mr nick's guide to cracking

BY MR NICK.1998

DISCLAIMER: Please note that this is for educational purposes only. It will teach someone how to remove protections from programs, but not encourage it for illegal purposes. The idea, in the guide is to show how people add protections onto software, and how you can use your skills as a computer expert to undo those protections etc..

Introduction

Welcome, this is the first in my installation of guides aimed at the 'newbies'. This though is different to all the other guides. Here is why.

This guide is aimed at the very begginer in cracking... it contains picutes, much like a book when you were a kid. This is to make things more easier to understand and it really didn't take that long to do... (honestly). I could have written this in 5 lines, but as I said this is for the newbie.

Please tell me if you want picutures or not..This is a new idea, and I am seeing if it helps or not. Remember this is for the NEWBIE.

What I know :-

1) Very basic knowledge of ASM

I know what POP does, what PUSH does, a vague knowledge of what the registers do etc... I have a rough understanding of what is happening.

2) Mediocre Knowledge of SOFTICE

I know how to make breakpoints on certain windows functions, and I know basically all you really need to know to get by and follow the tutorials of try some basic cracking.

3) Mediocre Knowledge of W32Dasm

I know how to search for a string, and what it means once I have found it.

4) Basic Knowledge of Turbo Pascal

I know enought to understand how the key generators work, and therefore enought to make one myself. Also, I know how to make patchers.

I hope that you should know the above, and probably more. Once again this is aimed at the newbie, and I class myself as a newbie. This tutorial is an experiment, so don't come shouting at me, that I am teaching you wrong tricks. If the protection has been cracked, then I don't see the problem. If I have mentioned something wrong, then please contact me at mrnick99@hotmail.com and I will bring it around in the next tutorial session.

What you need :-

1) Soft-Ice
2) W32Dasm 8.x
3) Hexedit / Psedit

All of the above are available from http://cracking.home.ml.org

---

WEEK 1 : WINX-FILES v2.8

NOTE: THIS HAS BEEN COVERED IN A PREVIOUS TUTORIAL. I DIDN'T REALISE UNTIL WRITING THIS ONE. THIS IS ANOTHER WAY, SOMEWHAT EASIER WAY OF CRACKING IT. (REF: PC'98 Tutorial 8)

You can download this program from the following address :

