WinHack v1.10
For Windows 95 and Windows 98

Contents:

WHAT'S NEW???

The registration key for WinHack v1.00 is completely compatible with v1.10.

Well... A few bug fixes. Mainly:

Got rid of all (I think) the annoying "" IS NOT A VALID INTEGER messages, cleaned up the search engines so that you shouldn't end up in an "endless search" anymore. AND.... Most importantly, jazzed up the search engine so that FAST mode
is now more reliable than before.

WinHack is now much FASTER than ever!
The documentation below is exactly the same as v1.00, no changes there except what I have just said. I will continue to fix all reported bugs with WinHack until I release v2.00

What is WinHack?

WinHack is a program that helps you cheat and crack games by letting you manipulate the memory that the game uses.

Remember Game Wizard? Well, this is like a Windows version of that.

WinHack has many features that will make cheating easy (assuming you have a little knowledge about how computers work).

Winhack is a tool aimed at knowledgeable beginners to experts.

WinHack will also let you create a stand-alone trainer which you can give away completely for free.

What can WinHack do?

Winhack has the following features:

- You can search memory for values that change of don't change.
- You can chop and change between 7 different and powerful search methods at any time to suit you
- You can view memory directly
- You can type directly into memory and modify memory directly like a HEX editor
- You can see immediately what the "real" decimal value of memory is just by placing your cursor over it.
- You can change the "real" value of memory without having to convert decimal to Hex first just with the click of a button.
- You can search memory for ASCII or HEX strings
- You can create a list of memory addresses called TAGS
- You can easily change the "offsets" of a tag list to point to the right area of memory if it changes from game to game.
- These TAGS can "poke" or freeze memory for you in many different and exciting ways.
- You can save and load lists of TAGS and distribute your TAG lists to anyone else who uses WinHack
- You can create a stand-alone trainer from a list of TAGS that will run without WinHack and you can give (or sell) to anyone you like.
- Any trainers you create will have YOUR name on them, not mine!
- You can register WinHack and enjoy all the benefits of complete game cheating power!! (cue evil laughter: mwahaHAHAHAHA!!!)

What is planned for the next version?

- A much faster engine to search through memory. More accurate as well.
- More functionality with tags. Almost allowing you to "Script" intelligent cheats without any programming at all.
- The ability to use the same methods and TAGS on Saved-Game files as well as memory.
- Commands to load and save portions of memory to and from the hard-disk at the touch of a button (Remember the item importing and exporting in Diablo cheaters?)
- Whatever you decide it should do. E-Mail me with your suggestions, and I'll try to add into WinHack what YOU want to see in a game cheating program.
- Complete and context-sensitive online help.
- A method of tracking down memory areas that move between playing a game today and playing the same game tomorrow.

How do I use WinHack?

Firstly, WinHack needs to know which game you want to cheat, so start the game, start WinHack and select the process (game in memory) you would like to work on. Once you have done this, the rest of the options will become visible, and you can start.

It is now up to you to find the memory you want to cheat (the bit of memory that the game uses to control your life, bullets, health, etc.) and work with it. How to do this will be covered a little further down.

Your first task would be to use the search engine or memory editor to find the memory that you want to cheat. You would then create a TAG at that point by clicking on the FIRST BYTE of the memory address in the memory editor, and then clicking on the CREATE TAG button.

Tags will be discussed in more detail later.

You can then use your created TAG LIST to cheat the game with a minimum of hassle. You can save your TAG LIST and give it to anyone else who has WinHack.

You could then create a stand-alone trainer from your tag list to give to other people.

WARNING: WARNING:
There is no guarantee then the memory regions your tags are pointing to now will stay the same every time you load the game. If they move, your trainer becomes useless. This is a problem that I am trying to overcome in Version 2 if I can. WinHack is broken down into four main areas.

- Search Engine
- Memory Editor
- Tag List
- Trainer Creator

Search Engine: This is the bit that allows you to search through the game's memory to find the bytes that control what you want to cheat.

There are several methods to choose from, and unlike some other programs like this, WinHack allows you to chop and change between methods half-way through a search to suit you.

When you start a search, you have the option of starting a search when the value you are looking for is unknown. Let's say you want to search for your life value, but it is shown as a bar instead of numbers. This is when you would start a search with an unknown value. If, however, you could see that you had, say, 95 life, you could start the search with the known value of 95.

You would then play the game a little and when your life had changed, you would come back and continue the search using one of the following methods:

If your life has changed from, say, 95 to 87, you would continue the search using the CHANGED TO method, and put 87 in the box.

