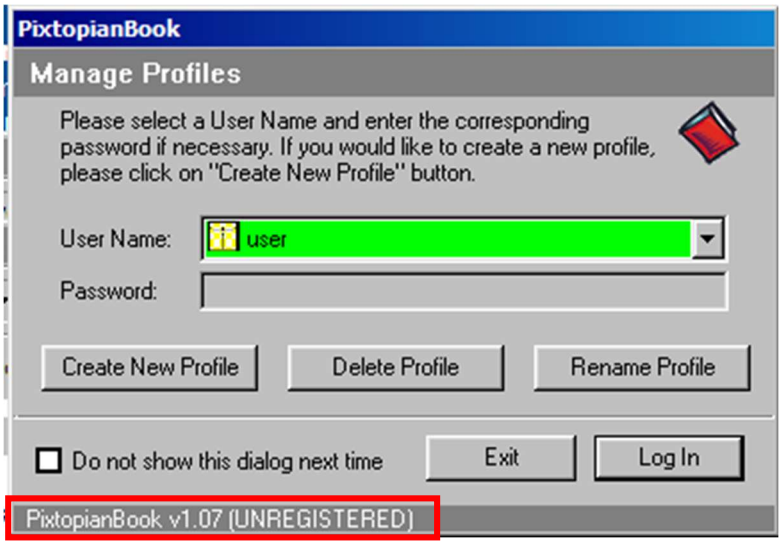
악성코드 분석 보고서

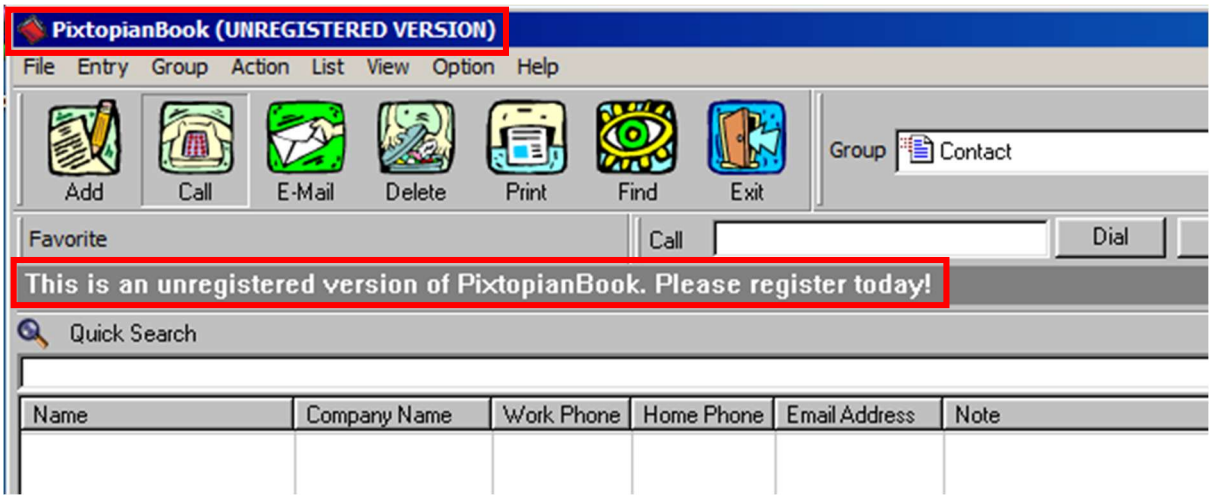
(sand-reversingwithlena-tutorials)

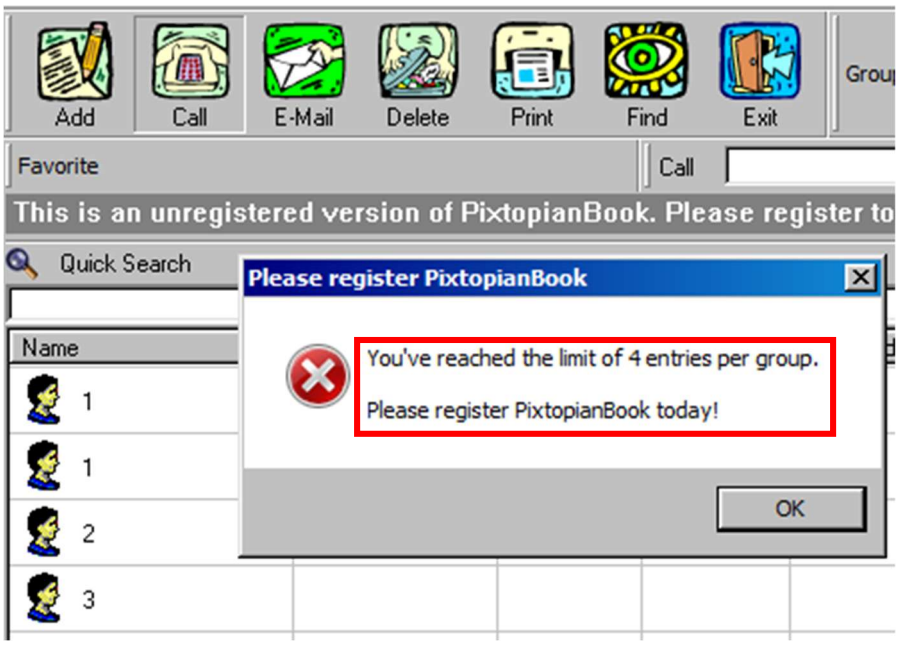
2025.05.27

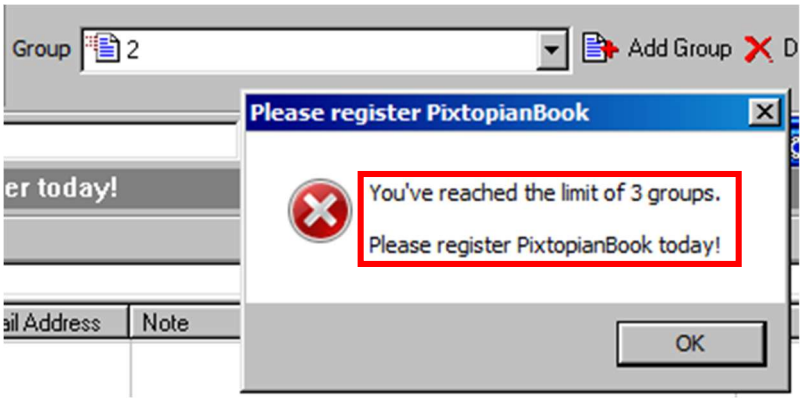
04

1. 문제


PixtopianBook
Manage Profiles
Please select a User Name and enter the corresponding password if necessary. If you would like to create a new profile, please click on "Create New Profile" button.
User Name:
user
Password:
Create New Profile
Delete Profile
Rename Profile
Do not show this dialog next time
Exit
Log In
PixtopianBook v1.07 (UNREGISTERED)


PixtopianBook (UNREGISTERED VERSION)
File Entry Group Action List View Option Help
Add
Call
E-Mail
Delete
Print
Find
Exit
Group
Contact
Favorite
Call
Dial
This is an unregistered version of PixtopianBook. Please register today!
Quick Search
Name
Company Name
Work Phone
Home Phone
Email Address
Note


Add
Call
E-Mail
Delete
Print
Find
Exit
Favorite
Call
This is an unregistered version of PixtopianBook. Please register to
Quick Search
Please register PixtopianBook
You've reached the limit of 4 entries per group.
Please register PixtopianBook today!
OK
Name
1
1
2
3



