

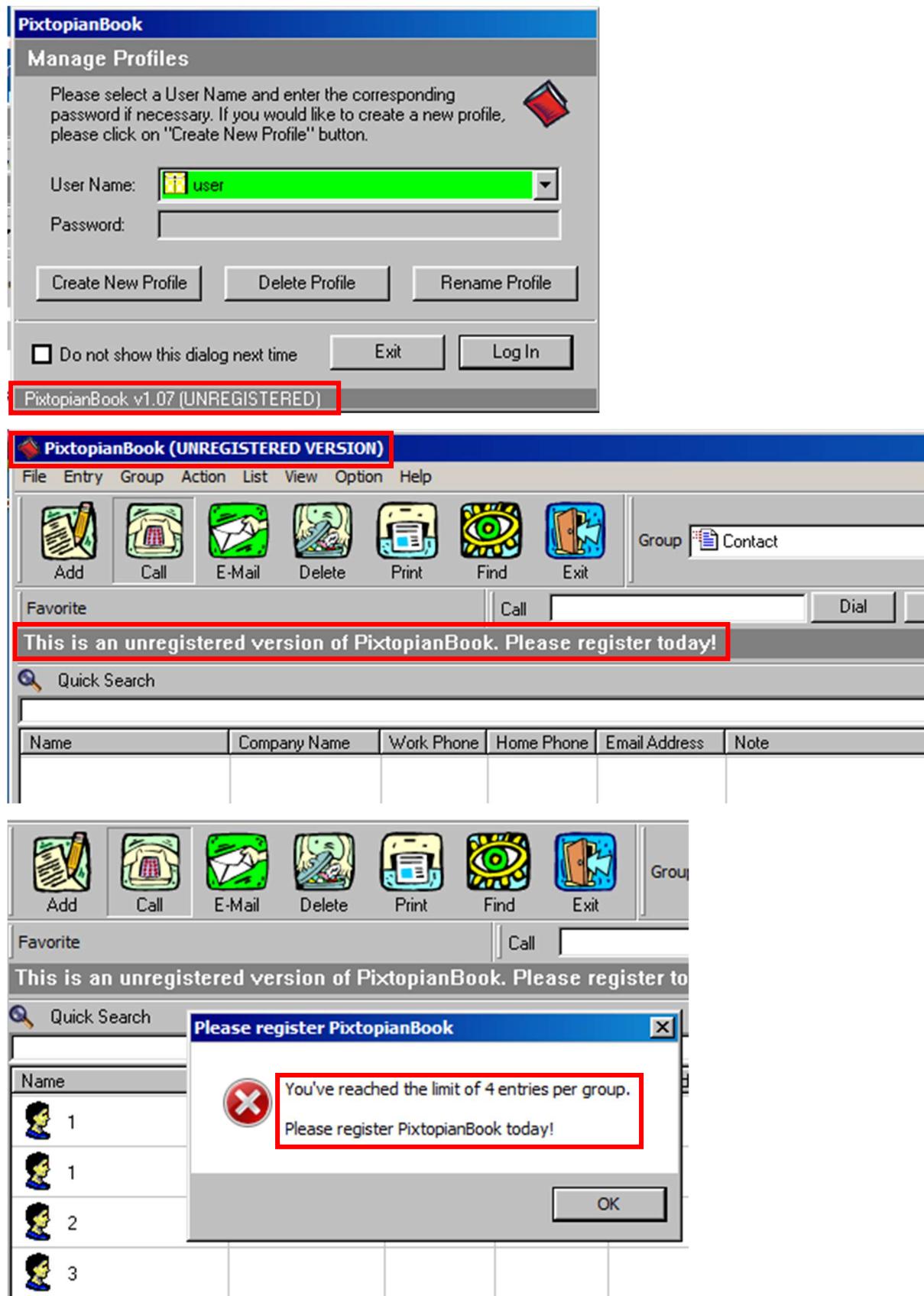
악성코드 분석 보고서

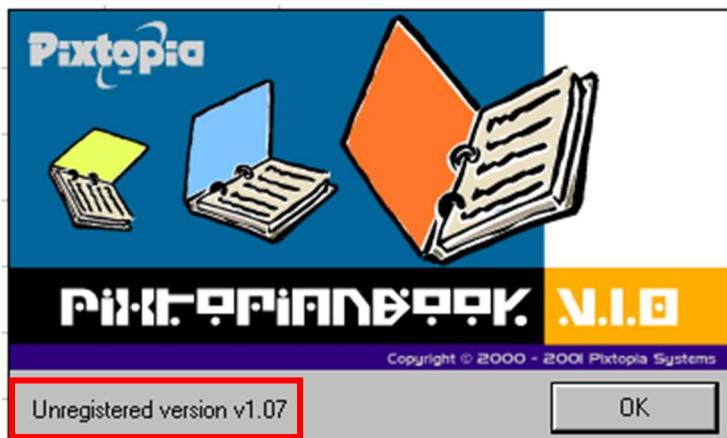
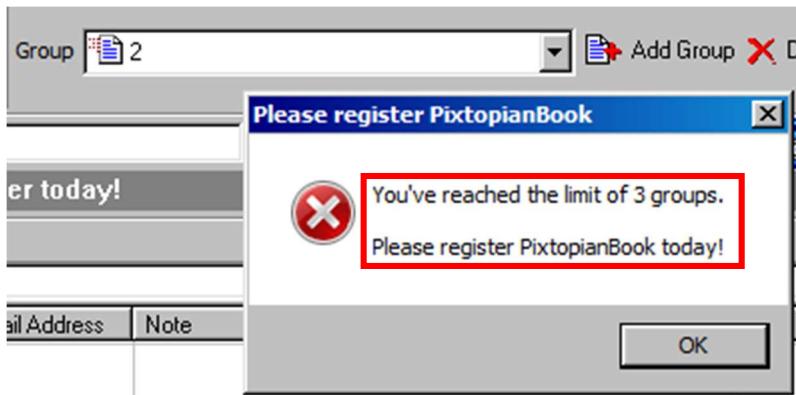
(sand-reversingwithlena-tutorials)

2025.05.27

04

1. 문제





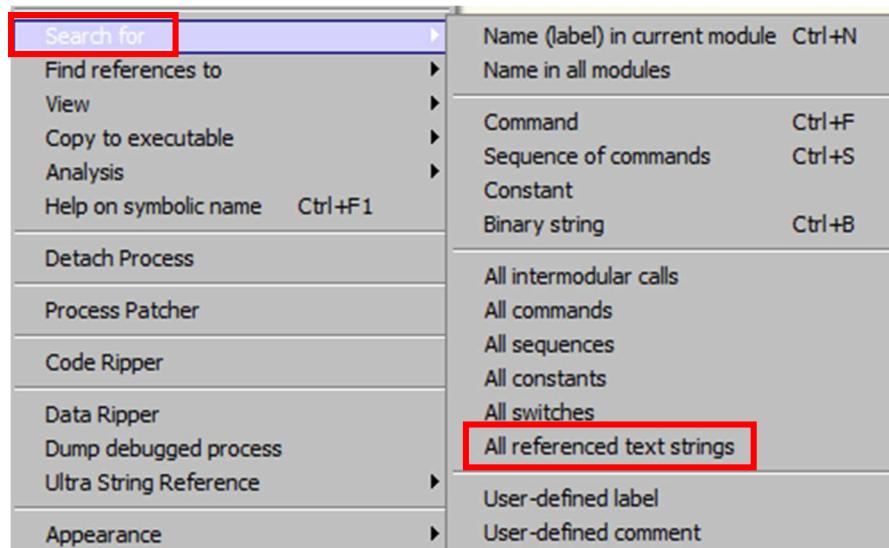
Unregistered -> registered 로 바꾸는 작업

User 추가를 4명 이상 가능하게, Group 추가를 3개 이상 가능하게 바꾸는 작업을 해야 함.

2. 해결 방법

1) 로그인 창

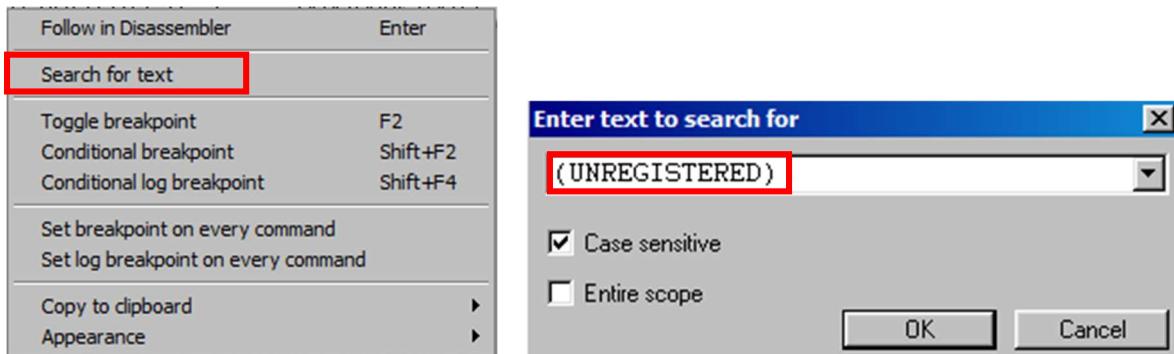
PixtopianBook v1.07 (UNREGISTERED) -> 0| 멘트 수정해야함.



OllyDbg Code부분에서 Search for > All references text strings 클릭.

R Text strings referenced in Pixtopia.text		
Address	Disassembly	Text string
00401025	MOV DWORD PTR DS:[ESI],Pixtopia.0047B8D0	ASCII "줄F"
0040102D	MOV EAX,Pixtopia.0047C104	ASCII "줄F"
00401059	MOV DWORD PTR DS:[EBX],Pixtopia.0047C111	ASCII "줄F"
00401062	MOV DWORD PTR DS:[ESI+68],Pixtopia.0047C111	ASCII "줄F"
00401078	MOV DWORD PTR SS:[EBP],Pixtopia.0047C110	ASCII "줄F"
0040109B	MOV DWORD PTR DS:[ESI],Pixtopia.004758A0	ASCII "줄F"
0040114F	MOV DWORD PTR DS:[ESI],Pixtopia.004758A0	ASCII "줄F"
00401210	MOV EAX,Pixtopia.004757D8	ASCII "줄G"
00401244	MOV DWORD PTR SS:[ESP+28],Pixtopia.004757D8	ASCII "줄F"
004017C2	MOV DWORD PTR DS:[ESI],Pixtopia.00475960	ASCII "줄F"
00401800	MOV EAX,Pixtopia.00475810	ASCII "줄G"
004019C9	MOV DWORD PTR SS:[ESP+18],Pixtopia.00475810	ASCII "줄F"
004019DD	MOV DWORD PTR SS:[ESP+10],Pixtopia.00475810	ASCII "줄F"
00401E55	MOV DWORD PTR DS:[ESI],Pixtopia.0047B800	ASCII "줄F"
00401E67	MOV DWORD PTR DS:[EDI],Pixtopia.0047C111	ASCII "줄F"
00401EAB	MOV DWORD PTR DS:[ESI],Pixtopia.00475AA0	ASCII "줄F"
00401F5F	MOV DWORD PTR DS:[ESI],Pixtopia.00475AA0	ASCII "줄F"
00401F90	MOV EAX,DWORD PTR DS:[00475A00]	ASCII "줄G"

현재 창이 나오는 걸 볼 수 있음.

