Outline of article(s) for UK magazines on making trainers / game editors.

Table of contents

Synopsis to publisher

This series of articles will show the end user how they can make the changes to the saved games as well as the games themselves on the fly so that they can make their own "trainers" or saved-game editors using freely available tools.

Such tools are: Magic Trainer Engine and its complementary tool Trainer Maker Kit (both freeware) and others. All the tools are available on the Internet, but there is one site that contains them all or at least links to them. The site is http://www.gamehacking.com, which I have no affiliation with at all. If it is OK to mention this site during my article, then I will do so.

There will be two articles, both include working examples of trainers and how these programs were created using some of the tools mentioned above. Lots of screenshots of dialog boxes will be necessary to show the step-by-step nature of making trainers et al. I've included them in this article at the relevant place, but you may require them all grouped into one place on the final article should you wish to publish it.

I originally did an article for a magazine called ST Applications some years ago on the routines and methods needed to make trainers for games on the Atari ST system. This article delved heavily into the 68000 assembly language used on that machine, whereas this current edition will not go any further than the differences between bytes, words and double-words and their uses within the realms of making cheats and trainers for games.

WRITING A TRAINER – A GUIDE

What is a trainer?

A trainer is a memory resident program that you usually load after your game (i.e. Press ALT & Tab to access Windows and load in the trainer from there) and it alters the variables inside the game to values that you would prefer. For example:

a) The number of bullets in your gun
b) How many energy packs you are carrying
c) The current state of your "lives" to stop them reaching zero

Trainers rely on the ability to detect your game in memory via its process name or window name. These are two settings that you may have come across before.

The Process Name is the title of the program you see if you press Ctrl, Alt & Del. The window you see contains the list of processes you currently have running in the background as well of those that you know that you have loaded in yourself. Background tasks such as Explorer and SysTray are necessary items to have under all copies of Windows 95/98.

The Window Name is that name that appears on your Taskbar when you press ALT & Tab out of the game to get to the Windows desktop. All programs when minimized will have a Window Name.

Starting off.

Where to begin? The two things you will need are:

a) A target game that you need that little bit of help with.
b) The relevant packages to enable you to search and create these trainers.

Knowledge of the various numbering systems on a computer. This small table will allow you to find out what kind of number ranges are stored in your PC and how many bytes of memory each type of number can hold.

BYTE	1 byte	0 –> 255 (00 -> FF)
WORD	2 bytes	0 -> 65535 (00 – FFFF)
DWORD	4 bytes	0 -> 4294967295 (00 -> FFFFFFFF)
FLOAT	4 bytes	
DOUBLE	8 bytes	

Doing your homework.

Before you start writing a trainer, play the game and get used to the variables in use and how they are affected.

1) How many bullets in that weapon (or weapons - **Delta Force** is a good example here)?
2) How many lives do you get? Or are there any other variables that decrease by a value of 1 each time?
3) How often does these values change and by how much? If your bullets count is low down, how often do you come across refill packs and by how much do they replenish your count of bullets?

It may be easier for you to pick on a game with as **few** variables as possible. Those of you wishing to delve straight in with your favourite Role Playing or Real Time Strategy game had better find something easy first to practice on. A perfect example is a shoot-em-up. Not everyone's cup of tea, but when it comes to making a trainer, they are the easiest target practice.

A Working Example – Asteroids by Activision

This updated conversion of the original arcade game is a fairly easy target to make a trainer for. It's now out on budget, so grab a copy from your local store for a few quid. Otherwise follow the various steps through this tutorial and use whatever game(s) you currently have as a basis and work out your own addresses and values.

The tools for the job are as follows.

a) Asteroids by Activision
b) Magic Trainer Creator v1.27
c) Notepad (for jotting down the addresses we find)

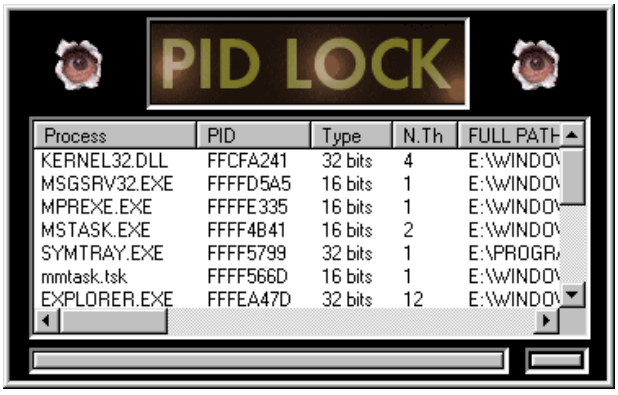
First load up the game and play it a few times. You will notice that the game starts you off with 5 ships (counting down from 4 through to 0). This is a bit stingy on the game makers part - why else would we be attempting to train a game, unless we thought it was too hard and impossible to finish?

