Olly Advanced

This plugin is a general purpose plugin for OllyDbg that fixes some annoying things of Olly / bugs of Olly v1.10 and also integrate new things. It includes also a full bunch of Anti-Anti-Debug.

Note: Version 1.25 works on NT-based systems only. If you use a Win9x system, stick with version 1.24! This was a necessary step to implement new functions.

PS: Use this tool only to test your Anti-Debug features and for Olly-Fixes.

Changelog

version 1.25

Note: You can use this version only on NT-based systems!

- added two new options to skip dialogs (ReadMemory + WriteMemory)

- added a full range of Anti-AntiDebug

- added protected application environment (very early stage; mainly against y0da's protector)

- plugin can handle Base of Code, Size of Code and Base of Data if checked (so you don't need to fix those values in header)

this option is good if such a value was faked and eats up CPU-resources.

- added option to ignore a faulty export-table
- completely reworked the options-dialog.
- option to maximize windows
- option to enable "Show all jumps and calls" always
- Added a process-patcher to the plugin (Mainly for EBFE injection)
- Added option for C0000008h Exception Handling
- Added option for Termination-ignore of already terminated targets

CPU-ASM window:

- added option to detach process
- added option for process patcher (also in option) with child-detection

Memory Map:

- added option to allocate memory
- added option to free memory
- added option to zero memory
- added option to dump memory area

Executable modules:

- added option to insert module
- added option to dump & dump-fix module

version 1.24

- removed two anti-attach routines and added a much more powerful one

version 1.23

- fixed some minor bugs

version 1.22

- fixed a bug for Options-dialog

- added fix for "Copy to executable"-dialog / "View" > "File" Dialog

version 1.21

- fixed bugs for modified versions (d2k2 version, ICU version)

version 1.2

- Windows 98 Fix

- added flexible breakpoints (non-CC breakpoints) - Win NT based systems only

- added support for Toolhelp32 instead of psapi.dll (you'll see more processes / suspended one's also)

- added a compatiblity-layer for Pausedex function of olly (prevent crashes by some plugins)

- options will be dealt now as real options, this means they will be overtaken immediately

- Copy to executable can be always used (use this function at your own risk)

version 1.12

- fixed a problem that could occur with some plugins on exit (olly crash)

version 1.11

- bugfix: some options could fail if Olly was launched from context-menu or when attaching.

version 1.1

- anti-anti-debug added (Against anti-attach tricks)

- added follow in disassembler for packed apps

- Advanced CTRL+G

- added WinUPack patch

- plugin-limitation patch now supports patched olly (Shadow, etc)

- added CRC-ignore option (so you don't have to reanalyze file on

modification, this keeps UDD and all BPs, patches, etc)

- added ignore modified BP, so olly doesn't disable BPs if memory is modified there

version 1.02

- supports now to patch plugin-limit of 32 up to 127 plugins (i guess so much are not available atm :-) if you have so much, i can simply expand the limitation lol)

version 1.01 - fixed for re-pair patched OllyDbgs

version 1.0

- Fixed analysis for a wrong value of NumOfRvaAndSizes.
- added options in plugins-menu
- fixes "%s%s" bug now also for files with "%s" in it. Olly can now also output debug-strings with "%s%s" in it and all other types of "%s%s".
- fixes a bug of olly (crashes for a faked imagebase on object-files scanning)
- added option to skip "Entry point alert"
- added option to skip "Too many patches"
- option for dll-handling

Non-Choicable (always enabled) features

We have two features which can't be disabled

- New error-dialog (instead of the standard windows-error)
- Automatic detection if plugin-support should be expanded

Copyright © 2006 MaRKuS TH-DJM

Current limitations

- dll-loading message isn't skipped when launching from context (because plugins aren't loaded then)

- limited hiding capability when launching from context. YOU SHOULD NEVER USE IT FROM CONTEXT! Olly has problems in general if you do this.

Note: This limitations can't be fixed by the plugin. The plugin is loaded to late to take action against this.