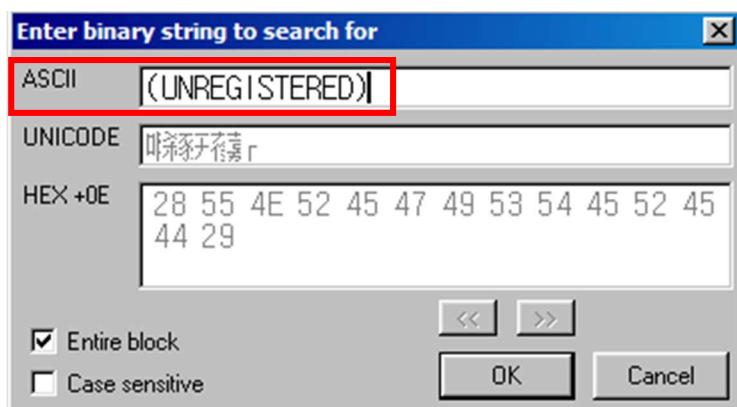


그럼 'Home' 키를 눌러서 맨 위로 올라간 다음 Search for text 클릭. 로그인 창에 있던 문자열 중 (UNREGISTERED) 검색해 보면 검색이 안됨.

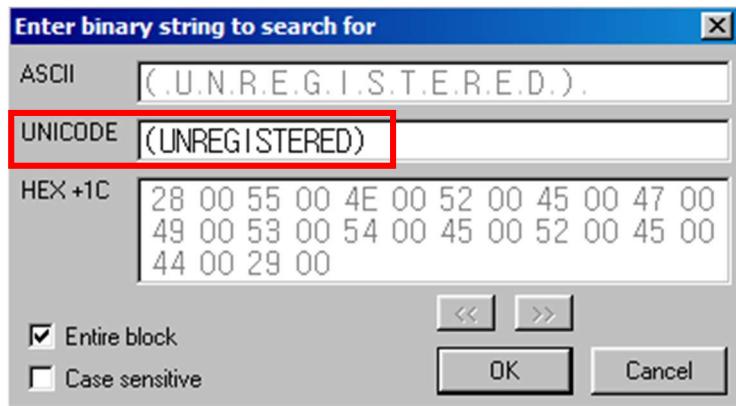
그럼 "Memory map" 을 눌러서 검색을 해줌.

Memory map									
Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as	
00010000	00010000				Map	RW	RW		
00020000	00001000				Priv	RW	RW		
0012D000	00001000				Priv	RW	Guard	RW	
0012E000	00002000				Priv	RW	Guard	RW	
00130000	00004000				Map	R	R		
00140000	00001000				Priv	RW	RW		
00150000	00067000				Map	R	R		
001C0000	00001000				Priv	RW	RW		
001D0000	00001000				Priv	RW	RW		
00280000	0002E000				Priv	RW	RW		
00400000	00001000	Pixtopia	.text	PE header	Imag	R	RWE		
00401000	00074000	Pixtopia	.text	code	Imag	R	RWE		

'Home' 키를 눌러서 맨 위로 올라간 다음 Search 클릭.



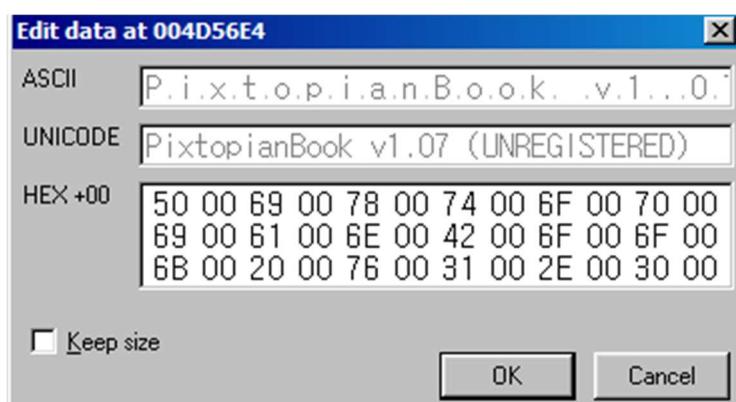
현재 창이 나타나고 'Shift+Insert' 키를 이용하여 로그인 창에 있던 문자열 중 (UNREGISTERED)을 ASCII에 검색해 보면 검색이 안됨.



이번에는 (UNREGISTERED)을 UNICODE에 검색해 보면 검색이되어서 아래 창이 발생하는 걸 볼 수 있음.

Dump - Pixtopia:.rsrc 0049D000..004E8FFF										
004D56AC	DD 00	10 00	14 00	14 00	FF FF	FF FF	FF FF	82 00	?	
004D56BC	FF FF	80 00	00 00	00 00	00 00	00 00	00 00	00 00	· · · · · · · · ·	
004D56CC	00 00	02 50	00 00	8C 00	FD 00	08 00	2A 04	00 00	.. . P . . ? ? * J ..	
004D56DC	FF FF	82 00	20 00	20 00	50 00	69 00	78 00	74 00	· · ? . . P . i . x . t	
004D56EC	6F 00	70 00	69 00	61 00	6E 00	42 00	6F 00	6F 00	o . p . i . a . n . B . o . o .	
004D56FC	6B 00	20 00	76 00	31 00	2E 00	30 00	37 00	20 00	K . . v . 1 . . 0 . 7 . .	
004D570C	28 00	55 00	4E 00	52 00	45 00	47 00	49 00	53 00	(. U . N . R . E . G . I . S .	
004D571C	54 00	45 00	52 00	45 00	44 00	29 00	00 00	00 00	T . E . R . E . D .)	
~ ~ ~ ~ ~	~ ~ ~ ~ ~	~ ~ ~ ~ ~	~ ~ ~ ~ ~	~ ~ ~ ~ ~	~ ~ ~ ~ ~	~ ~ ~ ~ ~	~ ~ ~ ~ ~	~ ~ ~ ~ ~	~ ~ ~ ~ ~	

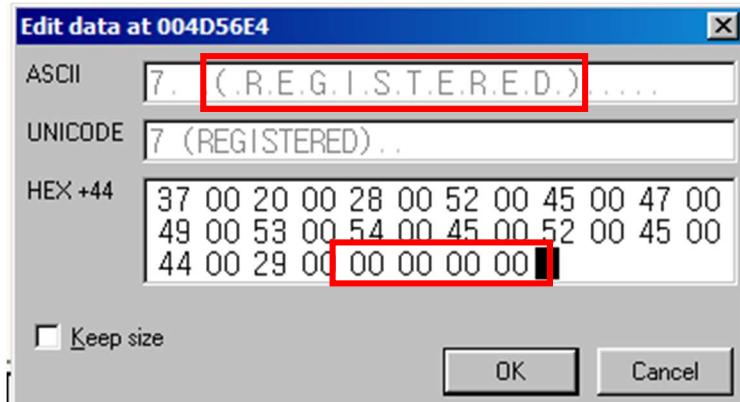
메모리 주소 0x004D56E4부터 시작하는 걸 볼 수 있음.



'ctrl+e' 키 누르면 위의 창이 나오는 걸 볼 수 있음.

PixtopianBook v1.07 (UNREGISTERED) -> PixtopianBook v1.07 (REGISTERED)으로 변경해 줘야함. 'UN'을 삭제해줘야하는데 현재의 사이즈랑 바꿨을 때 사이즈를 같게 해줘야함.

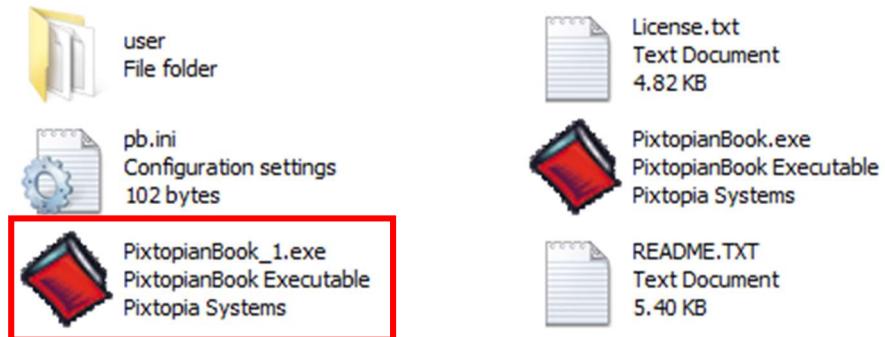
한 문자에 2byte인데 총 2개를 삭제해야하니까 'UN'을 삭제 후 뒤에 '00 00 00 00'을 추가해줘야함. 여기서 Keep size를 체크하면 크기 유지 때문에 삭제가 안되기 때문에 체크를 풀어주고 해야함.



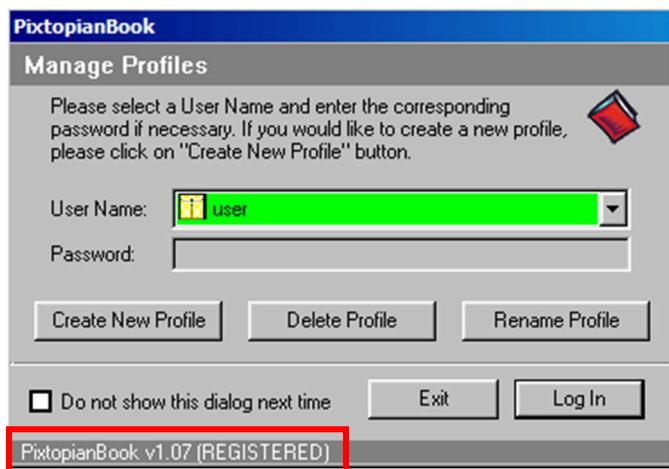
이런 식으로 바꾸고 메모리를 보면 바뀐 걸 볼 수 있음.

Address	Hex dump	ASCII
004D56E4	50 00 69 00 78 00 74 00 6F 00 70 00 69 00 61 00	P.i.x.t.o.p.i.a.
004D56F4	6E 00 42 00 6F 00 6F 00 6B 00 20 00 76 00 31 00	n.B.o.o.k..v.1.
004D5704	2E 00 30 00 37 00 20 00 28 00 52 00 45 00 47 00	.0.7..(.R.E.G.
004D5714	49 00 53 00 54 00 45 00 52 00 45 00 44 00 29 00	I.S.T.E.R.E.D.).
004D5724	00 00 00 00 00 00 00 00 00 00 00 00 C0 00 C0 80A.Æ
004D5734	00 00 00 00 0A 00 00 00 00 00 00 0F 01 7C 00 00 00‡.I....

메모리 부분에 오른쪽 마우스 클릭 > Copy to executable file 누른 후 하나의 Dump창이 생기는 걸 볼 수 있는데 거기서 오른쪽 마우스 클릭 > save file



생성이 확인된 걸 볼 수 있음.



이걸 실행해보면 바뀐 걸 볼 수 있음.

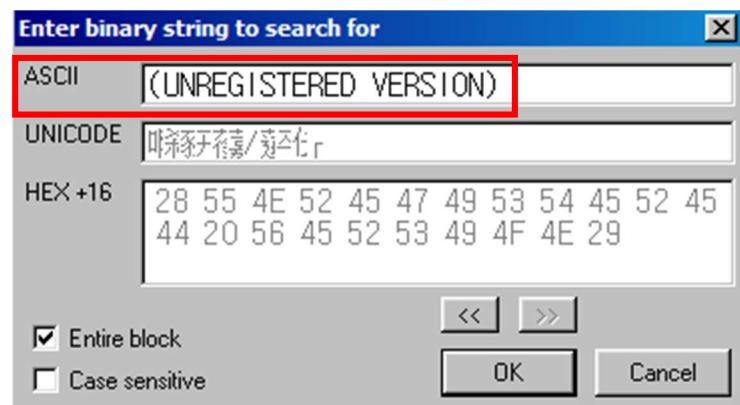
2) 타이틀 창

PixtopianBook_1.exe를 이용하여 타이틀 창의 문자열을 변경할거다.