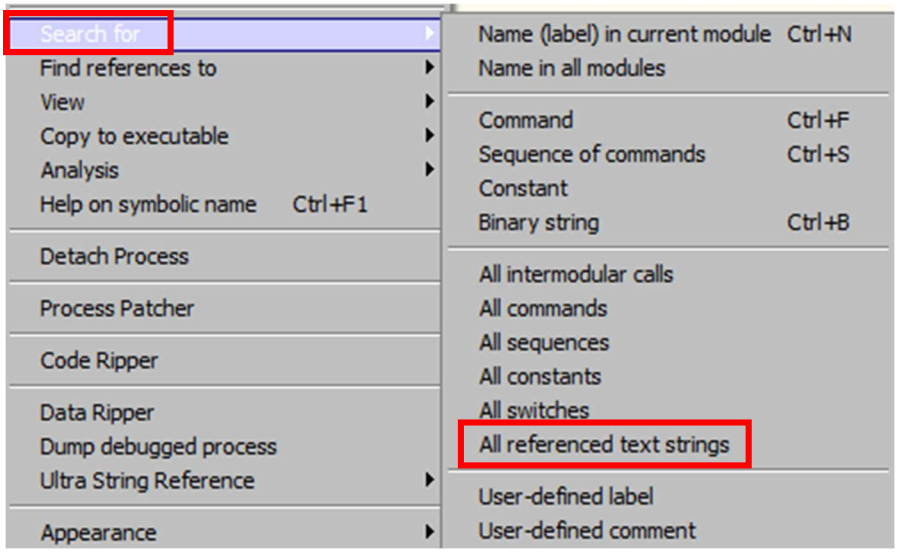
Unregistered -> registered 로 바꾸는 작업

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

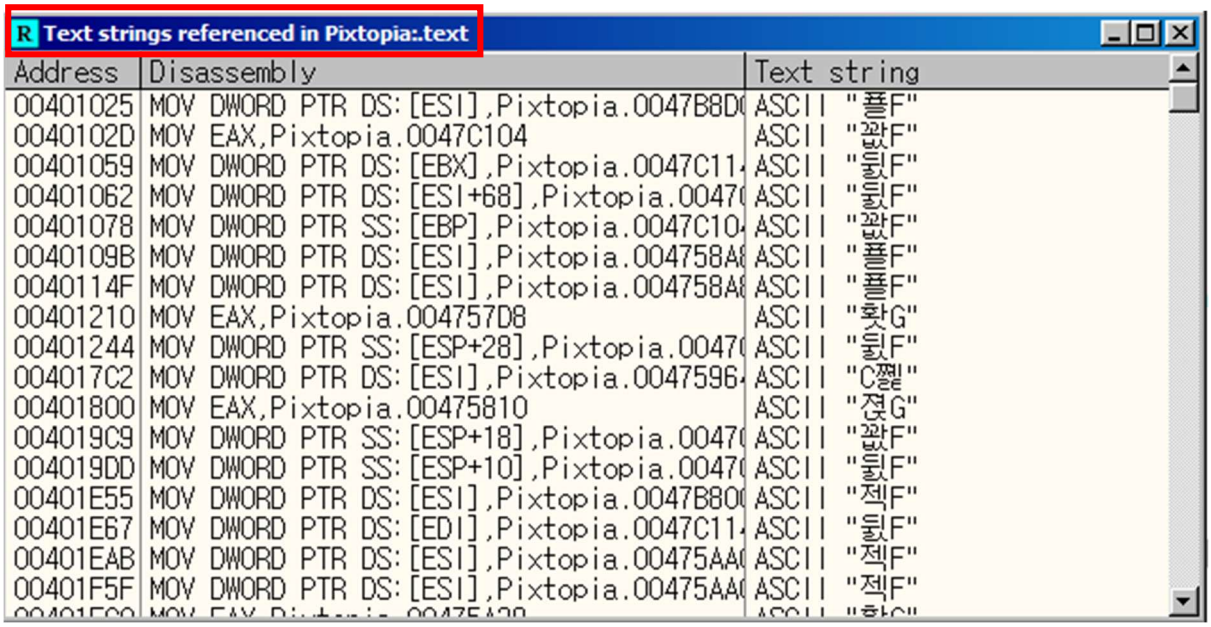
2. 해결 방법

1) 로그인 창

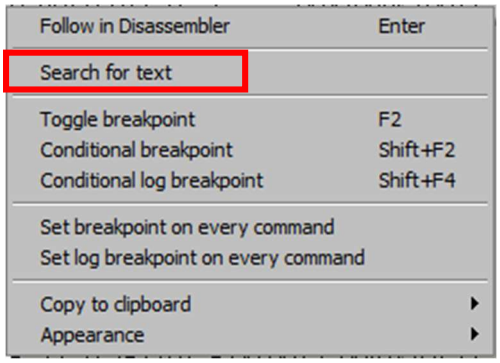
PixtopianBook v1.07 (UNREGISTERED) -> 이 멘트 수정해야함.

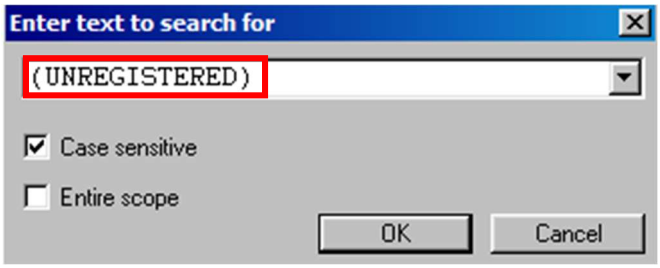


OllyDbg Code부분에서 Search for > All references text strings 클릭.



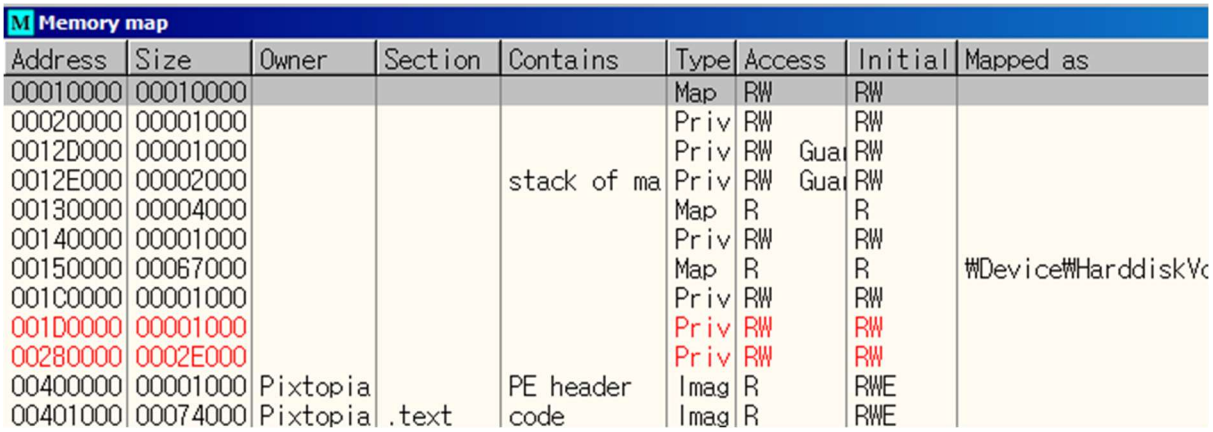
현재 창이 나오는 걸 볼 수 있음.



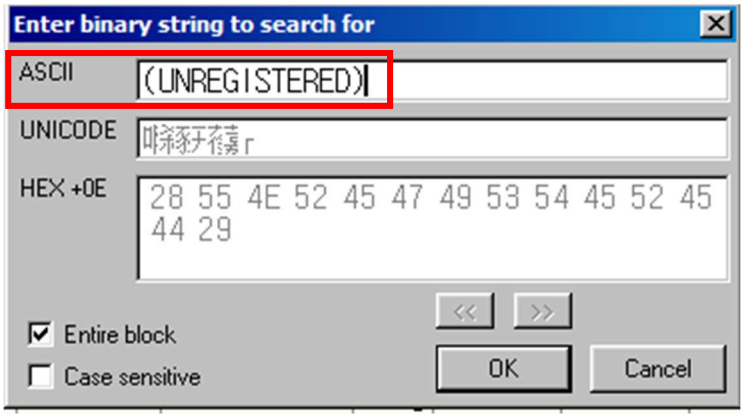


그럼 'Home' 키를 눌러서 맨 위로 올라간 다음 Search for text 클릭. 로그인 창에 있던 문자열 중 (UNREGISTERED) 검색해 보면 검색이 안됨.

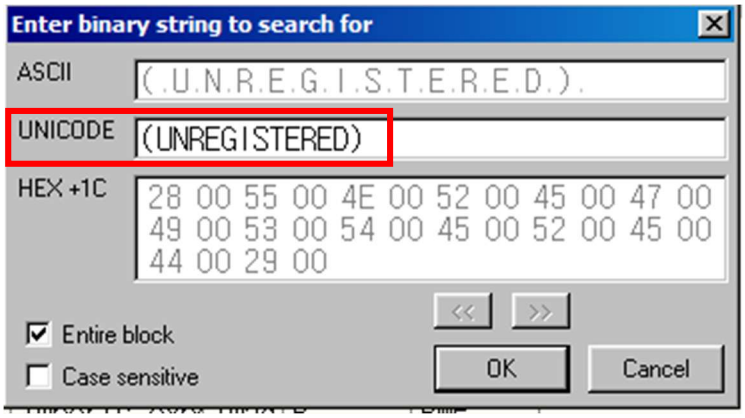
그럼 "Memory map" M을 눌러서 검색을 해줌.



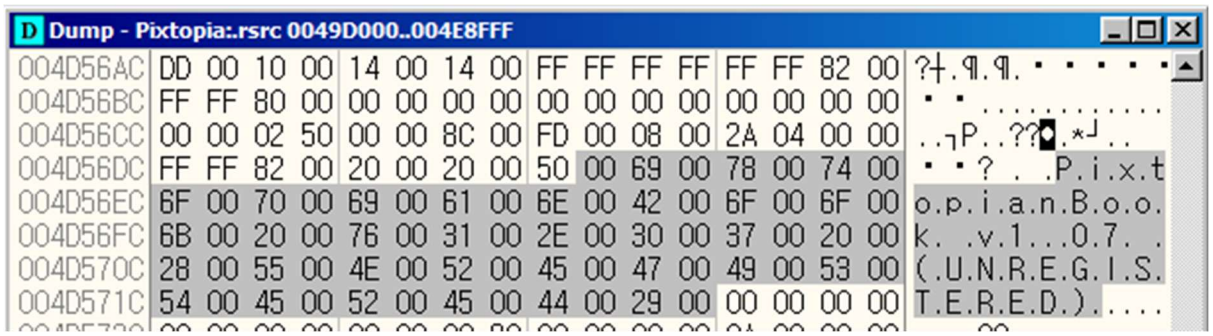
'Home' 키를 눌러서 맨 위로 올라간 다음 Search 클릭.



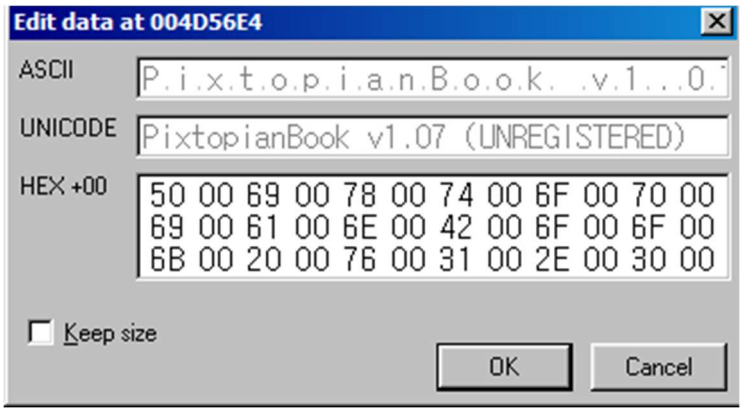
현재 창이 나타나고 'Sift+Insert' 키를 이용하여 로그인 창에 있던 문자열 중 (UNREGISTERED)을 ASCII에 검색해 보면 검색이 안됨.