http://www.pepsoft.com/wxf32_28.zip

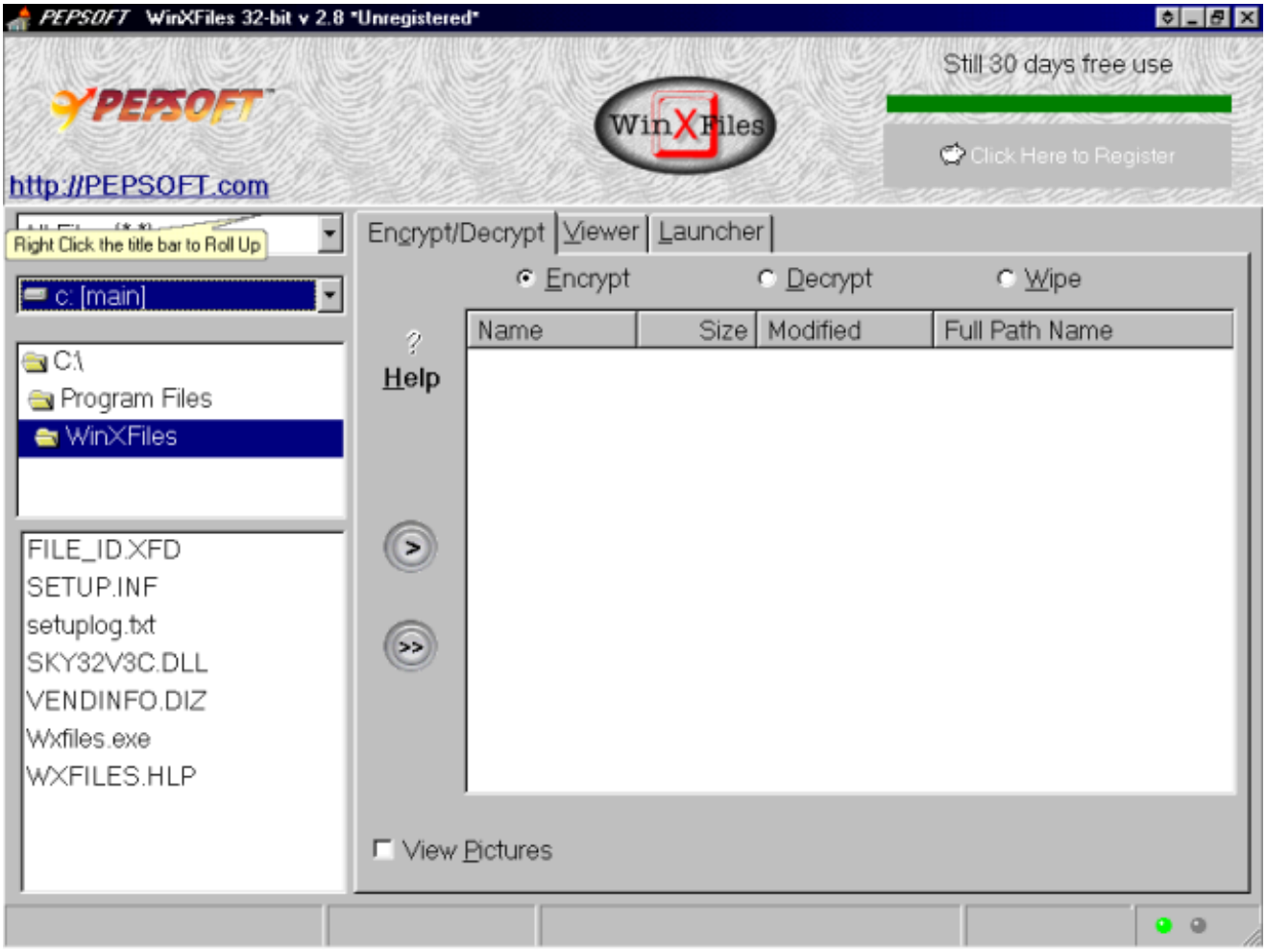
INTRO

In this lesson, we are going to crack this program so you can enter any name and any code to go with it.

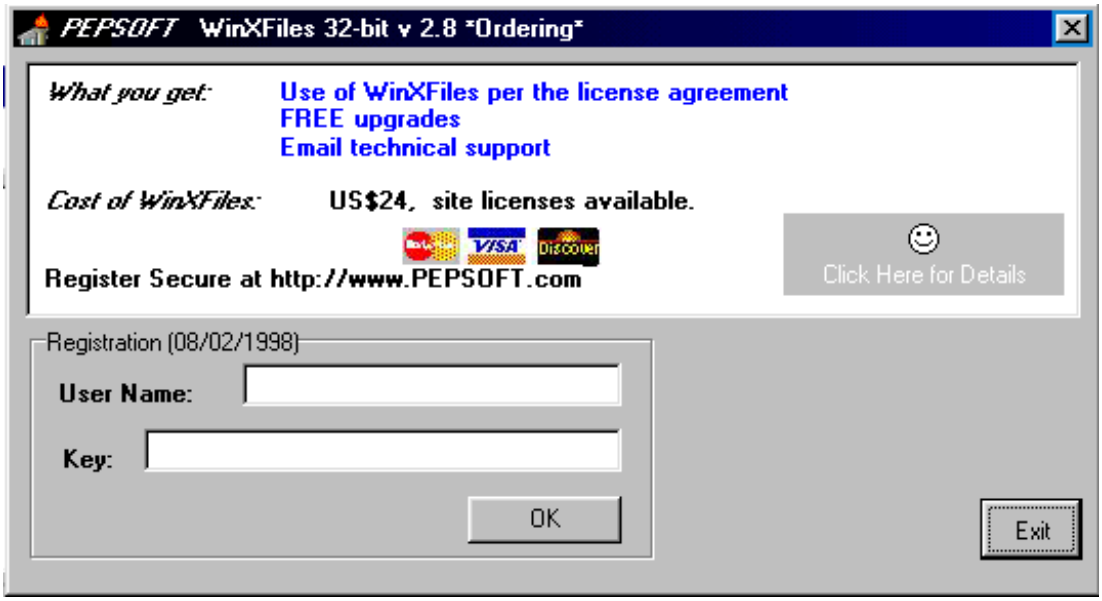
Step By Step

1) Win X-Files , the protection.

