

The Legend Of Random

Programming and Reverse Engineering

[Home](#) [Tutorials](#) [Tools](#) [Contact](#) [Forum](#) [Challenges](#)

Quick Guide To Some Important Ollydbg Plugins

by R4ndom on May.26, 2012, under [Intermediate](#) , [Reverse Engineering](#) , [Tools](#)

I have compiled a list of what I consider to be the most important Olly plugins for reverse engineering. Every one of these will be used at some point in my tutorials. Of course, this list is nowhere near exhaustive (for that I would go to [Tuts4You](#)

), and I'm sure there are plenty that I am missing that some would consider 'vital'. Mostly, I have listed these here for convenience for people going through my tutorials. I have included the name, the latest version that I could find, the author, and a quick outline of what they do. All of these can be downloaded from my [tools](#) page.

+BP-OLLY

Ver. 2.0 beta 4
By: Redh@wK

This plugin open up a new 'floating' toolbar at the top of Olly. It provides quick access to setting BP's on popular API's (with some for VB as well), Also provides a couple buttons for quickly launching some applications (Notepad, Calc, A user specified folder, and a command prompt)

Anti-Anti Hardware Breakpoint

Ver: 0.1
By: Mattwood^FRET

Search keywords

Login

☒ Remember me

[Recover password](#)

Recent Posts

[My Absence](#)

[What Are These Strange Posts?](#)

[Nice Beginning Article on Reversing Android](#)

[She Is 17-years-old, She Did It Publicly In High School And While Drunk](#)

[And The Most Posts Submitted In A Single Sitting Goes To...](#)

Recent Comments

[tip on A New Tutorial by Xor06 : Bypassing a Server Check](#)

[tip on R4ndom's Tutorial #23: TLS Callbacks](#)

Single minded, but does what it's supposed to. It hooks ntdll to restore the Drx registers after a Structured Exception Handler.

AnalyzeThis+

ver: 0.24
By: SMK

I think the author says it best:

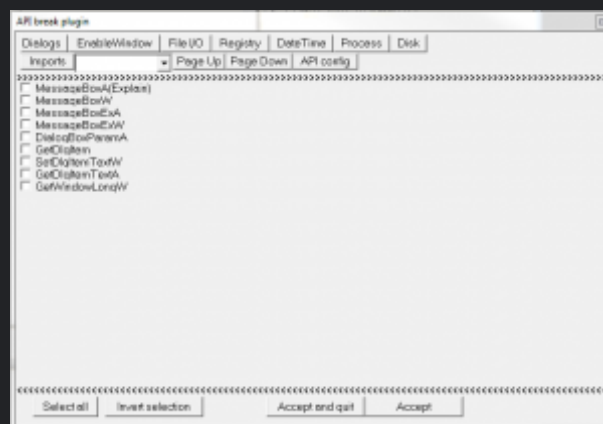
*"Sometimes (especially when dealing with packers) you may need to run OllyDbg's code analysis function, only to find it's not available to you because the EIP is currently outside the code segment as defined by the PE header. AnalyzeThis! is an OllyDbg plugin to allow OllyDbg's analysis function to operate outside of the marked code segment, by telling OllyDbg the current segment *is* the code segment. "*

This is another 'can't do without' plugin. It is indispensable, especially when working with packers.

API Break

Ver: 0.2
By: Dazzling Blue & Baby2008

This plugin allows you to set a breakpoint on many popular Windows API's. It opens a dialog listing many API's by category. It is nicer than trying to remember what the API call is to get the current time (in millis)...



