mov push call call so push call call mov push call call so push call call so push call so push call call so push call so push call call so push call call so push call so so push call so push call so so push call so so push call so push call so so push call so push call so so push call so so so so so so so so so so so so so	<pre>LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadMenuA [ebp+UAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+UAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONotDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111j ecx, [ebp+UAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeIsNowOf; "God mode is now off." 3 0] sub_409B3D esp, 0Ch [ebp+var_10] edx, [ebp+var_10] edx sub_4073BF </pre>
9042EBC6 9042EBC8 9042EBC8 9042EBC8 9042EBC9 9042EBD3 9042EBD3 9042EBD4 9042EBD4 9042EBD4 9042EBF4 9042EBF4 9042EBF3 9042EBF4 9042EBF4 9042EBF4 9042EBF4 9042EBF4 9042EC05 9042EC05 9042EC05 9042EC07 9042EC07 9042EC07 9042EC12 9042EC18 9042EC17 9042EC17 9042EC18 9042EC18 9042EC20 9042EC20 9042EC21 9042EC21 9042EC21 9042EC21 9042EC21 9042EC21 9042EC21 9042EC3 9042EC21 9042EC21 9042EC3 9042EC21 9042EC21 9042EC21 9042EC21 9042EC21 9042EC22 9042EC22 9042EC22 9042EC22 9042EC22 9042EC3 9042EC4 9042EC	LOCAL_GODOFF:	call jmp push mov push call mov push call cmp jz mov push call call royMenu6 mov push call royMenu6 mov push call call call call mov push call call mov push call call mov push call call so push call call mov push call call mov push call call mov push call call so push call call mov push call call so push call call so push call so push call call so push call so push call call so push call call so push call so so push call so push call so so push call so so push call so push call so so push call so push call so so push call so so so so so so so so so so so so so	<pre>LOCAL_GOREturn ; CODE XREF: sub_42EAF0+3C1j 6Ah ; 1pMenuName edx, GLOBAL_hInstance edx ; hInstance ds:LoadHenuA [ebp+VAR_hMenuLoaded], eax dword_18A3FB4, 0 short loc_42EBFA eax, [ebp+VAR_hMenuLoaded] eax ; hMenu ecx, dword_18A4B84 edx, [ecx+4] edx [; hWnd ds:SetHenu ; CODE XREF: sub_42EAF0+F41j GLOBAL_hMenu, 0 short LOCAL_DONOtDestroyMenu6A eax, GLOBAL_hMenu eax ; hMenu ds:DestroyMenu A: ; CODE XREF: sub_42EAF0+1111 ecx, [ebp+VAR_hMenuLoaded] GLOBAL_hMenu, ecx offset aGodModeISNowOf; "God mode is now off." 3 0 sub_409B3D esp, 0Ch [ebp+var_10] edx offset dword_141BB78 sub_404854 esp, 8 eax, eax short LOCAL_GOREturn</pre>

MENU FUN

Since all clients we investigated so far (5.0.8.3 / Demo / Pre-Alpha / GOD) support the menu 6Ah (106) we will now investigate if the support is actually implemented beyond the LoadMenu call.

To do so, open Resource Hacker, save the menu (from either the Pre-Alpha or GOD client) to a RES file and import it again in to the target client (5.0.8.3 or the Demo or any other client you desire to test for menu support).

- 1. Open Resource Hacker
- 2. Open your Source Client
- 3. Go To Menu 106 (1033)
- 4. Save as a RES file:

<u>File E</u> dit <u>V</u> iew	Action Help	<i>i</i>
🗉 🛅 Cursor	Save Resource as a bi <u>n</u> ary file	Linda
🖶 🫅 Bitmap 🚦	Save Resource as a *.res file	Hide <u> </u>
🕀 🧰 Icon	Save [Menu : 106] to *.rc file	
 ➡ Menu ➡ 105 ➡ 106 ➡ 119 ➡ 119 ➡ 119 ➡ 128 ➡ Dialog ➡ Cursor G ➡ Cursor G ➡ Cursor G ➡ Con Grou 	Save [Menu] resources Save <u>a</u> ll Resources	ENGLIS
	Replace <u>I</u> con Replace <u>C</u> ursor Replace <u>B</u> itmap Replace other <u>R</u> esource	"Eξ
	Update all Resources Add a ne <u>w</u> Resource	"Chan "Chan
	R <u>e</u> name Resource [Menu : 106 : 1033] Delete Resource [Menu : 106 : 1033] Change Language [Menu : 106 : 1033]	"&Ful "Musio "Sound "Bull

