Really Simple Software Cracking
Or "How I spent an hour cracking my first program" (nostalgic sigh)
by The Observer

(Well, not too nostalgic--this was only a few days ago. But anyway.)

This file is for educational purposes only. I don't support cracking software as an alternative to paying for it, and I sincerely ask anyone who uses these directions not to distribute cracked versions of Relax (I didn't), which is the program we'll be discussing.

The Scenario...
There's a shareware program called Relax (which may have been included with this file), which plays some little nature sounds in the background. Nice, but not where I'm going to spend my money. In order to get you to pay up, the authors pop up a reminder dialog whenever you open the unregistered version. You have to wait a few seconds until the OK button to dismiss it is enabled. Then comes a screen for a few seconds while it loads the sounds into memory. I wanted to be able to open the program without any of these silly dialogs popping up, so I could open the program and get right back to what I was doing.

First things first...
There's a nice set of two files on oleBuzzard's web site [see bottom] called How to Crack. While a lot of what was in these were over my head, one thing they had mentioned stuck--to find a piece of offending code, use ResEdit to find the DLOG ID you want to get rid of--then look for it in the code. I'd done enough Mac programming to know the basics of dialog boxes--GetNewDialog to show them, ModalDialog to get events within them, and a few other toolbox calls that proved helpful.

But anyway. A quick peek with ResEdit revealed that I wanted to avoid DLOG 9990. Swapping this into hex, we get 2706. Onwards into the code.

Resorcerer...
Resorcerer, for those who don't know, is a totally fucking kickass program. The only way I can describe it is ResEdit done right, on steroids--except that that doesn't begin to describe its code viewing/editing features. Just get it. Now.

OK, now that you've got your Resorcerer (I used 1.2.5), open up the CODE resource. Do a search for 2706. Whaddaya know--only one instance. Had there been more, there were a few things which were pretty good signs I was in the right place, even though I know next to no assembler:
1. It's in a move.w just before a _GetNewDialog (this is a pretty big giveaway)
2. The procedure it's in also has _Delay and _HiliteControl calls, which I recognized as being responsible for de-/activating the OK button and (surprise!) causing a delay before it was activated.

To illustrate, here's the code that I'm blabbering about:

```
move.w    #$2706,-(sp)
```

```
clr.l     -(sp)
pea       -$0001
_GetNewDialog        ; TB trap
[some little dialog preparation stuff here...]
_HiliteControl       ; TB trap
move.l    a4,-(sp)
_DrawDialog          ; TB trap
lea       -$001A(a6),a1
movea.w   #$00C8,a0
_Delay               ; OS trap
```

OK, so we've found the annoying procedure. The obvious next step--delete the whole thing!!

Not quite...
Even in this file, I've omitted certain blunders I made before hitting on this method. Not that I'm embarrassed, but they're not very interesting or educational. This one, on the other hand, is a mistake I made from which I actually learned something which seems pretty significant.

I tried deleting the whole procedure (technically, I set it all to NOP, which I assume means No Operation--see, I told you I don't know much assembler). This made the program just stop in its tracks. Whoops. It hadn't frozen, though; a force quit took me back to the Finder.

Here's the end of the procedure:

```
_DisposeDialog       ; TB trap
tst.b     d7
beq.s     <Anon_08>+$72
movem.l   (sp)+,d7/a4
unlk      a6
rts
```

The last line in the procedure is "rts," which seems to be common at the end of all procedures. Guessing that rts had something to do with returning after a procedure (pretty logical, given that the program had just plain stopped), I NOP'ed the entire thing except that line. And it worked--no more delayed box to click out of!!

Cool, but not quite done...
Getting rid of the splash screen was actually a little trickier, as the next dialog to get rid of was 200, or C8. Being a much more common number than 2706, there were quite a few C8's in the code. I decided it would be easier to look for a _GetNewDialog or _GetDialog without much else near it (particularly _ModalDialog, which handles events in dialog boxes. Remember, this next dialog doesn't need a click, just a few seconds). Relax is a pretty small program, so this method was practical enough.

I found one, and instead of NOP'ing it out, I had Resorcerer branch around just about the whole procedure. I don't know the merits, if any, of one method against the other--I was just playing around, and it worked, so I wasn't

complaining. If anyone more knowledgeable is reading this, and wants to shed some light on this issue, please let me know at the addresses at the bottom of the file.

But back to the story. Now the dialogs were gone, but the about box still had "UNREGISTERED COPY" glaring in my face. I was on a roll, and didn't like this. The solution--delete the "UN" from each of two instances of "UNREGISTERED COPY" in the DATA resource. What then showed up was "GISTERED COPY" and then some high ASCII garbage. The solution I hit upon was really simple, and since it doesn't involve any technical knowledge (just a touch of thinking), I'll leave it as a little closing exercise.

That's it...
I'm not making any claims that this was some humungous technical effort, as should be apparent to anyone reading this fairly short file. But I'd always considered this sort of thing way out of my league, and I do think it's pretty cool that I could pull off even a minor crack like this. Of course, as I have the time, I'll be working on other stuff... Hope to have some more advanced files being put out as time progresses.

Comments, questions, suggestions, and by all means corrections--Observer on k0p, or an407599@anon.penet.fi. (Sorry bout the anon address, but otherwise it's a little too easy for people to give me shit about this...)

I mentioned oleBuzzard's web site earlier--if it's not THE place to start checking out the Mac underground, I don't know what would be.
http://www.uccs.edu/~abusby/k0p.html

<PREACH>
I really do want to say that distributing cracked versions of shareware is a great way to kill what is a pretty lively Mac shareware scene. Sure, it's cool to be able to crack software, but there's something to be said for paying for (or at least not distributing cracked versions of) the things you really enjoy as well. Don't start thinking you own the world, because if you haven't known most of the stuff in this file, a lot of the people you're not paying can probably program circles around you.

And in all honesty, I might even break down and send Software Perspectives their $10 after all. :-) Since I'm basically inviting the world to crack their program, I feel like I should at least include their address, just in case anyone else feels an urge:
Software Perspectives
3084 Peachtree Court
Lake Ridge, Virginia 22192-1518
</PREACH>