Bugfixes

Olly Advanced 1.25 Masters Edition				
Bugfixes Additional Options Anti-Anti-Debug				
C Bugfixes				
Expand plugin-limit to 127 plugins				
✔ Kill %s%s bug (full fix in string-routine)				
🔽 Kill NumOfRva Bug				
✓ Kill little Analysis-Crash-Bug				
✓ Ignore faulty image (WinUPack)				
✓ Follow in Disasm for packed images				
Handle exceptions in OD Pausedex				
Always enable "Copy all" (own risk)				
✓ Fix "View file" & "Copy to exe" Dialog				
Show all jumps and calls - Allow action in Olly while using				
✓ Ignore faked Export Table				
Handle Base of Code, Size of Code				
✓ Ignore and skip C0000008h (Inv Handle)				
Ignore faulty handle when terminating proc				
Ok Cancel About MaRKuS TH-DJM ©2006				

Copyright © 2006 MaRKuS TH-DJM

Expand plugin limit to 127 plugins

This is a self-explaining option of the plugin. it allows you to use more than *32 plugins* like in the standard olly version.

Copyright © 2006 MaRKuS TH-DJM

Kill %s%s bug

here is our little sample application. it does nothing more than output the debug string "%s%s%s%s" and then terminate.

00401000 55		PUSH psbug.00403000	<pre>FString = "%s%s%s%s%s"</pre>
00401005 .	E8 0E000000	CALL	OutputDebugStringA
0040100A .		PUSH Ø	<pre>FExitCode = 0</pre>
0040100C L.	E8 01000000	CALL <pre>/JMP.&kernel32.ExitProcess</pre>	LExitProcess
00401011	CC	INT3	
		JMP DWORD PTR DS: [<&kernel32.ExitProces	
	FF25 0020400	JMP_DWORD_PTR_DS:[<&kernel32.OutputDebu	kernel32.OutputDebugStringA
00401015	00	DD 00	

however, Olly can't handle those %s%s very well.

Olly Advanced			
Exception occured @Address 004A74CF			
ОК			

Olly crashes at address 4A74CF (this non-standard error box was also introduced with Olly Advanced plugin)

Then, if we enable the option to kill this bug, we won't have any errors anymore.

Debug string: - M%s - %sÉÂ -

the string isn't shown 100% correctly, but Olly won't crash anymore.

Kill NumOfRva Bug

I've modified our sample-application a bit.

NumOfRvaAndSizes: 0BADC0DE

This is a well known technique to fool Olly.



Now with this plugin-option enabled:



Olly loads the application as expected.

```
Copyright © 2006 MaRKuS TH-DJM
```

Kill little Analysis-Crash bug

This is only a very small handler which prevents a crash if you press CTRL+A. there are sometimes crashes if you analyze outside the executable module.

Copyright © 2006 MaRKuS TH-DJM

Ignore faulty image (WinUPack)

This one is also a self-explaining option. OllyDbg has problems with WinUPack packed applications, it shows an error. This option enables you WinUPack compatiblity mode and you can debug the application as usual.

-

Copyright © 2006 MaRKuS TH-DJM

Follow in Disasm for packed images

Target-Program: ASPacked application (or any other packed PE)

Problem:

Olly doesn't display the "Follow in Disassembler" for Stack-Window anymore.



This option implements a <u>*new way*</u> of checking the target-address (it validates it for read-access) and then, if there is access, it restores the "Follow in Disassembler" again.



Note: This problem can also be partly resolved by option "Handle Base of Code, Size of Code and Base of Data".

Copyright © 2006 MaRKuS TH-DJM

Handle Exceptions in OD Pausedex

This is a plugin-compatiblity option. some plugins modify the registers in this function and so cause a crash of OllyDbg. This compatiblity-option **should be always turned on** .

Copyright © 2006 MaRKuS TH-DJM

Always enable "Copy all"

This option enables the "Copy all" option in Olly always when you've done modifications. This option sometimes disappear for unpacked applications too by an Olly-fault.



"All modifications" can also disappear if Base of Code is changed.

Note: This option is heavy influenced by option "Handle Base of Code, Size of Code and Base of Data". Modifications are taken then PE-Wide, that means also YOUR OWN changes (not changes by the program) are included from every section.

Fix "View file" & "Copy to exe" Dialog

Problem:



If you do any changes in this Dialog (Or "Copy to Executable" Dialog), and then click "X" (Close), Olly asks you if you want so save changes. But the choice "Cancel" acts like "No". It closes the dialog. You have no chance to do more changes without opening the window again. This is a bug. By clicking this option in the plugin, the "Cancel" button acts like it should. it should simply go back to the dialog again.