- 5. Open the Target Client6. Import (using Add a new Resource):

N7 10	ker - C:\Target\UoDemo+\UoDemo+.exe
2.00 E E E E	Action Help
🖽 🧰 Bitmap	Save Resource as a binary file
E-Con	Save Resource as a *.res file Save Decompiled Resource
🗄 🦲 Dialog	Zave Decomplied Kesparce
🗄 🧰 Accelerat	Save [Bitmap] resources
🛓 📄 Icon Grou	Save <u>a</u> ll Resources
	Replace Icon
	Replace <u>C</u> ursor
	Replace Bitmap
	Replace other <u>R</u> esource
	Update all Resources
1	Add a ne <u>w</u> Resource
<u>85</u>	
5 1 / N/	100 (1000) 1 A 11 D
Select – Menu Kadd a New R o	106 (1033) - and press Add Resou
Add a New R	esource
Add a New R	22010-220 110
Add a New Ro	esource
Add a New Ro	esource
Add a New Ro	esource
Add a New Ro Open 1 C:\TargetW	esource
Add a New Ro Open 1 C:\TargetW Select new E- Mer	esource file with new resource O - Clients WENU 106.res resource: nu 106
Add a New Ro Open 1 C:\TargetW Select new E- Mer	esource file with new resource O - Clients WENU 106.res resource: nu
Add a New Ro Open 1 C:\TargetW Select new E- Mer	esource file with new resource O - Clients WENU 106.res resource: nu 106
Add a New Ro Open 1 C:\TargetW Select new E- Mer	esource file with new resource O - Clients WENU 106.res resource: nu 106
Add a New Ro Open 1 C:\TargetW Select new E- Mer	esource file with new resource O - Clients WENU 106.res resource: nu 106
Add a New Ro Open 1 C:\TargetW Select new E- Mer	esource file with new resource O - Clients WENU 106.res resource: nu 106
Add a New Ro Open 1 C:\TargetW Select new E- Mer	esource file with new resource O - Clients WENU 106.res resource: nu 106
Add a New Ro Open 1 C:\TargetW Select new E- Mer	esource

8. When done, save the executable (make sure you have backup somewhere).

9. Do a test run; make sure the game is in Windowed Mode though



On the previous screenshot we can see that the demo will load the menu from the Pre-Alpha Client, if you would repeat the steps and actually play with the menu you will find that the demo (and client 5.0.8.3) is reacting to the menu options.

Conclusion: the game is responding to a menu that is initially not available. This makes me angry! This means there is some secret code inside the client, bad programming that is!

UNCOVERING SOME SECRETS

According to the Windows API programs have to respond to menu options through the WM_COMMAND handler inside a WindowProc. The Ultima Online client has only one WindowProc function so locating WM_COMMAND becomes easy.

I've done the research for you and the demo will arrive here when responding to a menu option:

; CODE XREF: FUNC_WindowProc+5D5[†]j

004FDBFA	100	4FDBFA:
004FDBFA	mov	ecx, [ebp+var 60]
004FDBFD	sub	ecx, 40004
004FDC03	mov	[ebp+var 60], ecx
004FDC06	cmp	[ebp+var_60], 139
004FDC0D	ja	loc_4FDDF8
004FDC13	mov	eax, [ebp+var_60]
004FDC16	xor	edx, edx
004FDC18	mov	dl, ds:byte_4FE31F[eax]
004FDC1E	jmp	ds:off_4FE2EF[edx*4]

The menu is handled in the original C language with a switch/case statement. The compiler translated it to a jump-table. The jump-table for the demo is here:

AA4FF2FF	nf	f_4FE2EF dd offset loc_4FDCCE ; DATA XREF: FUNC_WindowProc+6131r
		offset loc 4FDDB4
		offset loc ⁴ FDC3C
		offset loc 4FDC85
004FE2FF	dd	offset loc 4FDD4A
		offset loc 4FDD9F
004FE307	dd	offset loc 4FDD7A
004FE30B	dd	offset loc 4FDCF3
004FE30F	dd	offset loc_4FDCCE
004FE313	dd	offset loc_4FDD3E
004FE317	dd	offset loc_4FDD62
		offset loc_4FDDF8
004FE31F	by	<mark>te_4FE</mark> 31F db 0,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0B
004FE31F		; DATA XREF: FUNC_WindowProc+60D1r
004FE31F	db	0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,
004FE31F	db	0Bh,0Bh,0Bh,0Bh,1,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh
004FE31F	db	0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,
004FE31F	db	0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,
004FE31F	db	0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,
		0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,4,5,0Bh,0Bh,0Bh,6,0Bh,0Bh,0Bh,7,8,0Bh,0Bh,0Bh
		0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,0Bh,
004FE3AA	db	ØAh

This is similar to the jump-table we saw earlier of the Pre-Alpha Client, one option has been added. Most GOD commands are unhandled (0Bh) so the Ultima Online Demo does not contain the GOD client in it. Note: The server side contains GOD code but that's another story for another day.