Now start a fresh game, but pause it as soon as your ship is on screen. Now press ESCAPE to pause the game and then press ALT & TAB to access your Windows desktop. Depending on how much RAM you have in your machine, will depend on how quick your desktop appears.

Find and launch your copy of the Magic Trainer Creator. It can be a rather daunting screen to look at when you first run the program. I doubt whether you will use all the facilities of the program and there is a help file – of sorts as it is in pigeon-English.

The first option you will need for this trainer we are about to make is the Process selection. We need to tell Magic Trainer Creator which program in memory we want to look for the game variables in. Find the section to the right and click on the grey square next to it.

A list of the various process names is listed in a window called PID Lock. PID stands for Process ID. You will see a list of all the programs you normally have running in the background as well as your game.



The one we are interested in is of the game we want to train. On my own machine it is listed as ASTEROIDS. Double click on it and a large hexadecimal number will appear under the word Process ID.

We are going to be doing a normal search for the number of ships in the game, so click on the Normal button where it says Search mode. I will explain Advance and Progressive options later on under other game examples.

Where it says value to search for, enter 4.

Now click on Search. Magic Trainer Creator will look for all the values between the start and end of the Asteroids program file for all occurrences of the number 4. It will then store these until we notify that the value has changed. On my own machine (a P2-400 with 128MB of RAM) it took a lot of time to search through all the possible occurrences of the number 4 - so you can expect a wait if the addresses listed in the Begin Address & End Address are far apart. Smaller programs or values not as frequently used, as 4 will be found a lot quicker.

My own search revealed on the first pass that there were 249027 occurrences of the number 4. This is way too much for either human intervention or Magic Trainer Creator to handle.

So we must now alter this value in the game so make it easier to find.

Alt & TAB to go back to the Asteroids game press Return on "Continue Game" and lose another life on purpose. When it says you now have 3 ships on screen, press ESCAPE to pause the game and then press ALT & TAB again to go back to Magic Trainer Creator.

Delete the 4 from the search box and enter 3. Click on the search button again.

This time, the number of occurrences where an address that used to have the number 4 stored there and now has the number 3 in it has dropped to 35. This is manageable but only if you really want to see what happens if you alter the value of 3 in all of these addresses to a higher value and then go back to the game to test it. This is just not worth it in the long run – unless you really need to pass that length of time! Go back to the game, lose another life and come back to Magic Trainer Creator.

Delete the 3 from the search box and enter 2. Click on the search button again.

Hey presto! There's only 1 address listed. Magic Trainer Creator has found a single address whereby the number of ships of the player is stored and subtracted from every

time you lose a ship. It is now up to you to decide how many ships you want in the game.

But before you can alter the current value, you need to know a little hexadecimal. Load up Calculator on the Windows desktop, and enter 100, then click on the Hex button and you get the value 64. Go back into Magic Trainer Creator and double-click on the single address displayed in the "Addresses Found" box, it will be transferred to the "Address" box with the "Write" and "Read" buttons in.

On my own machine, the address displayed was 44C248 it could be different on your own machine.

Type in 64 into the box and click on the Write button. Click on the OK when the "Operation Done" message appears.

Now we need to test that this value has worked. So go back to game, press Return to continue and see how many ships you now have. 100 ships are now available and this should be enough for you to survive until the end of the game – unless you are really bad at it!

There are now 2 options for you:

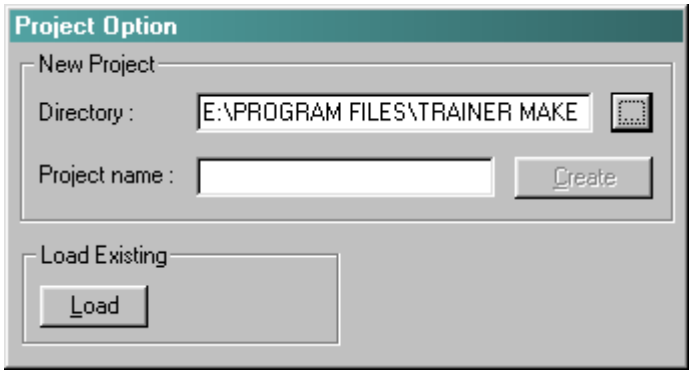
a) Convert this working cheat into a proper trainer program that you can use instead of working through the above rigmarole every time you want 100 lives.
b) Carry on and work out what other values you can stop from decreasing in the game.

