Chapter 6- Key Disk Protection Schemes

There are a couple of different ways commercial software authors implement Key Disk Protection. Key disk protection essentially is software that requires the original floppy diskettes to run correctly. These types of programs come with an installer for copying them onto a hard drive. Some packages offer three installs to a hard drive; if you need more copies, you have to use the original disk each time you run that program.

Essentially what is happening here is this. On the floppy disk there are files with their INVISIBLE bit set meaning they will not bee seen or accounted for in the volume info. Therefore, if you try to copy the program onto a hard drive the invisible files will not be copied and the copy will not work properly. If you just turn the INVISIBILITY bit off using ResEdit and then copy the files, the program will work. But, this is only for programs that do not always need the key disk. Other programs require the key disk every time you run the application. In those cases, the key disk has a purposely bad block. When you run the application, it will read from the floppy and test the block's status. If it is bad it will continue on knowing it is the original disk, it the block is ok it means that the program has been copied onto another disk which is not the original or key disk. The best way to operate around this scheme is to trace through the program to where it actually reads from the floppy, then change the BRANCH condition after the COMPARE. This will fool the program into always thinking that the block that is read is bad.