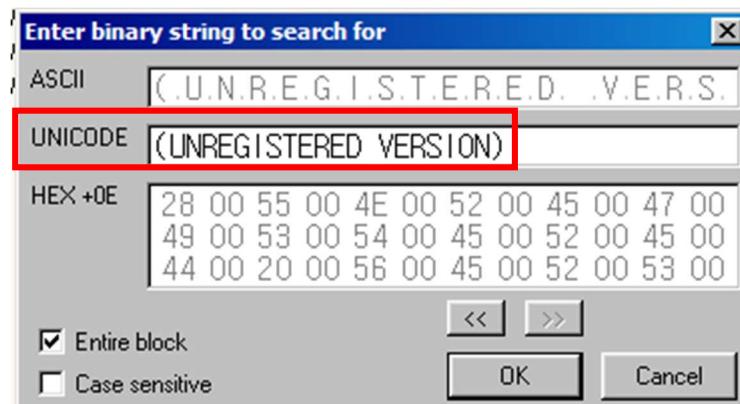
All references text strings에서 타이틀 창 있던 문자열 중 (UNREGISTERED VERSION) 검색해 보면 검색이 안됨. 그럼 “Memory map” 을 눌러서 검색을 해줌.

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	RW	RW	
00020000	00001000				Priv	RW	RW	
0012D000	00001000				Priv	RW	Guard	RW
0012E000	00002000			stack of main thread	Priv	RW	Guard	RW
00130000	00004000				Map	R	R	
00140000	00001000				Priv	RW	RW	
00150000	00067000				Map	R	R	#Device#HarddiskV0
001C0000	00001000				Priv	RW	RW	
001D0000	00001000				Priv	RW	RW	
00280000	0002E000				Priv	RW	RW	
00400000	00001000	Pixtopian	.text		PE header	Image	R	RWE
00401000	00074000	Pixtopian	.text		code	Image	R	RWE

‘Home’ 키를 눌러서 맨 위로 올라간 다음 Search 클릭.



현재 창이 나타나고 ‘Shift+Insert’ 키를 이용하여 로그인 창에 있던 문자열 중 (UNREGISTERED VERSION)을 ASCII에 검색해 보면 검색이 안됨.

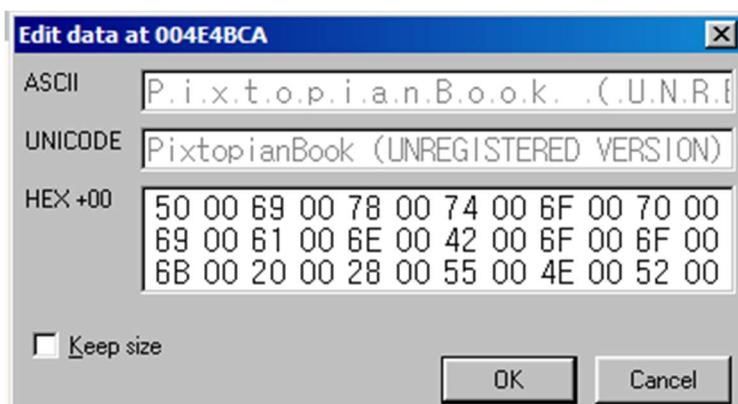


이번에는 (UNREGISTERED VERSION)을 UNICODE에 검색해 보면 검색이되어서 아래 창이

발생하는 걸 볼 수 있음.

Dump - Pixtopia:.rsrc 0049D000..004E8FFF															
004E4BA6	F8	87	77	77	77	77	80	00	00	00	88	88	88	88	88
004E4BB6	88	88	88	88	88	88	88	88	88	80	00	00	00	00	00
004E4BC6	00	00	24	00	50	00	69	00	78	00	74	00	6F	00	70
004E4BD6	69	00	61	00	6E	00	42	00	6F	00	6F	00	6B	00	20
004E4BE6	28	00	55	00	4E	00	52	00	45	00	47	00	49	00	53
004E4BF6	54	00	45	00	52	00	45	00	44	00	20	00	56	00	45
004E4C06	52	00	53	00	49	00	4F	00	4E	00	29	00	00	00	00
004E4C16	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

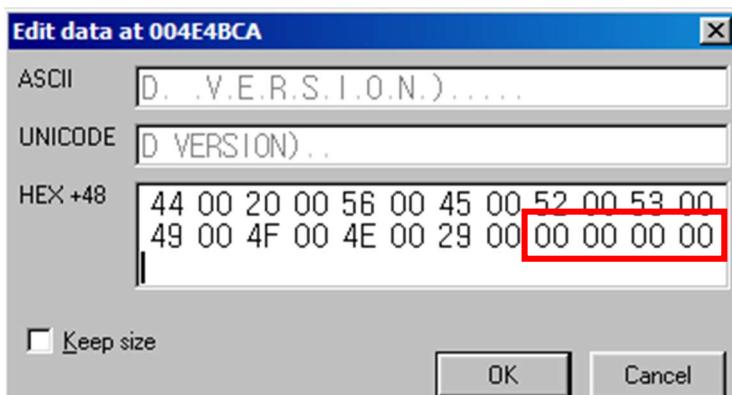
메모리 주소 0x004E4BCA부터 시작하는 걸 볼 수 있음.



'ctrl+e' 키 누르면 위의 창이 나오는 걸 볼 수 있음.

PixtopianBook (UNREGISTERED VERSION) -> PixtopianBook (REGISTERED VERSION)으로 변경해줘야함. 'UN'을 삭제해줘야하는데 현재의 사이즈랑 바꿨을 때 사이즈를 같게 해줘야함.

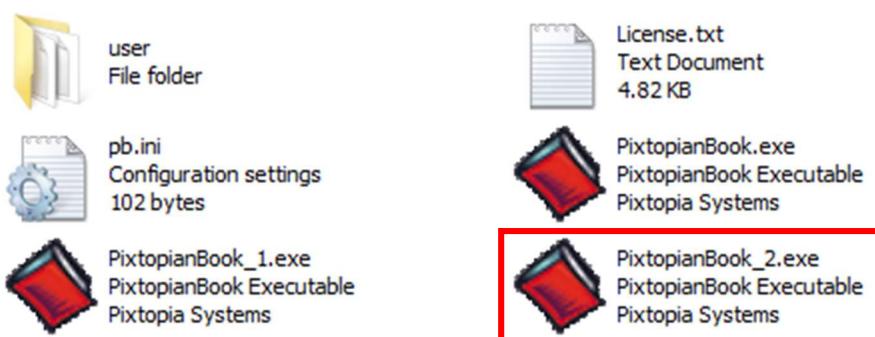
한 문자에 2byte인데 총 2개를 삭제해야하니까 'UN'을 삭제 후 뒤에 '00 00 00 00'을 추가해줘야함. 여기서 Keep size를 체크하면 크기 유지 때문에 삭제가 안되기 때문에 체크를 풀어주고 해야함.



D Dump - Pixtopia:.rsrc 0049D000..004E8FFF															
004E4BA6	F8	87	77	77	77	77	80	00	00	88	88	88	88	88	?www...奔驰奔驰
004E4BB6	88	88	88	88	88	88	88	88	88	80	00	00	00	00	奔驰奔驰奔驰....
004E4BC6	00	00	24	00	50	00	69	00	78	00	74	00	6F	00	70
004E4BD6	69	00	61	00	6E	00	42	00	6F	00	6F	00	6B	00	20
004E4BE6	28	00	52	00	45	00	47	00	49	00	53	00	54	00	45
004E4BF6	52	00	45	00	44	00	20	00	56	00	45	00	52	00	53
004E4C06	49	00	4F	00	4E	00	29	00	00	00	00	00	00	00	R.E.D. .V.E.R.S.
004E4C16	00	00	00	00	00	00	00	00	00	00	00	00	00	00	I.O.N.).....

바뀐 걸 볼 수 있음.

메모리 부분에 오른쪽 마우스 클릭 > Copy to executable file 누른 후 하나의 Dump창이 생기는 걸 볼 수 있는데 거기서 오른쪽 마우스 클릭 > save file



생성이 확인된 걸 볼 수 있음.



이걸 실행해보면 바뀐 걸 볼 수 있음.

3) 중간 배너 창

PixtopianBook_2.exe를 이용하여 배너 창의 문자열을 변경할거임.

All references text strings에서 타이틀 창 있던 문자열 중 This is an unregistered version of PixtopianBook. 검색해 보면 아래와 같은 곳에 멈추는 걸 볼 수 있음.

R Text strings referenced in Pixtopia:text		
Address	Disassembly	Text string
0040BB0F	PUSH Pixtopia.0048F96C	ASCII "default"
0040BB1B	MOV DWORD PTR DS:[ESI],Pixtopia.0047686E	ASCII "0월"
0040BBBF	MOV DWORD PTR DS:[ESI],Pixtopia.0047686E	ASCII "0월"
0040BC50	MOV EAX,Pixtopia.004767B8	ASCII "월"
0040C237	PUSH Pixtopia.0048F974	ASCII "This is an unregistered version of PixtopianBook. Please regis
0040DC00	MOV EAX,Pixtopia.00476958	ASCII "월"

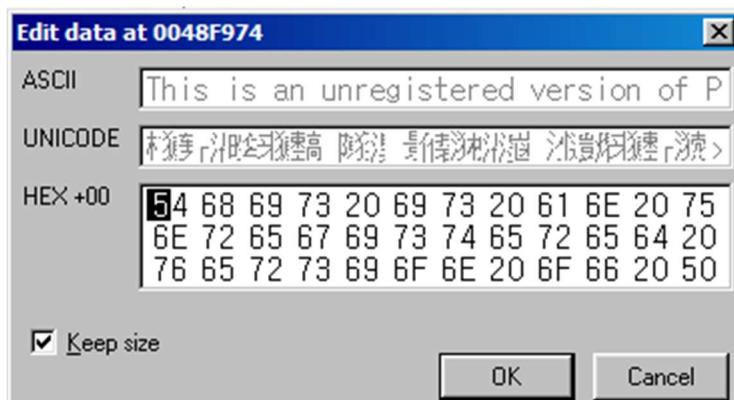
멈춘 곳을 더블클릭해보면 CPU 코드 창에서 현재 클릭한 곳을 찾아주는 걸 볼 수 있음.

C CPU - main thread, module Pixtopia		
0040C22B	. 5B	POP EBX
0040C22C	. C2 0400	RETN 4
0040C22F	> 81FD 07090000	CMP EBP, 907
0040C235	.~ 75 1A	JNZ SHORT Pixtopia.0040C251
0040C237	. 68 74F94800	PUSH Pixtopia.0048F974
0040C23C	RRCC	MOV ECX EST

그럼 'PUSH' 명령어를 이용하여 0x0048F974에 있는 문자열을 참조하는 걸 볼 수 있음.

Address	Hex dump	ASCII
0048F974	54 68 69 73 20 69 73 20 61 6E 20 75 6E 72 65 67	This is an unreg
0048F984	69 73 74 65 72 65 64 20 76 65 72 73 69 6F 6E 20	istered version
0048F994	6F 66 20 50 69 78 74 6F 70 69 61 6E 42 6F 6F 6B	of PixtopianBook
0048F9A4	2E 20 50 6C 65 61 73 65 20 72 65 67 69 73 74 65	. Please registe
0048F9B4	72 20 74 6F 64 61 79 21 00 00 00 00 43 49 6E 69	r today!...CIni
0048F9C4	74 44 69 61 6C 6F 67 42 61 72 00 00 43 4C 65 66	tDialogBar..CLe
0048F9D4	74 46 6F 72 6D 56 69 65 77 00 00 00 4E 6F 74 65	fFormView...Note
0048F9E4	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	

0x0048F974에 들어가보면 문자열이 있는 걸 확인할 수 있음.

