M A S T E R C H E A T E R

CORSICA

PRODUCTION

by olivier pasqualini

SUMMARY :

SEE INSTALLATION FIRST

http://www.geocities.com/TimesSquare/1323/

INTRODUCTION

So, it's my second tool after MTC.
MC support the 3dfx and alt-tab protected game
yet this is an alpha so you can found several bugs.
This program work only under win95 and w98's based games.and don't support dos games!!!!!!!

When you use this software you do so at your own risk. If you do not agree with these terms delete this software now.and don't ask me for sources!!!!!.

mc may not support all graphic cards,especially when it's an 2d-3d card who use his own drivers.

Key Features of Master cheater:

-Call mc with the hotkey.
-Freeze values in memory.
-Hexa editor.
-Search for an value,+,-,change,nochange.
-Hexa/ascii search.
-Secial search.
-View points.
-Convert (decimal <-> hexa).
-Calculator
-Reindex list addresses found.
-Memory map.
-Support 3dfx,alt-tab protected games.
-Save addresses found on a file.
-Copy memory area to .txt file.
-Trainer maker (doesn't support 3dfx games yet)

This program support only voodoo cards who use the glide :

- 3Dfx Interactive reference boards
- Diamond Monster 3D
- Orchid Righteous 3D
- Deltron Realvision Flash 3D
- Skywell Technology Magic 3D
- Guillemot MaxiGamer
- Canopus Pure 3D
- Miro HiScore

- Hercules Stingray 128-3D
- Jazz Multimedia Adrenaline Rush 3D
- Intergraph Intense 3D Voodoo

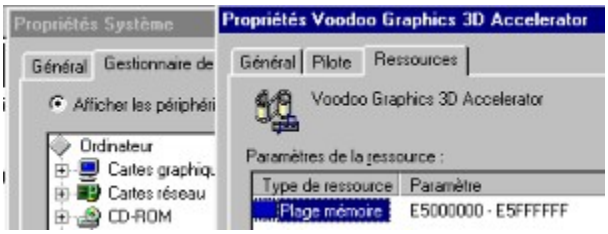
i have only tested under the Deltron Realvision Flash 3D and the Diamond Monster 3D

CTRL-S : call master cheater.
CTRL-X or EXIT for return to the game

INSTALLATION

Follow theses instructions.that important !!!!.
warning mc may not work if you use fastvid.

-Run the installation program and reboot.
-You can call MC with CTRL-S another one for quit MC
-Config mcheater for the 3dfx if you have one with the 3dfx command.
for that you have just to guive the memory area of the 3dfx :



here : 3dfx E5000000

-Now you have to set a directory for you mcd file (gtc under mtc) and for the file that need the search. for that : create a directory with win95 or use the directory where is intalled the help of MC
use the setdir command.
EX : setdir c:\mcheater it's really important !!!!

WHAT'S NEW

- alpha v0.1 -

-normal search (ns)
-save table to mcd file
-support 3dfx (3dfx)
-support alt-tab protected
-hexa search (hs)
-memory map (map)
-hexa editor (edit)

- alpha v0.2 -

-view points
-convert (decimal <-> hexa) (dtoh,htod)
-tab (last lines enter)
 -freeze addresses

- alpha v0.3 -

-ascii search (as)
-reindex list command (reindex)
-new search mode (ps)

- alpha v0.4 -

-calculator (calc)
-special search (sp)

- alpha v0.5 -

-trainer maker(doesnt support 3dfx games yet)

MTC AND MC HOME PAGE : http://www.geocities.com/TimesSquare/1323/

email : mtcbox@hotmail.com
home page : http://www.geocities.com/TimesSquare/1323/

pseudos : 

CONFIG

Commands:

keybfr : french keyboard
keybus : us keyboard

range : Ex : range 400000 to 800000 OR range auto (range of the search)
3dfx : Ex : 3dfx E5000000 OR 3dfx none
ftimer : Ex : ftimer 4000 (set the freeze timer between 100 and 100000000 ms.100 ms is the faster!!!!).
setdir : Ex : setdir c:\mcheater
svmax : Ex : svmax 400 (set the max view point than the v-p search can set)
config : show current config

