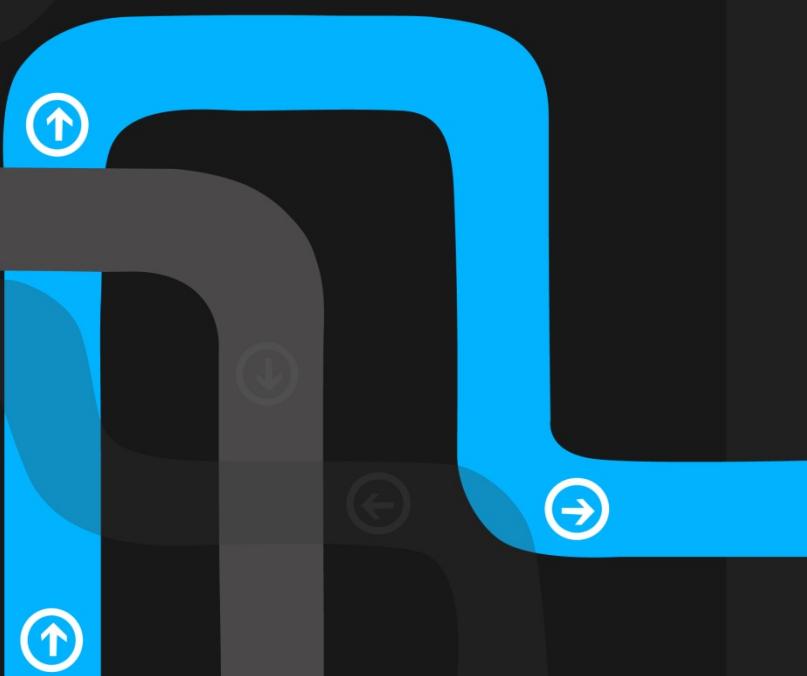


IT PRO|DEV CONNECTIONS 2012



IT PRO|DEV
CONNECTIONS
11111011100





Life after Blue Screen of Death

.κιόμας υπάρχε



@sitoiG



IT PRO|DEV
CONNECTIONS
11111011100



BSODs



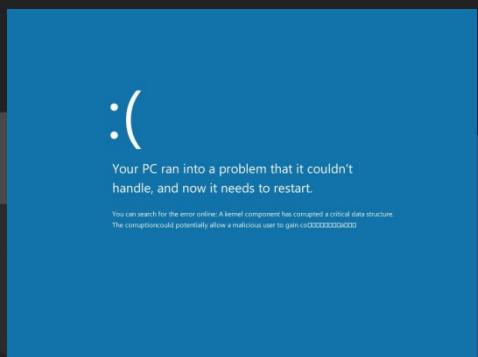
Windows 98



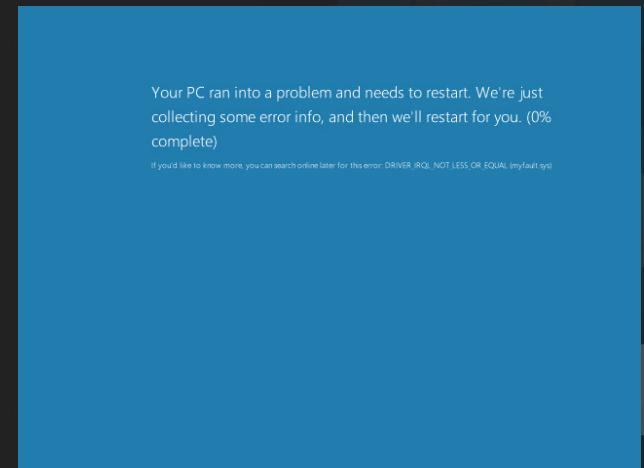
Windows 7



Server 2008 R2



Windows 8



Server 2012

BSODs



Walmart

London Olympics



Toronto

BSOD: Γιατί;

