reverse engineering

Reverse engineering is taking apart an object to see how it works in order to duplicate or enhance the object. It's a practice taken from older industries that is now frequently used on computer hardware and software. In the automobile industry, for example, a manufacturer may purchase a competitor's vehicle, disassemble it, and examine the welds, seals, and other components of the vehicle for the purpose of enhancing their vehicles with similar components.

Software reverse engineering involves reversing a program's machine code (the string of 0s and 1s that are sent to the logic processor) back into the source code that it was written in, using program language statements. Software reverse engineering is done to retrieve the source code of a program because the source code was lost, to study how the program performs certain operations, to improve the performance of a program, to fix a bug (correct an error in the program when the source code is not available), to identify malicious content in a program such as a virus, or to adapt a program written for use with one microprocessor for use with a differently-designed microprocessor. Reverse engineering for the sole purpose of copying or duplicating programs constitutes a copyright violation and is illegal. In some cases, the licensed use of software specifically prohibits reverse engineering.

Someone doing reverse engineering on software may use several tools to disassemble a program. One tool is a hexadecimal dumper, which prints or displays the binary numbers of a program in hexadecimal format (which is easier to read than a binary format). By knowing the bit patterns that represent the processor instructions as well as the instruction lengths, the reverse engineer can identify certain portions of a program to see how they work. Another common tool is the disassembler. The disassembler reads the binary code and then displays each executable instruction in text form. A disassembler cannot tell the difference between an executable instruction and the data used by the program so a debugger is used, which allows the disassembler to avoid disassembling the data portions of a program. These tools might be used by a cracker to modify code and gain entry to a computer system or cause other harm.

Hardware reverse engineering involves taking apart a device to see how it works. For example, if a processor manufacturer wants to see how a competitor's processor works, they can purchase a competitor's processor, disassemble it, and then make a processor similar to it. However, this process is illegal in many countries. In general, hardware reverse engineering requires a great deal of expertise and is quite expensive.

Another type of reverse engineering involves producing 3-D images of manufactured parts when a blueprint is not available in order to remanufacture the part. To reverse engineer a part, the part is measured by a coordinate measuring machine (CMM). As it is measured, a 3-D wire frame image is generated and displayed on a monitor. After the measuring is complete, the wire frame image is dimensioned. Any part can be reverse engineered using these methods.

The term forward engineering is sometimes used in contrast to reverse engineering.