IMPORTANT

- REMEMBER: AN ADDRESS FOUND CAN BE WRITE IN MEMORY WITH 1,2,4,8 bytes.
Data type: 1 byte : 0 -> 255
0->FF
2 bytes: 0 -> 65535
0->FFFF
3 bytes: 0-> 16777215
0->FFFFFF
4 bytes: 0-> 4294967295
0->FFFFFFFF

- REMEMBER: IN MEMORY ALL IS WRITE IN HEXA,AND REVERSE. EX : 1568 decimal = 620 hexa and write in memory : 20 06 .
- MAP OF THE MEMORY :
Ms-dos compatibility 0x00000000 to
0x003FFFFF.
Win32: 0x00400000
to 0x7FFFFFFF.
DOS,Win16: 0x80000000 to
0xBFFFFFFF.
system of exploitation : 0xC0000000 to
0xFFFFFFFF.
- A PROGRAM CAN HAVE MORE 1 ADDRESS FOR AN VALUE.
- DON'T ASK ME FOR SOURCES.
-PROGRESIVE SEARCH:
If you choice to initialise with a dword for exemple and you want found the address of the value in red : 88 10 22 03 88 28 who is coded on 1 byte.
the value change to 88 10 22 02 66 88 28 .so if you have choice change you found the address.
the value don't change 88 10 22 02 66 88 28. so if you have choice nochange you found the address.
but now the hexa chain is 88 10 99 02 11 88 28.the value that you search don't change but 2 values around it change.if you have choice no change you will found nothing,because the search is initialised on 4 bytes

INFO

SEARCH COMMANDS

Hexa search (hs):

hs : EX hs 99 88 77 55 (hexa search)
again hs for continue

Ascii search (as) :

as : Ex aslife
again as for continue

aslife not egal to as life
^ ^
first char first char (space+life)

aslife not egal to aslife
^ ^
last char last char

the search is case not sensitive

Normal search (ns):

ns : Ex ns 5444 ; ns byte/word/dword 5444

Progressive search (ps):

first :
ps : Ex ps byte ; ps byte/word/dword

after:
ps : Ex ps change ; ps change/nochange/+/-

def:

byte = 1 bytes
word = 2 bytes
dword = 4 bytes

reset : reset normal search and progressive search
view : view addresses found

Special search (sp): NOT FOR NOVICE

sp : Ex sp 50 or sp 455414 (unsigned long) or sp off

the principle is simple at each instruction executed by the game,mc will check if any register of the game is egal with the value of the search.
now when you are in the game ctrl-e : enable the search
ctrl-r : disable the search

all info found will be saved in the mcheater directory under the file name : log special search.txt

1°) if you have the special search ON : dos programs run slowly!!!! so disable the special search before run a dos game (sp off) !!!!
2°) the view points list must be empty before use this command !!!!
3°) because the game run in step by step it's really slow!!!!!!

EX:
1°) in a game where you have 5000 energy.
you set the special search at 5000 : sp 5000
return to the game
just before the energy change press ctrl-e
after the change press ctrl-r
and go into the mc directory for show the log special search.txt
and you will got all the addresses's routines who use the value 5000

2°) in a game or the address of the life for example change at each game
if the address of the life is 450000
you set the special search at 450000 so sp 450000
return to the game
just before the life change press ctrl-e
after the change press ctrl-r
and go into the mc directory for show the log special search.txt
and you will got all the addresses's routines who read or write at this address if the game need calculate the address of the life at each access and if it put it in a register.