Load up Win X-Files (WXF) and notice that the product has *UNREGISTERED* all over it.



Click on the button marked.. 'Click here to register'

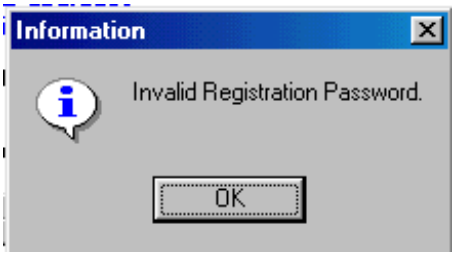


You will be presented with this screen.

Enter a name like :- MR NICK

Enter a key like :- 999999999

You will then get a message saying :-



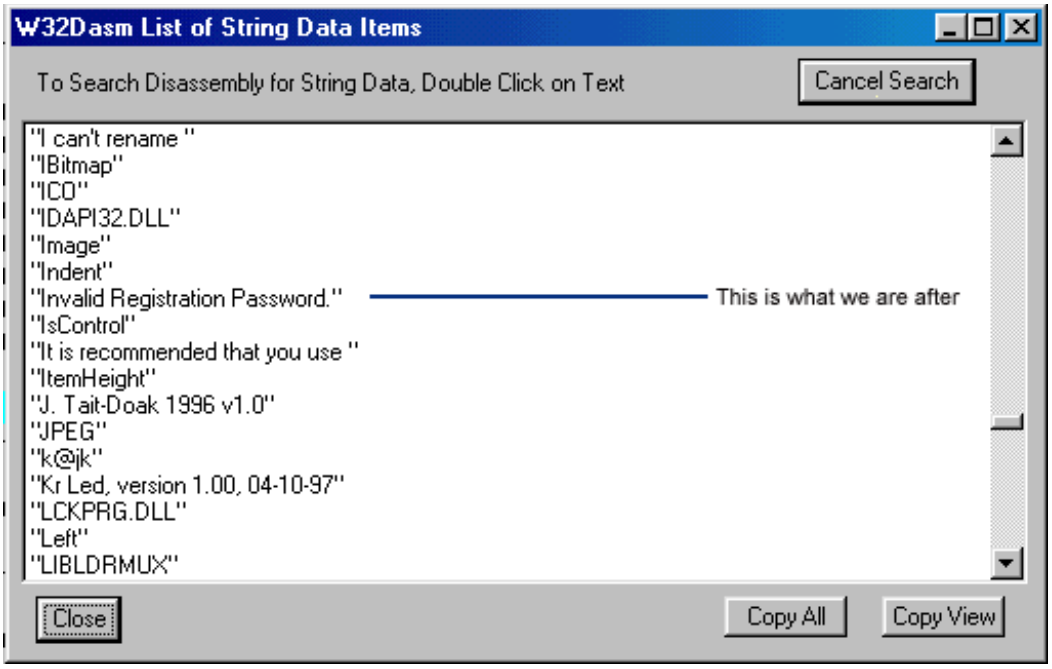
No Problemo.....

2) Cracking WXF.

Load up WXF into W32Dasm 8.x.