Το πλέον παρεξηγημένο χαρακτηριστικό κάθε Windows έκδοσης

Τυπικό παράδειγμα:

Driver με πρόσβαση στο kernel (π.χ. ο GPU driver) προσπαθεί να «γράψει» σε read-only μνήμη ή να «διαβάσει» από κάποια διεύθυνση της, η οποία δεν υπάρχει

Αποτέλεσμα:

Τα Windows αναγνωρίζουν πως κάτι το οποίο δεν έπρεπε να συμβεί, έχει συμβεί. Ένας driver ο οποίος έχει πρόσβαση σε όλο το σύστημα συμπεριλαμβανομένου και του hardware, δεν παρουσιάζει προβλεπόμενη συμπεριφορά

BSODs: Γιατί;

Αποτέλεσμα:

Τα Windows εμφανίζουν την μπλε οθόνη και προλαμβάνουν την αλυσιδωτή αντίδραση αποτέλεσμα της οποίας θα ήταν ο περαιτέρω κατακερματισμός της μνήμης, των δεδομένων του σκληρού, ακόμα και η μόνιμη βλάβη κάποιου υλικού

Παρά το γεγονός πως αναφέρει ρητά το λόγο για τον οποίο εμφανίστηκε, τείνει να θεωρείται πάντα ως σφάλμα των Windows

A problem has been detected and windows has been shut down to prevent damage to your computer.

"A problem..?"

BSODs: Under the hood

KeBugCheckEx routine ([MSDN link](#))

- Αναλαμβάνει να σταματήσει όλους τους επεξεργαστές
- Αλλάζει την εμφάνιση της οθόνης σε VGA
- Εμφανίζει το μπλε φόντο
- Παρουσιάζει το stop code μαζί με κάποιες προτροπές στον χρήστη
- Δίνει την ευκαιρία στους drivers του συστήματος να σταματήσουν τη λειτουργία των συσκευών τους
- Καλεί τους drivers να προσθέσουν πληροφορίες στο crash dump μέσω της KeRegisterBugCheckReasonCallback

BSODs: Under the hood

KeBugCheckEx routine ([MSDN link](#))

Έχει μια μεταβλητή και τέσσερις παραμέτρους

Εάν κάποια από τις διευθύνσεις που αναφέρονται στις παραμέτρους ανήκει σε τμήμα του λειτουργικού ή σε κάποιο driver, εμφανίζεται το όνομα του και πληροφορίες σχετικά με αυτόν

A problem has been detected and Windows has been shut down to prevent damage to your computer.

Stop Code
DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

Stop Code	Parameters
*** STOP: 0x0000000D1 (0xFFFFF8A001A6E800, 0x0000000000000002, 0x00000000000000000000000000000000)	0xFFFFF88006754385

*** myfault.sys - Address FFFF88006754385 base at FFFF88006753000, DateStamp 4f806ca1

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 60

Windows Server 2008 R2 BSOD

BSODs: Under the hood

Ο Session Manager ελέγχει το κλειδί

*HKLM\ SYSTEM\ CurrentControlSet\ Control\ Session
Manager\Memory Management\ExistingPageFiles*
για πληροφορίες σχετικά με το page file

Καλεί την *SmpCheckForCrashDump* να ελέγξει την ύπαρξη
crash dumps στον header του page file

Ελέγχει το κλειδί

HKLM\SYSTEM\CurrentControlSet\Control\CrashControl
με τις ρυθμίσεις του συστήματος για τα crashes, μια από τις
οποίες περιέχει το όνομα του προσφάτου crash dump
(default: C:\Windows\Memory.dmp)

Session Manager

SmpCheckForCrashDump



*HKLM\ SYSTEM\ CurrentControlSet\ Control\ Session
Manager\Memory Management\ExistingPageFiles*