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



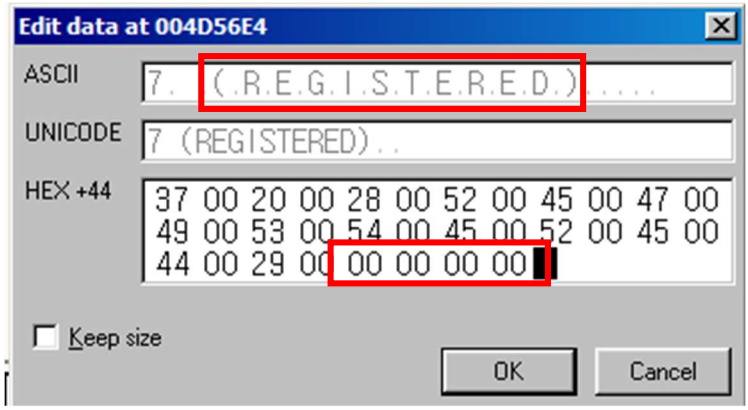
메모리 주소 0x004D56E4부터 시작하는 걸 볼 수 있음.



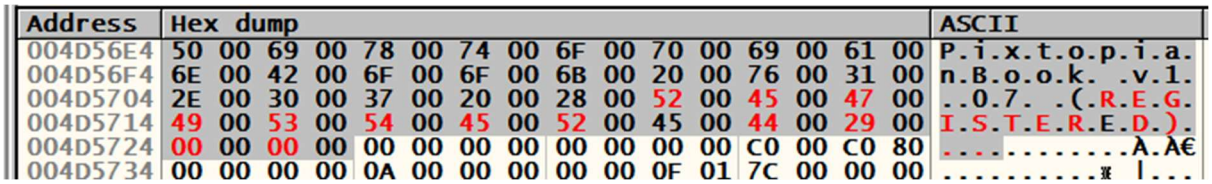
'ctrl+e' 키 누르면 위의 창이 나오는 걸 볼 수 있음.

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

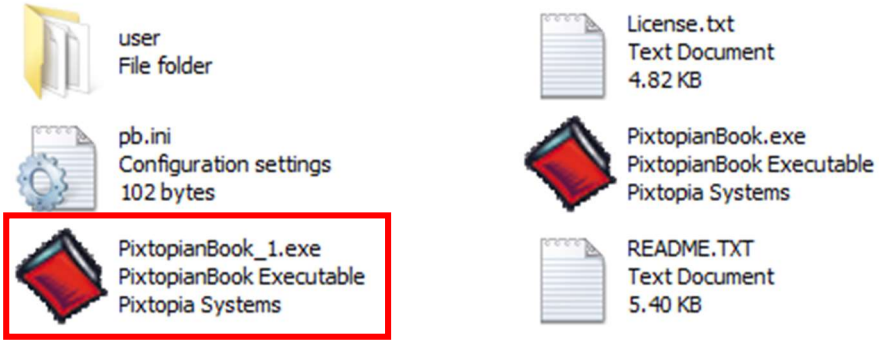
한 문자에 2byte인데 총 2개를 삭제해야하니까 'UN'을 삭제 후 뒤에 '00 00 00 00'을 추가해줘야함. 여기서 Keep size를 체크하면 크기 유지 때문에 삭제가 안되기 때문에 체크를 풀어주고 해야함.



이런 식으로 바꾸고 메모리를 보면 바뀐 걸 볼 수 있음.



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



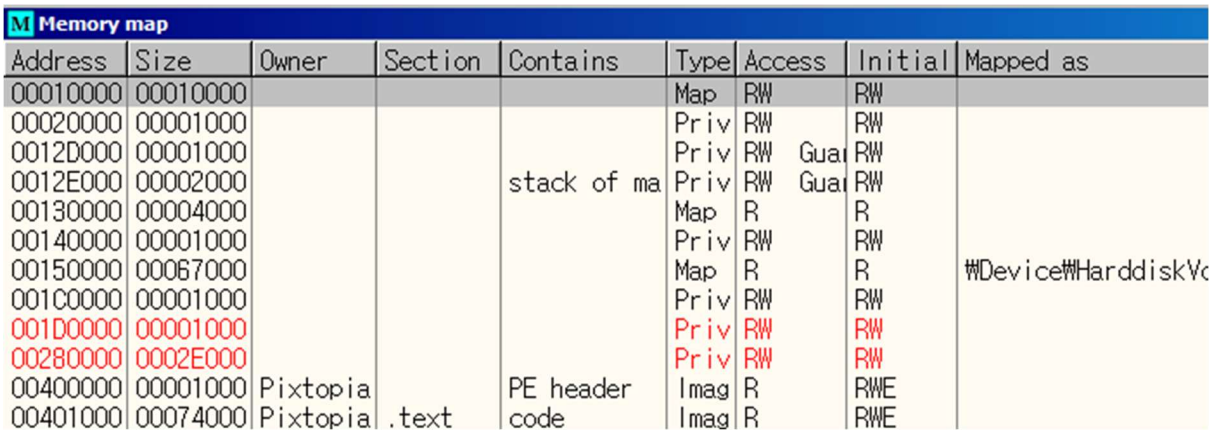
생성이 확인된 걸 볼 수 있음.

이걸 실행해보면 바뀐 걸 볼 수 있음.

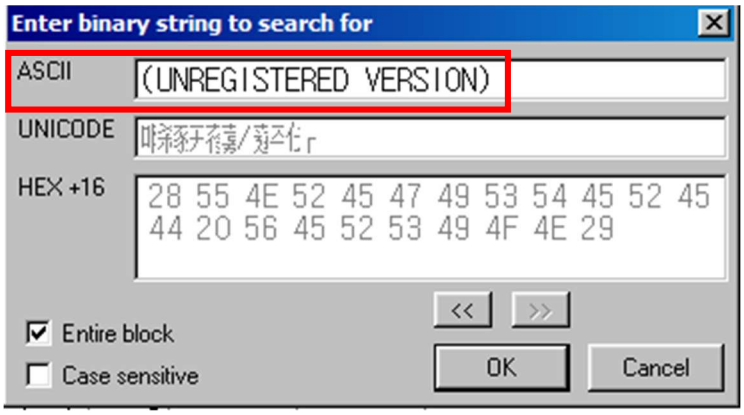
2) 타이틀 창

PixtopianBook_1.exe를 이용하여 타이틀 창의 문자열을 변경할거다.

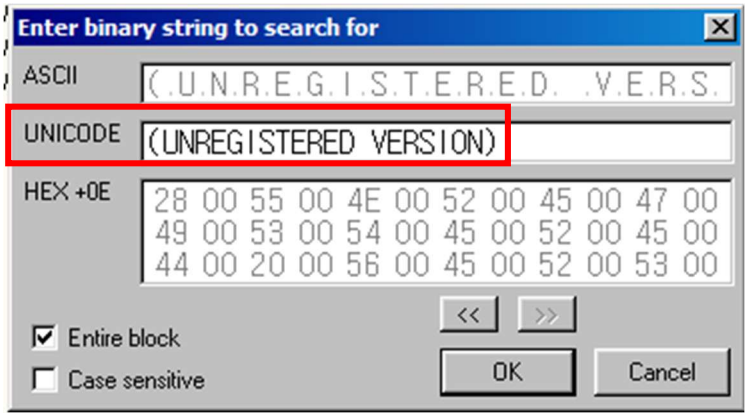
All references text strings에서 타이틀 창 있던 문자열 중 (UNREGISTERED VERSION) 검색해 보면 검색이 안됨. 그럼 "Memory map" M을 눌러서 검색을 해줌.



'Home' 키를 눌러서 맨 위로 올라간 다음 Search 클릭.

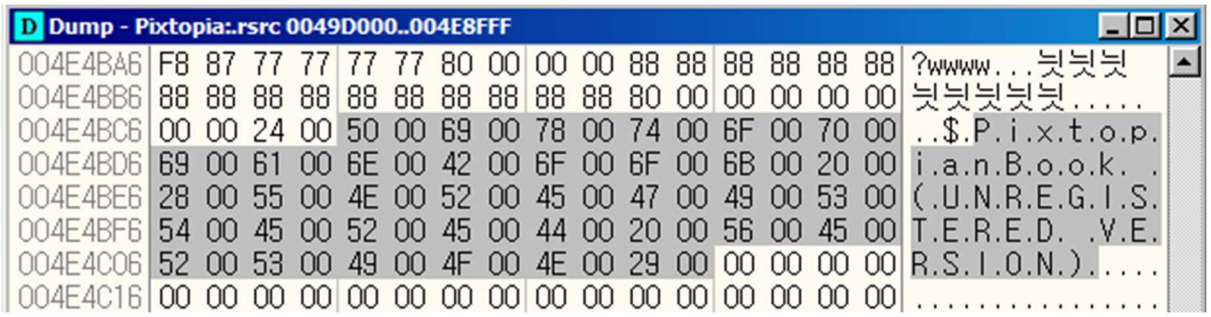


현재 창이 나타나고 'Sift+Insert' 키를 이용하여 로그인 창에 있던 문자열 중 (UNREGISTERED VERSION)을 ASCII에 검색해 보면 검색이 안됨.