C4lculated on R4ndom's Tutorial #17:
Working With Delphi Binaries

X-Programmer on Tutorial #1 : What is
Reverse Engineering

shub on R4ndom's Tutorial #9: Solution

Archives

October 2012

September 2012

August 2012

July 2012

June 2012

May 2012

Categories

Beginner

Challenges

Intermediate

Modifying Binaries

Random's Ramblings

Reverse Engineering

Tools

Tutorials

Uncategorized

Meta

Register

Log in

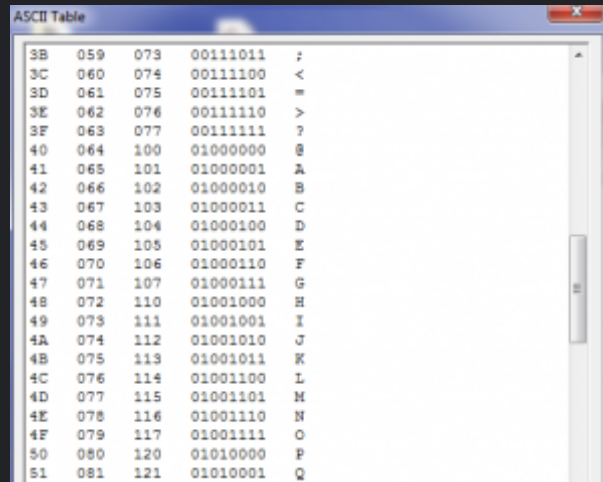
Entries [RSS](#)

ASCII Table

Ver: 1.1

By: REACTION

AsciiTable quickly displays the ASCII chart in hex, decimal, octal and ascii. I hope the author get's around to fixing some of the bugs, tho (when you first load it, everything is highlighted, the window is not sizable, the text is editable...). But overall, extremely helpful.



3B	059	073	00111011	:
3C	060	074	00111100	<
3D	061	075	00111101	=
3E	062	076	00111110	>
3F	063	077	00111111	?
40	064	100	01000000	@
41	065	101	01000001	A
42	066	102	01000010	B
43	067	103	01000011	C
44	068	104	01000100	D
45	069	105	01000101	E
46	070	106	01000110	F
47	071	107	01000111	G
48	072	110	01001000	H
49	073	111	01001001	I
4A	074	112	01001010	J
4B	075	113	01001011	K
4C	076	114	01001100	L
4D	077	115	01001101	M
4E	078	116	01001110	N
4F	079	117	01001111	O
50	080	120	01010000	P
51	081	121	01010001	Q

Attach Anyway

Ver: 0.1

By: Jow Stewart

From the author:

"AttachAnyway is a PoC OllyDbg plugin designed to show how to remove a process' hook on NtContinue by the anti-debugger-attach method devised by Piotr Bania here. [http://pb.specialised.info/all/anti-dattach.asm/

This is not intended to be a universal plugin for all anti-attach methods, just one example of how you can do it. It works by enumerating all processes, searching their virtual memory space for a JMP hook on the NtContinue method, then replacing the jump with the original bytes from a non-hooked process, then calling the OllyDbg Attachtoactiveprocess API."

Comments [RSS](#)

[WordPress.org](#)

Subscribe

Enter your email to subscribe to future updates

RSS Feed

Bookmark

Ver: 1.06
By: Oleh Yuschuk & Eviloid

This handy plugin allows the user to set bookmarks (no more using BP's to remember where that code was!!!). Simply right-click on an instruction and choose bookmark->New bookmark. Simple, but sweet.

Code Ripper

Ver: 1.3
By: Ziggy

This nice plugin allows you to copy code from the binary in a nicely formatted way. Very convenient if you need to copy sections of code to look at later or show someone else.

CommandBar

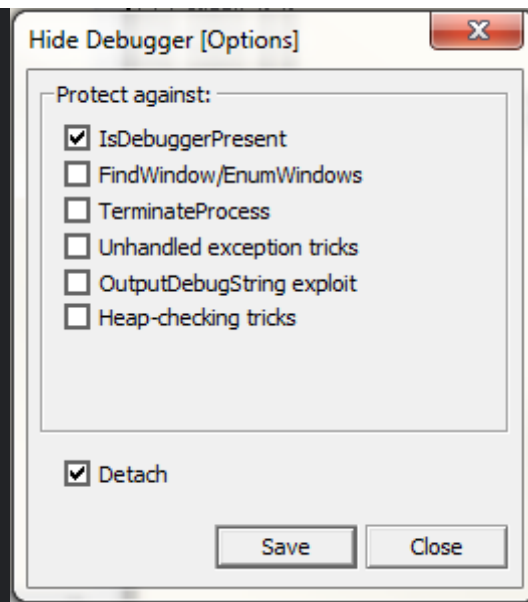
Ver: 3.20.110
By: Gigapede

Allows quickly applying breakpoints, finding API's etc. Sometimes typing is a lot quicker than searching thru windows 😊

HideDebugger

Ver: 1.2.4
By : Asterix

This plugin hides OllyDbg from many debugger detection tricks. These include IsDebuggerPresent, FindWindow, TerminateProcess, Unhandled Exception tricks, OutputDebugString, and some heap-checking tricks.