Session Manager

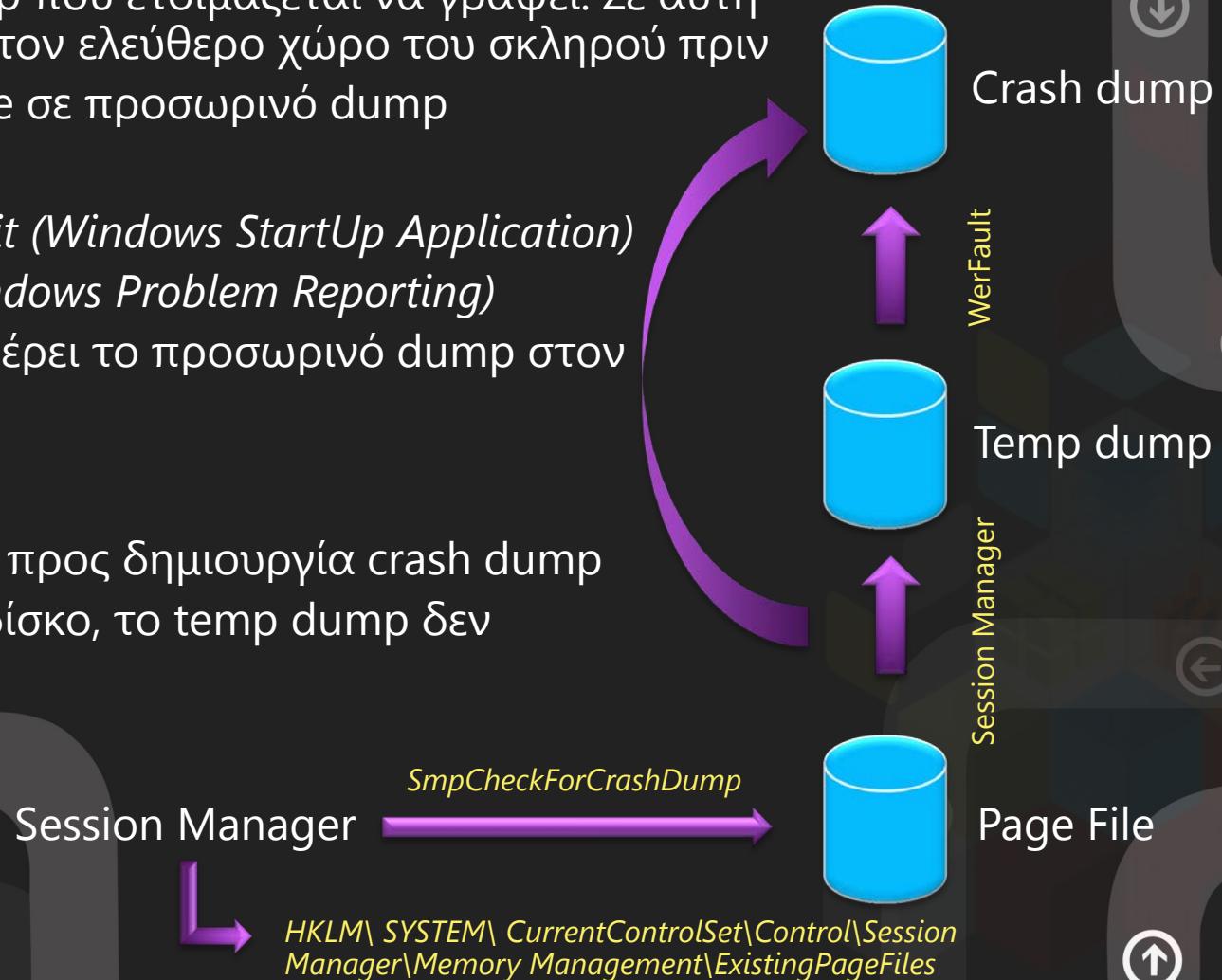
Page File

BSODs: Under the hood

Ελέγχει εάν το page file βρίσκεται σε διαφορετικό σκληρό δίσκο με το crash dump που ετοιμάζεται να γράψει. Σε αυτή τη περίπτωση ελέγχει τον ελεύθερο χώρο του σκληρού πριν μετατρέψει το page file σε προσωρινό dump