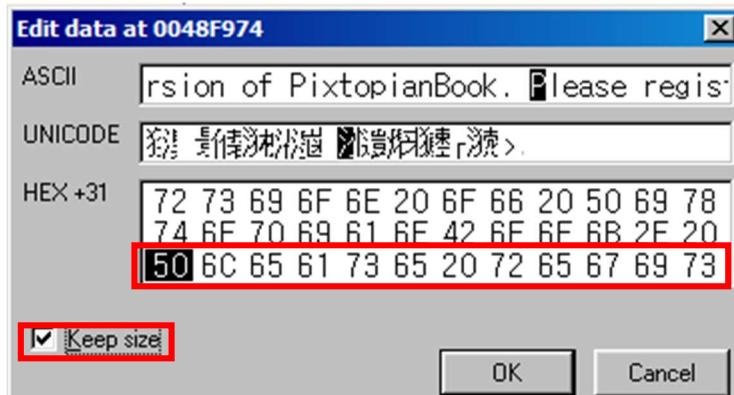


'ctrl+e' 키 누르면 위의 창이 나오는 걸 볼 수 있음.

This is an unregistered version of PixtopianBook. Please register today! -> This is an unregistered version of PixtopianBook.으로 변경해줘야함. 'UN' 삭제 후 마지막 문자열을 삭제해줘야함.

먼저 Keep size를 체크를 해제하고 여기서 ASCII코드로 되어있기 때문에 한 문자에

1byte임. 근데 총 2개를 삭제해야하니까 'UN'을 삭제 후 뒤에 '00 00'을 추가해줘야함.



그리고 Keep size를 체크해주고 현재 위치부터 다 '00'으로 바꿔준다.

Address	Hex dump	ASCII
0048F974	54 68 69 73 20 69 73 20 61 6E 20 72 65 67 69 73	This is an regis
0048F984	74 65 72 65 64 20 76 65 72 73 69 6F 6E 20 6F 66	tered version of
0048F994	20 50 69 78 74 6F 70 69 61 6E 42 6F 6F 6B 2E 20	PixtopianBook.
0048F9A4	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0048F9B4	00 00 00 00 00 00 00 00 00 00 00 00 43 49 6E 69CIn
0048F9C4	74 44 69 61 6C 6F 67 42 61 72 00 00 43 4C 65 66	tDialogBar..CLef
0048F9D4	74 46 6F 72 6D 56 69 65 77 00 00 00 4E 6F 74 65	tFormView...Note

이렇게 변한 걸 볼 수 있다.

메모리 부분에 오른쪽 마우스 클릭 > Copy to executable file 누른 후 하나의 Dump창이 생기는 걸 볼 수 있는데 거기서 오른쪽 마우스 클릭 > save file



생성이 확인된 걸 볼 수 있음.



이걸 실행해보면 바뀐 걸 볼 수 있음.

4) group 추가 창

PixtopianBook_3.exe를 이용하여 그룹을 더 추가할 수 있게 만들거다.

All references text strings에서 group 추가 창에 있던 문자열 중 You've reached the limit of 3 groups. 검색해 보면 아래와 같은 곳에 멈추는 걸 볼 수 있음.

R Text strings referenced in Pixtopia.text		
Address	Disassembly	Text string
00408B33	PUSH Pixtopia.0048F5BC	ASCII "Invalid group name. The group is not renamed."
00408B6C	MOV DWORD PTR SS:[ESP+74],Pixtopia.00470	ASCII "EFL"
00408B43	PUSH Pixtopia.0048F5AB	ASCII "Group is renamed."
00408B0C	PUSH Pixtopia.0048F700	ASCII "Please register PixtopianBook"
00408B11	PUSH Pixtopia.0048F6B4	ASCII "You've reached the limit of 3 groups. Please re
00408B57	PUSH Pixtopia.0048F6AB	ASCII "New Group"
00408B5C	PUSH Pixtopia 004AF800	ASCII "PixtopianBook"

멈춘 곳을 더블클릭해보면 CPU 코드 창에서 현재 클릭한 곳을 찾아주는 걸 볼 수 있음.

CPU - main thread, module Pixtopia		
00408B0A	. 6A 10	PUSH 10
00408B0C	. 68 00F74800	PUSH Pixtopia.0048F700
00408B11	. 68 B4F64800	PUSH Pixtopia.0048F6B4
00408B16	RRRR	Mov ECX ECX

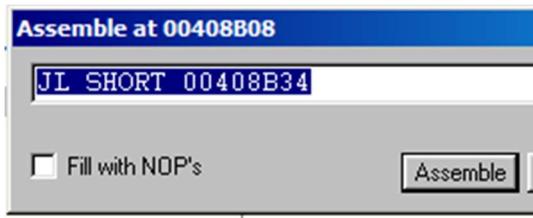
우리는 그룹을 3개 이상 만들 수 있게 해야하고 레지스터 키 등록해달라는 창이 안나오게 해야한다. 그러면 그 주변 코드를 봐야한다.

00408AF7	. 6A 00	PUSH 0	wParam = 0
00408AF9	. 68 46010000	PUSH 146	Message = CB_GETCOUNT
00408AFE	. 50	PUSH EAX	hWnd
00408AFF	. FF15 D0564700	CALL DWORD PTR DS:[<&USER32.Send	SendMessageA
00408B05	. 82F8 03	CMP EAX, 3	
00408B08	. 7C 2A	JL SHORT Pixtopia.00408B34	
00408B0A	. 6A 10	PUSH 10	
00408B0C	. 68 00F74800	PUSH Pixtopia.0048F700	ASCII "Please register PixtopianBook"
00408B11	. 68 B4F64800	PUSH Pixtopia.0048F6B4	ASCII "You've reached the limit of 3 groups."
00408B16	. 8BEB	MOV ECX, EBX	
00408B18	. E8 D0D70400	CALL Pixtopia.004562ED	
00408B1D	. 5E	POP ESI	
00408B1E	. 5B	POP EBX	
00408B1F	. 8B3C24 34010	MOV ECX, DWORD PTR SS:[ESP+134]	
00408B26	. C1 890D 0000	MOV DWORD PTR FS:[0], ECX	

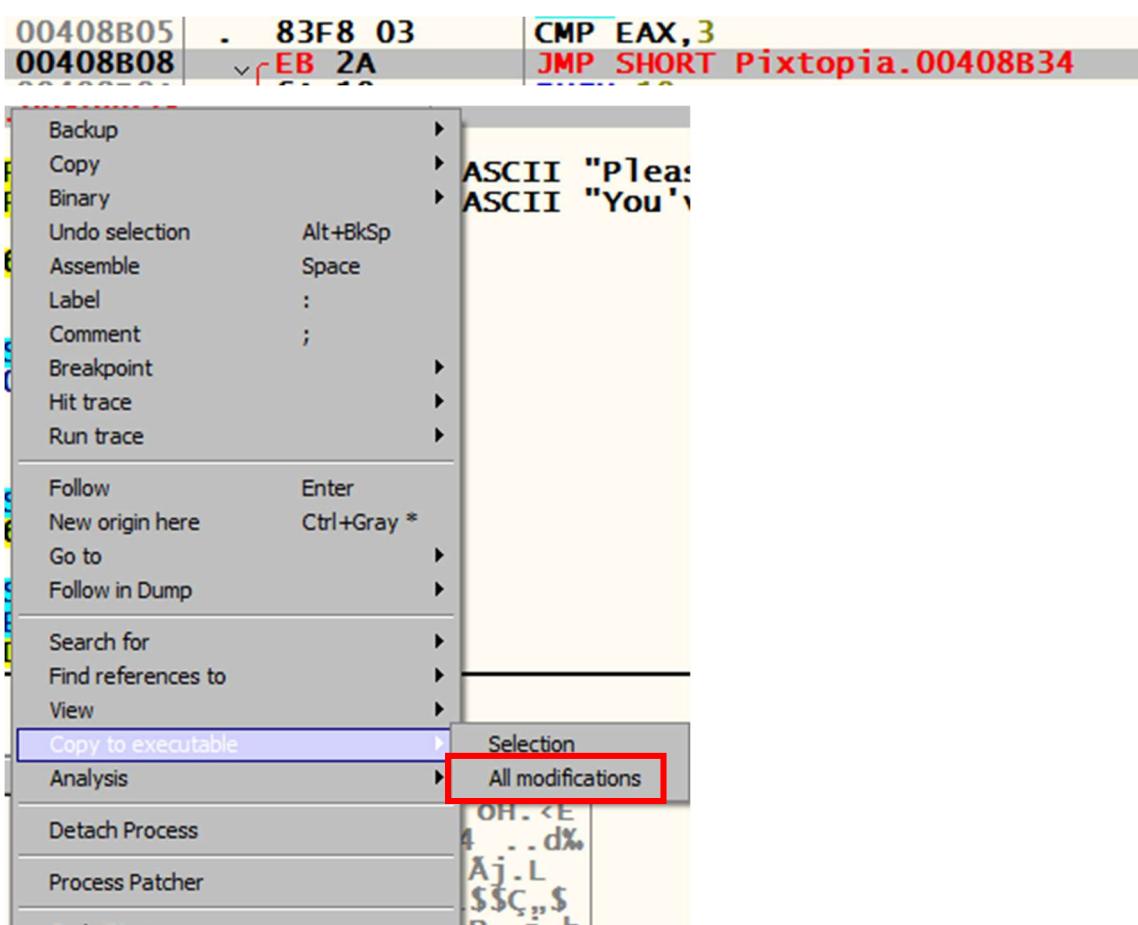
이 코드를 실행해보면 0x004088B08에서 점프를 안하고 실행되는 걸 볼 수 있다. 그럼 결국 그 창은 계속 발행하고 그룹은 3개 이상 만들지 못하는 걸 볼 수 있다.

그려려면 코드를 바꿔줘야하는데 JL (cmp a, b에서 a가 작을 때 점프)이 있는 부분을 바꾸거나 CMP EAX, 3을 바꿔줘야 한다.

1. JL을 바꾸는 경우는 위에 EAX와 3이 비교하므로 EAX가 커져도 점프할 수 있게 하려면 조건 없이 JMP 명령어로 바꾸는 것이 좋다. (JMP는 무조건 점프이기 때문에)
2. CMP를 바꾸는 경우는 위에 EAX와 3이 비교하므로 3이 아니라 더 큰 숫자로 바꾸는 방법이 있다. 하지만 숫자를 정해 놓으면 언젠가는 끝에 도달하니까 이 방법은 좋지 않은 방법이다.



0x00408B08 코드를 더블 클릭한 후 JL -> JMP로 바꿔서 코드를 수정해준다.

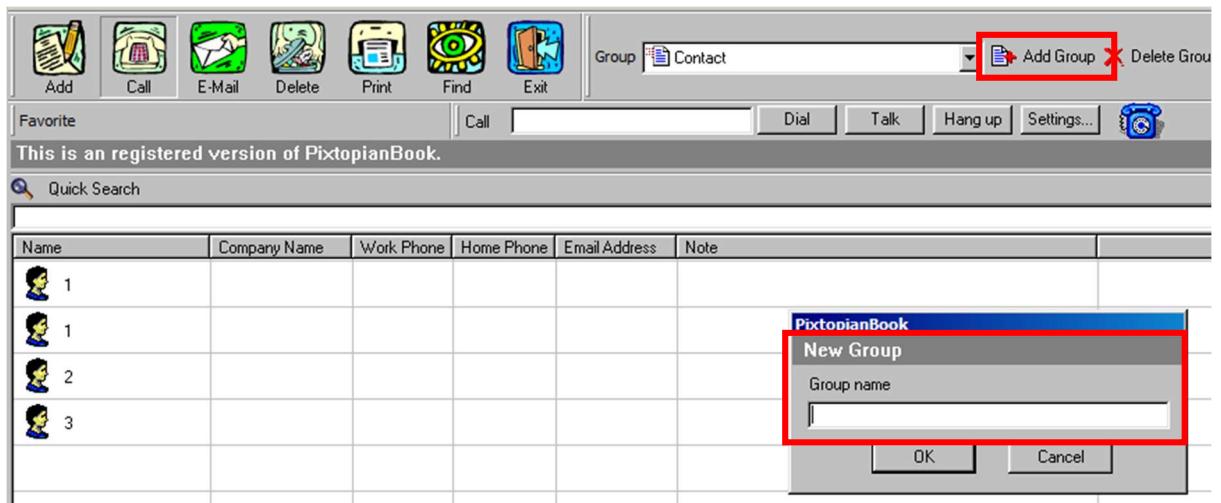


Copy to executable > All modifications > Copy All 누르면 Dump창이 나오는 걸 볼 수 있다.