MASTER CHEATER DATA FILE

load : load an mcd file
save : Ex : save name (save an mcd file)
list : show the current mcd list
erase : erase mcd list
poke : write all the mcd list in memory
reindex : Ex: reindex +45544 or reindex -7778 (add or subtract an value to all the mcd list)

OTHER COMMANDS

cls : clear text zone
edit : Ex : edit 500000 (hex editor)
sm : Ex : sm 400000 400100 name (length max 0x10000)
map : memory map
exit : return to the game
help : help in mc

VIEW-POINT

vp : Ex : vp 500000 (set view point)
vl : list of view-point
vs : Ex : vs a1 00 50 50 00 (search for the chain and set a view point)
vs again for continue if more found.
historysave : Ex historysave name (save the break/view point history).

always set the view point at the begining of the instruction:
452110 mov eax,[502e00] a1 00 2e 50 00

vp 452110 right
vp 452111 wrong

the command vs is really usefull for found which routines are used and when.

1°) warning : theses command are not for novice !!!!!!!.
2°) if you have a view point enable,dos programs run slowly!!!! so disable all view points before run a dos game!!! (sp off)
3°) the special search must be off before use this command !!!!

SPECIAL KEYS

ctrl-s : call master cheater
ctrl-x : exit master cheater
ctrl-e : enable the search
ctrl-r : disable the search
tab : display last lines on the command line
esc : escape the current line

CONVERT

htod : hexa -> decimal
dtoh : decimal -> hexa
calc : calculator
sign & = hexa
sign # = decimal
Ex: calc &10+&60
calc #10*#55
calc #584-&554
calc #584+&554/&44

TRAINER MAKER

List of commands:
tmlist : made the mct list.
tmerase : erase the current mct list.
tmload : restore an mct file.
tmsave : save the current mct list into an file.
tmpload : restore the project (all in tmbuild and tmbutton).
tmpsave : save the project (all in tmbuild and tmbutton).

tmbutton : set your trainer.
tmbuild : set the about,title,name,process name to search of the trainer and build it.
tmreset : reset tmbutton and tmbuild.

Made a trainer in 3 steps:

1°) Made mct files
You must made an mct file for all buttons that you want set. it's same as an mcd file but you can write only a byte 0-ff for each addresses to poke.

2°)Set buttons that you want use in the trainer and load mct files in them.
write the command tmbutton in mc.now 1screen will be display.

```
BUTTONS  TITLE      ON       OFF      STATUS
                  EMPTY    EMPTY    NOT USED
                  EMPTY    EMPTY    NOT USED
                  EMPTY    EMPTY    NOT USED
                              ........
                  EMPTY    EMPTY    NOT USED
```

```
You can set 18 buttons.
```
-set a text in buttons title
-select the status between : NOT USED(the button is not display),ON(the user can write the hexa chain in memory loaded in ON),ON-OFF(the user have the choice between the hexa chain loaded in OFF and the hexa chain loaded in ON,FREEZE(the user can freeze the memory with the hexa chain loaded in ON).
-now load the mct files in on and off slot:
STATUS ON : load only in the ON button
STATUS ON-OFF: load in the ON and OFF buttons
STATUS FREEZE : load only in the ON button

press escape when you ave finish

3°) Build it

write the command tmbuild in mc.now 4 screens successive will be display.

1-You can write all you want in theses 8 lines.theses lines will be display in the about section of the trainer.after press [N]EXT.
2-Choice the title of your trainer and press [N]EXT.
3-Choice the exe name of your trainer and press [N]EXT.
4-Choice the process name to search in memory for found the game.(ex: the long name is totala.exe but you can search for totala) the process name is display at the bottom right of mc and press [N]EXT for build the exe.
You will found the exe in the mc directory.

important:

-the file : mt.dat must be in the mc directory,and the config dir must be correctly set in mc.
-currently trainers made by mc doesn't support 3dfx games but you can when it's possible : do an alt-tab, switch to the desk,and call the trainer.
-doesn't support dos games.
-if you launch a game from the auto start of the cd-rom ,may be it will not at the same position in memory.
-if you launch a game from a ms dos command the process name for the trainer will be a dos name like starcra~ and not starcraft.
-you can only have 1 trainer in memory.
-don't try to run mc when the trainer screen is display and vice-versa.
-when you call the trainer ,the game is not blocked.