Στη συνεχεία το *Wininit* (*Windows StartUp Application*) καλεί το *WerFault* (*Windows Problem Reporting*) προκειμένου να μεταφέρει το προσωρινό dump στον τελικό του προορισμό

Εάν το page file και το προς δημιουργία crash dump βρίσκονται στον ίδιο δίσκο, το temp dump δεν χρησιμοποιείται



BSODs: Under the hood

Το page file από τα ματιά μιας μπλε οθόνης

Page file = Εικονική μνήμη

«Δεν χρειάζεται, έχω x GB ram» ➔ Crash dump;

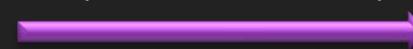
Το μέγεθος του εξαρτάται από τον τύπο του crash dump που επιθυμείτε να πάρετε μετά από μια μπλε οθόνη

Session Manager



HKLM\ SYSTEM\ CurrentControlSet\ Control\ Session Manager\ Memory Management\ ExistingPageFiles

SmpCheckForCrashDump



BSODs: Page File

Small memory dump (minidump):

Περιέχει πληροφορίες σχετικά με το stop code και τους drivers

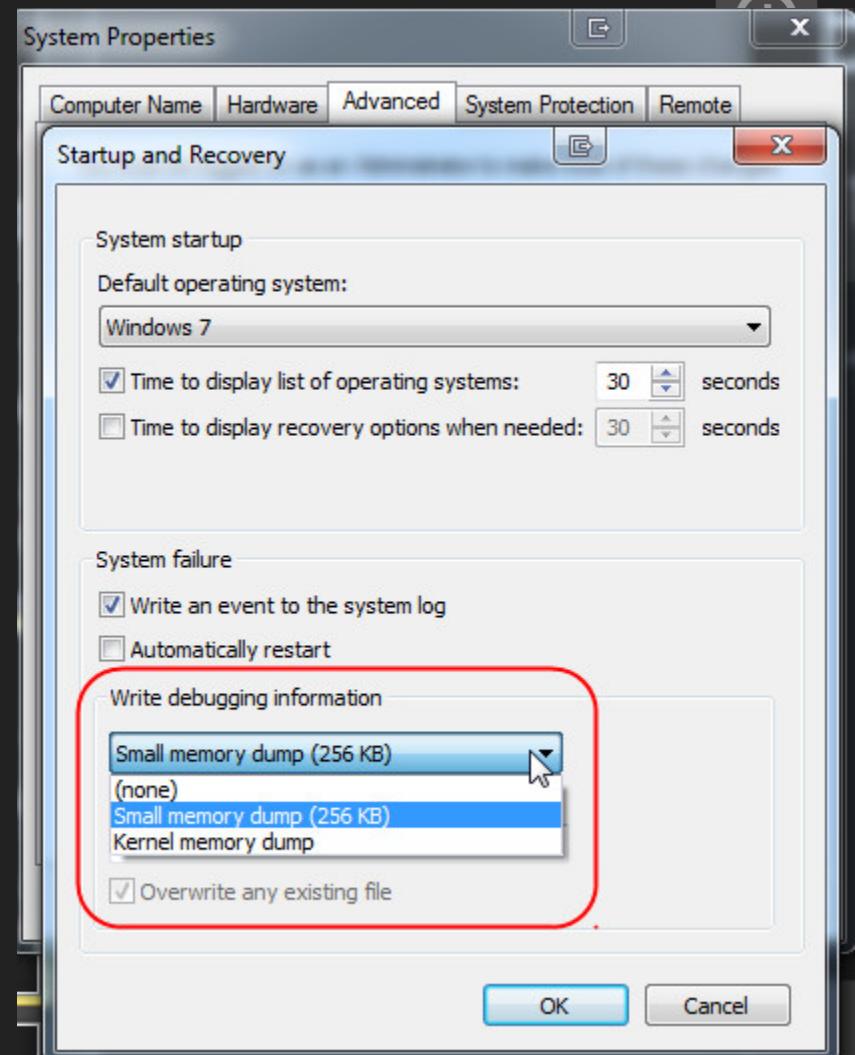
Kernel memory dump:

Περιέχει τα πάντα εκτός από πληροφορίες σχετικά με διεργασίες που ανήκουν στο User-Mode.