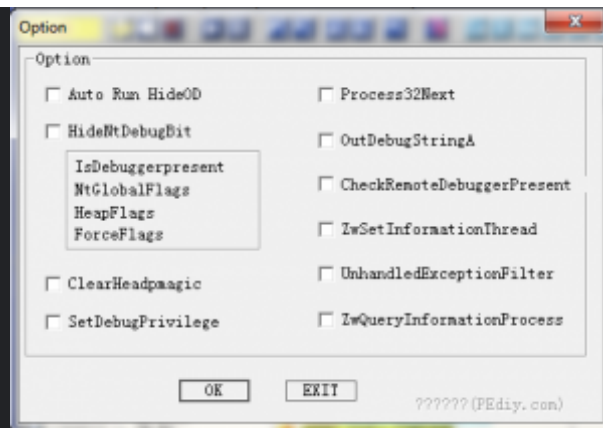
HideOD

Ver : 0.181
By: Kanxue

HideOD allows Olly to be hidden from the debugged application. It allows setting the following:

1. **HideNtDebugBit (IsDebuggerPresent, NtGlobalFlags, HeapFlags, ForceFlags)**
2. **ClearHeadpmagic**
3. **SetDebugPrivilege**
4. **Process32Next**
5. **OutDebugStringA**
6. **CheckRemoteDebuggerPresent**
7. **ZwSetInformationThread**
8. **UnhandledExceptionFilter**
9. **ZwQueryInformationProcess**

It also has an autoset feature and a memory allocator (I think for code caves, tho I could be wrong 😊)
Most of these features are included in Olly Advanced (see below).

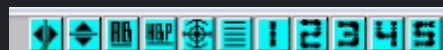


IDAFicator

Ver: 2.0.11.45

By: Zool@nder

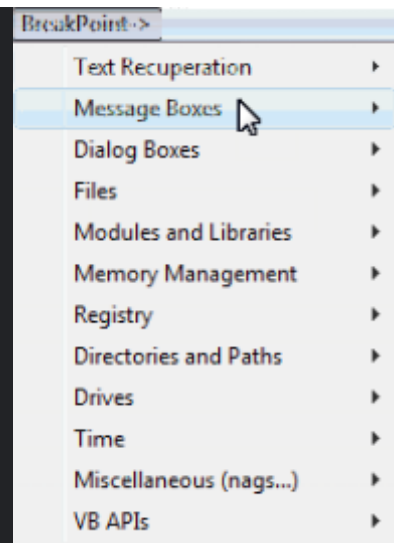
IDAFicator is an immense collection of utilities for Olly. It add a new toolbar at the top of the screen with various cool features, such as go to next/previous line I was on, Go to beginning/end of current method (nice!), a displayable hardware breakpoint window (finally!), a button to immediately search for referenced text strings, a button to open the folder of the target app, and an assembler window similar to NanoWrite.



The 1-5 icons are user settable (though I didn't find this to be the case in all versions of this plugin 😞)

Next, IDAFicator has added several options for the mouse middle button, such as copying and pasting binary data, RVA's etc. It allows setting of breakpoints in the dump window, and a handy stolen bytes retriever (that even changes the bytes to match a specific compiler).

Last but not least, this plugin creates two new menu items in the Olly menu bar. The first is called "Tools". This allows you to add any external programs (and folders 😊) you use regularly and open them with a simple mouse click. It's even drag-and-drop. The second menu option added is a "BreakPoint" item, allowing very easy setting of breakpoints on popular API functions:



IsDebugPresent

Ver: 1.4

By: SV

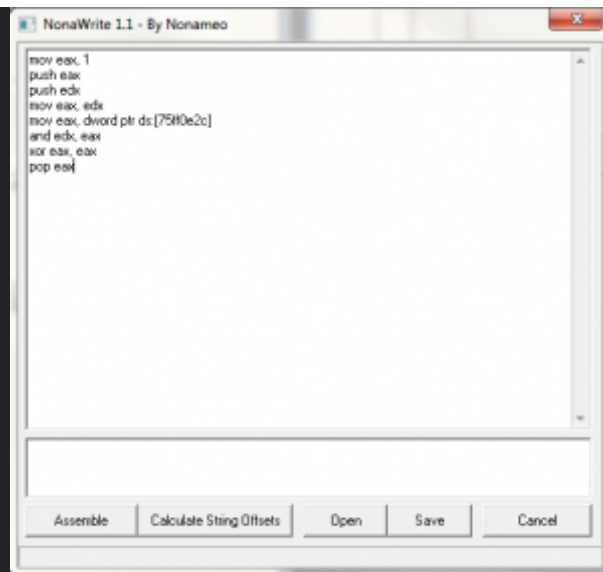
This Plugin is intended to hide debugger from IsDebuggerPresent Windows API. This functionality is in a lot of plugins, so it will probably be overridden if you install many others. Most of these features are included in Olly Advanced (see below).