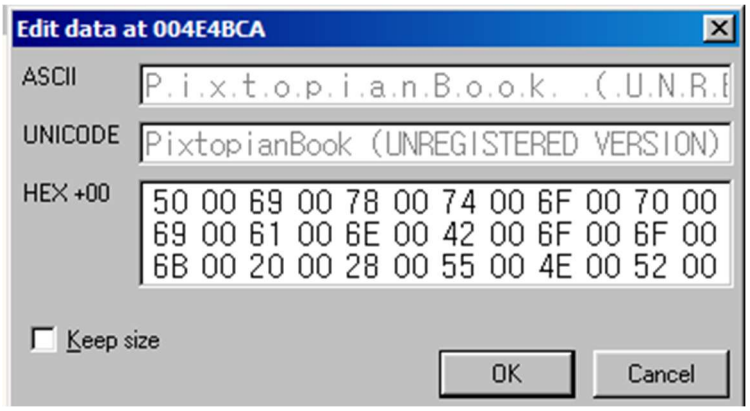


이번에는 (UNREGISTERED VERSION)을 UNICODE에 검색해 보면 검색이되어서 아래 창이

발생하는 걸 볼 수 있음.



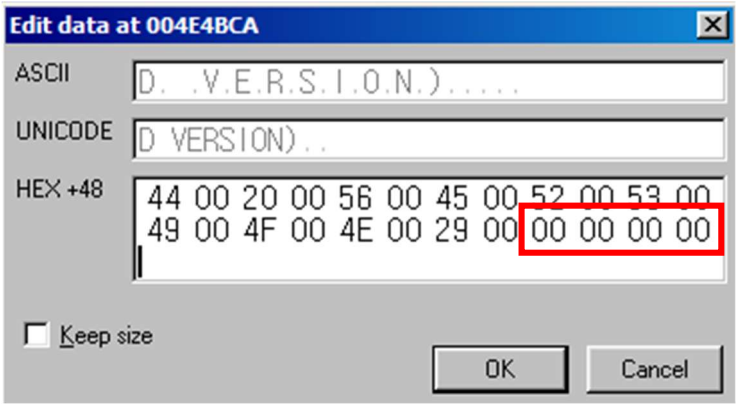
메모리 주소 0x004E4BCA부터 시작하는 걸 볼 수 있음.

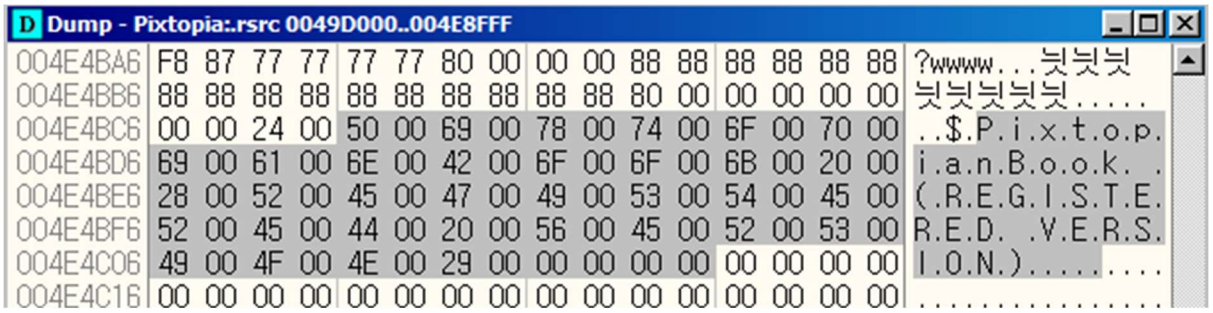


'ctrl+e' 키 누르면 위의 창이 나오는 걸 볼 수 있음.

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

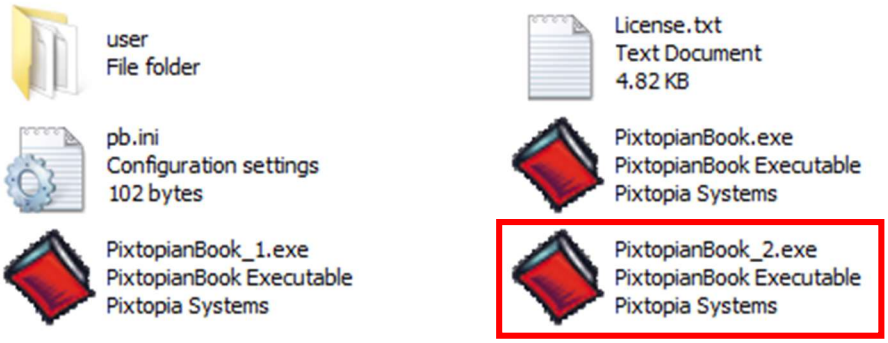
한 문자에 2byte인데 총 2개를 삭제해야하니까 'UN'을 삭제 후 뒤에 '00 00 00 00'을 추가해줘야함. 여기서 Keep size를 체크하면 크기 유지 때문에 삭제가 안되기 때문에 체크를 풀어주고 해야함.



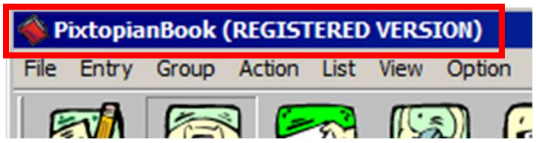


바뀐 걸 볼 수 있음.

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.

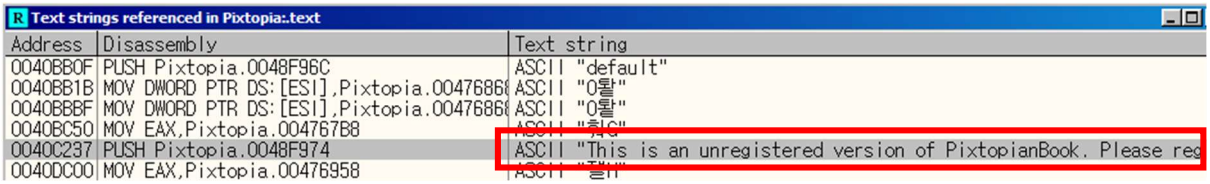


이걸 실행해보면 바뀐 걸 볼 수 있음.

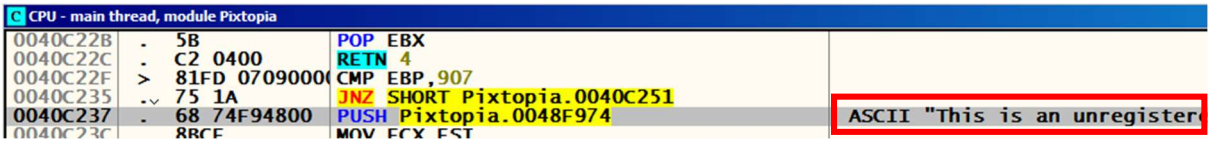
3) 중간 배너 창

PixtopianBook_2.exe를 이용하여 배너 창의 문자열을 변경할거임.

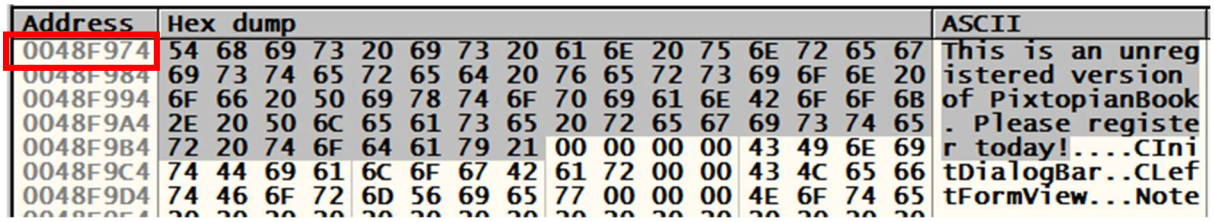
All references text strings에서 타이틀 창 있던 문자열 중 This is an unregistered version of PixtopianBook. 검색해 보면 아래와 같은 곳에 멈추는 걸 볼 수 있음.



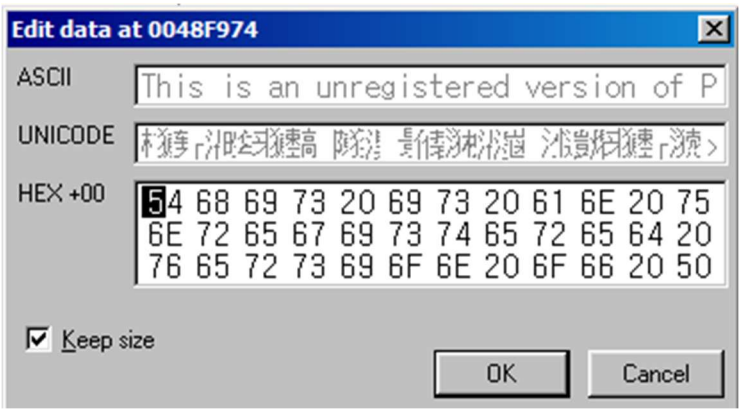
멈춘 곳을 더블클릭해보면 CPU 코드 창에서 현재 클릭한 곳을 찾아주는 걸 볼 수 있음.



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



0x0048F974에 들어가보면 문자열이 있는 걸 확인할 수 있음.