Show all jumps and calls - Allow action in Olly while using

Problem:

00401000 \$ E8 3F0000000 CALL psbug.00401044 00401007 . E8 3A000000 CALL psbug.00401044 00401007 . E8 3B000000 CALL psbug.00401044 00401007 . E8 3B000000 CALL psbug.00401044 00401017 . E8 2B000000 CALL psbug.00401044 00401018 . E8 2S000000 JMP SHORT psbug.00401044 00401017 . E8 2S JMP SHORT psbug.00401044 00401021 . E8 1F JMP SHORT psbug.00401044 00401023 . E8 1F JMP SHORT psbug.00401044 00401027 . E8 1S JMP SHORT psbug.00401044 00401027 . E8 15 JMP SHORT psbug.00401044 00401028 . E8 15 JMP SHORT	
ИО401052 . ИООЛADD_BYTE_PTR_DS:[FBX].0 Local calls/jumps from <noduleentrypoint>, 00401005, 00</noduleentrypoint>	401000 0040100F 00401014 00401019 Copy pane to clipboard
Oddress Hey durp	Go to CALL from <moduleentrypoint></moduleentrypoint>
Address Hex dump 08482808 98 98 98 98 98 98 98 98 98 98 98 98 98 98 98 98 08482818 98 98 98 98 98 98 98 98 98 98 98 98 98	Go to CALL from 00401005
ରବ୍ୟବିଅସମାର ଗର	Go to CALL from 0040100A
ରତ୍ୟରମ୍ବରର ବର	Go to CALL from 0040100F
ରତ୍ୟତ୍ୟତ୍ୟତ୍ତ ପର୍ବତ ତତ ତ	Go to CALL from 00401014
00402070 00 00 00 00 00 00 00 00 00 00 00 00	Go to JMP from 00401019
	Go to JMP from 0040101B
00402050 00 00 00 00 00 00 00 00 00 00 00 00	Go to JMP from 0040101D
004020C0 00 00 00 00 00 00 00 00 00 00 00 00	Go to JMP from 0040101F
004020F0 00 00 00 00 00 00 00 00 00 00 00 00	Go to JMP from 00401021 Go to JMP from 00401023
	Go to JMP from 00401025
00402130 00 00 00 00 00 00 00 00 00 00 00 00 0	Go to JMP from 00401025
00402150 00 00 00 00 00 00 00 00 00 00 00 00 0	Go to JMP from 00401029
00402160 00 00 00 00 00 00 00 00 00 00 00 00 0	Go to JMP from 00401028
00402190 00 00 00 00 00 00 00 00 00 00 00 00 0	Go to JMP from 0040102D
	Show all jumps and local calls

Show all jumps and local calls. If we use this dialog, it locks up Olly and we can't set any breakpoints in Olly which would be very useful.

So ticking this option in the plugin prevents Olly from locking up and so you can set breakpoints and do other actions in Olly.

Copyright © 2006 MaRKuS TH-DJM

E.

Ignore faked export table

Problem: Someone inserted a faked (non-existant) export-table in the PE. Olly has problems with that.

ExportTable: 00500000 00500000 0050000

By ticking the option in the plugin, Olly will ignore such error and go on as usual.

1

Copyright © 2006 MaRKuS TH-DJM

Handle Base of Code, Size of Code and Base of Data

Problem:

BaseOfCode:	40001000
BaseOfData:	40002000

Someone faked BaseOfCode and / or BaseOfData. Olly has problems with such thing again. In a combination with a faked SizeOfCode, **Olly will eat up our RAM** and so get the computer in a slow-performance state.

By enabling this option, Olly will have a new system for BaseOfCode, BaseOfData and SizeOfCode.

- BaseOfCode is set to first section VA, SizeOfCode to size of first section <u>or</u> to ImageSize (in memory) - first section VA. this way, a complete analysis of the whole file is done. this is useful especially for packed targets. Also PE-wide changes are catched.

- BaseOfData will be set to second section VA, *or*, if not available, to first section VA.

Ignore and skip C000008h (Inv Handle)

This option correctly handles the Invalid Handle Exception, the program is simply resumed. This way such an exception is skipped and Olly can't be detected.

Copyright © 2006 MaRKuS TH-DJM

Ignore faulty handle when terminating proc

Sometimes Olly doesn't let you restart the target and shows an error if the target was already terminated / detached. With this option, this is fixed.