NanoWrite

Ver: 1.2

By: Nonameo

NanoWrite is a plugin for OllyDbg that helps you write code injection. It allows multiple lines of code to be written at once, and then injected into the binary. Very handy for patching more than one line of code (or for code caves).



MapConv

Ver: 1.0

By: godfather+

MapConv converts map files from IDA or DeDe to OllyDBG when debugging Delphi files. Really useful if you have a nasty app written in Delphi.

Mnemonic Helper

Ver: 1.1

By: 3070

A nice little plugin that displays information about the currently selected opcode mnemonic. very handy when you reach an obscure x86 line of code.

Olly Advanced

Ver: 1.27
By:MaRKuS TH-DJM

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 a bunch of Anti-Anti-Debug. It is sort of the Swiss army knife of plugins. If you could only have one plugin, this would be the one!

Bug fixes include:

1. Expand plugin limit to 127 plugins
2. Kill %s%s bug
3. Kill NumOfRva Bug
4. Kill little Analysis-Crash bug
5. Ignore faulty image (WinUPack)
6. Follow in Disasm for packed images
7. Handle Exceptions in OD Pausedex
8. Always enable "Copy all"
9. Fix "View file" & "Copy to exe" Dialog
10. Show all jumps and calls – Allow action in Olly while using
11. Ignore faked export table
12. Handle Base of Code, Size of Code and Base of Data
13. Ignore and skip C0000008h (Inv Handle)
14. Ignore faulty handle when terminating proc

Additional Options:

1. Enable Advanced CTRL+G (allows address to be entered as VA/RVA/offset – very nice.
2. Skip "Entry point outside code" – that was sooooo annoying...
3. Skip "More than 1000 patches"
4. Skip compressed code warning
5. Skip "Load dll"
6. Ignore changed memory @BP
7. If CRC was altered
8. Flexible Breakpoints (instead of using 0xCC BPs)
9. Use Toolhelp32 instead of psapi.dll
10. Skip "ReadMemory failed"
11. Skip "WriteMemory failed"
12. Maximize Olly when starting
13. Maximize all Olly Child-Windows
14. Always enable "Show all jumps and calls"

Anti-Anti Features:

1. Kill anti-attach
2. UnhandledExceptionFilter
3. Process32Next
4. Module32Next
5. CheckRemoteDebugPresent
6. ZWSetInformationThread

7. ZwQueryInformationProcess
8. ZwQuerySystemInformation (this has a tendency to make some apps load improperly)
9. ZwQueryObject
10. GetTickCount (increases GetTickCount every call by 1)
11. TerminateProcess
12. Scrambled Export Table
13. IsDebuggerPresent
14. NtGlobalFlag
15. HeapFlags
16. ForceFlags
17. SuspendThread (used by y0da)
18. BlockInput (used by y0da)
19. Break on TLS Callback (I noticed that this causes some apps to crash olly)

Many of these have a S-option box. This 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.

Lastly, here are a couple **additional features** (in the context menu):

1. Allocate Memory : Select “Allocate Memory” and a block of 1000h bytes will be allocated .
2. Insert Module : Allows you to insert any DLL / OCX in the target-process
3. Detach Process : It let's you detach from debugged process.
4. Process Patcher : Allows you to apply patches to child threads.
5. Dump Module : similar to Olly's own.
6. Dump Memory-Area

Olly Breakpoint Manager

Ver: 0.1

By: Pedram Amini

I think the author says it best:

“The Olly Breakpoint (BP) Manager was written to provide three main functions – breakpoint exporting, breakpoint importing and automatic breakpoint loading. Breakpoint importing/exporting are straight forward features and can be accessed from the main plug-in menu as well as the right-click context menu of the breakpoints window. Olly BP Manager was designed to support both regular and log (with expression/explanation) breakpoints. Conditional breakpoints have not yet been implemented.