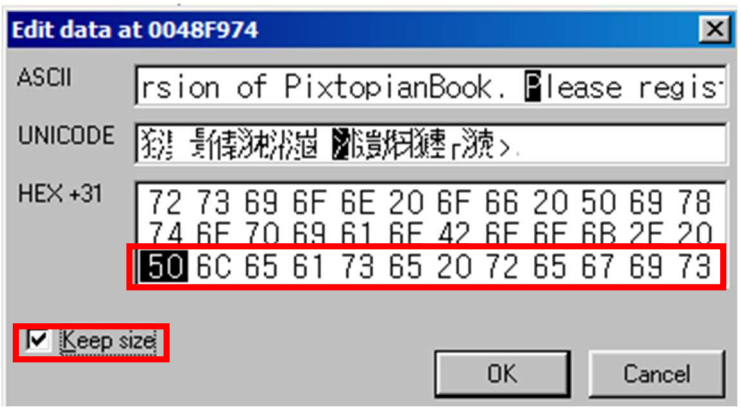


'ctrl+e' 키 누르면 위의 창이 나오는 걸 볼 수 있음.

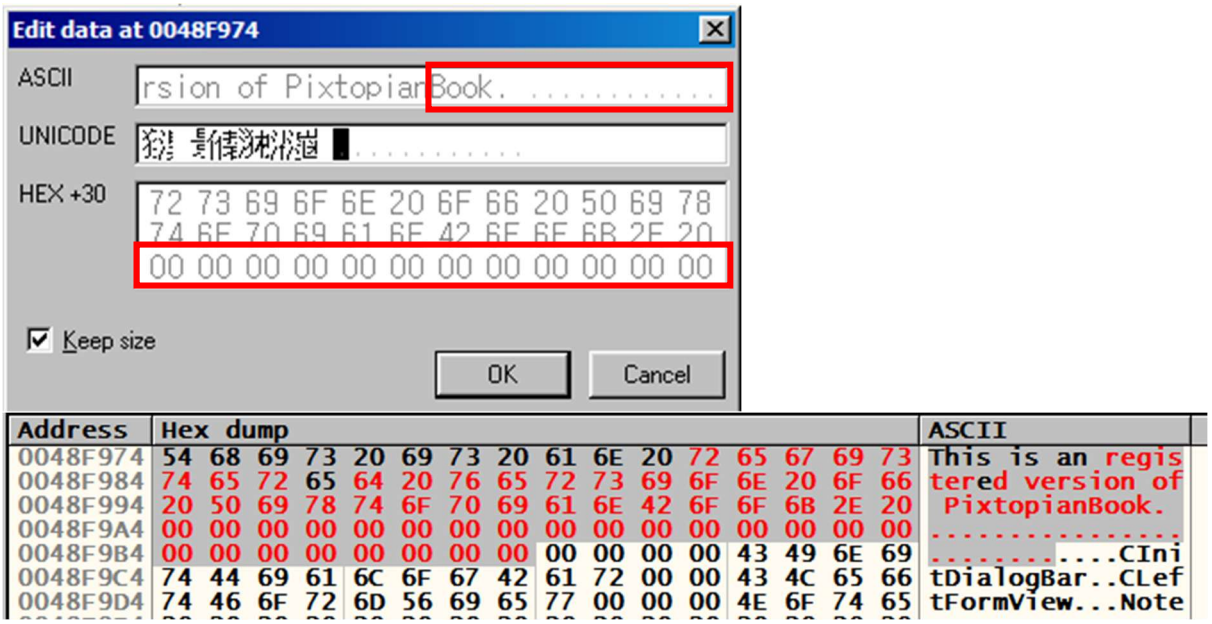
This is an unregistered version of PixtopianBook. Please register today! -> This is an unregistered version of PixtopianBook.으로 변경해줘야함. 'UN' 삭제 후 마지막 문자열을 삭제해줘야함.

먼저 Keep size를 체크를 해제하고 여기서 ASCII코드로 되어있기 때문에 한 문자에

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

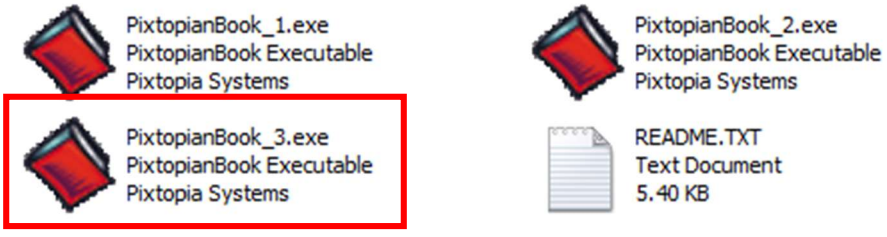


그리고 Keep size를 체크해주고 현재 위치부터 다 '00'으로 바꿔준다.

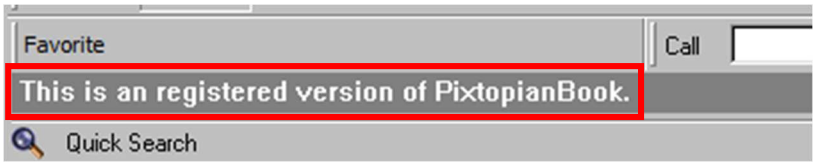


이렇게 변한 걸 볼 수 있다.

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.

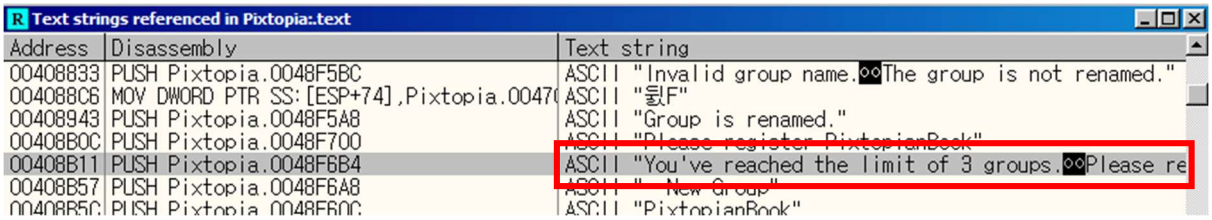


이걸 실행해보면 바뀐 걸 볼 수 있음.

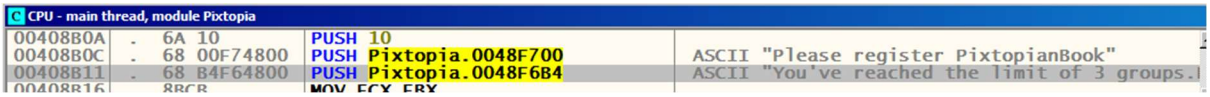
4) group 추가 창

PixtopianBook_3.exe를 이용하여 그룹을 더 추가할 수 있게 만들거다.

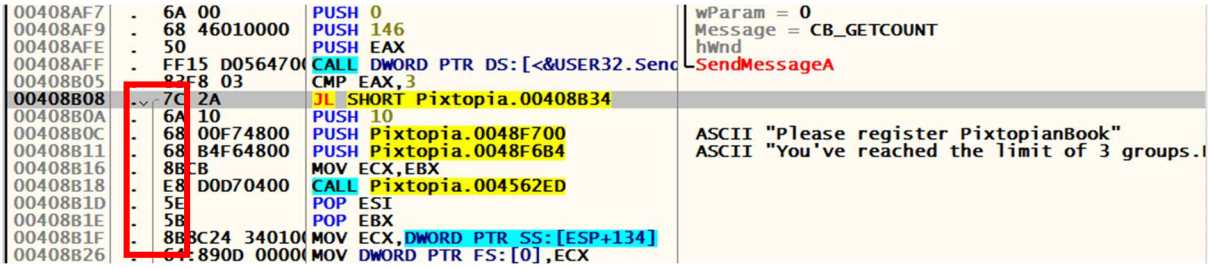
All references text strings에서 group 추가 창에 있던 문자열 중 You've reached the limit of 3 groups.검색해 보면 아래와 같은 곳에 멈추는 걸 볼 수 있음.



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



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

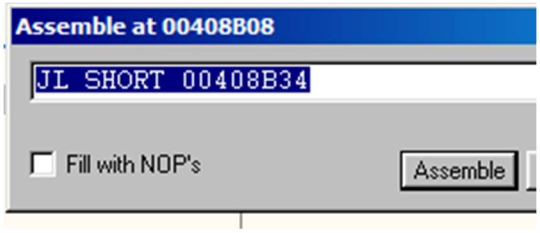


이 코드를 실행해보면 0x004088B08에서 점프를 안하고 실행되는 걸 볼 수 있다. 그럼 결국 그 창은 계속 발행하고 그룹은 3개 이상 만들지 못하는 걸 볼 수 있다.