1

Copyright © 2006 MaRKuS TH-DJM

Olly Advanced Help Additional Options

Olly Advanced 1.25 Masters Edition				
Bugfixes Additional Options Anti-Anti-Debug				
C Additional options				
Enable Advanced CTRL+G				
Skip "Entry point outside code"				
Skip "More than 1000 patches"				
O Scan				
Delete all patches				
Skip compressed code warning and				
Analyse				
🔾 do nothing				
Skip "Load dll" and				
Load up DLL				
🔾 do nothing				
Ignore changed memory @BP				
If CRC was altered				
O do complete reanalyze				
do nothing Flexible Breakpoints				
Use Toolhelp32 instead of psapi.dll				
(=see more / suspended processes)				
Skip "ReadMemory failed"				
Skip "WriteMemory failed"				
Maximize Olly when starting				
Maximize all Olly Child-Windows				
Always enable "Show all jumps and calls"				
Ok Cancel About				
MaRKuS TH-DJM ©2006				

Copyright © 2006 MaRKuS TH-DJM

Þ

Enable Advanced CTRL+G

This option modifies the dialog which appears when you press CTRL+G.



You can either follow any address by VA / API (Olly standard) or additional by RVA or Offset.

This includes also relocated DLLs / OCX.

Of course every input is saved like in original dialog.

This option especially makes sense if you used file-comparing tools and don't want to calculate all the Offsets to VA first.

Skip "Entry point outside code"

This option skips the message which appears if you load packed files.

-

Copyright © 2006 MaRKuS TH-DJM

Skip "More than 1000 patches"

This option skips another dialog and executes the selected operation.

NOTE: This dialog normally appears if you have self-modifying apps or replaced much binary by "Binary paste". If you did that, the dialog will come up every time you close it. you are forced to Terminate Olly if you don't have this option checked.

Copyright © 2006 MaRKuS TH-DJM

Skip compressed code warning

This option skips another dialog and executes the selected operation.

NOTE: This message normally appears if you open up packed PE-files.

Illy Advanced Help

Skip "Load dll"

Olly asks every time you load up a dll if it should try to load the dll. This message is annoying. You can skip it by checking this option.

NOTE: It won't work if you open up a dll from context-menu of explorer. At this time plugin isn't loaded.

Copyright © 2006 MaRKuS TH-DJM

Ignore changed memory @BP

Olly places a CC for every breakpoint you set. You can't see such CC in Olly. Sometimes (especially self-modifying apps) overwrite such a CC. By checking this option, Olly won't complain about such thing and simply reapplies the BP (else it would disable all breakpoints).

-

```
Copyright © 2006 MaRKuS TH-DJM
```

If CRC was altered

You can either analyse the whole file again (if you modified something; Olly default) or do nothing.

This option is a bit different to the option in Olly (Ignore CRC of code-section). It won't analyse the file again as long a .UDD file exist.

NOTE: By option "do nothing", all Patches, Analysis, Breakpoints etc are still there and saved! In original Olly all these get lost.

Copyright © 2006 MaRKuS TH-DJM

Flexible Breakpoints

As explained before, all breakpoints are done by CC.

Through this option, an alternative Breakpoint system is used (and also flexible because it uses different OPCodes to throw an exception by coincidence). The old CC-breakpoint system is completely thrown out then because nearly every protector can detect those CC-breakpoints.

NOTE: This option won't work on 9x-based systems.

Copyright © 2006 MaRKuS TH-DJM

Use Toolhelp32 instead of psapi.dll

Toolhelp32 method to enumerate processes is a windows-based method to detect all processes while psapi uses it's own system.

By checking this option, Olly will use Toolhelp32 instead of the psapi method. This way, you have sometimes better results in attach-window, however, you won't see path of the processes.

Copyright © 2006 MaRKuS TH-DJM

Skip "ReadMemory failed"

This option simply skips the dialog which occurs if Olly couldn't read a specific memory-area.

_

Copyright © 2006 MaRKuS TH-DJM

Skip "WriteMemory failed"

This option simply skips the dialog which occurs if Olly couldn't write to a specific memory-area.

_

Copyright © 2006 MaRKuS TH-DJM

Maximize Olly when starting

Olly sometimes loose it's last window-state. With this option, you make sure Olly gets always maximized.