If you compare the menu of the Demo with the menu of the Pre-Alpha Client you will notice they are almost equal in design:

Pre-Alpha: 40001 - 0 - Exit 40004 - 1 - Change Text Font 40006 - 2 - Change Text Foreground Color 40043 - 3 - Full Screen Mode 40073 - 4 - Toggle Music 40074 - 5 - Toggle Sound 40089 - 6 - Unknown 40112 - 7 - Bulletin Board 40115 - 8 - Unknown 40116 - 9 - Unknown Demo: 40001 - / - Exit 40004 - 0 - Open Client Config 40043 - 1 - Full Screen Mode 40073 - 2 - Toggle Music 40074 - 3 - Toggle Sound 40115 - 4 - Unknown 40116 - 5 - Unknown 40120 - 6 - Unknown 40124 - 7 - Unknown 40125 - 8 - Unknown 40140 - 9 - Unknown 40143 - A - Unknown

Menu ID 40043 was changed from "Change Text Font" to "Open Client Config" in the demo. This is also seen in the GOD client's menu definition. The Bulletin Board has been removed. Menu option 40089 seems to be unique for the Pre-Alpha Client but the menu is not defined in that client's resource, so it's a hidden menu option! Menu 40115 and 40116 are also not defined in both the demo and the Pre-Alpha Client (and the GOD client). Secrets!

Menu ID 40124 also appears in the GOD client and equals "Obscenity Filter" and menu ID 40140 equals "Request Assistance". For the understanding the others more hacking is required.

An easy way to enable these options is to edit the menu with the Resource Hacker and add them.

MENU EDITING

Edit the menu so it looks like this:

```
<u>Compile Script</u> Hide Menu

106 MENU

LANGUAGE LANG_ENGLISH, SUBLANG_ENGLISH_US

{

POPUP "File"

{

MENUITEM "E&xit", 40001

}

POPUP "&Options"

{

MENUITEM "Client Config...", 40004

MENUITEM "GFull Screen Mode", 40043

MENUITEM "Music", 40073

MENUITEM "Music", 40074

}

POPUP "&Hacker"

{

MENUITEM "Unknown 40115", 40115

MENUITEM "Unknown 40116", 40116

MENUITEM "Unknown 40120", 40120

MENUITEM "Unknown 40125", 40125

MENUITEM "Unknown 40143", 40143

}
```

When you're done, press the Compile Script button and save the executable, then run it. If all went okay your game will look like this:



It now becomes a process of trial and error, press the menu options and see what happens.

The menu design became this:

```
Pre-Alpha:
40001 - 0 - Exit
40004 - 1 - Change Text Font
40006 - 2 - Change Text Foreground Color
40043 - 3 - Full Screen Mode
40073 - 4 - Toggle Music
40074 - 5 - Toggle Sound
40089 - 6 - Unknown
40112 - 7 - Bulletin Board
40115 - 8 - Toggle Combat
40116 - 9 - Open Spellbook
Demo:
40001 - / - Exit
40004 - 0 - Open Client Config (see 8)
40043 - 1 - Full Screen Mode
40073 - 2 - Toggle Music
40074 - 3 - Toggle Sound
40115 - 4 - Toggle Combat
40116 - 5 - Open Spellbook
40120 - 6 - Open Radar
40124 - 7 - Obscenity Filter
40125 - 8 - Open Client Config (see 0)
40140 - 9 - Request Assistance
40143 - A - Toggle Footsteps
```

Menu ID 40116 was a bit trickier for me to understand; this turned out to be the Open Spellbook packet (thanks Garret & Derrick for aiding me here).

