Routine Performances while cracking:

Opening a program in HIEW:

Drag the program you want to crack on top of hiew, and drop it. This will open that program in hiew.
Keep a Shortcut to Hiew always handy on your desktop, you can also drop the program on the shortcut to open it.

Quick Drag and drop progtocrack.exe on hiew.exe

Finding the Location in HIEW:

In W32Dasm go and stand on the line you want to patch. Now look in the bottom (Status Bar) of w32dasm. It will say something like this:

Line 169 Pg 3 of 66 Code Data @:00401075 @Offset 00000475h in File Tutor1.exe

The important number here to remember is **475**, the Offset number.

Now switch over to Hiew. Press Enter twice. This will get you into Decode mode of Hiew. This mode can also be accessed through choosing F4, -->Decode
Now you are in decode mode. Push F5 and you can type in the offset you want to go to. Type in the offset number. In this case **475**. When you press enter you will land straight at the place you also were standing on in wdasm.

Quick Get Real Offset, Enter twice in Hiew, F5, Type in real offset

Extra
W32Dasm shows you the Relative virtual addresses, while hiew shows you the real addresses. Hiew starts always from 0, while w32dasm starts from an address that is defined in the executable file header.

Modifying a machine code :

Make sure you are on the right address in hiew. Press F3 (Edit Mode).
Now you can change any machine code to another machine code.
To save your changes, hit F9, and F10 to exit.

Most assembled Machine Codes :

In Edit mode you can change mostly the following:

Anything → 90.

```
74xx → 9090       ; removing a conditional jump
75xx → 9090       ; removing a conditional jump


EBxx → 9090       ; removing an unconditional jump

0F85xxxxxxxx → 0F8500000000   ; removing a conditional jump
```

Assembling a new Assembler instruction:

Open the file to edit, go to the right offset, and press F3 (Edit) and then press F2 (Assemble) to assemble a new assembler instruction.

String References:
In W32Dasm, Select Refs-> String Data References.
Same effect can be achieved by pushing the "Strn Ref" Button next to the printer button.

Executing a Jump:
Go stand on the line you want to jump from. The color of this line should be green now and the "Jump To" button is enabled. Press this button to execute the jump.
Press the "Ret Jmp" button to return to the same place.

Executing a Call:
Go stand on the line you want to call from. The color of this line should be green now and the "Call" button is enabled. Press this button to execute the call.
Press the "Ret" button to return to the same place.

Going to an Address:
In w32Dasm menu, select GoTo -> Goto Code Location. Then type in the address you want to go to, and press ok.

You can also simply select the "Cd Loc" button from the toolbar to open the code location dialog.