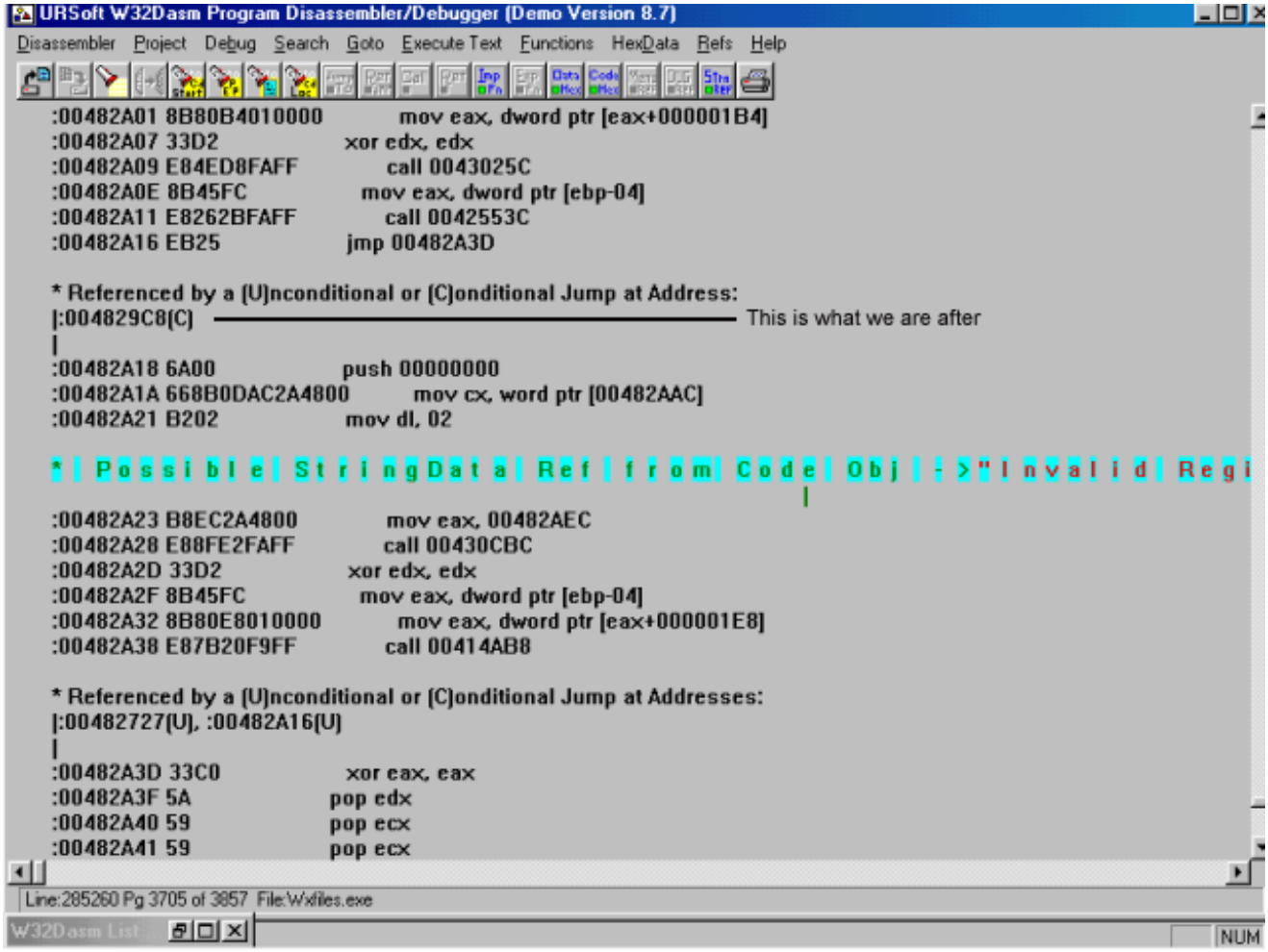
Once this has loaded click on  on the toolbar.

This will bring up the following box.



As you can see, if you scroll down the box that popped up for us when we entered the wrong code, is actually here. What a peice of luck.