A screenshot of the same uodemo jump-table with all menu handlers renamed to something more meaningful based on the done analysis:

```
004FE2EF off 4FE2EF dd offset LOCAL Menu OpenSettings
                                 ; DATA XREF: FUNC_WindowProc+6131r
BBLFF2FF
004FE2F3 dd offset LOCAL_Menu_ToggleFullScreen
004FE2F7 dd offset LOCAL_Menu_ToggleMusic
004FE2FB dd offset LOCAL_Menu_ToggleSound
004FE2FF dd offset LOCAL_Menu_ToggleCombat
004FE303 dd offset LOCAL_Menu_SendUnknownPacket12type43
004FE307 dd offset LOCAL_Menu_OpenRadar
004FE30B dd offset LOCAL Menu ObsenityFilter
004FE30F dd offset LOCAL Menu OpenSettings
004FE313 dd offset LOCAL Menu RequestAssistence
004FE317 dd offset LOCAL_Menu_ToggleFootsteps
004FE318 dd offset LOCAL_Menu_Ignore
; DATA XREF: FUNC_WindowProc+60D1r
004FE31F
004FE31F db 08h,08h,08h,08h,08h,08h,4,5,08h,08h,08h,6,08h,08h,08h,7,8,08h,08h,08h
004FE3AA db
        ØAh
```

MENU COMPARISON

Client 5.0.8.3 (2007) is still responding to the menu options similar to the ones found in the Ultima Online Demo from 1998. This is very interesting, especially since both clients come without any menu.

I made a comparison of the 3 client menus (GOD client excluded).

Pre-Alpha: (the original menu, with 3 secrets and 1 item disabled) 40001 - 0 - Exit 40004 - 1 - Change Text Font 40006 - 2 - change Text Foreground Color 40043 - 3 - Full Screen Mode 40073 - 4 - Toggle Music 40074 - 5 - Toggle Sound 40089 - 6 - Unknown 40112 - 7 - Bulletin Board 40115 - 8 - Toggle Combat 40116 - 9 - Open spellbook

Demo: (new item but their ID's indicate they were added soon after Pre-Alpha) 40001 - / - Exit 40004 - 0 - Open Client Config (see 8) 40043 - 1 - Full Screen Mode 40073 - 2 - Toggle Music 40074 - 3 - Toggle Sound 40115 - 4 - Toggle Combat 40116 - 5 - Open Spellbook 40120 - 6 - Open Radar 40124 - 7 - Obscenity Filter 40125 - 8 - Open Client Config (see 0) 40140 - 9 - Request Assistance 40143 - A - Toggle Footsteps

```
Client 5.0.8.3:

(almost equal to the demo but with 40087 (re-?)added, why?)

40001 - 0 - Exit

40004 - 1 - Open Client Config (see between 8-9)

40043 - 2 - Full Screen Mode (see between 4-5)

40073 - 3 - Toggle Music

40074 - 4 - Toggle Sound

40087 - 2 - Full Screen Mode (see 2)

40115 - 5 - Toggle Combat

40116 - 6 - Open Spellbook

40120 - 7 - Open Radar

40124 - 8 - Obscenity Filter

40125 - 1 - Open Client Config (see 1)

40140 - 9 - Request Assistance

40143 - A - Toggle Footsteps
```

THE FINAL MENU

The following menu definition is the final menu for the Ultima Online Demo client (also for client 5.0.8.3 and most likely, for the many other clients out there). I renamed most options and reorganized the layout:

```
106 MENU
LANGUAGE LANG_ENGLISH, SUBLANG_ENGLISH_US
{
POPUP "&Game"
{
     MENUITEM "Toggle &Combat Mode", 40115
     MENUITEM SEPARATOR
     MENUITEM "Open Spell&book", 40116
     MENUITEM "Open &Radar", 40120
     MENUITEM SEPARATOR
     MENUITEM "E&xit", 40001
}
POPUP "&Options"
{
     MENUITEM "&Full Screen Mode", 40043
     MENUITEM SEPARATOR
     MENUITEM "Footste&ps", 40143
     MENUITEM "&Music", 40073
     MENUITEM "&Sound",
                         40074
     MENUITEM SEPARATOR
     MENUITEM "&Obscenity Filter", 40120
     MENUITEM SEPARATOR
     MENUITEM "Client & Config", 40004
}
POPUP "&Help"
{
     MENUITEM "Request & Assistance", 40140
}
}
```

FIXING THE DEMO

When you go in full screen mode with the menu enabled you will see the menu is active in full screen mode and when you return to windowed mode the menu is gone (forever).

Let's fix this behavior and turn it around; going in full screen mode will make the menu go away and when you enter windowed mode it will return.