If your life is unknown, but you know that you have taken, say, 7 point of damage, you would continue using the INCREASED BY or DECREASED BY options, putting 7 in the respective box.

If your life is a bar, you don't know what it was, or what it has changed to, you can use the VALUE HAS INCREASED or VALUE HAS DECREASED to check for any memory that has gone up or down by any amount

In the absolute worst case scenario, you can use the VALUE HAS CHANGED or VALUE HAS NOT CHANGED methods if you really don't know what you are looking for.

TIP: Always tell WinHack as much about what you are searching for if you can. Only use the more general methods if you can't find the memory any other way.

WinHack can only store up to 65000 or so possible addresses at one time, and if the game is large, it might reach this number before finishing searching through all the memory. What you have to do then is to change the START and END addresses at the top of the screen and try again.

When you have found memory addresses, they will be put in a list on the right. Simply double-click on an address to be taken straight to the **memory editor.**

Memory Editor: This allows you to see straight into the memory of a game, and even type directly into the memory of a game.

You can use the arrow-buttons on the right to move the window up and down. When you place your cursor over a byte (the block you are in goes blue), the bottom-right of the screen will tell you in real-world numbers what the values under your cursor are. If you change one of these numbers, the memory your cursor is at will be changed to reflect the change.

You can also search here for ASCII (text strings) and HEX strings here. By typing an ASCII (text) string into the **BOTTOM** text box and clicking the FIND NOW button, WinHack will start searching. If the IGNORE CASE check box is checked, it will treat capital letters and lowercase as the same thing. You can type a HEX string into the **TOP** text box (e.g. FF00A0FE) to search for the corresponding hex string.

When WinHack finds the string, it will move the memory window to that place and let you take a look at it. If you want to continue searching, click the FIND NEXT button to start where you left off.

If you already know the address of memory you want to look at, you can type it directly into the text box next to the GO TO button, and then click on GO TO.

If you have found an interesting bit of memory and want to create a tag, put your cursor over the FIRST byte (the box in the edit memory window goes blue) and click on CREATE TAG.

Tags will be discussed further later on.

TAG LIST: This part organizes the tags you have created, and lets you freeze and poke into memory easily. When you click in the text box that has the data for that tag, you will see that the information in the SELECTED TAG box in the lower-left corner changes to show you information about your

selected tag. You can change a tag's data type and tag type here, as well as the memory it point to, and any offset you want to apply to that tag.

You can save the TAG LIST by clicking the SAVE TAG LIST button, load a previously saved TAG LIST the same way, delete the currently selected tag, or SORT the tag list by it's ADDRESS value in ascending order.

The NORMALISE TAGS button will add the OFFSET value of a tag to it's ADDRESS value, and set the OFFSET value to 0, e.g. If a tag is pointing at address $00001000 and it's offset is 5, clicking the NORMALISE TAGS button will make it's address $00001005 and it's offset 0. This is useful if you are adding new tags to a previously loaded tag list that has different addresses and offsets.

Offsets were added because the memory of a game can change when you start a new game. WinHack has made it easy for you to change the address your tags point to.

Let's say you have created a tag list yesterday, and now you load it and all the values are wrong. You can automatically change the offset of all the tags by a certain amount by placing that amount (negative values are allowed) in the text box next to OFFSET ALL TAG BY button and clicking on the button. You can then NORMALISE all the tags and carry on as if nothing had happened.

If you don't know by how much the memory has changed, WinHack can also help you there.

Let's say that your first tag is a STRING tag pointing to the name of your character in a game. All you have to do is find the new address of your character's name in memory, put that into the text box next to CALCULATE OFFSET FROM button and click. This will place the right value in the OFFSET ALL TAGS BY box, and you can just click to make the changes.

It get's even easier!! If you go into the memory editor screen and place your cursor (the box goes blue) over the first byte of your character's name, all you have to do is double-click in the empty CALCULATE OFFSET FROM text box to make WinHack enter the value for you!

The different types of tags will be discussed a little later (I promise!).

Trainer Creator: If you want to create a stand-alone trainer from a tag-list, this allows you to enter the information you want the trainer to show, eg. The name of the game you are hacking, any comments, e.g. and let's you select whether to create the trainer from the tag list you have currently got in memory, or one you have already saved.