오른쪽 마우스 클릭 > save file 하고 보면



생성이 확인된 걸 볼 수 있음.



PixtopianBook_4.exe를 실행 후 Add Group를 해보면 그룹을 더 추가할 수 있게 되었다.

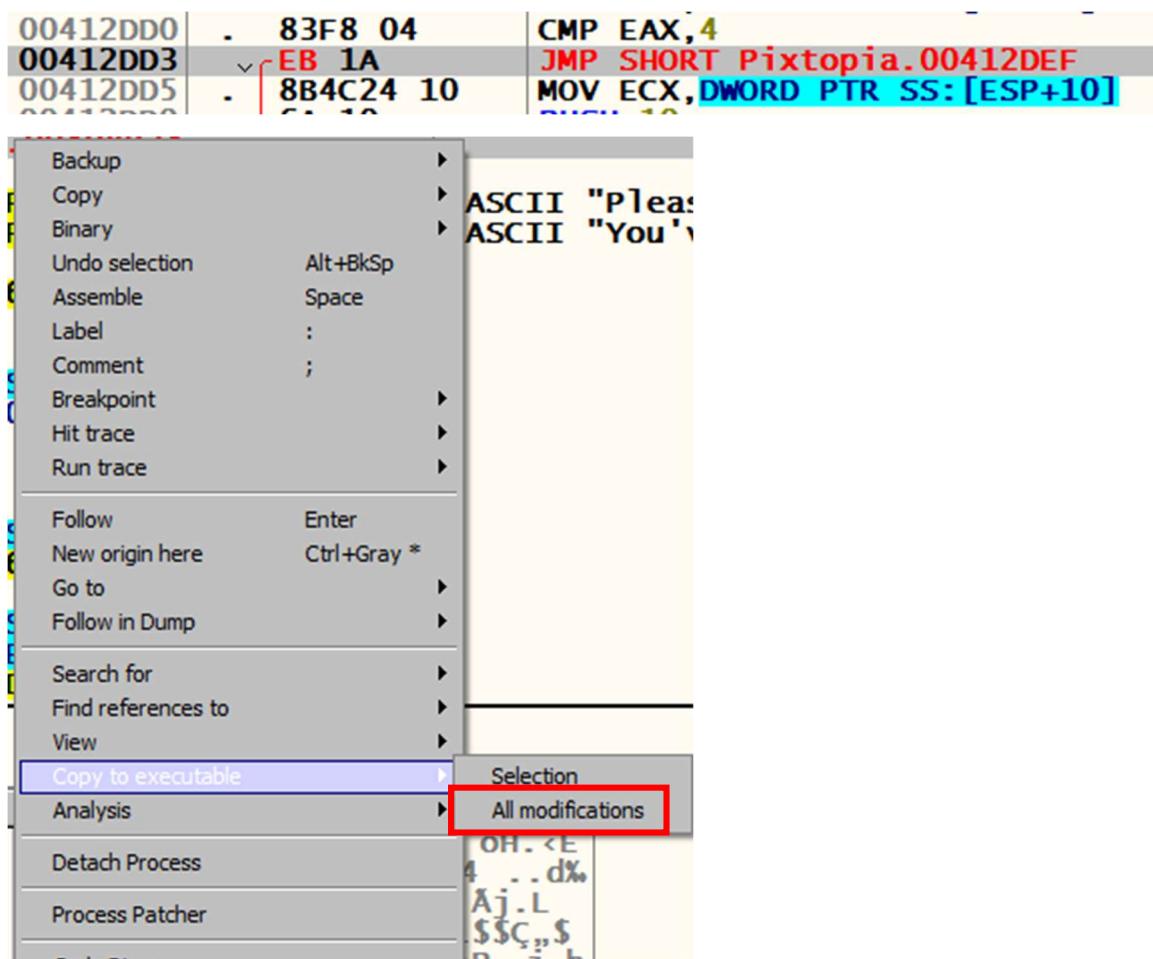
5) useradd 추가 창

PixtopianBook_4.exe를 이용하여 사용자를 더 추가할 수 있게 만들거다.

All references text strings에서 User Add 추가 창에 있던 문자열 중 You've reached the limit of 4 entries per group. 검색해 보면 아래와 같은 곳에 멈추는 걸 볼 수 있음.