Locate the code where switching between full screen and windowed mode is handled. Because we have renamed the menu handlers this becomes an easy task:

004FDDB4 004FDDB4		lenu_ToggleFullScreen:	; CODE XREF: FUNC_WindowProc+A21j ; FUNC WindowProc+13E1j
004FDDB4		dword 82246C, 8	1 rono_nindom roo roc.j rin
004FDDBB	1.000000000	short loc 4FDDD8	
004FDDBD	Contraction of the second s	dword 7022A8, 1	
004FDDC7	The second second	sub 4FD41E	
004FDDCC	mov	dword 7022A8, 8	
004FDDD6		short loc 4FDDF1	
004FDDD8	-		
004FDDD8			
004FDDD8	loc 4FC	DD8:	; CODE XREF: FUNC WindowProc+780 [†] j
004FDDD8	mov	dword 7022A8, 1	A MUMBER SECTOR CONTRACTOR CONTRACTORS
004FDDE2	call	sub 4FD4E7	
004FDDE7	mov	dword 7022A8, 8	
004FDDF1		17. 18 A	
004FDDF1	loc 4FC	DDF1:	; CODE XREF: FUNC_WindowProc+7CB†j
004FDDF1	xor	eax, eax	
004FDDF3	imp	1oc 4FE2BC	

The trick is to understand the function and modify its design. This is not an easy task and probably takes some practice if you are new to this.

On the following pages I will give screenshots of the original code and the code I changed. Compare and learn from it.

This is not an assembler tutorial nor a patching tutorial so I will not go in too much detail. Let the code speak for itself.

FULL SCREEN: ON - ORIGINAL CODE

004FD439	6A	FØ					push	OFFFFFFOh	-	nIndex
004FD43B			20	70	00		mov	eax, GLOBAL ClientWindow	245	100012-000
004FD440		5175	1000	105	12/22		push	eax		hWnd
004FD441	17.00	15	AC.	58	96	88	100 A 100	ds:GetWindowLongA	100	CONTRACT.
004FD447							MOV	[ebp+dwNewLong], eax		
004FD44A	12.2						MOV	ecx, [ebp+dwNewLong]		
004FD44D				FF	39	FF	100 C C C C C C C C C C C C C C C C C C	ecx, ØFF39FFFFh		
004FD453				0.0010	1000	10000	mov	[ebp+dwNewLong], ecx		
004FD456							MOV	edx, [ebp+dwNewLong]		
004FD459	1000	000000	1000	00	00	80	125557156	edx, 80000000h		
004FD45F				1010	00	1000	MOV	[ebp+dwNewLong], edx		
004FD462							MOV	eax, [ebp+dwNewLong]		
004FD465	102.222						push	eax		duNeul ong
004FD466	72054	FØ					push	OFFFFFFOh	1	
004FD468		1000	18	20	78	88		ecx, GLOBAL ClientWindow	3.0	minuca
004FD46E		00	10	20	10	00	push	ecx		h⊌nd
004FD46F	1000	15	50	57	00	00	Constant States of the	ds:SetWindowLongA		THINK .
004FD475	10.0	1.55	222025	-	7.554	70.700	FMOU	[ebp+Rect.top], 0		
004FD47C	1000	1000	10000		1000	1000	FMOV	[ebp+Rect.left], 0		
004FD483						20052	MOU	[ebp+Rect.bottom], 1E0h		
004FD48A	12025	100		100.00	51.25	5.50		[ebp+Rect.right], 280h		
004FD491				00	OL.	00	push	OFFFFFFECh	10	nIndex
004FD493			18	28	70	88		edx, GLOBAL ClientWindow	28	HINGEA
004FD499		1.5	19	20		00	push	edx	10	blind
004FD49A		15	80	58	00	00		ds:GetWindowLongA		manu
004FD4A0		1	00	20	×.		push	eax	-	duEvStulo
004FD4A1	120.70	19	20	70	88		mov	eax, GLOBAL ClientWindow	15	uwenseyre
004FD4A6		10	20	1.0	00		push	eax, acount_critentwindow		blind
004FD4A7		10	0.0	E7	00	88	I VALLEY AND A DECK	ds:GetMenu		inmitu
004FD4A7			60	21	711	00		eax		
004FD4AF	1000	1207.0					neg sbb			
004FD481	1000	12.2						eax, eax eax		
004FD4B1		VO					neg		42	bHopu
004FD4B3	125025	EB					push	eax OFFFFFFFOh	2	
004FD4B4	1000	1000	10	90	70	00	push	ecx, GLOBAL ClientWindow	23	ITTILIEX
004FD4BC	1.2	00	10	20	7.0	00	(2001)			blind
004FD4BC	2212	40	00	ro.	00	00	push	ecx dc.Patilindaul.apa0	•	IIWIU
김 (김 (김희학 김) (김) (김)	1000	15	06	20	AH	00		ds:GetWindowLongA	1	duChu7a
004FD4C3	1000	er.					push	eax		uwstyte
004FD4C4 004FD4BD				E0	00	00	lea	edx, [ebp+Rect]		
		15	90	20	Ан	99		ds:GetWindowLongA	-	duCtula.
004FD4C3 004FD4C4		EF	E.P.				push	eax	ntWindow ; hWnd eax ong] ecx ong] edx ong] ; dwNewL ; nIndex ntWindow ; hWnd A a; dwExSt ntWindow ; hWnd A ; dwExSt ; nIndex ; hWnd A ; j mindex ; hWnd ; hWnd	
전 전 문 문 것 같은 것 같은 것 같이		22	r U				lea	edx, [ebp+Rect]	_1	InBoot
004FD4C7		40	E0	E7	00	00	push	edx dc:0diuctWindowRootEv	; dwNewLo ; nIndex ; hWnd ; hWnd ; dwExSty ; hWnd ; bMenu ; nIndex	
004FD4C8	FF	15	20	57	AH	00	Call	ds:AdjustWindowRectEx		