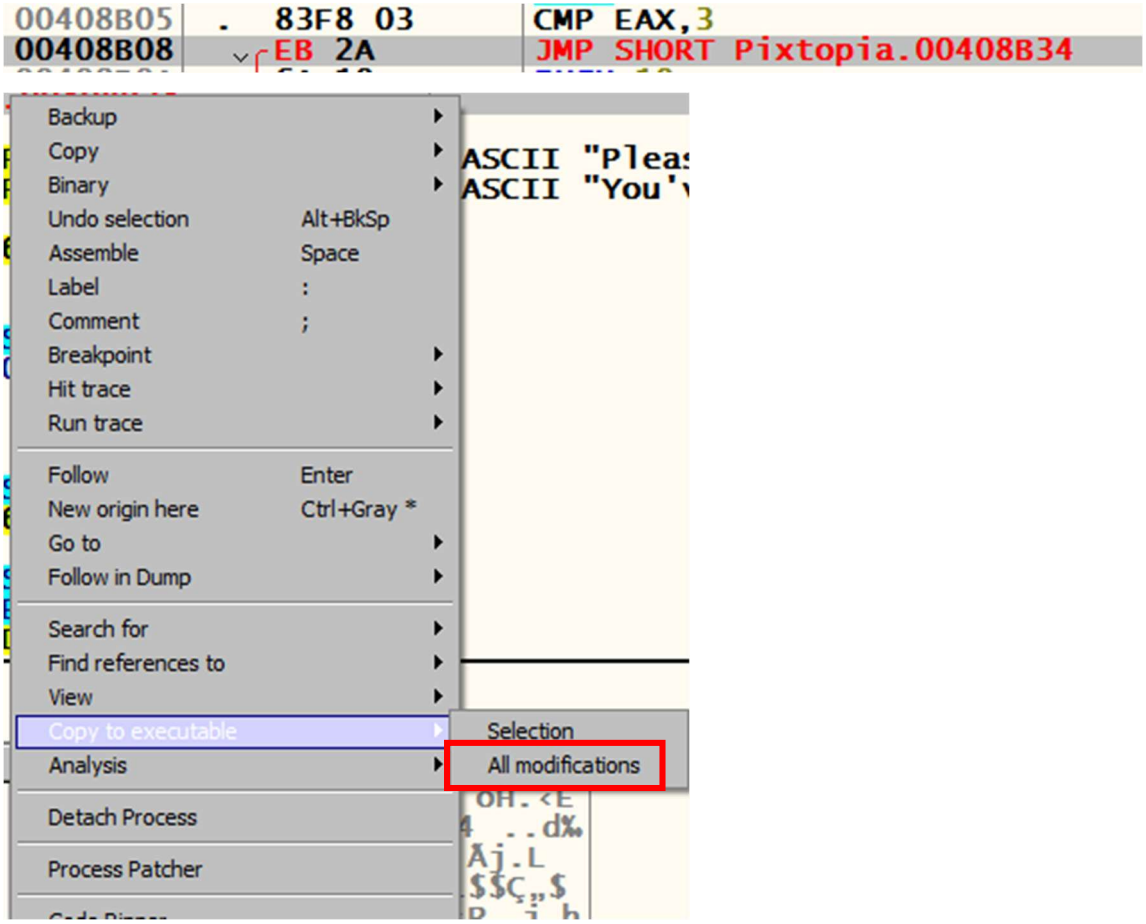
그러려면 코드를 바꿔줘야하는데 JL (cmp a, b에서 a가 작을 때 점프)이 있는 부분을 바꾸거나 CMP EAX, 3을 바꿔줘야 한다.

1. JL을 바꾸는 경우는 위에 EAX와 3이 비교하므로 EAX가 커져도 점프할 수 있게 할려면 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.



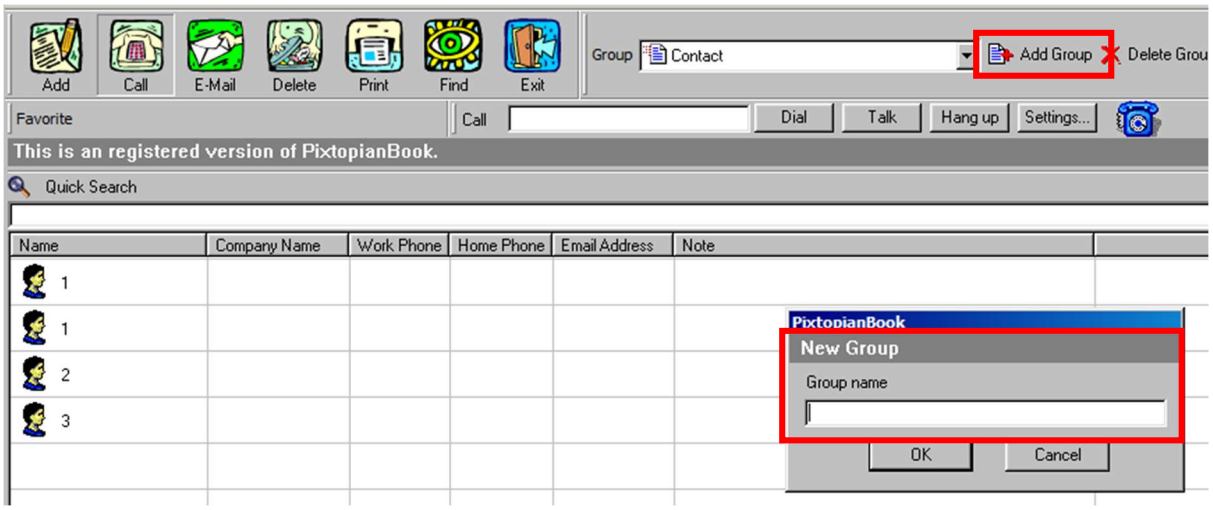
0x00408B08 코드를 더블 클릭한 후 JL -> JMP로 바꿔서 코드를 수정해준다.



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.

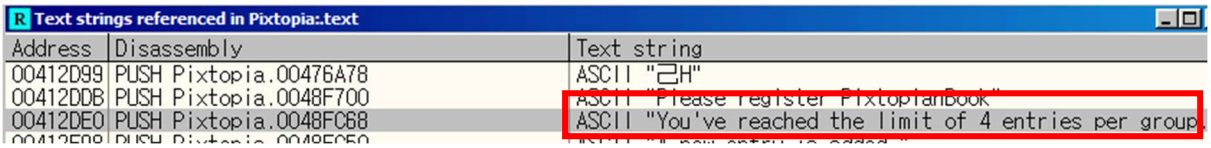


PixtopianBook_4.exe를 실행 후 Add Group를 해보면 그룹을 더 추가할 수 있게 되었다.

5) useradd 추가 창

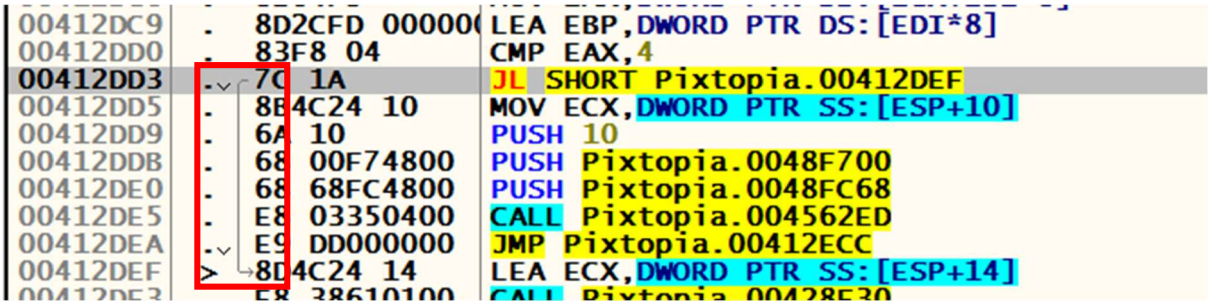
PixtopianBook_4.exe를 이용하여 사용자를 더 추가할 수 있게 만들거다.

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.



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

우리는 사용자를 4개 이상 만들 수 있게 해야하고 레지스터 키 등록해달라는 창이 안나오게 해야한다. 그러면 그 주변 코드를 봐야한다.

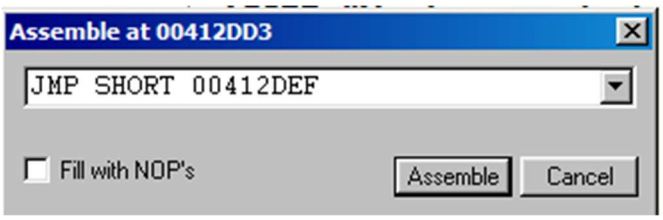


이 코드를 실행해보면 0x00412DD3에서 점프를 안하고 실행되는 걸 볼 수 있다. 그럼 결국 그 창은 계속 발행하고 사용자는 4개 이상 만들지 못하는 걸 볼 수 있다.

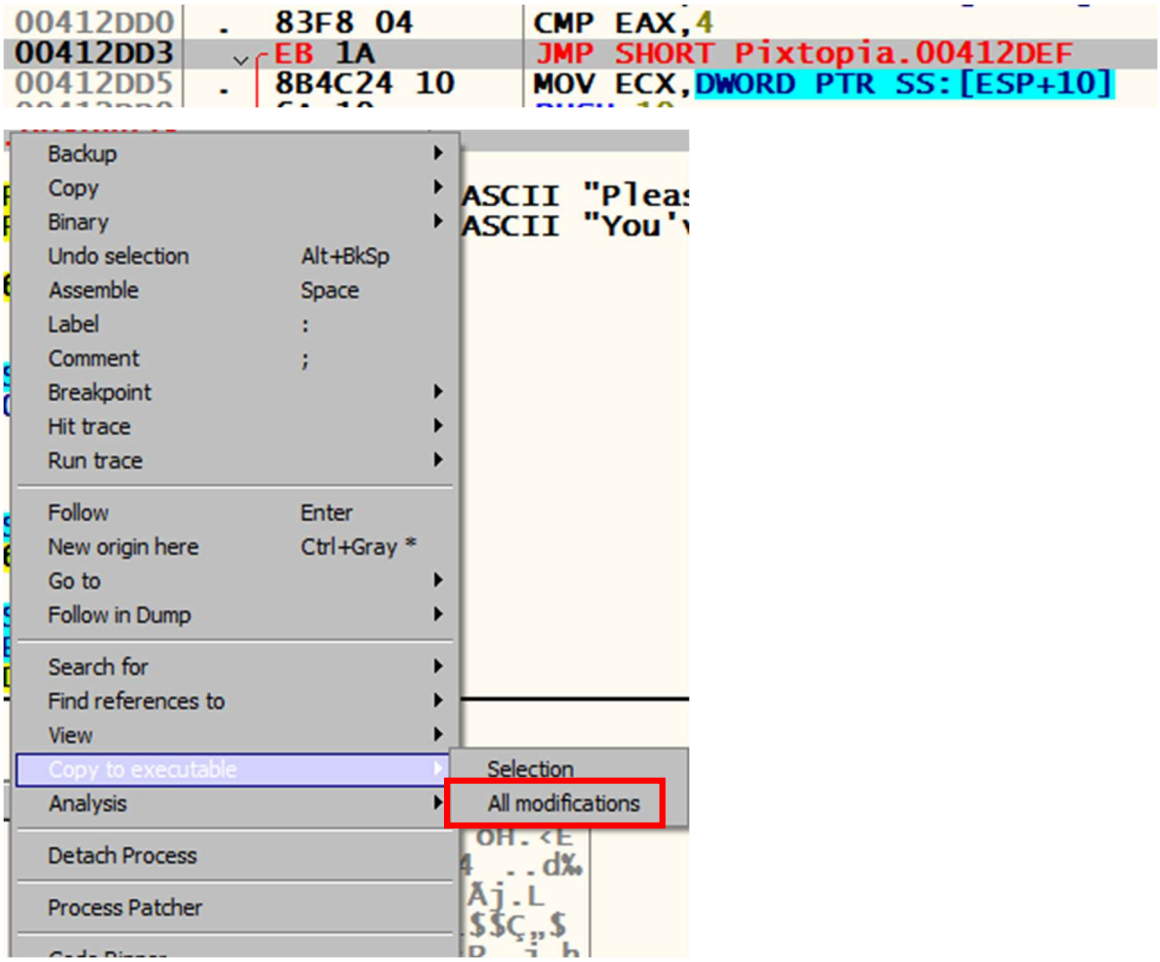
그러려면 코드를 바꿔줘야하는데 JL (cmp a, b에서 a가 작을 때 점프)이 있는 부분을 바꾸거나 CMP EAX, 4를 바꿔줘야 한다.