We are going to go with option (a) for now.

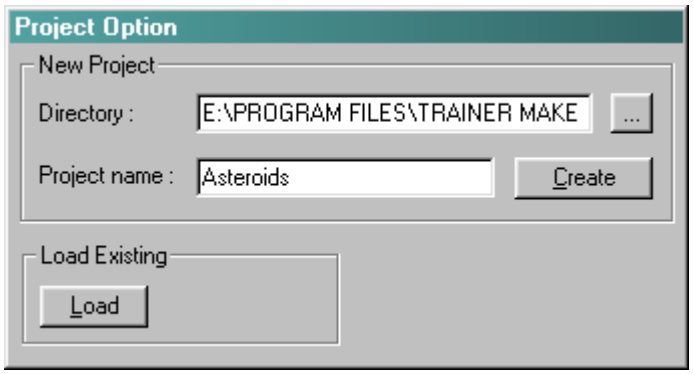
Creating a stand-alone trainer program for Asteroids.

To do this we are going to need another program by the author of Magic Trainer Creator called the Trainer Maker Kit. The latest version is always available from http://fly.to/mtc. The version that I am using for this article is v1.5.

Install the program if you haven't already done so. Load up the Trainer Maker Kit and the first dialog box that appears will be one asking you if you want to create a new trainer or open an existing trainer project.



Type in Asteroids into the Create box and click on the Create button.



A separate folder will now be made inside the h/drive location of Trainer Maker Kit with the name of "Asteroids" and all relevant files belonging to that project are stored within.

Click on the intro text to get past the message telling you what version of the Trainer Maker Kit you are using.

You are now presented with an empty dialog box, which is the background screen to your trainer.

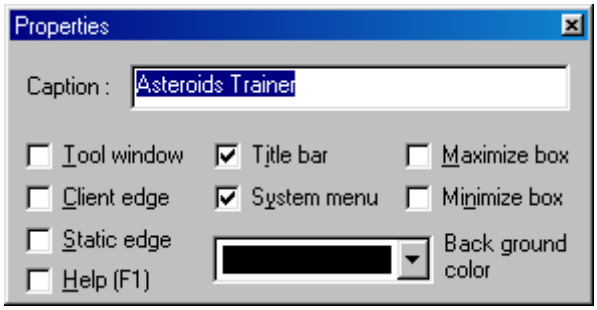
You can add all sorts of text messages, pictures, scroll bars, input boxes and even play sounds when certain options are selected, but for this simple project we are going to add two buttons.

Why two options? One will be for the instant upgrade to 100 ships and the other will be to freeze the ships counter at this value giving the inference that we will never be able to get to the "GAME OVER" message as we will permanently freeze the number of remaining ships at 100!

The first option is known as a poke or write-once option, the other is known as a freeze option.

First thing we will do is to change the name of the dialog box so that it means more to us than just "Dialog1". Press the right mouse button on the empty space within the dialog box and click on the word properties.

Fill in the Caption button to something similar to the above picture. Click on the background color (US spelling intentional!) option and change it to black.

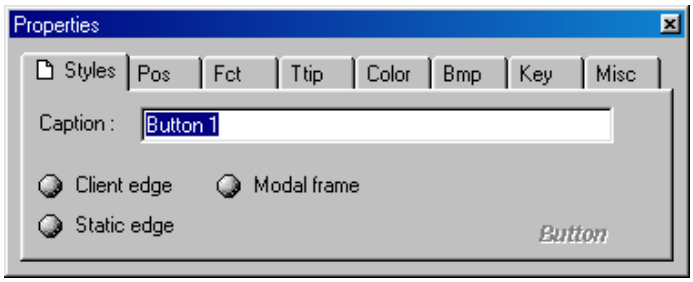


Now close the box and the screen should now show the following	

We are now going to add the two options we outlined above. We do this by selecting one of the icons from the button bar on the top of the screen. But first, a little explanation of what buttons do.

a) Build a button option – i.e. Click-able option
b) Enter a text message
c) Insert a picture
d) Insert an editable box – i.e. the user is able to change values themselves
e) Insert a scroll bar – i.e. allow the user to select a value between a start and end value
f) Insert a group box – i.e. group similar options into a separate sub-window
g) Insert a text scroller, star field or movie (AVI format) – i.e. to really make your trainer stand out!
h) Stop the build of the trainer
i) Debug your trainer – i.e. check what values and addresses are being altered (back to school with the maxim "always check your work"!)
j) Build your trainer into a separate program
k) Run your trainer – to test it and see what all your buttons do.