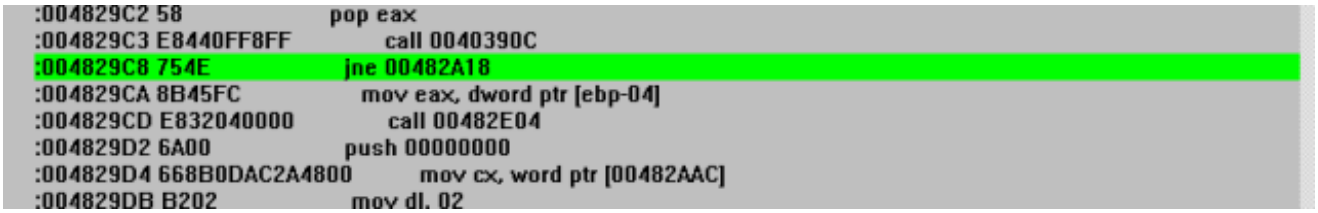
Double click on this string and the following will be shown on your screen.



Know this is where I don't really know what is going on.. But I know enough to understand what is happening. The line that is highlighted is the box that is called when we enter the wrong code. Above that, the three lines, is I think, what is happening when we type in the wrong code.
The thing to look for is what called this code. What part of the program actually said "Let's show a dialog box saying 'Invalid Registration Code etc....."
We trace up to the nearest reference, which is the line that reads.

"This is what we are after"

That is where the call came from for the invalid box to be shown. So we trace upto that line and we are presented with the following.

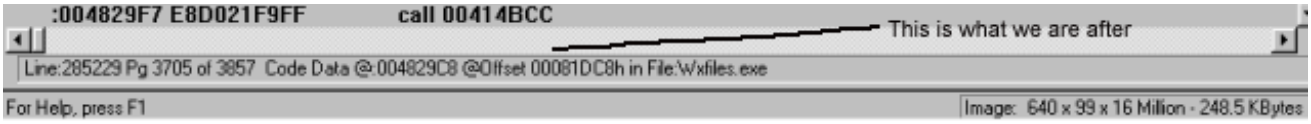


The bit highlighted in green is the code that we want.

At the moment, it is going to the invalid code if something is not equal. You can ignore all of the above for this tutorial, and this crack. This is the first point of call. You try out this first, if it doesn't work then you try something else, find out what it does to call that invalid box etc.

So, all we have to do is change the **jne** to a **je** ...what this will do is if you enter the wrong code, it will carry on and run the code for the correct code. If you enter the correct code, it will tell you it is wrong.

This is the most important bit. At the bottom of the screen is a line with the corresponding postition in hexedecimal.



OK, so the one that we are after is the **Offset**.... not the Code Data. In my case the number is

00081DC8 (ignore the h at the end, that shows that it is hexidecimal.)

3) Editing the Value, and trying again.

Exit W32DASM. and run **HEXEDIT/PSEDIT.**

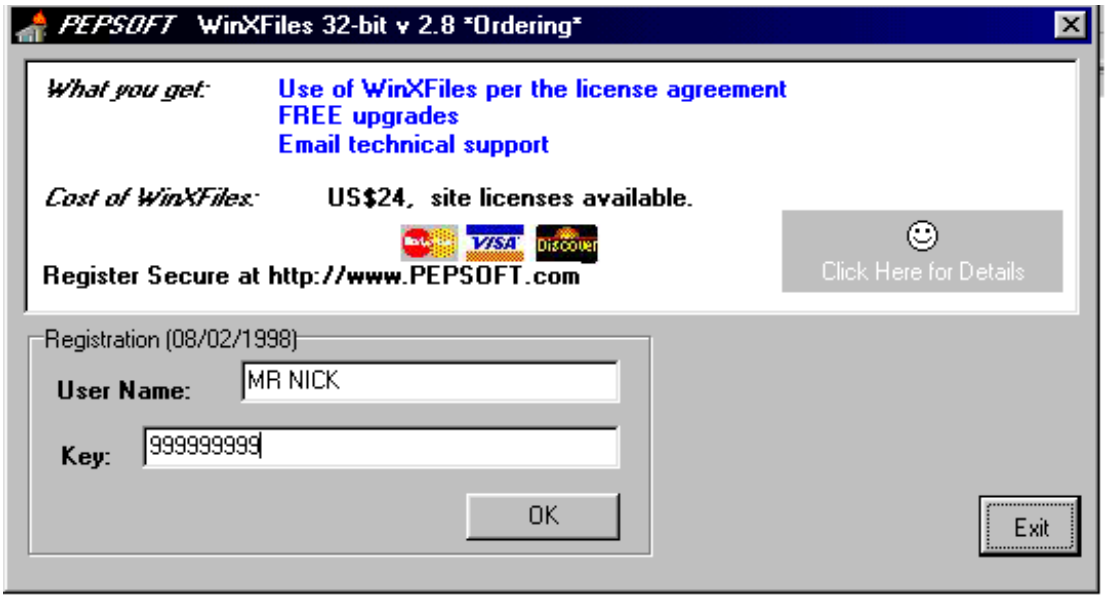
Scroll down to the point where the above code corresponds. i.e. 00081DC8 in my case. You will see the code that was in W32Dasm. You will see 75 4E.