1. JL을 바꾸는 경우는 위에 EAX와 4가 비교하므로 EAX가 커져도 점프할 수 있게 할려면 조건 없이 JMP 명령어로 바꾸는 것이 좋다. (JMP는 무조건 점프이기 때문에)

2. CMP를 바꾸는 경우는 위에 EAX와 4가 비교하므로 4가 아니라 더 큰 숫자로 바꾸는 방법이 있다. 하지만 숫자를 정해 놓으면 언젠가는 끝에 도달하니까 이 방법은 좋지 않은 방법이다.

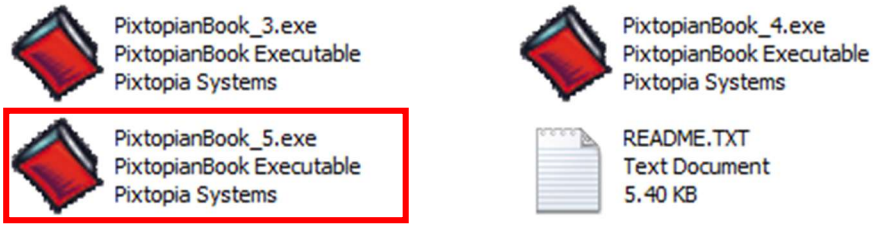


0x00412DD3코드를 더블 클릭한 후 JL -> JMP로 바꿔서 코드를 수정해준다.

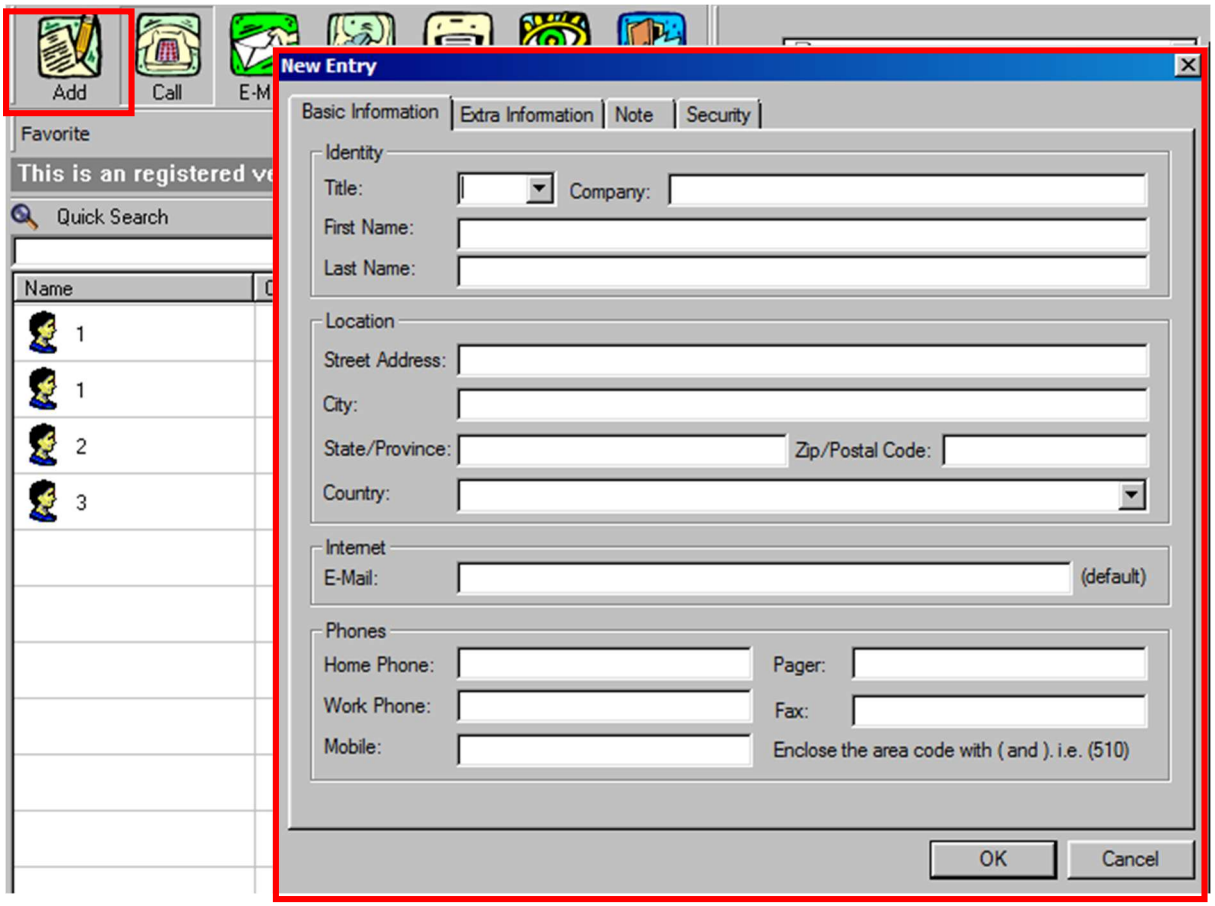


Copy to executable > All modifications > Copy All 누르면 Dump창이 나오는 걸 볼 수 있다.

오른쪽 마우스 클릭 > save file 하고 보면



생성이 확인된 걸 볼 수 있음.

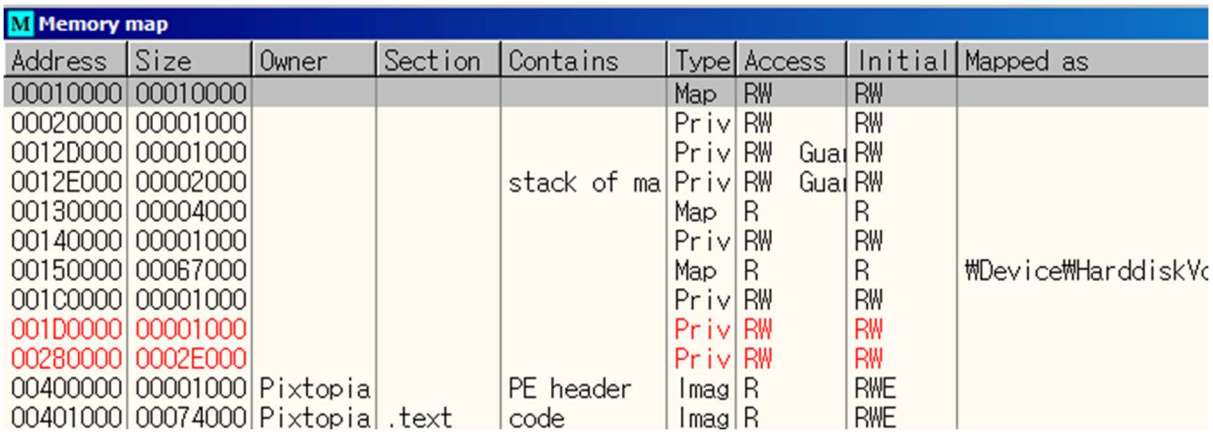


PixtopianBook_5.exe를 실행 후 Add를 해보면 그룹을 더 추가할 수 있게 되었다.

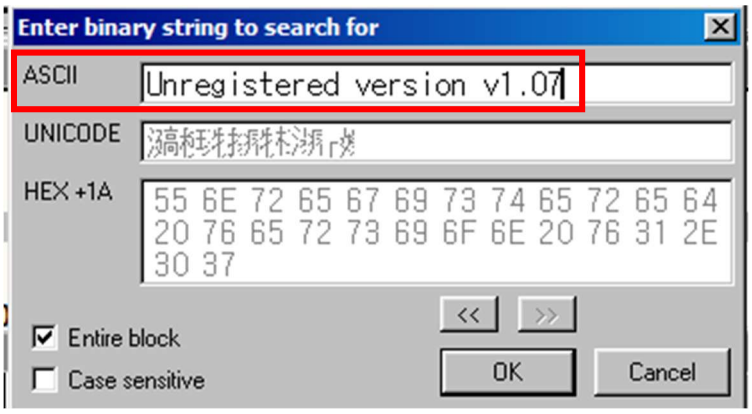
5) Heip 창

PixtopianBook_5.exe를 이용하여 Heip 창 의 문자열을 변경할거다.