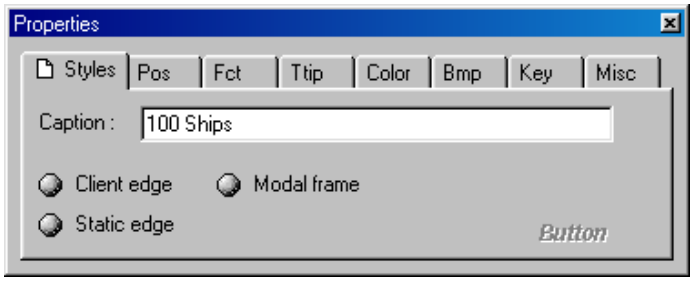
Click on the icon for a button on the menu bar and "Button 1" will appear on your dialog. Now press the right mouse button on it, and click on the word Properties.



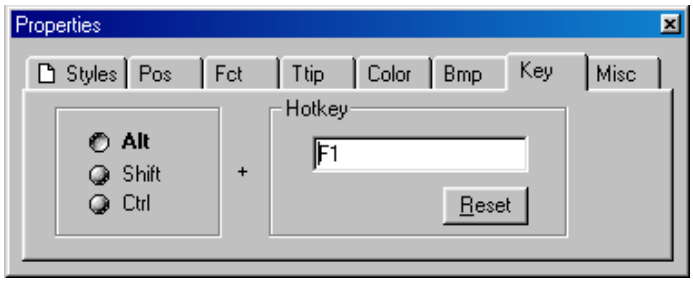
In this dialog box are all the values associated with this button, and what happens when you click on it. For the arty ones out there, you can even associate three separate bitmaps for this button, just like a bitmap on a web page.

To keep with this simple project, all we want to do is to name the button and tell the machine that we would like a "hot-key" associated with the option so we can access it from within the game instead of having to ALT & TAB out every time we want to pump the values up to 100.

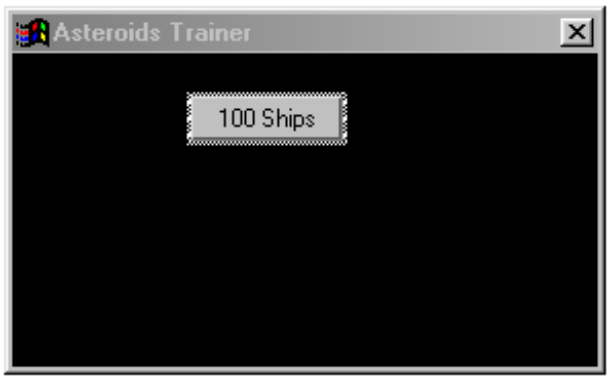
So, change the text on the first button from "Button1" to "100 Ships".



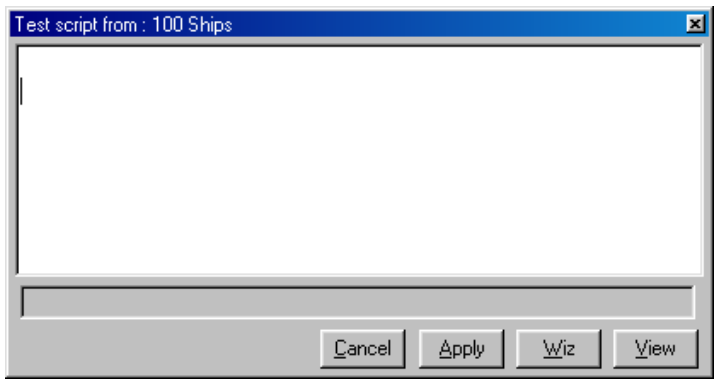
Now click on the second to last option "Key" and we will set-up a hotkey. Change the key used to ALT & F1. To do this, you click on the option for "ALT" and press F1 on the keyboard. The box should now look like this.



Close this dialog box and look at the trainer workspace area. It should look like the one here.