FULL SCREEN: ON -CHANGED CODE

004FD4A1	A1	18	20	70	00		MOV	eax, GLOBAL_ClientWindow		
004FD4A6	6A	00					push	9	;	hMenu
004FD4A8	50						push	eax	;	hWnd
004FD4A9	FF	15	24	58	9A	00	call	ds:SetMenu		
004FD4AF	90						nop			
004FD4B0	90						nop			
004FD4B1	90						nop			
004FD4B2	6A	00					push	0	- 2	bMenu

FULL SCREEN: OFF – ORIGINAL CODE

004FD5D0 8B 4D EC MOV 004FD5D3 51 push 004FD5D4 88 55 E4 mou 004FD5D7 52 push 004FD5D8 6A 00 push 004FD5DA 6A 00 push 004FD5DC 6A FE push 004FD5DE A1 18 20 70 00 MOU 004FD5E3 50 push 004FD5E4 FF 15 20 58 9A 00 call 004FD5EA 6A 00 nush 004FD5EC 6A 00 push 004FD5EE 88 0D 18 20 70 00 mov 004FD5F4 51 push 004FD5F5 FF 15 1C 58 9A 00 call 004FD538 51 push 004FD539 FF 15 5C 57 9A 00 call 004FD53F 6A 20 push 004FD541 FF 15 20 57 9A 00 call 004FD547 8D 94 00 80 02 00+lea 004FD54E 89 55 E4 mov 004FD551 6A 21 push 004FD553 FF 15 20 57 9A 00 call 004FD559 88 F0 MOV 004FD55B 6A 04 push 004FD55D FF 15 20 57 9A 00 call 004FD563 8D 84 70 E0 01 00+lea 004FD56A 89 45 EC MOV 004FD56D C7 45 F4 00 00 00+mov 004FD574 C7 45 F0 00 00 00+mov 004FD57B 8B 4D EC MOV 004FD57E 89 40 FC mnu 004FD581 8B 55 E4 mov 004FD584 89 55 F8 MOV 004FD587 6A 00 push 004FD589 A1 18 20 70 00 MOV 004FD58E 50 push 004FD58F FF 15 24 58 9A 00 call 004FD595 6A EC push 004FD597 8B 0D 18 20 70 00 MOV 004FD59D 51 push 004FD59E FF 15 0C 58 9A 00 call 004FD5A4 50 push 004FD5A5 6A 00 push 004FD5A7 6A F0 push 004FD5A9 8B 15 18 20 70 00 mov 004FD5AF 52 pust push 004FD5B0 FF 15 0C 58 9A 00 call 004FD5B6 50 push 004FD5B7 8D 45 F0 lea 004FD5BA 50 push 004FD5BB FF 15 58 57 9A 00 call 004FD5C1 B9 60 24 82 00 mov 004FD5C6 E8 CE 34 02 00 call 004FD5CB 68 12 01 00 00 push 004FD5D0 8B 4D EC MOV 004FD5D3 51 push MOV 004FD5D4 88 55 E4 004FD5D7 52 push 004FD5D8 6A 00 push 004FD5DA 6A 00 push 004FD5DC 6A FE push 004FD5DE A1 18 20 70 00 MOV 004FD5E3 50 push 004FD5E4 FF 15 20 58 9A 00 call 004FD5EA 6A 00 push 004FD5EC 6A 00 push 004FD5EE 88 0D 18 20 70 00 MOV 004FD5F4 51 push 004FD5F5 FF 15 1C 58 9A 00 call ecx, [ebp+cy] ecx edx, [ebp+var_1C] edx B **OFFFFFFFF** eax, GLOBAL_ClientWindow eax ds:SetWindowPos ecx, GLOBAL_ClientWindow ecx ds:InvalidateRect ecx ds:SetWindowLongA 26h : ds:GetSystemMetrics edx, [eax+eax+280h] [ebp+var_10], edx 21h ; '!' ds:GetSystemMetrics esi, eax ds:GetSystemMetrics eax, [eax+<mark>esi</mark>*2+1E0h] [ebp+cy], eax [ebp+Rect.top], 8 [ebp+Rect.left], 0 ecx, [ebp+cy] [ebp+Rect.bottom], ecx edx, [ebp+var 10] [ebp+Rect.right], edx eax, GLOBAL_ClientWindow eax ds:SetMenu **OFFFFFFECh** ecx, GLOBAL ClientWindow ecx ds:GetWindowLongA eax **OFFFFFFF**Oh edx, GLOBAL_ClientWindow edx ds:GetWindowLongA eax eax, [ebp+Rect] eax ds:AdjustWindowRectEx ecx, offset dword_822460 sub 520A99 112h ecx, [ebp+cy] ecx edx, [ebp+var_1C] edx R A **OFFFFFFF** eax, GLOBAL_ClientWindow eax ds:SetWindowPos 6 ecx, GLOBAL_ClientWindow ecx ds:InvalidateRect