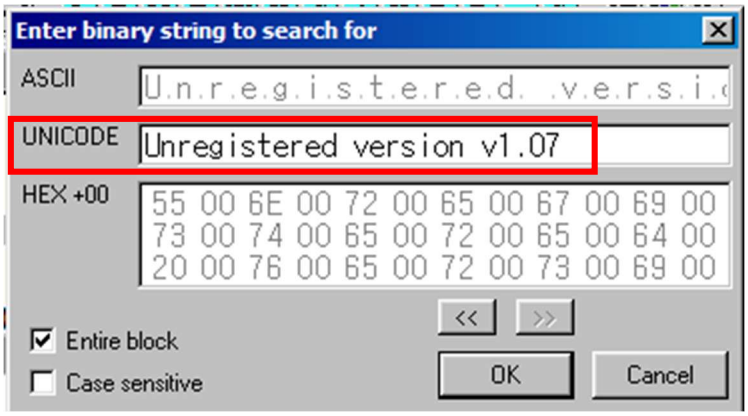
All references text strings에서 타이틀 창 있던 문자열 중 Unregistered version v1.07 검색해 보면 검색이 안됨. 그럼 "Memory map" M을 눌러서 검색을 해줌.



'Home' 키를 눌러서 맨 위로 올라간 다음 Search 클릭.

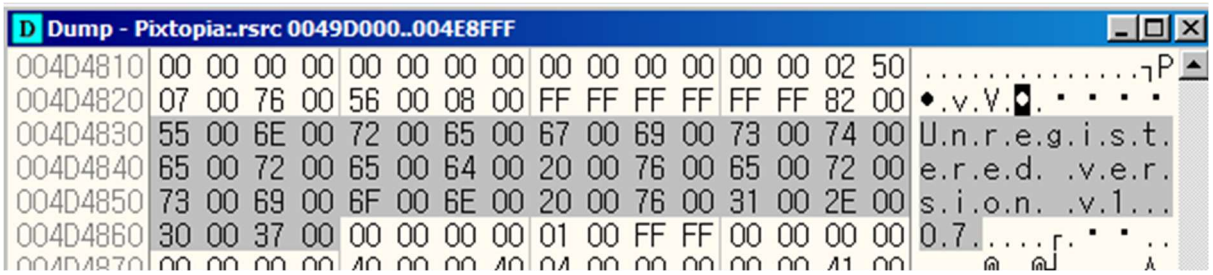


현재 창이 나타나고 'Sift+Insert' 키를 이용하여 로그인 창에 있던 문자열 중 Unregistered version v1.07를 ASCII에 검색해 보면 검색이 안됨.

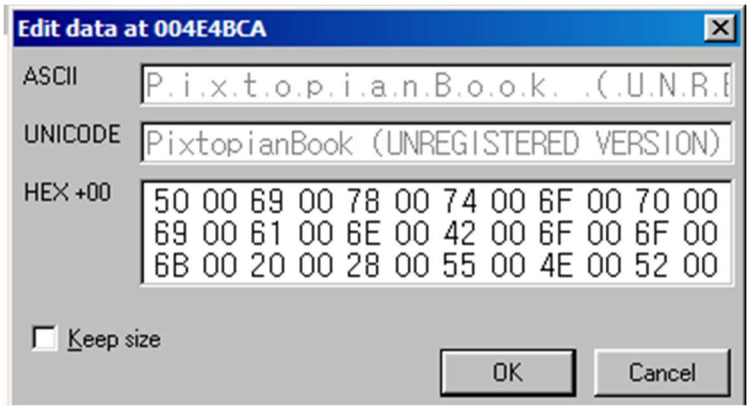


이번에는 Unregistered version v1.07를 UNICODE에 검색해 보면 검색이되어서 아래 창이

발생하는 걸 볼 수 있음.



메모리 주소 0x004D4830부터 시작하는 걸 볼 수 있음.

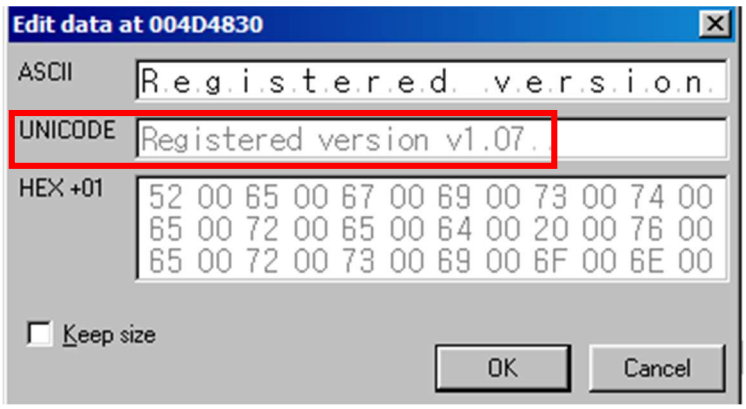


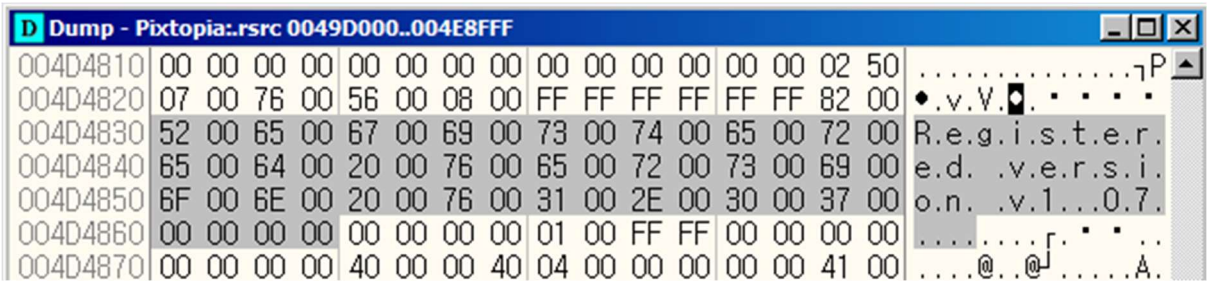
'ctrl+e' 키 누르면 위의 창이 나오는 걸 볼 수 있음.

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.





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.

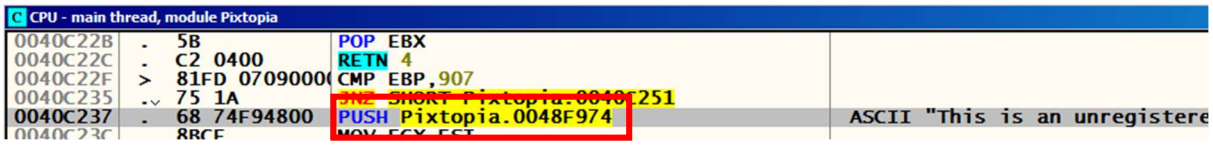
문제 해결!

★ 여기서 중요한 점

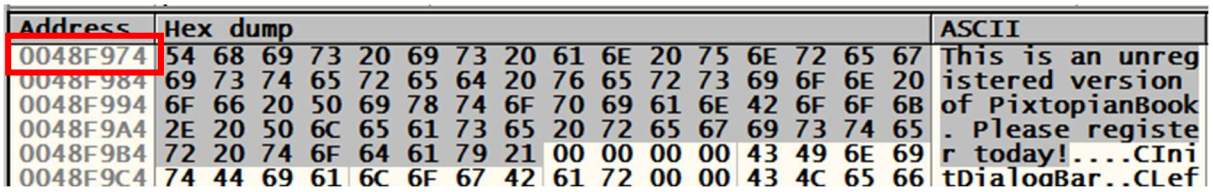
All references text strings과 Memory map의 차이점!

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

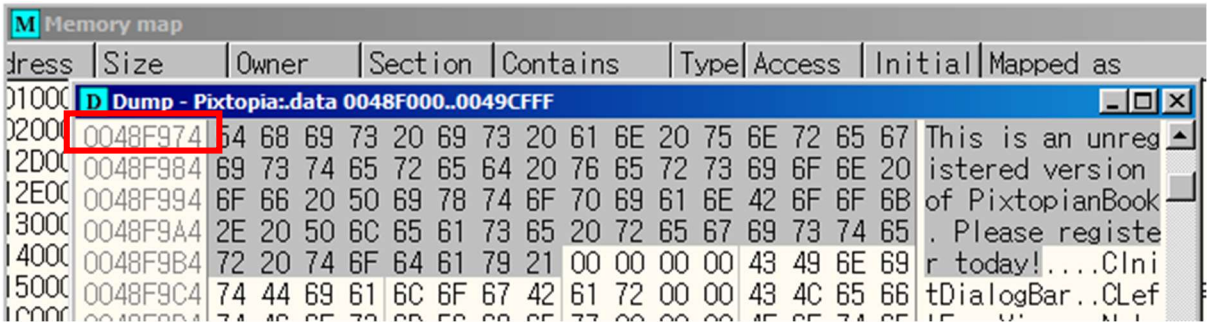
Memory map은 메모리에 저장된 문자열만 볼 수 있음. Memory map에서는 참조된 문자열도 볼 수 있음.



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



0x0048F974를 메모리 창에서 찾아보면 있는 걸 확인할 수 있음.



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.