Change the **75** to a **74**.

Exit and save.

4) Running the program, and seeing if it all has worked.

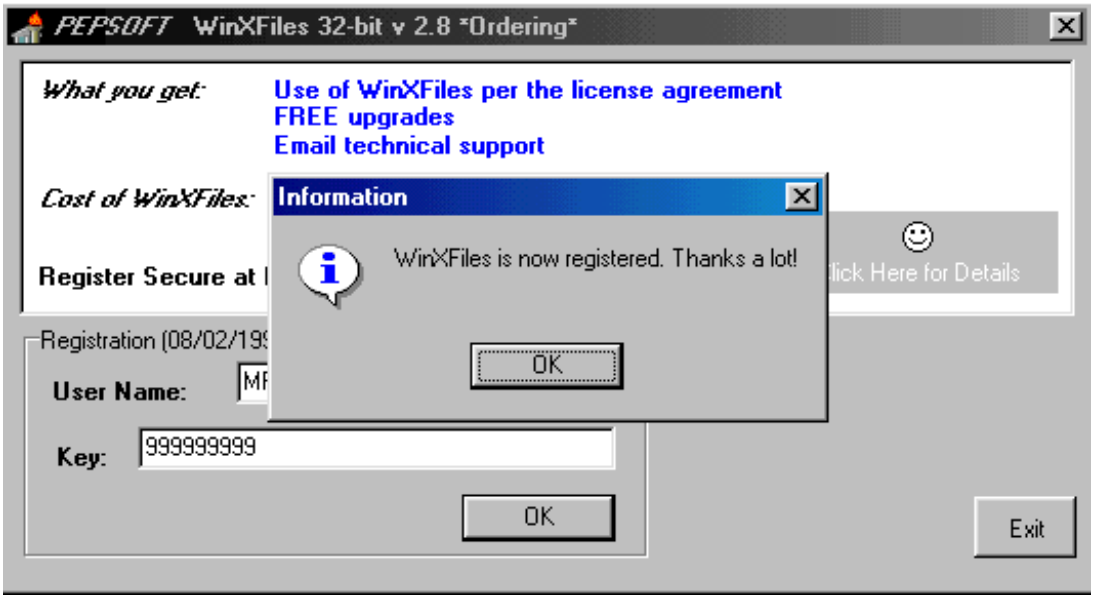
As before goto the registration and enter all the details, as you did before..



Here we go..... are you ready.....

Click on **O.K**.

BINGO



You did it.. the program is now registered.

BUT

I have come across programs, that do this, but once you load it up again, it needs you to register. This is becuase you are just stopping the box from coming up. This program will actually place all your details into the registry office, so it saves it.

You now have a free copy of Win X- Files. Please though pay for the product, as it is good, and this is only for educational purposes.

Week 2 : How to make a Patcher for this product
Week 3 : How to crack Nuts and Bolts '97
Week 4 : Don't know.....

Thanks very much for doing this guide with me, I have enjoyed writing it, and please spread this around as much as possible. BUT do not change anything in here. i.e. put your own name in etc.. that wouldn't be fair.

How to contact me :-

NAME: MR NICK
EMAIL: mrnick99@hotmail.com
ICQ: 9431128