Default ρύθμιση στα Windows Server 2008 R2

Complete memory dump:

Περιλαμβάνει και το User-Mode



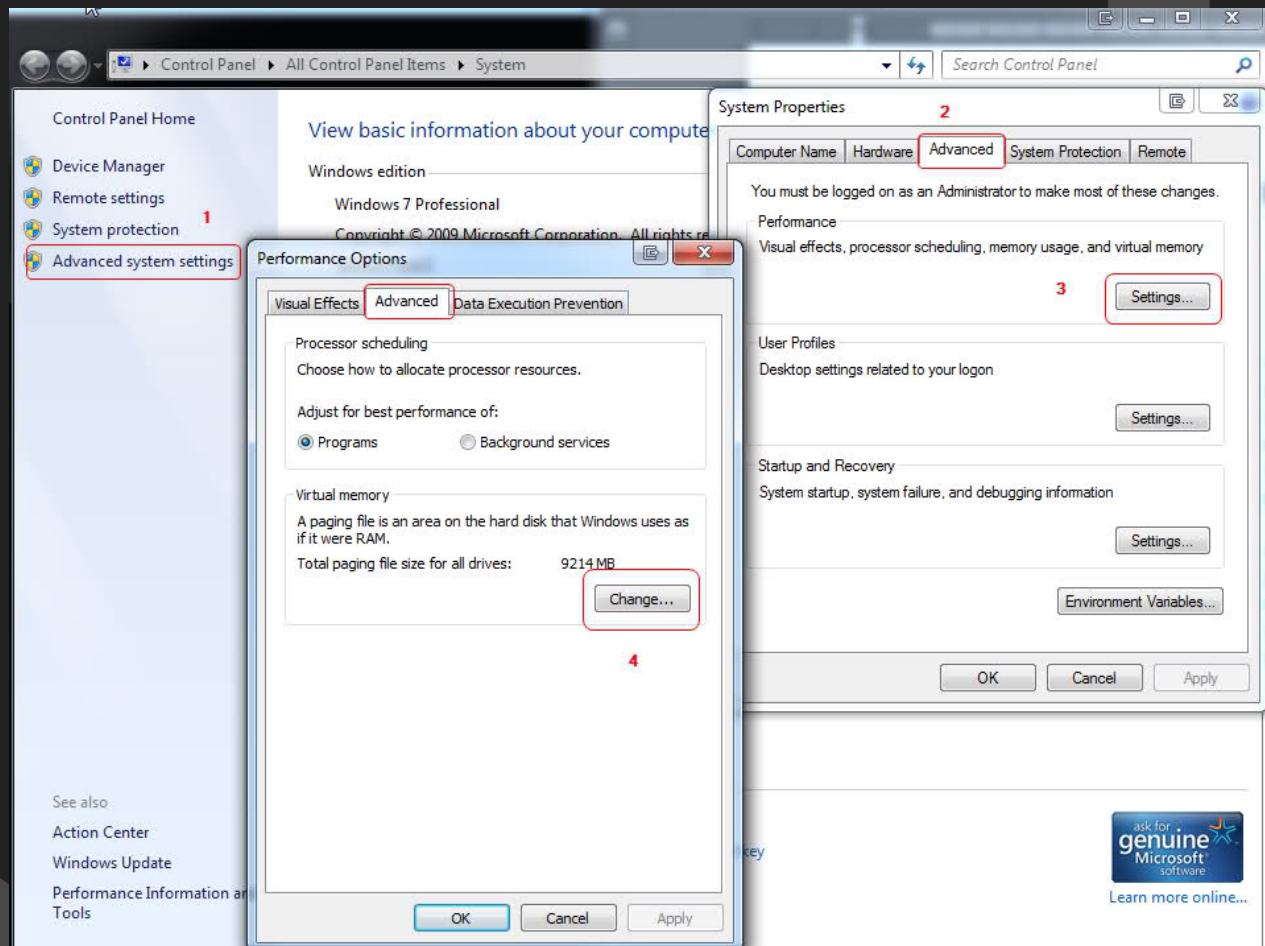
BSODs: Page File

Μέγεθος

Εάν κάνετε χρήση του small memory dump, λίγα MBs είναι αρκετά

Το μέγεθος του kernel dump διαφέρει από σύστημα σε σύστημα

To complete memory dump χρειάζεται page file ισο με τη ram, συν 1 MB για τον header του



BSODs: Page File

«Δεν έχω αρκετό χώρο στο C:\ για μεγάλο page file και για kernel/complete dump ταυτόχρονα»

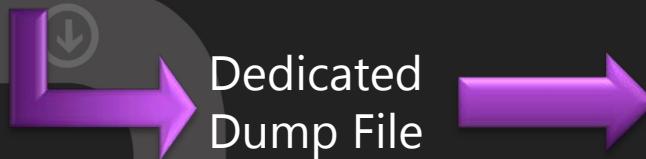


Key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\CrashControl