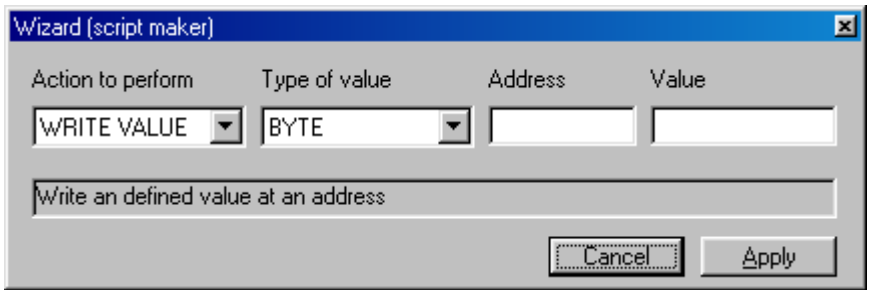


Click the right mouse button on our new button and click on the option "Write memory actions". Another dialog box will appear.

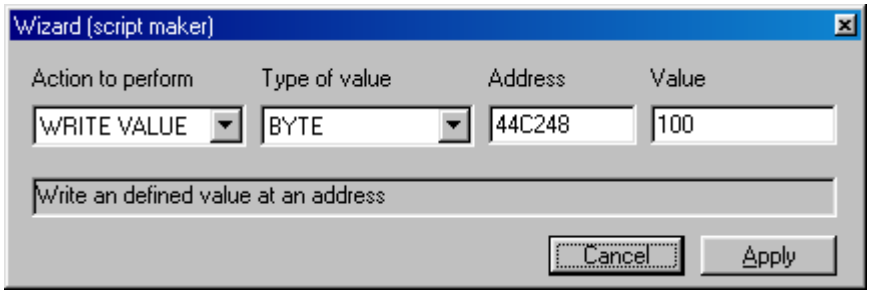


This is where we will be adding the various instructions that will happen when we click on our "100 ships" button. Luckily we are only altering a single address, but other trainers you may design might require the current number of lives/ships or whatever to be entered into several different addresses in memory.

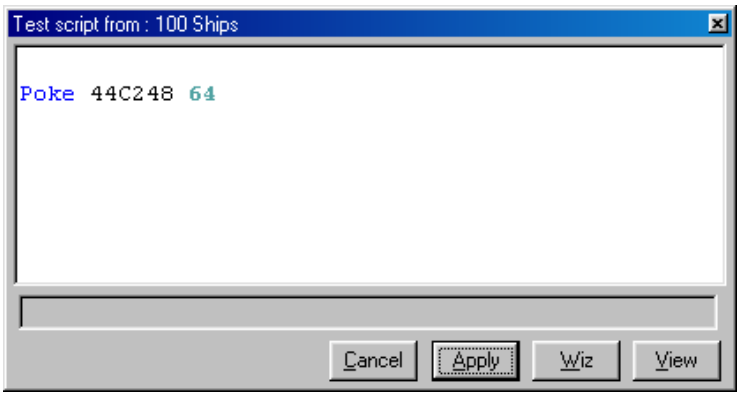
Luckily this tool has a "Wizard" which allows us to create the action that will change the current value of ships to 100. Click on the "Wiz" button.



You should see the above box appear. We now need to change this action so that it puts our new value of 100 into the correct address. This is where your notepad comes in – I assume you wrote down the address you found in Asteroids. In my case (and might also be in yours) the value for the amount of ships was stored at 44C248. So type in this address into the "Address" box. We want to force the value of 100 into this address when we click on our new button, so enter 100 into the "Value" box. Your Wizard box should now look like this:



Click on Apply and you will now see an entry into the script window, which states that we will be poking the address of 44C248 with 64 (100 in hexadecimal).



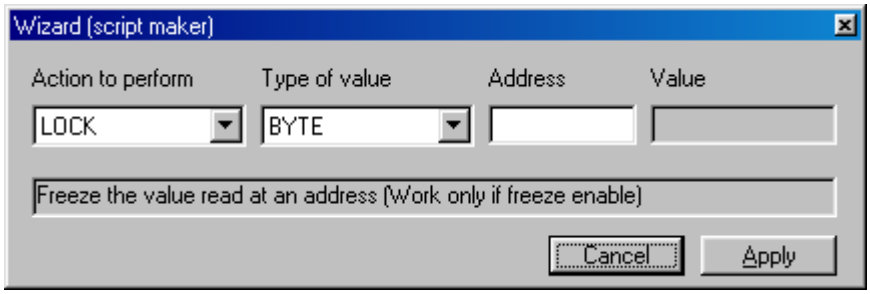
Click on Apply again and you will be back to the main dialog box. We now have a button that we can either click on when the trainer is running, or in the game we can just press ALT & F1 at the same time to get the same effect.