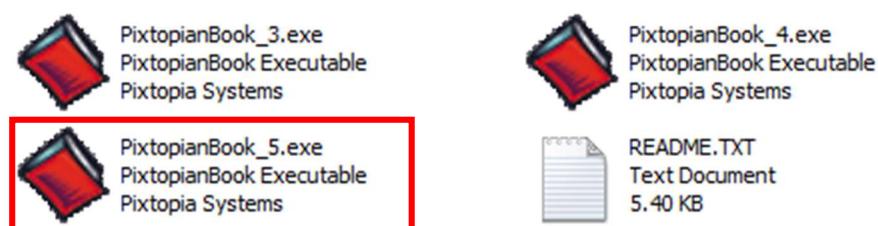
R Text strings referenced in Pixtopia:text		
Address	Disassembly	Text string
00412D99	PUSH Pixtopia.00476A78	ASCII "금H"
00412DBB	PUSH Pixtopia.0048F700	ASCII "Please register Pixtopianbook."
00412DE0	PUSH Pixtopia.0048FC68	ASCII "You've reached the limit of 4 entries per group."
00412E00	DU ₁ D ₂ D ₃ D ₄ D ₅ D ₆ D ₇ D ₈ D ₉ D ₁₀ D ₁₁ D ₁₂ D ₁₃ D ₁₄ D ₁₅ D ₁₆ D ₁₇ D ₁₈ D ₁₉ D ₂₀ D ₂₁ D ₂₂ D ₂₃ D ₂₄ D ₂₅ D ₂₆ D ₂₇ D ₂₈ D ₂₉ D ₃₀ D ₃₁ D ₃₂ D ₃₃ D ₃₄ D ₃₅ D ₃₆ D ₃₇ D ₃₈ D ₃₉ D ₄₀ D ₄₁ D ₄₂ D ₄₃ D ₄₄ D ₄₅ D ₄₆ D ₄₇ D ₄₈ D ₄₉ D ₅₀ D ₅₁ D ₅₂ D ₅₃ D ₅₄ D ₅₅ D ₅₆ D ₅₇ D ₅₈ D ₅₉ D ₆₀ D ₆₁ D ₆₂ D ₆₃ D ₆₄ D ₆₅ D ₆₆ D ₆₇ D ₆₈ D ₆₉ D ₇₀ D ₇₁ D ₇₂ D ₇₃ D ₇₄ D ₇₅ D ₇₆ D ₇₇ D ₇₈ D ₇₉ D ₈₀ D ₈₁ D ₈₂ D ₈₃ D ₈₄ D ₈₅ D ₈₆ D ₈₇ D ₈₈ D ₈₉ D ₉₀ D ₉₁ D ₉₂ D ₉₃ D ₉₄ D ₉₅ D ₉₆ D ₉₇ D ₉₈ D ₉₉ D ₁₀₀ D ₁₀₁ D ₁₀₂ D ₁₀₃ D ₁₀₄ D ₁₀₅ D ₁₀₆ D ₁₀₇ D ₁₀₈ D ₁₀₉ D ₁₁₀ D ₁₁₁ D ₁₁₂ D ₁₁₃ D ₁₁₄ D ₁₁₅ D ₁₁₆ D ₁₁₇ D ₁₁₈ D ₁₁₉ D ₁₂₀ D ₁₂₁ D ₁₂₂ D ₁₂₃ D ₁₂₄ D ₁₂₅ D ₁₂₆ D ₁₂₇ D ₁₂₈ D ₁₂₉ D ₁₃₀ D ₁₃₁ D ₁₃₂ D ₁₃₃ D ₁₃₄ D ₁₃₅ D ₁₃₆ D ₁₃₇ D ₁₃₈ D ₁₃₉ D ₁₄₀ D ₁₄₁ D ₁₄₂ D ₁₄₃ D ₁₄₄ D ₁₄₅ D ₁₄₆ D ₁₄₇ D ₁₄₈ D ₁₄₉ D ₁₅₀ D ₁₅₁ D ₁₅₂ D ₁₅₃ D ₁₅₄ D ₁₅₅ D ₁₅₆ D ₁₅₇ D ₁₅₈ D ₁₅₉ D ₁₆₀ D ₁₆₁ D ₁₆₂ D ₁₆₃ D ₁₆₄ D ₁₆₅ D ₁₆₆ D ₁₆₇ D ₁₆₈ D ₁₆₉ D ₁₇₀ D ₁₇₁ D ₁₇₂ D ₁₇₃ D ₁₇₄ D ₁₇₅ D ₁₇₆ D ₁₇₇ D ₁₇₈ D ₁₇₉ D ₁₈₀ D ₁₈₁ D ₁₈₂ D ₁₈₃ D ₁₈₄ D ₁₈₅ D ₁₈₆ D ₁₈₇ D ₁₈₈ D ₁₈₉ D ₁₉₀ D ₁₉₁ D ₁₉₂ D ₁₉₃ D ₁₉₄ D ₁₉₅ D ₁₉₆ D ₁₉₇ D ₁₉₈ D ₁₉₉ D ₂₀₀ D ₂₀₁ D ₂₀₂ D ₂₀₃ D ₂₀₄ D ₂₀₅ D ₂₀₆ D ₂₀₇ D ₂₀₈ D ₂₀₉ D ₂₁₀ D ₂₁₁ D ₂₁₂ D ₂₁₃ D ₂₁₄ D ₂₁₅ D ₂₁₆ D ₂₁₇ D ₂₁₈ D ₂₁₉ D ₂₂₀ D ₂₂₁ D ₂₂₂ D ₂₂₃ D ₂₂₄ D ₂₂₅ D ₂₂₆ D ₂₂₇ D ₂₂₈ D ₂₂₉ D ₂₃₀ D ₂₃₁ D ₂₃₂ D ₂₃₃ D ₂₃₄ D ₂₃₅ D ₂₃₆ D ₂₃₇ D ₂₃₈ D ₂₃₉ D ₂₄₀ D ₂₄₁ D ₂₄₂ D ₂₄₃ D ₂₄₄ D ₂₄₅ D ₂₄₆ D ₂₄₇ D ₂₄₈ D ₂₄₉ D ₂₅₀ D ₂₅₁ D ₂₅₂ D ₂₅₃ D ₂₅₄ D ₂₅₅ D ₂₅₆ D ₂₅₇ D ₂₅₈ D ₂₅₉ D ₂₆₀ D ₂₆₁ D ₂₆₂ D ₂₆₃ D ₂₆₄ D ₂₆₅ D ₂₆₆ D ₂₆₇ D ₂₆₈ D ₂₆₉ D ₂₇₀ D ₂₇₁ D ₂₇₂ D ₂₇₃ D ₂₇₄ D ₂₇₅ D ₂₇₆ D ₂₇₇ D ₂₇₈ D ₂₇₉ D ₂₈₀ D ₂₈₁ D ₂₈₂ D ₂₈₃ D ₂₈₄ D ₂₈₅ D ₂₈₆ D ₂₈₇ D ₂₈₈ D ₂₈₉ D ₂₉₀ D ₂₉₁ D ₂₉₂ D ₂₉₃ D ₂₉₄ D ₂₉₅ D ₂₉₆ D ₂₉₇ D ₂₉₈ D ₂₉₉ D ₃₀₀ D ₃₀₁ D ₃₀₂ D ₃₀₃ D ₃₀₄ D ₃₀₅ D ₃₀₆ D ₃₀₇ D ₃₀₈ D ₃₀₉ D ₃₁₀ D ₃₁₁ D ₃₁₂ D ₃₁₃ D ₃₁₄ D ₃₁₅ D ₃₁₆ D ₃₁₇ D ₃₁₈ D ₃₁₉ D ₃₂₀ D ₃₂₁ D ₃₂₂ D ₃₂₃ D ₃₂₄ D ₃₂₅ D ₃₂₆ D ₃₂₇ D ₃₂₈ D ₃₂₉ D ₃₃₀ D ₃₃₁ D ₃₃₂ D ₃₃₃ D ₃₃₄ D ₃₃₅ D ₃₃₆ D ₃₃₇ D ₃₃₈ D ₃₃₉ D ₃₄₀ D ₃₄₁ D ₃₄₂ D ₃₄₃ D ₃₄₄ D ₃₄₅ D ₃₄₆ D ₃₄₇ D ₃₄₈ D ₃₄₉ D ₃₅₀ D ₃₅₁ D ₃₅₂ D ₃₅₃ D ₃₅₄ D ₃₅₅ D ₃₅₆ D ₃₅₇ D ₃₅₈ D ₃₅₉ D ₃₆₀ D ₃₆₁ D ₃₆₂ D ₃₆₃ D ₃₆₄ D ₃₆₅ D ₃₆₆ D ₃₆₇ D ₃₆₈ D ₃₆₉ D ₃₇₀ D ₃₇₁ D ₃₇₂ D ₃₇₃ D ₃₇₄ D ₃₇₅ D ₃₇₆ D ₃₇₇ D ₃₇₈ D ₃₇₉ D ₃₈₀ D ₃₈₁ D ₃₈₂ D ₃₈₃ D ₃₈₄ D ₃₈₅ D ₃₈₆ D ₃₈₇ D ₃₈₈ D ₃₈₉ D ₃₉₀ D ₃₉₁ D ₃₉₂ D ₃₉₃ D ₃₉₄ D ₃₉₅ D ₃₉₆ D ₃₉₇ D ₃₉₈ D ₃₉₉ D ₄₀₀ D ₄₀₁ D ₄₀₂ D ₄₀₃ D ₄₀₄ D ₄₀₅ D ₄₀₆ D ₄₀₇ D ₄₀₈ D ₄₀₉ D ₄₁₀ D ₄₁₁ D ₄₁₂ D ₄₁₃ D ₄₁₄ D ₄₁₅ D ₄₁₆ D ₄₁₇ D ₄₁₈ D ₄₁₉ D ₄₂₀ D ₄₂₁ D ₄₂₂ D ₄₂₃ D ₄₂₄ D ₄₂₅ D ₄₂₆ D ₄₂₇ D ₄₂₈ D ₄₂₉ D ₄₃₀ D ₄₃₁ D ₄₃₂ D ₄₃₃ D ₄₃₄ D ₄₃₅ D ₄₃₆ D ₄₃₇ D ₄₃₈ D ₄₃₉ D ₄₄₀ D ₄₄₁ D ₄₄₂ D ₄₄₃ D ₄₄₄ D ₄₄₅ D ₄₄₆ D ₄₄₇ D ₄₄₈ D ₄₄₉ D ₄₅₀ D ₄₅₁ D ₄₅₂ D ₄₅₃ D ₄₅₄ D ₄₅₅ D ₄₅₆ D ₄₅₇ D ₄₅₈ D ₄₅₉ D ₄₆₀ D ₄₆₁ D ₄₆₂ D ₄₆₃ D ₄₆₄ D ₄₆₅ D ₄₆₆ D ₄₆₇ D ₄₆₈ D ₄₆₉ D ₄₇₀ D ₄₇₁ D ₄₇₂ D ₄₇₃ D ₄₇₄ D ₄₇₅ D ₄₇₆ D ₄₇₇ D ₄₇₈ D ₄₇₉ D ₄₈₀ D ₄₈₁ D ₄₈₂ D ₄₈₃ D ₄₈₄ D ₄₈₅ D ₄₈₆ D ₄₈₇ D ₄₈₈ D ₄₈₉ D ₄₉₀ D ₄₉₁ D ₄₉₂ D ₄₉₃ D ₄₉₄ D ₄₉₅ D ₄₉₆ D ₄₉₇ D ₄₉₈ D ₄₉₉ D ₅₀₀ D ₅₀₁ D ₅₀₂ D ₅₀₃ D ₅₀₄ D ₅₀₅ D ₅₀₆ D ₅₀₇ D ₅₀₈ D ₅₀₉ D ₅₁₀ D ₅₁₁ D ₅₁₂ D ₅₁₃ D ₅₁₄ D ₅₁₅ D ₅₁₆ D ₅₁₇ D ₅₁₈ D ₅₁₉ D ₅₂₀ D ₅₂₁ D ₅₂₂ D ₅₂₃ D ₅₂₄ D ₅₂₅ D ₅₂₆ D ₅₂₇ D ₅₂₈ D ₅₂₉ D ₅₃₀ D ₅₃₁ D ₅₃₂ D ₅₃₃ D ₅₃₄ D ₅₃₅ D ₅₃₆ D ₅₃₇ D ₅₃₈ D ₅₃₉ D ₅₄₀ D ₅₄₁ D ₅₄₂ D ₅₄₃ D ₅₄₄ D ₅₄₅ D ₅₄₆ D ₅₄₇ D ₅₄₈ D ₅₄₉ D ₅₅₀ D ₅₅₁ D ₅₅₂ D ₅₅₃ D ₅₅₄ D ₅₅₅ D ₅₅₆ D ₅₅₇ D ₅₅₈ D ₅₅₉ D ₅₆₀ D ₅₆₁ D ₅₆₂ D ₅₆₃ D ₅₆₄ D ₅₆₅ D ₅₆₆ D ₅₆₇ D ₅₆₈ D ₅₆₉ D ₅₇₀ D ₅₇₁ D ₅₇₂ D ₅₇₃ D ₅₇₄ D ₅₇₅ D ₅₇₆ D ₅₇₇ D ₅₇₈ D ₅₇₉ D ₅₈₀ D ₅₈₁ D ₅₈₂ D ₅₈₃ D ₅₈₄ D ₅₈₅ D ₅₈₆ D ₅₈₇ D ₅₈₈ D ₅₈₉ D ₅₉₀ D ₅₉₁ D ₅₉₂ D ₅₉₃ D ₅₉₄ D ₅₉₅ D ₅₉₆ D ₅₉₇ D ₅₉₈ D ₅₉₉ D ₆₀₀ D ₆₀₁ D ₆₀₂ D ₆₀₃ D ₆₀₄ D ₆₀₅ D ₆₀₆ D ₆₀₇ D ₆₀₈ D ₆₀₉ D ₆₁₀ D ₆₁₁ D ₆₁₂ D ₆₁₃ D ₆₁₄ D ₆₁₅ D ₆₁₆ D ₆₁₇ D ₆₁₈ D ₆₁₉ D ₆₂₀ D ₆₂₁ D ₆₂₂ D ₆₂₃ D ₆₂₄ D ₆₂₅ D ₆₂₆ D ₆₂₇ D ₆₂₈ D ₆₂₉ D ₆₃₀ D ₆₃₁ D ₆₃₂ D ₆₃₃ D ₆₃₄ D ₆₃₅ D ₆₃₆ D ₆₃₇ D ₆₃₈ D ₆₃₉ D ₆₄₀ D ₆₄₁ D ₆₄₂ D ₆₄₃ D ₆₄₄ D ₆₄₅ D ₆₄₆ D ₆₄₇ D ₆₄₈ D ₆₄₉ D ₆₅₀ D ₆₅₁ D ₆₅₂ D ₆₅₃ D ₆₅₄ D ₆₅₅ D ₆₅₆ D ₆₅₇ D ₆₅₈ D ₆₅₉ D ₆₆₀ D ₆₆₁ D ₆₆₂ D ₆₆₃ D ₆₆₄ D ₆₆₅ D ₆₆₆ D ₆₆₇ D ₆₆₈ D ₆₆₉ D ₆₇₀ D ₆₇₁ D ₆₇₂ D ₆₇₃ D ₆₇₄ D ₆₇₅ D ₆₇₆ D ₆₇₇ D ₆₇₈ D ₆₇₉ D ₆₈₀ D ₆₈₁ D ₆₈₂ D ₆₈₃ D ₆₈₄ D ₆₈₅ D ₆₈₆ D ₆₈₇ D ₆₈₈ D ₆₈₉ D ₆₉₀ D ₆₉₁ D ₆₉₂ D ₆₉₃ D ₆₉₄ D ₆₉₅ D ₆₉₆ D ₆₉₇ D ₆₉₈ D ₆₉₉ D ₇₀₀ D ₇₀₁ D ₇₀₂ D ₇₀₃ D ₇₀₄ D ₇₀₅ D ₇₀₆ D ₇₀₇ D ₇₀₈ D ₇₀₉ D ₇₁₀ D ₇₁₁ D ₇₁₂ D ₇₁₃ D ₇₁₄ D ₇₁₅ D ₇₁₆ D ₇₁₇ D ₇₁₈ D ₇₁₉ D ₇₂₀ D ₇₂₁ D ₇₂₂ D ₇₂₃ D ₇₂₄ D ₇₂₅ D ₇₂₆ D ₇₂₇ D ₇₂₈ D ₇₂₉ D ₇₃₀ D ₇₃₁ D ₇₃₂ D ₇₃₃ D ₇₃₄ D ₇₃₅ D ₇₃₆ D ₇₃₇ D ₇₃₈ D ₇₃₉ D ₇₄₀ D ₇₄₁ D ₇₄₂ D ₇₄₃ D ₇₄₄ D ₇₄₅ D ₇₄₆ D ₇₄₇ D ₇₄₈ D ₇₄₉ D ₇₅₀ D ₇₅₁ D ₇₅₂ D ₇₅₃ D ₇₅₄ D ₇₅₅ D ₇₅₆ D ₇₅₇ D ₇₅₈ D ₇₅₉ D ₇₆₀ D ₇₆₁ D ₇₆₂ D ₇₆₃ D ₇₆₄ D ₇₆₅ D ₇₆₆ D ₇₆₇ D ₇₆₈ D ₇₆₉ D ₇₇₀ D ₇₇₁ D ₇₇₂ D ₇₇₃ D ₇₇₄ D ₇₇₅ D ₇₇₆ D ₇₇₇ D ₇₇₈ D ₇₇₉ D ₇₈₀ D ₇₈₁ D ₇₈₂ D ₇₈₃ D ₇₈₄ D ₇₈₅ D ₇₈₆ D ₇₈₇ D ₇₈₈ D ₇₈₉ D ₇₉₀ D ₇₉₁ D ₇₉₂ D ₇₉₃ D ₇₉₄ D ₇₉₅ D ₇₉₆ D ₇₉₇ D ₇₉₈ D ₇₉₉ D ₈₀₀ D ₈₀₁ D ₈₀₂ D ₈₀₃ D ₈₀₄ D ₈₀₅ D ₈₀₆ D ₈₀₇ D ₈₀₈ D ₈₀₉ D ₈₁₀ D ₈₁₁ D ₈₁₂ D ₈₁₃ D ₈₁₄ D ₈₁₅ D ₈₁₆ D ₈₁₇ D ₈₁₈ D ₈₁₉ D ₈₂₀ D ₈₂₁ D ₈₂₂ D ₈₂₃ D ₈₂₄ D ₈₂₅ D ₈₂₆ D ₈₂₇ D ₈₂₈ D ₈₂₉ D ₈₃₀ D ₈₃₁ D ₈₃₂ D ₈₃₃ D ₈₃₄ D ₈₃₅ D ₈₃₆ D ₈₃₇ D ₈₃₈ D ₈₃₉ D ₈₄₀ D ₈₄₁ D ₈₄₂ D ₈₄₃ D ₈₄₄ D ₈₄₅ D ₈₄₆ D ₈₄₇ D ₈₄₈ D ₈₄₉ D ₈₅₀ D ₈₅₁ D ₈₅₂ D ₈₅₃ D ₈₅₄ D ₈₅₅ D ₈₅₆ D ₈₅₇ D ₈₅₈ D ₈₅₉ D ₈₆₀ D ₈₆₁ D ₈₆₂ D ₈₆₃ D ₈₆₄ D ₈₆₅ D ₈₆₆ D ₈₆₇ D ₈₆₈ D ₈₆₉ D ₈₇₀ D ₈₇₁ D ₈₇₂ D ₈₇₃ D ₈₇₄ D ₈₇₅ D ₈₇₆ D ₈₇₇ D ₈₇₈ D ₈₇₉ D ₈₈₀ D ₈₈₁ D ₈₈₂ D ₈₈₃ D ₈₈₄ D ₈₈₅ D ₈₈₆ D ₈₈₇ D ₈₈₈ D ₈₈₉ D ₈₉₀ D ₈₉₁ D ₈₉₂ D ₈₉₃ D ₈₉₄ D ₈₉₅ D ₈₉₆ D ₈₉₇ D ₈₉₈ D ₈₉₉ D ₉₀₀ D ₉₀₁ D ₉₀₂ D ₉₀₃ D ₉₀₄ D ₉₀₅ D ₉₀₆ D ₉₀₇ D ₉₀₈ D ₉₀₉ D ₉₁₀ D ₉₁₁ D ₉₁₂ D ₉₁₃ D ₉₁₄ D ₉₁₅ D ₉₁₆ D ₉₁₇ D ₉₁₈ D ₉₁₉ D ₉₂₀ D ₉₂₁ D ₉₂₂ D ₉₂₃ D ₉₂₄ D ₉₂₅ D ₉₂₆ D ₉₂₇ D ₉₂₈ D ₉₂₉ D ₉₃₀ D ₉₃₁ D ₉₃₂ D ₉₃₃ D ₉₃₄ D ₉₃₅ D ₉₃₆ D ₉₃₇ D ₉₃₈ D ₉₃₉ D ₉₄₀ D ₉₄₁ D ₉₄₂ D ₉₄₃ D ₉₄₄ D ₉₄₅ D ₉₄₆ D ₉₄₇ D ₉₄₈ D ₉₄₉ D ₉₅₀ D ₉₅₁ D ₉₅₂ D ₉₅₃ D ₉₅₄ D ₉₅₅ D ₉₅₆ D ₉₅₇ D ₉₅₈ D ₉₅₉ D ₉₆₀ D ₉₆₁ D ₉₆₂ D ₉₆₃ D ₉₆₄ D ₉₆₅ D ₉₆₆ D ₉₆₇ D ₉₆₈ D ₉₆₉ D ₉₇₀ D ₉₇₁ D ₉₇₂ D ₉₇₃ D ₉₇₄ D ₉₇₅ D ₉₇₆ D ₉₇₇ D ₉₇₈ D ₉₇₉ D ₉₈₀ D ₉₈₁ D ₉₈₂ D ₉₈₃ D ₉₈₄ D ₉₈₅ D ₉₈₆ D ₉₈₇ D ₉₈₈ D ₉₈₉ D ₉₉₀ D ₉₉₁ D ₉₉₂ D ₉₉₃ D ₉₉₄ D ₉₉₅ D ₉₉₆ D ₉₉₇ D ₉₉₈ D ₉₉₉ D ₁₀₀₀ D ₁₀₀₁ D ₁₀₀₂ D ₁₀₀₃ D ₁₀₀₄ D ₁₀₀₅ D ₁₀₀₆ D ₁₀₀₇ D ₁₀₀₈ D ₁₀₀₉ D ₁₀₁₀ D ₁₀₁₁ D ₁₀₁₂ D ₁₀₁₃ D ₁₀₁₄ D ₁₀₁₅ D ₁₀₁₆ D ₁₀₁₇ D ₁₀₁₈ D ₁₀₁₉ D ₁₀₂₀ D ₁₀₂₁ D ₁₀₂₂ D ₁₀₂₃ D ₁₀₂₄ D ₁₀₂₅ D ₁₀₂₆ D ₁₀₂₇ D ₁₀₂₈ D ₁₀₂₉ D ₁₀₃₀ D ₁₀₃₁ D ₁₀₃₂ D ₁₀₃₃ D ₁₀₃₄ D ₁₀₃₅ D ₁₀₃₆ D ₁₀₃₇ D ₁₀₃₈ D ₁₀₃₉ D ₁₀₄₀ D ₁₀₄₁ D ₁₀₄₂ D ₁₀₄₃ D ₁₀₄₄ D ₁₀₄₅ D ₁₀₄₆ D ₁₀₄₇ D ₁₀₄₈ D ₁₀₄₉ D ₁₀₅₀ D ₁₀₅₁ D ₁₀₅₂ D ₁₀₅₃ D ₁₀₅₄ D ₁₀₅₅ D ₁₀₅₆ D ₁₀₅₇ D ₁₀₅₈ D ₁₀₅₉ D ₁₀₆₀ D ₁₀₆₁ D ₁₀₆₂ D ₁₀₆₃ D ₁₀₆₄ D ₁₀₆₅ D ₁₀₆₆ D ₁₀₆₇ D ₁₀₆₈ D ₁₀₆₉ D ₁₀₇₀ D ₁₀₇₁ D ₁₀₇₂ D ₁₀₇₃ D ₁₀₇₄ D ₁₀₇₅ D ₁₀₇₆ D ₁₀₇₇ D ₁₀₇₈ D ₁₀₇₉ D ₁₀₈₀ D ₁₀₈₁ D ₁₀₈₂ D ₁₀₈₃ D ₁₀₈₄ D ₁₀₈₅ D ₁₀₈₆ D ₁₀₈₇ D ₁₀₈₈ D ₁₀₈₉ D ₁₀₉₀ D ₁₀₉₁ D ₁₀₉₂ D ₁₀₉₃ D ₁₀₉₄ D ₁₀₉₅ D ₁₀₉₆ D ₁₀₉₇ D ₁₀₉₈ D ₁₀₉₉ D ₁₁₀₀ D ₁₁₀₁ D ₁₁₀₂ D ₁₁₀₃ D ₁₁₀₄ D ₁₁₀₅ D ₁₁₀₆ D ₁₁₀₇ D ₁₁₀₈ D ₁₁₀₉ D ₁₁₁₀ D ₁₁₁₁ D ₁₁₁₂ D ₁₁₁₃ D ₁₁₁₄ D ₁₁₁₅ D ₁₁₁₆ D ₁₁₁₇ D ₁₁₁₈ D ₁₁₁₉ D ₁₁₂₀ D ₁₁₂₁ D ₁₁₂₂ D ₁₁₂₃ D ₁₁₂₄ D ₁₁₂₅ D ₁₁₂₆ D ₁₁₂₇ D ₁₁₂₈ D ₁₁₂₉ D ₁₁₃₀ D ₁₁₃₁ D ₁₁₃₂ D ₁₁₃₃ D ₁₁₃₄ D ₁₁₃₅ D ₁₁₃₆ D ₁₁₃₇ D ₁₁₃₈ D ₁₁₃₉ D ₁₁₄₀ D ₁₁₄₁ D ₁₁₄₂ D ₁₁₄₃ D ₁₁₄₄ D ₁₁₄₅ D ₁₁₄₆ D ₁₁₄₇ D ₁₁₄₈ D ₁₁₄₉ D ₁₁₅₀ D ₁₁₅₁ D ₁₁₅₂ D ₁₁₅₃ D ₁₁₅₄ D ₁₁₅₅ D ₁₁₅₆ D ₁₁₅₇ D ₁₁₅₈ D ₁₁₅₉ D ₁₁₆₀ D ₁₁₆₁ D ₁₁₆₂ D<sub	