; cy CX ; Y ; X ; hWndInsertAfter ; hWnd ; bErase ; 1pRect ; hWnd ; hWnd ; nIndex ; nIndex ; nIndex ; hMenu : hWnd ; nIndex ; hWnd ; dwExStyle bMenu ; nIndex ; hWnd ; dwStyle ; 1pRect ; uFlags ; cy CX 2 Y ; X ; hWndInsertAfter ; hWnd ; bErase ; 1pRect ; hWnd

FULL SCREEN: OFF - CHANGED CODE

004FD57B	8B	55	E4				MOV	edx, [ebp+var 10]		
004FD57E	89	45	FC				mov	[ebp+Rect.bottom], eax		
004FD581	89	55	F8				mov	[ebp+Rect.right], edx		
004FD584	A1	50	21	70	00		mov	eax, hMenu		
004FD589	8B	35	18	20	70	00	mov	esi, GLOBAL ClientWindow		
004FD58F	50						push	eax	-	hMenu
004FD590	56						push	esi	- 2	hWnd
004FD591	2028	15	24	58	98	88	call	ds:SetMenu		
004FD597	68	EC	1005	27.20	2020		push	ØFFFFFECh		nIndex
004FD599		1.1.1					push	esi		hWnd
004FD59A	2.2	15	96	58	98	00	call	ds:GetWindowLongA		a contraction of
004FD5A0		100	1		1000	66	push	eax	;	dwExStyle
004FD5A1	A1	50	21	78	88		MOV	eax, hMenu	- 16	
004FD5A6	1000						push	eax	3	bMenu
004FD5A7	2.00	FØ					push	OFFFFFFOh		nIndex
004FD5A9	282						push	esi		hWnd
004FD5AA	2022	15	80	58	9A	66	and the second se	ds:GetWindowLongA		
004FD5B0	1.1.1	0.0		10.0	000		push	eax		dwStyle
004FD5B1	2020	45	FØ				lea	eax, [ebp+Rect]		dustyle
004FD5B4	0.00		100				push	eax		1pRect
004FD5B5	-	15	58	57	96	88	call	ds:AdjustWindowRectEx	- 68	Thucce
004FD5BB		12	20	~	2.0	00	nop	as .najasen indowneecers		
004FD5BC	2021						nop			
004FD5BD							nop			
004FD5BE	202						260062			
004FD5BF	2.00						nop			
004FD3DF	2.6						nop			

THE PATCH MORE OR LESS EXPLAINED

nop

What will happen after the patch?

004FD5C0 90

Well, when you go to Full Screen Mode the fix will call "SetMenu(hWnd, NULL)" to remove the menu. "AdjustWindowRectEx" will be called with "hMenu" set to "FALSE".

The opposite will happen when you enter Windowed Mode. The fix will call "SetMenu(hWnd, hMenu)" and will call "AdjustWindowRectEx" with "hMenu" converted to a "BOOL".