Copyright © 2006 MaRKuS TH-DJM
Maximize all Olly Child-Windows

Olly will make sure that all sub-windows get maximized (CPU for example) and also when you open a new Sub-Olly-Window it will get maximized.

Note: This happens only for Olly's MDI Windows, not for any Option-Dialogs or others.

Copyright © 2006 MaRKuS TH-DJM

Always enable "Show all jumps and calls"

This option enables "Show all jumps and calls" also if only one jump / call goes to specified address.



Copyright © 2006 MaRKuS TH-DJM

Anti-Anti-Debug

Olly Advanced 1.25 Masters Edition				
Bugfixes	Additional Options	Anti-Anti-Debug		
Anti-Debug (NT-Based OS only)				
🔽 Kill Ar	nti-Attach (Hardcore m	ethod)		
🔽 Unha	ndledExceptionFilter	🗆 S		
✓ Process32Next S				
Module32Next S				
CheckRemoteDebuggerPresent S				
ZwSetInformationThread S				
	erySystemInformation			
	eryInformationProces	s		
a second s	ieryObject			
GetTi				
	nateProcess			
<u> </u>	nble Export Table			
Debug B				
	IsDebuggerPresent			
✓ NtGlobalFlag (not recommended)				
Heap				
Force	-			
Protecte	d Application Environ	ment		
and the second se	endThread			
Block	Input			
COther-				
🗹 Break	on TLS Callback			
		About		
	MaRKuS TH-DJM @	/2006		

1

Copyright © 2006 MaRKuS TH-DJM

The S-Options

S stands for System Breakpoint.

if this option is activated, the anti-debug will be applied when you are @System Breakpoint. this is good if your program uses an Anti-Debug dll which is loaded on Startup. then you are protected against this also.

Why is it not available for all?

The positions where the other options will be applied are fixed.

Copyright © 2006 MaRKuS TH-DJM

Kill Anti-Attach

Some apps try to prevent you from attaching. This option does the needed operations do attach to the target for nearly all anti-attach methods before Olly attaches to the target.

-

Copyright © 2006 MaRKuS TH-DJM

UnhandledExceptionFilter

Some targets use UnhandledExceptionFilter trick. This means, the app works different depending if it's debugged or not. By using this option, this will be prevented.

-

Copyright © 2006 MaRKuS TH-DJM

Process32Next

This option stops apps in debugger to use the Process32Next function which is often used to detect Olly.

-

Copyright © 2006 MaRKuS TH-DJM

Module32Next

This option stops apps in debugger to use the Module32Next which can be used to detect the dlls loaded by a process.

1

Copyright © 2006 MaRKuS TH-DJM

Olly Advanced Help CheckRemoteDebuggerPresent

Nearly similar to IsDebuggerPresent. this option fakes the return-value.

-1

Copyright © 2006 MaRKuS TH-DJM

ZwSetInformationThread

This API can stop the app from being debugged. By using this option, you can stop that.

-1

Copyright © 2006 MaRKuS TH-DJM

ZwQuerySystemInformation

This API can detect a debugger by the class 23 which is SystemDebuggerInfo. With this option you disable it.

Copyright © 2006 MaRKuS TH-DJM

ZwQueryInformationProcess

This API can detect Debugger by InfoClass 7 or get the target-process and disable it by class 0. This option will stop them.

Copyright © 2006 MaRKuS TH-DJM

ZwQueryObject

This API can detect the Debugger by the DebugPort. By checking this option, the return-table gets cleared.

Copyright © 2006 MaRKuS TH-DJM

GetTickCount

This option disables the GetTickCount API which can be used for timed checks.

Note: Disable it if you don't need it! Some programs may not run with this option activated.

-

Copyright © 2006 MaRKuS TH-DJM

TerminateProcess

This disables the TerminateProcess API to stop any Olly-Termination.

-

Copyright © 2006 MaRKuS TH-DJM

Scramble Export Table

By checking this option, the export table gets cleared up after loading up the plugins in Olly as well as in the PE-Header. This prevents any detection of Olly through the export-table.

1

Copyright © 2006 MaRKuS TH-DJM

Debug Bits

This area includes all changes which are done in / through informations of the PEB.

-1

Copyright © 2006 MaRKuS TH-DJM

IsDebuggerPresent

This option does not patch the IsDebuggerPresent API, it clears the Debug Bit (BeingDebugged) of the PEB to prevent any debugger-detections on base of the PEB.