WARNING: WARNING:
When you create a trainer, it will only work for the CURRENTLY SELECTED PROCESS. In other words, the name of the process you selected at the start will be what the trainer will look for when you load it. If you have clicked on, say, EXPLORER, and create a trainer using a tag list you made cheating the game DIABLO, it won't work with DIABLO, it will try and cheat EXPLORER, got it?

Using Tags

An Explanation Of Tags: (At last!!)

Anyone who has ever used a program called Universal Game Editor will understand this easily.

When you create a tag, you are really creating a text box that points to a place in the game's memory. If you change the value in the tag's text box, that change will be made in the game's memory automatically.

When you create a tag, you can choose the following types of tag:

Poke Memory
Freeze Memory
Freeze To Tag

Poke Memory: This is easy, it takes the value you placed in the tag's text box and writes it ONCE to the game's memory

Freeze Memory: WinHack will take the value you placed in the tag's text-box and write it to the game's memory 100 time per second, in effect freezing that memory at a certain value.

Freeze To Tag: Here's where it get's clever <grin>. You can tell this type of tag to point to a place in memory, but FREEZE IT AT THE VALUE OF A DIFFERENT TAG. This comes in useful if the game has something like TOTAL MAGIC and CURRENT Magic. You can set a Poke tag to TOTAL MAGIC, and then set a Freeze To tag at Current magic that will freeze that value to whatever your TOTAL MAGIC happened to be at that time!. So that if your TOTAL MAIC changes, so will your CURRENT MAGIC and you will always have a full amount of magic!

Tag Data Type: A Tag can be one of five different things. It can be a string of up to 20 characters, it can be a BYTE (0 to 255), it can be a WORD (0 to 65535), it can be a DWORD (0 to 16777315) or it can be a float (e.g. 5.67).

NB. NB. NB. NB.
If you have created a Freeze To tag, it will always be a WORD tag, and the value in the tag's box MUST BE THE NUMBER OF SOME OTHER TAG. If your TOTAL MAGIC tag is number 7, and your CURRENT MAGIC tag (Freeze To tag) is number 8, the value in TOTAL MAGIC could be something like 500, but the value in CURRENT MAGIC **MUST** be 7, which is the number of your TOTAL MAGIC tag, got it?

Why Should I Register?

Well, the obvious answer is that it's the right and proper thing to do!, but there's an even better answer.

For just $20, about £8, which is less than the price of a game, you get all this cheating power, and what's more, you get YOUR NAME on it!!.

Yea, I suppose you could just get a cracked version, but then it wouldn't have YOUR NAME on it would it? Which means that all your genius in cracking a game would never be recognized.

If you register, everyone will know that the you, the HackMeister Supreme has once again exerted the fantastic talent that legends are made of to crack a game for the betterment of all mankind!

All this for just $20!! You can't go wrong!

How do Register?

At the moment, you can't. As I type this, WinHack is in Beta Mode which means that it is in Test Mode. When the Release Version is um.. er.. released, All the necessary information will be here. The basic options will be this:

Send me a check in UK Pounds Sterling, a Postal Order in UK Pounds Sterling.

Until I can get Credit-Card Registration up and running, it will have to be the slow way, sorry.. You can find the order form in the .Zip file as **ORDER.TXT**

What do I get for Registering?

Well... peace of mind?

No seriously.. You get your name plastered all over WinHack and **any trainer's you create!!**. All the great and nifty features get unlocked so you can use WInHack to it's full potential.

You get to be a GOD when it comes to games, you get to defeat the programmers and prove your mastery over your environment, you get to.... oh, right, I'll shut up now..<grin>.

You get everything I've gone on and one about above for less than the price of a good game!

How do I register?

Simple, fill out the order form that came with the Zip file you got this out of (it's called ORDER.TXT) , fill it in, bung in the correct amount's worth money and send the whole shebang my way.

As soon as I get your money, I'll send you your registration key by the means you preferr, E-Mail or Real Mail..

Easy as that, and when I get the Credit-Card registration system up and running (slated for later this year), you'll be able to register and get your key ONLINE!

Yea!

But why wait?

Get cheating TODAY!!! Yes!! TODAY!!! (well... maybe tomorrow.. you know how slow mail is... <grin>

Thanks to:

Jeremy Pallant: His outstanding help with advanced pointer logic made this program possible. Without him, I'd probably still be pulling my hair out and reading every technical manual I could get my hands on.

Patrick van Loon: All hail my primary Beta-Tester in Windows 98. Without him, I could not guarantee that WinHack would even RUN on Windows 98. Keep up the good work, Patrick. Next time you find yourself in London, I'll buy you a pint <GRIN>.