0x00412DD3코드를 더블 클릭한 후 JL -> JMP로 바꿔서 코드를 수정해준다.

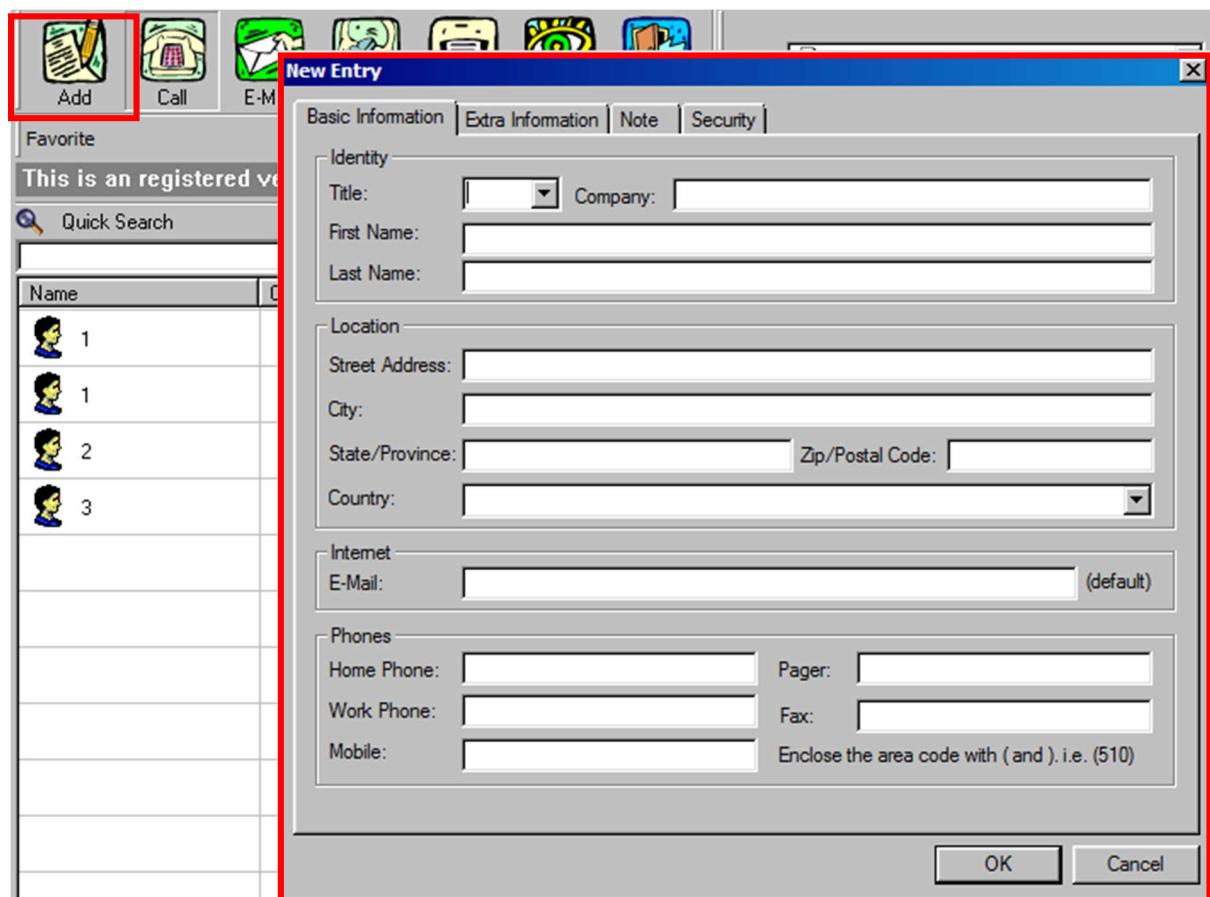


Copy to executable > All modifications > Copy All 누르면 Dump창이 나오는 걸 볼 수 있다.