-

Copyright © 2006 MaRKuS TH-DJM

NtGlobalFlag

This clears the NtGlobalFlag which can be used to detect the debugger in combination with the registry.

NOTE: This will make the plugin NtGlobalFlag which is useful for Execryptor unusuable. Disable it if you deal with Execryptor. This should be only activated in some special cases where Debugger is detected through Registry. Disable it if not REALLY NEEDED!!!

Copyright © 2006 MaRKuS TH-DJM

HeapFlags

E

Prevents detection through HeapFlags.

-

Copyright © 2006 MaRKuS TH-DJM

ForceFlags

Prevents detection through ForceFlags.

-1

Copyright © 2006 MaRKuS TH-DJM

Protected Application Environment

This should be a new feature which i also call the "DRM for Debugged Apps". It needs very much development, but it should hide the debugger through restricting / filtering to a level where it can't detect any debugger.

NOTE: To the current state of development, it's only additional Anti-Debug.

Copyright © 2006 MaRKuS TH-DJM

SuspendThread

This disables the SuspendThread API which is used in y0da's Protector to kill OllyDbg.

Note: Disable this option if you don't need it! Some programs may not run with this activated.

-

Copyright © 2006 MaRKuS TH-DJM

BlockInput

This disables the BlockInput API which is also used in y0da's protector to block you out.

-

Copyright © 2006 MaRKuS TH-DJM

Break on TLS Callback

This is a useful feature if you deal with Execryptor. This way, you won't break on EP first, you'll break on the TLS Callback first. Olly will show Status in the Footer.

NOTE: You can have this also activated if you don't deal with Execryptor. You'll be informed if you break on TLS in Olly's infobar.

1

Copyright © 2006 MaRKuS TH-DJM

Allocate Memory

Through this function, you can allocate memory in the target-application. Simply select "Allocate Memory" and a block of 1000h bytes will be allocated and shown in a messagebox where it got allocated.



Here you can insert how many memory to allocate and where memory should be allocated. If you leave it blank, any free space will be used. You'll get status-message then (Olly's Footer).



Copyright © 2006 MaRKuS TH-DJM

Free Memory

This is close to "Allocate Memory", but with this function you free unneeded (allocated) memory.

_

Copyright © 2006 MaRKuS TH-DJM

Insert Module

This is an additional feature which belongs to the "Executable Modules". If you click "Insert module" you can insert any DLL / OCX in the target-process you select in the upcoming dialog.

Executable modules		
Actualize View memory	.0 IS	
View code in CPU Enter Follow entry Dump data in CPU		
View names Ctrl+N	_	
Update .udd file now View executable file	-	
View all resources View resource strings	C	
Analyze all modules		
Insert Module Copy to dipboard		
Sort by Appearance		

Copyright © 2006 MaRKuS TH-DJM

Detach Process

This is an option of CPU-Window. It let's you detach from debugged process.

CPU		
Detach Process Analyze This!		
Asm2Clipboard		
Code Ripper		
Data Ripper Run Script		
Appearance	Þ	

NOTE: The process must be running in Olly before detach or it will crash.

1

Copyright © 2006 MaRKuS TH-DJM

Process Patcher

This is a helpful feature for Armadillo Copymem II. you can inject your patches through the patcher. it will also detect the child-process when it is created.

	Olly Advanced		
Process 00000808 is Child of your debugged process. Should patcher assign to this process			
Olly Advanced: Process Pate Address to Inject:	her Patch		
Bytes to Inject:	h Inject EBFE		
explorer.exe	Close		
Main Thread Information EAX: 00000001 ECX: 00000000 EDX: 00000000 EBX: 00000003 ESP: 0007FEF0 EBP: 0007FF08 ESI: 0000E6C80 EDI: 00000000	Process Information PID: 046C Parent PID: 043C Number of Threads: 0012 Base of Image: 01000000 Size of Image: 000FF000 Path: C:\WINDOWS\Explorer.EXE		

Copyright © 2006 MaRKuS TH-DJM

Dump Module

This option is available in **Executable modules** window. It simply dumps the file from memory and allows you to **Dump-Fix** it.

1

Copyright © 2006 MaRKuS TH-DJM

Dump Memory-Area

This is a feature in the **Memory Map** Window. It allows you to dump **any memory-area** you want to dump.

1

Copyright © 2006 MaRKuS TH-DJM