Previously the client was not doing anything when going from Windowed Mode to full Screen mode. Strangely enough, "SetMenu" was being called to remove the menu when entering Windowed Mode.

NOTE: "hMenu" is coming from the call to "DestroyMenu":

004FCB4C							10c_4F	CB4C:
004FCB4C	83	3D	50	21	70	00-	+cmp	hMenu, 0
004FCB53	74	OD					jz	short loc_4FCB62
004FCB55	8B	15	50	21	70	00	MOV	edx, <mark>hMenu</mark>
004FCB5B							push	edx
004FCB5C	FF	15	C 8	57	9A	00	call	ds:DestroyMenu

🖞 <u>File E</u> dit <u>S</u>	earch	⊻ie	w <u>A</u>	nalys	is E	xtras	; <u>W</u> i	ndow	1 2				_16	킨.
👌 🕭 • 🔚	Same	-	+	12		*	AN	SI		•	he	x		
UoDemoWith	Menu	.exe	1											
Offset(h)	00	01	02	03	04	05	06	07	08	09	OA	OB		-
OOOFCSAO	50	A1	18	20	70	00	6A	00	50	FF	15	24	P;. p.j.Pÿ.\$	
OOOFC8AC	58	9A	00	90	90	90	6A	00	6A	FO	8B	OD	Xšj.jð«.	
OOOFC8B8	18	20	70	00	51	FF	15	oc	58	91	00	50	. p.QÿXš.P	
000FC8C4	8D	55	FO	52	FF	15	58	57	94	00	В9	60	.UðRÿ.XWš.'`	
OOOFC8DO	24	82	00	E8	66	33	02	00	68	60	E4	8C	\$,.èf3h`äŒ	
OOOFC8DC	00	FF	15	EO	55	98	00	8B	E5	5D	C3	55	.ÿ.àUš.<å]ÃU	
OOOFC8E8	8B	EC	83	EC	1C	56	68	60	E4	8C	00	FF	<ìfì.Vh`äŒ.ÿ	
OOOFC8F4	15	E4	55	9A	00	C7	05	54	1B	70	00	00	.äUš.Ç.T.p	
000FC900	00	00	00	6A	FO	A1	18	20	70	00	50	FF	jð;. p.Pÿ	100
OOOFC90C	15	OC	58	94	00	89	45	E8	8B	4D	E8	81	Xš.‱Eè <mè.< td=""><td></td></mè.<>	
000FC918	E1	FF	FF	FF	7F	89	4D	E8	8B	55	E8	81	áÿÿÿ.‰Mè <uè.< td=""><td></td></uè.<>	
000FC924	CA	00	00	C6	00	89	55	E8	8B	45	E8	50	ÊÆ.‰Uè‹EèP	
000FC930	6A	FO	8B	OD	18	20	70	00	51	FF	15	5C	jð< p.Qÿ.∖	
000FC93C	57	9A	00	6A	20	FF	15	20	57	91	00	8D	Wš.j ÿ. Wš	
000FC948	94	00	80	02	00	00	89	55	E4	6A	21	FF	‴.€‱Uäj!ÿ	
000FC954	15	20	57	9A	00	8B	FO	6A	04	FF	15	20	. Wš.<ðj.ÿ.	
000FC960	57	9A	00	8D	84	70	EO	01	00	00	89	45	Vš"pà≿E	
000FC96C	EC	C7	45	F4	00	00	00	00	C7	45	FO	00	ìÇEôÇEð.	
000FC978	00	00	00	8B	55	E4	89	45	FC	89	55	F8	(UäzEüzUø	
000FC984	A1	SC	21	70	00	8B	35	18	20	70	00	50	;\!p.<5. p.P	
000FC990	56	FF	15	24	58	94	00	6A	EC	56	FF	15	Vÿ.\$Xš.jìVÿ.	
000FC99C	OC	58	9Å	00	50	A1	SC.	21	70	00	50	6A	.Xš.P;\!p.Pj	
000FC9A8	FO	56	FF	15	OC	58	94	00	50	8D	45	FO	ðVÿXš.P.Eð	
000FC9B4	50	FF	15	58	57	9A	00	90	90	90	90	90	Pÿ.XWš	
000FC9C0	90	89	60	24	82	00	E8	CE	34	02	00	68	. ¹ `\$,.èÎ4h	

A screenshot of a hex editor with the newly patched bytes:

Apply these changes and go play the Ultima Online Demo with a working menu :-).