The breakpoint manager also supports automatic loading of breakpoint lists at runtime. Whenever a module is loaded by the target process, BP Manager will check the ‘breakpoints’ subdirectory under the OllyDBG install directory. If a breakpoint list matching the loaded module name is identified, breakpoints will be loaded and inserted into the module.

For example, to automatically load a breakpoint list for kernel32.dll copy your breakpoint list to:

C:\Program Files\OllyDBG\Breakpoints\kernel32.dll.obp

The module name is case insensitive. This feature is especially useful when working with breakpoints in modules not loaded at startup.”

After you've had a full window of breakpoints disappear when re-loading an app, you'll understand the importance of the plugin!

Olly Toolbar Manager

Ver: Gold
By: arjuns

For those who do not have a custom version of Olly with all of the shiny toolbar buttons, this plugin allows you to create your own toolbar, providing quick-click access to your favorite external programs. Really nice if you don't want to spend the time single-stepping through Olly code trying to find out how to add a button



OllyDump

Ver: 3.00.110
By: Gigapede

OllyDump is a staple for reverse engineers. I don't consider Olly complete unless you have this plugin. It allows you to dump the debugged process after you have modified it. It also has two more advanced features (Find OEP by section hop: Trace and Trace Into). I use both of these options as well. Gotta have it!

OllyPad

Ver: 1.1
By: SHaG / The Kluger

OllyPad lets you create notes for the currently debugged application and stores them for later use. Next time you open the application in OllyDbg your notes along with OllyPad window size and placement will be restored.

Press ALT-F11 to show the plugin window and ALT to hide it (this functionality is coded by The Kluger).

Because sometimes you can't find a pencil 😊

OllybonE

Ver: 0.1

By: Joe Stewart

Break-on-Execute for OllyDbg. Specifically, it sets break-on-execute on virtual memory sections.

OllyDBG Script

Ver: 0.92

By: SHaG

This plugin allows Olly to run of the thousands of scripts written for Olly. Mostly, they are used for unpacking or decrypting, but there also scripts out there that do a great deal more. This is an invaluable plugin.

StrongOD

Ver: 0.4.6.816

By: 海风月影

This plugin was written by a native Chinese speaker, so it's a little tough to figure out what some of it does. Maybe if someone comment or sends me a note if they know, I will fill them in. Anyway, this plugin is similar to Olly Advanced in it's sheer number of options. That aside (if I may so easily do that), the keyboard shortcuts added by this plugin are astounding. It is a virtual smorgasbord of keypresses, some of which you'll wonder how you ever did without. Here is just a sampling:

1. Press "INSERT" will fill the selected data with ZERO(0x0)
2. Press "DELETE" will fill the selected data with NOP(0x90)
3. Press "SHIFT + ENTER" will sync dump and assembly

4. Press "CTRL" and double click or "CTRL + ENTER" will sync the DUMP window with the selected address
5. Press "ESC" in stack window will sync the STACK window with ESP
6. Press "SHIFT + ENTER" will follow the DWORD value of the selected address in the DUMP window
7. Press "CTRL + 1 ~ 8" will sync the DUMP window with (EAX,ECX,EDX,EBX,ESP,EBP,ESI,EDI)

and lots more...

Besides keyboard shortcuts, StrongOD has a collection of ant-anti tricks:

1. HidePEB
2. !*PatchFloat (whatever that is?)
3. Advanced Ctrl-G (**See below)
4. KernalMode (?)
5. ShowBar (this shows a cool bar at the bottom ???)
6. Break on TLS
7. Load Symbols (?)
8. KillBadPEBug (I don't know which bad PE bug tho)
9. AdvEnumModule (?)
10. Anti-Anti Attach
11. Skip some Exceptions (which ones?)
12. Remove EP One-shot
13. Break on Ldr
14. AutoUpdate (tho I don't know what I'm updating automatically!)

There is also a "CreateProcess Option" field that allows you to select between "Normal", "CreateAsUser", and "CreateAsStrict", tho I don't know what this means. There's also a "SuperMode" that's greyed out. Sounds intriguing.

Other options include a memory allocator, a 'Detach' option, a Check Update option (?), a "PatchOD" option which seems to make Olly stop and restart itself in a really scary way, a CheckVMP option (for VMProtect) and an "Inject DLL" option which sounds really fun, though I haven't played with it yet.