The other option we will add is the ability for the really bad players to freeze the number of ships left at the current value. This option is also handy if certain games have an extra check for the amount of lives you have and trigger off a "you have been cheating" alarm and that hi-score you were after becomes unattainable. It's happened before so I won't say which game(s) are the culprits in case you own one of them!

As before, click on the "New Button" icon and press the right mouse button on it so that we can alter the text from "Button2" to "Freeze Ships". Also enable the hotkey selection and this time place it under ALT & F2. Your dialog should now look like this:

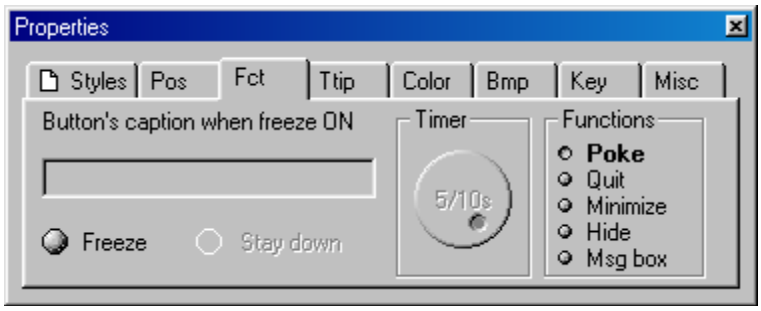
Don't worry about it still looking ugly – functionality being better than beauty at the moment. It's a Skoda style-trainer at the moment and we will make it look like a Ferrari later on in the article!

Press the right mouse button on the new "Freeze Ships" button and click on the option "Write memory actions". A similar dialog box will appear as before and click on the "Wiz" option again. This time we will not be making a "Write Value" cheat, but one that locks the value at a constant level. Click on the "Action to Perform" drop-down box and change it to LOCK.



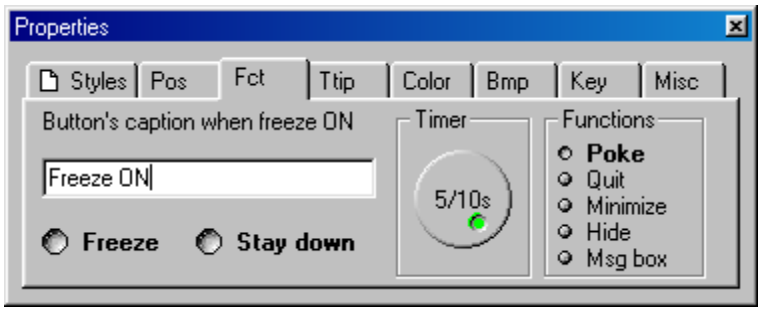
Do you see the note underneath? That is to remind us of another option in the properties section of our new button. So, as before, use the same address as we did for the 100 lives option before and in the Address box enter 44C248 then click on Apply.

For the freeze option to work, we have to add another function to the button. So it's back to the "Freeze Lives" button properties and this time click on the "Fct" option.



This allows us to associate a number of functions with each button we create. The default option is Poke so that's where we shall leave it. The timer option is set so that every 5/10th's of a second the lives counter will be set to the same continuous value.

Click on Freeze and if you want the button to look as if it has been pushed in, then also click on the Stay down option. In the caption box enter the words "Freeze ON". It should now look like this:



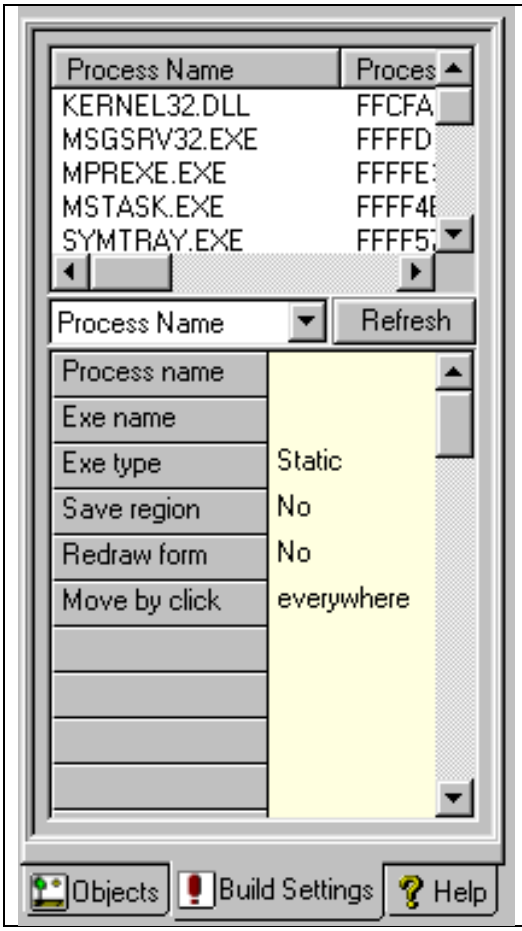
Close the dialog. We now have two working buttons that will give the user two options in this Asteroids trainer. Depending on how much of a cheat they feel like, they can either bolster up their ships counter to 100 or leave it permanently set at 4.