오른쪽 마우스 클릭 > save file 하고 보면



생성이 확인된 걸 볼 수 있음.



PixtopianBook_5.exe를 실행 후 Add를 해보면 그룹을 더 추가할 수 있게 되었다.

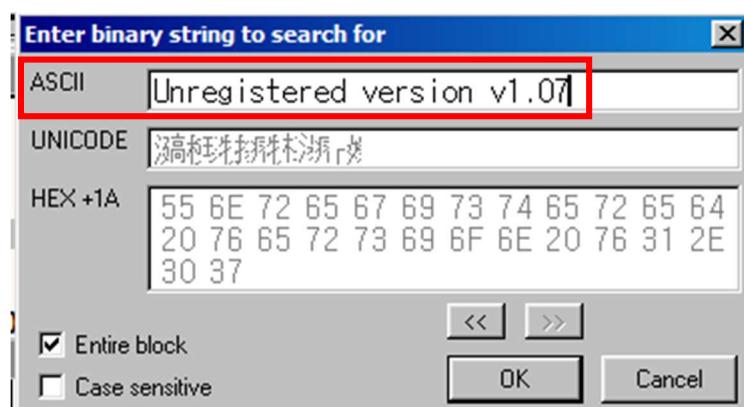
5) Help 창

PixtopianBook_5.exe를 이용하여 Help 창의 문자열을 변경할거다.

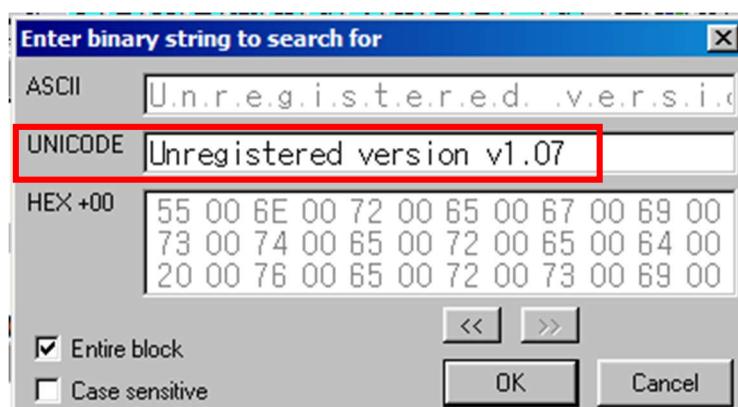
All references text strings에서 타이틀 창 있던 문자열 중 Unregistered version v1.07 검색해 보면 검색이 안됨. 그럼 “Memory map” 을 눌러서 검색을 해줌.

M Memory map									
Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as	
00010000	00010000				Map	RW	RW		
00020000	00001000				Priv	RW	RW		
0012D000	00001000				Priv	RW	Guard	RW	
0012E000	00002000			stack of ma	Priv	RW	Guard	RW	
00130000	00004000				Map	R	R		
00140000	00001000				Priv	RW	RW		
00150000	00067000				Map	R	R	#Device#HarddiskVc	
001C0000	00001000				Priv	RW	RW		
001D0000	00001000				Priv	RW	RW		
00280000	0002E000				Priv	RW	RW		
00400000	00001000	Pixtopia	PE header		Image	R	RWE		
00401000	00074000	Pixtopia	.text	code	Image	R	RWE		

‘Home’ 키를 눌러서 맨 위로 올라간 다음 Search 클릭.



현재 창이 나타나고 ‘Shift+Insert’ 키를 이용하여 로그인 창에 있던 문자열 중 Unregistered version v1.07를 ASCII에 검색해 보면 검색이 안됨.

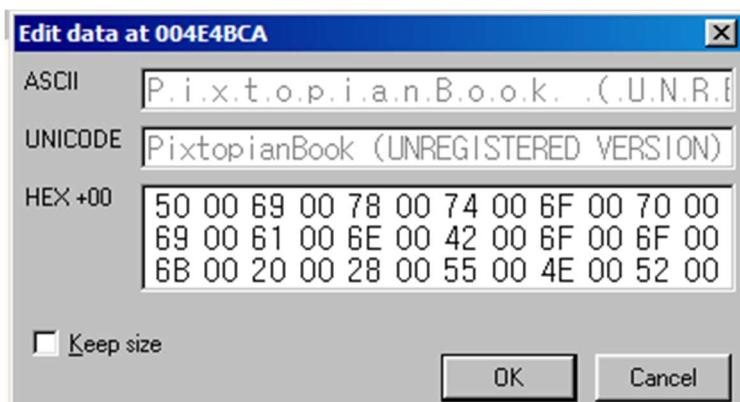


이번에는 Unregistered version v1.07를 UNICODE에 검색해 보면 검색이되어서 아래 창이

발생하는 걸 볼 수 있음.

D Dump - Pixtopia:rsrc 0049D000..004E8FFF															
004D4810	00	00	00	00	00	00	00	00	00	00	00	00	02	501P
004D4820	07	00	76	00	56	00	08	00	FF	FF	FF	FF	FF	82	00
004D4830	55	00	6E	00	72	00	65	00	67	00	69	00	73	00	74
004D4840	65	00	72	00	65	00	64	00	20	00	76	00	65	00	72
004D4850	73	00	69	00	6F	00	6E	00	20	00	76	00	31	00	2E
004D4860	30	00	37	00	00	00	00	00	01	00	FF	FF	00	00	00
004D4870	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

메모리 주소 0x004D4830부터 시작하는 걸 볼 수 있음.

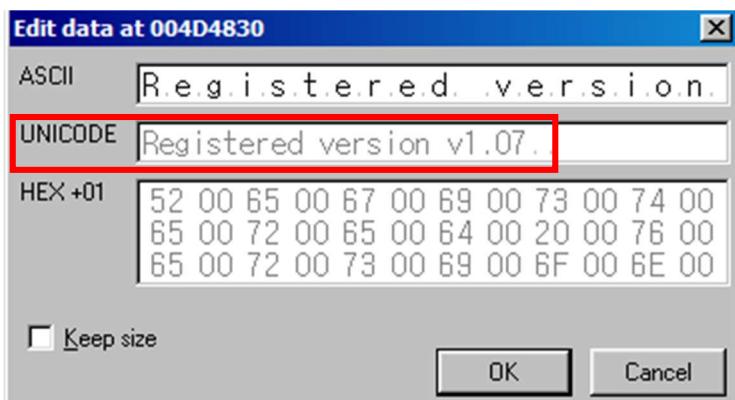


'ctrl+e' 키 누르면 위의 창이 나오는 걸 볼 수 있음.

Unregistered version v1.07 -> Registered version v1.07으로 변경해줘야함. 'UN'을 삭제 해주고 R을 대문자로 바꿔줘야하는데 우선은 현재의 사이즈랑 바꿨을 때 사이즈를 같게 해줘야함.

한 문자에 2byte인데 총 2개를 삭제해야하니까 'UN'을 삭제 후 뒤에 '00 00 00 00'을 추가해줘야함. 여기서 Keep size를 체크하면 크기 유지 때문에 삭제가 안되기 때문에 체크를 풀어주고 해야함.

그리고 대문자 'R'로 바꿔줘야함.



```

D Dump - Pixtopia:.rsrc 0049D000..004E8FFF
004D4810 00 00 00 00|00 00 00 00|00 00 00 00|00 00 02 50|. .....
004D4820 07 00 76 00|56 00 08 00|FF FF FF FF|FF FF 82 00|•.v.V. .
004D4830 52 00 65 00|67 00 69 00|73 00 74 00|65 00 72 00|R.e.g.i.s.t.e.r.
004D4840 65 00 64 00|20 00 76 00|65 00 72 00|73 00 69 00|e.d. .v.e.r.s.i.
004D4850 6F 00 6E 00|20 00 76 00|31 00 2E 00|30 00 37 00|o.n. .v.1...0.7.
004D4860 00 00 00 00|00 00 00 00|01 00 FF FF|00 00 00 00|.....
004D4870 00 00 00 00|40 00 00 40|04 00 00 00|00 00 41 00|....@...@....A.

```

바뀐 걸 볼 수 있음.

메모리 부분에 오른쪽 마우스 클릭 > Copy to executable file 누른 후 하나의 Dump창이 생기는 걸 볼 수 있는데 거기서 오른쪽 마우스 클릭 > save file



생성이 확인된 걸 볼 수 있음.



이걸 실행해보면 바뀐 걸 볼 수 있음.

-> 이거는 리버싱이라기보다는 사용자와 그룹을 더 추가시키는 것까지 바꾸기 때문에 크랙에 더 가까움.

문제 해결!

★ 여기서 중요한 점

All references text strings과 Memory map의 차이점!

All references text strings은 코드에서 참조한 문자열만 찾을 수 있음. 즉, 코드 창에서 'PUSH' 명령어를 이용해서 주소를 참조한 코드만 볼 수 있음.

Memory map은 메모리에 저장된 문자열만 볼 수 있음. Memory map에서는 참조된 문자열도 볼 수 있음.

CPU - main thread, module Pixtopia	
0040C22B	. 5B POP EBX
0040C22C	. C2 0400 RETN 4
> 0040C22F	> 81FD 07090000 CMP EBP, 907
0040C235	..> 75 1A JNE SHORT Pixtopia.0040C251
0040C237	. 68 74F94800 PUSH Pixtopia.0048F974
0040C23C	RRCC MOV ECX ECX

All references text strings에서 찾은 것을 들어가보면 PUSH Pixtopia.0048F974가 있는 걸 볼 수 있음.

Address	Hex dump	ASCII
0048F974	54 68 69 73 20 69 73 20 61 6E 20 75 6E 72 65 67	This is an unreg
0048F984	69 73 74 65 72 65 64 20 76 65 72 73 69 6F 6E 20	istered version
0048F994	6F 66 20 50 69 78 74 6F 70 69 61 6E 42 6F 6F 6B	of PixtopianBook
0048F9A4	2E 20 50 6C 65 61 73 65 20 72 65 67 69 73 74 65	. Please registe
0048F9B4	72 20 74 6F 64 61 79 21 00 00 00 00 43 49 6E 69	r today!....CIni
0048F9C4	74 44 69 61 6C 6F 67 42 61 72 00 00 43 4C 65 66	tDialogBar..CLef

0x0048F974를 메모리 창에서 찾아보면 있는 걸 확인할 수 있음.

M Memory map	
Address	Size
01000	D Dump - Pixtopia:.data 0048F000..0049CFFF
02000	0048F974 54 68 69 73 20 69 73 20 61 6E 20 75 6E 72 65 67
12D00	0048F984 69 73 74 65 72 65 64 20 76 65 72 73 69 6F 6E 20
12E00	0048F994 6F 66 20 50 69 78 74 6F 70 69 61 6E 42 6F 6F 6B
13000	0048F9A4 2E 20 50 6C 65 61 73 65 20 72 65 67 69 73 74 65
14000	0048F9B4 72 20 74 6F 64 61 79 21 00 00 00 00 43 49 6E 69
15000	0048F9C4 74 44 69 61 6C 6F 67 42 61 72 00 00 43 4C 65 66

Memory Map에서도 볼 수 있음.

즉, 'PUSH'를 이용해서 주소를 참조를 해도 그 주소에 문자열이 메모리에 저장되어 있는 것과 같음.

그래서 All references text strings에서 먼저 찾아보고 없으면 Memory map에서 찾아보는 거다.