One important note about this plugin: if you have any other ctrl-G overrides (like OllyAdvanced) you must disable them in those plugins or StrongOD will crash. Since StrongOD's goto box is similar to OllyAdvanced, it's not a big deal. (there are also workarounds to this...)

Ultra String Reference

Ver: 0.12
By: Luo

This is a supped-up version of the built in "search for String References". It searches for both ASCII and UNICODE, searches the entire memory space, and finds strings the built-in search function won't. After using this, you will wonder how you ever used Olly's built in string searcher.

ollydbg , plugins

9 Comments for this entry



ludkiller

May 27th, 2012 on 3:54 am

Awesome, I was tired searching for these plugins and now, I can find all of them at one place thanks to you 😊 Keep more Tutorials Coming and also I am out of town for a while so will not be regular for 2-5 days 😊
Thank you again, and I am gonna download that full package as soon as I get home 😊
Thanks Again

Reply



Cariana

June 1st, 2012 on 1:59 am

your blog is very cool.

Reply



Dúlia

June 1st, 2012 on 2:26 pm

these kind of articles really help me. so thank you.

Reply



Bianca

June 1st, 2012 on 10:25 pm

haha! i agree with you!

Reply



Merrill

April 8th, 2013 on 7:49 am

Heya are using WordPress for your blog platform?
I'm new to the blog world but I'm trying to get started and set up my own. Do you need any html coding knowledge to make your own blog?
Any help would be greatly appreciated!

Feel free to surf to my blog post – Merrill

Reply



Charlieb000

September 11th, 2013 on 1:35 am

Hi,
since i dont see what i want in the things above i ask if perhaps there is a plug in to do this.

I notice "hit trace" has been removed in this cooler version of olly you distribute in Tutorial3. is there a way to limit the hit trace hilight to the previous 100 or so lines in the program? (for times that it decides to suddenly close) .. or perhaps even remember the program paremeters from 100 lines ago and simply revert to when it was back...

Or perhaps hilight a new command or jump that did not occur/run in the previous execution of the program or perhaps stop the first line that hasnt been run before in the currently running code?

Charlie.

Reply



Charlieb000

September 11th, 2013 on 2:08 am

nvm

i found the tutorial on olly's site.. a little unintuitive though... "run trace" gives one output and so i thought that was the function of "trace", but "trace into"/over" gives what was needed.

Charlie.

Reply



Charlie000

September 11th, 2013 on 6:45 am

i have run into problems with trace on Random's version. (cant use the original as it doesnt seem to work with the program). Now the Trace is missing what is going on in the program, unless if i step through the commands. the original olly does work ok.

And the trace Protocol options are missing. The closest in random's is "set condition" menu item (condition to pause run trace) however these settings dont appear to do what the "set protocol" menu item (commands protocolled by run trace) did, which was ignore everything outside the specified range. so this is making things more difficult.

Charlie.

Reply



Charlie000

September 11th, 2013 on 11:16 pm

Ok i think i get it now... random is still using v1, when there is v2 available.

cb

Reply

2 Trackbacks / Pingbacks for this entry

The Reverse Engineers Toolkit « The Legend Of Random

May 31st, 2012 on 5:36 pm

[...] to thwarting pretty much every anti-debugging trick invented, the plugins are a must have. (See my guide to Olly plugins for specific information on some of the most important [...])

Tools Programming and Reverse Engineering | msg1len Official Website

July 2nd, 2012 on 1:14 pm

[...] DLL plugins. There is no source code, text files, or any additional elements.) You can also view my page describing all of these plugins if you're unsure as to what they [...]

Leave a Reply

Name

Mail (will not be published)

Website

Leave comment

[RSS](#) feed for this post (comments)

· [TrackBack](#) [URI](#)

Recent Posts

My Absence
What Are These Strange Posts?
Nice Beginning Article on Reversing Android
She Is 17-years-old, She Did It Publicly In High School And While Drunk

Archives

October 2012
September 2012
August 2012
July 2012
June 2012

Tags

adding functionality assembly language binary code
cave code caves **cracking** crackme ebook
exploiting binaries Guide **Olly ollydbg** olly tutorial
plugins **reverse engineering** sandbox Tools
tutorial

And The Most Posts Submitted In A Single
Sitting Goes To...

Copyright © 1996-2010 The Legend Of Random. All rights reserved.

Jarrah theme by [Templates Next](#) | Powered by [WordPress](#)