Making your trainer into a stand-alone file.

This is the end result that you have been working towards. The completion of the trainer into a single file that you can give to your friends, upload to a cheat depository website or even make your own website up with just your trainers on – whatever you want to do with it, you need to build it and test it first.

So far through this tutorial, you've stayed in one of the main sections (Objects) of the Trainer Maker Kit. Now it's time to see what the other two are for. The third is the help file and very useful it is too. Read through the help section when you do not understand why your new option is not working.

The other section is the "Build Settings" one. Click on it and you have a small range of settings to choose from.



In this section you will recognise the **Process Name** selection from the Magic Trainer Creator. You have to tell Trainer Maker Kit what process it is to look for before changing the values you have opted to alter and fiddle with! You therefore have to have the Asteroids program running temporarily in order for you to select it. Click on Refresh until you see Asteroids listed and then double-click on it.

Exe Name is the name of your trainer. In our case "Asteroids Trainer +2" seems enough for now.

Exe Type is whether you expect the person running this trainer to have the latest copy of the MFC .DLL file installed in their machine. Windows 98 users are OK, but if you set this to Linked and the user is running Windows 95, they may come across a few problems running it.

Once you have set up the first three options, you can click on the Build icon on the top row of buttons and a true program file created to your specifications will be built and stored in the main Trainer Maker Kit folder on your hard-drive.

Now all you have to do is test your trainer! Test it on your machine, someone else's machine, or any other machine that is of a slightly different specification than your own.

Once that is all up and running and working perfectly, it is up to you what you do with it. I've included a section at the end of this article on what to do with your trainer next if worldwide publication is your thing ☺

Another search example – Progressive searching

We will be using a different game now .. something that I can guarantee that everyone has somewhere on their PC. That's it, a card game. Some of you may want to use Solitaire, but a much better clone of the game is Hardwood Solitaire. Download it from any of the decent download websites – such as http://www.download.com/.

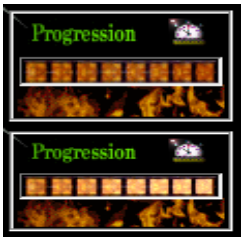
Load up Hardwood Solitaire and then load up Magic Trainer Creator. Go to the process ID selection box and select HWSOLII. Now we are ready to use one of the other styles of search available in Magic Trainer Creator.

The first thing we need to do is tell Magic Trainer Creator that we are going to do a Progressive Search. Click the mouse on that correct button in the Search group.

Now click on Start. There will be a slight pause and it needs to write to a temporary file a lot of information. You will see a series of brighter orange squares will fill up the "Progression" box – once these are full, you can start to play the game.

Empty means it is ready to start a fresh or continue a previous search.

It is nearly ready to continue searching.



Where the box says "Value to Search", look underneath this box and you will need to click on it to change it to a "+" sign. This means we are looking for values that have increased (i.e. the current value for the time in Hardwood Solitaire) and not decreased.

To make the searching easier, click on the Menu option when you are in Hardwood Solitaire and this will pause the timer. We can now go back and forth between the two programs finding out where the time counter is stored in memory.

This can go on for a few attempts as Magic Trainer Creator whittles the possible addresses down from several thousand to something a little more manageable.

As this example screen grab shows us that after a few clicks of "continue" that this is too much for us or Magic Trainer Creator to comprehend. So let the time increase a little more and click on continue again and again until the box displays a selection of addresses.

Eventually, you will be presented with a few possible addresses. Look at the current time in Hardwood Solitaire, convert it to hexadecimal and then double-click on each address and click on the "Read" button. It will display the current value - if this is near enough to your time in hexadecimal (give or take a few extra seconds if you weren't quick enough to pause the game) then this is more than likely the time value. On my own machine the result was C00770.

We can now go about freezing the time.

Create a new project in Trainer Maker Kit. This time add 2 new buttons and 1 edit box.

a) 1st button will poke in a new value for the time
b) 2nd button will freeze the current value for the time
c) Edit box will be used to display the current time.

I will leave the design and implementation of the trainer up to you. This is purely a test – I don't think the world is ready for a huge release of trainers for Hardwood Solitaire or Solitaire! But here's a screenshot of my own one - which *may* be available with this article If I feel embarrassed enough at writing and then releasing a trainer for a card game!

Adding extras to tart up your trainer

OK, your work of art is ready and it works. Now doesn't it look ugly? Luckily the only limitations of the trainer and what it looks like are down to you. There are countless things you can do to change the look and feel of the trainer, but still keep its functionality.

Add some graphics. All graphics have to be in Windows Bitmap format, so wherever you get them from or design them yourself – remember to save them in .BMP files. The graphics could be used in the following ways:

a) as a splash screen that appears for a few seconds (or user presses a key)
b) as a background (you can make any BMP file with any form of shape as the background instead of a boring dialog box)
c) as buttons .. design three buttons or keep two the same and use another as the "ON" button.
d) Design a mini-logo that the people can click on and it emails you in case of bug reports etc.

Sounds can also be added to your trainer. But remember that not everyone has got the time to wait for some ditty you've created in Dance Ejay to finish playing before they can switch on the trainer options. Keep em small and sweet and preferably lower the sample rate from CD quality to Radio quality. Everything you add as "an extra" to your trainer can increase the overall build size of the trainer. No-one wants to download a trainer that is bigger than the game they want to cheat at!

Icons – Trainer Maker Kit has an option whereby you can grab the icon from any other executable source. I normally just grab the icon from the main program file of the game I have trained, but you may want to design your own or edit the icon so that it looks slightly different. However you go about it, as long as it adds to the "look" of the trainer. Anything looks better than the standard one that Trainer Maker Kit includes.

Text scrollers, rotating bitmaps, .AVI files are all possible. Design an animated logo in Xara 3D and then export it as an AVI file. As per the sound options, the more you add the larger your trainer file becomes.

Think of those with less hardware than yourself. There are still machines out there with 32MB on board. They've got the game installed in memory and now they have to wade through a trainer that just might tip their system over the edge because you wanted a 2MB rendered intro to it!

Places to send your trainer to

Why not? You've spent the best part of a few hours wading through the game finding out what goes where and what happens if you alter figure ***x*** at location ***y***.

There are plenty of websites that specialise in cheats, hints and tips and trainers. So pop along to these sites, see if there are some trainers for the game you've just done and download them.

Run the trainers with your game. Run a check between your trainer and the one (or ones) you have downloaded.

a) Does it have any extra facilities that yours does not?
b) Does the trainer work with your game? You could have patched your copy of the game and the trainer only works with the initial release.
c) Does the trainer only work with a release from a particular country?

Mention all these differences either on the trainer dialog box as well as in any accompanying README.TXT or FILE_ID.DIZ file you include in with the ZIP file before you send it to the person who handles all the incoming trainers. They just want to open the email from you with your new trainer, examine the accompanying text file and then add it to their site.

Above all – test your trainer before you send it to ANYONE. You'll only suffer at the hands of others email if you release a trainer that does not work. If you have a Pentium 2 machine, then test it on an AMD K6. If you have a TNT2 graphics card then test it on an ATI Rage.

Some sites:

http://www.avault.com/cheats

One of the largest depositories of cheats, walkthroughs and trainers. Check this site out for other trainers of the game you have just done to compare notes! Or if there is a list of level passwords, then make these available from within your trainer via the Msgbox option under the FCT section of the button properties.

http://www.gamehacking.com

The latter is a website which contains all the "tools of the trade" as well as more hints and tips for using other programs like Magic Trainer Creator and the Trainer Maker Kit. They also run as a group of trainer makers helping each other out. Check out their releases page to see what trainers they have made as well as what options they include.

Voodoo Banshee cards – a word of warning to future trainer makers

The current Banshee range (not so sure about the newer Voodoo 2000/3000 series) will NOT allow ALT & TAB back to the desktop when you are inside a game that is using the 3DFX commands.

I suffered this for more than a few months whilst I had a Banshee card – no trainers were possible except for playing the games in Software Rendering mode. The games looked ugly and I had no way of testing that the same trainer would work under 3DFX.

There may be other graphics cards that do not allow task switching. As more people read this document and let me know about their own hassles, then I can add more to the list. Maybe the latest drivers for the Banshee card overcome this problem or maybe not. I got so fed up that I went and bought an ATI Rage 128 instead!