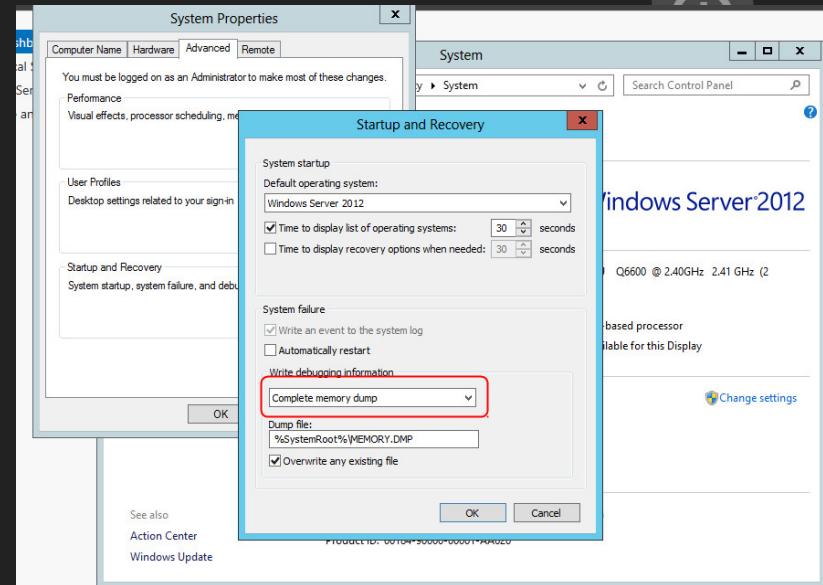
Name: DedicatedDumpFile

Type: REG_SZ

Value: D:\Dumps\DedicatedDump.sys



Dedicated
Dump File



Name: DumpFileSize

Type: REG_DWORD

Value: 1024 (μέγεθος σε MBs)

BSODs: Troubleshooting

A problem has been detected and Windows has been shut down to prevent damage to your computer.

Δυο βασικές κατηγορίες

BSOD



Software

Hardware

BSODs: Troubleshooting

- **Hardware**

RAM	Memtest (bootable)
Σκληροί δίσκοι	Vendor diagnostics
CPU	Prime95, Lynx
PSU	OCCT
Θερμοκρασίες	Realtemp, Coretemp
Ελαττωματικές PCI	"Trial and error"
Καλώδια	"Trial and error"

BIOS settings : DEFAULT!

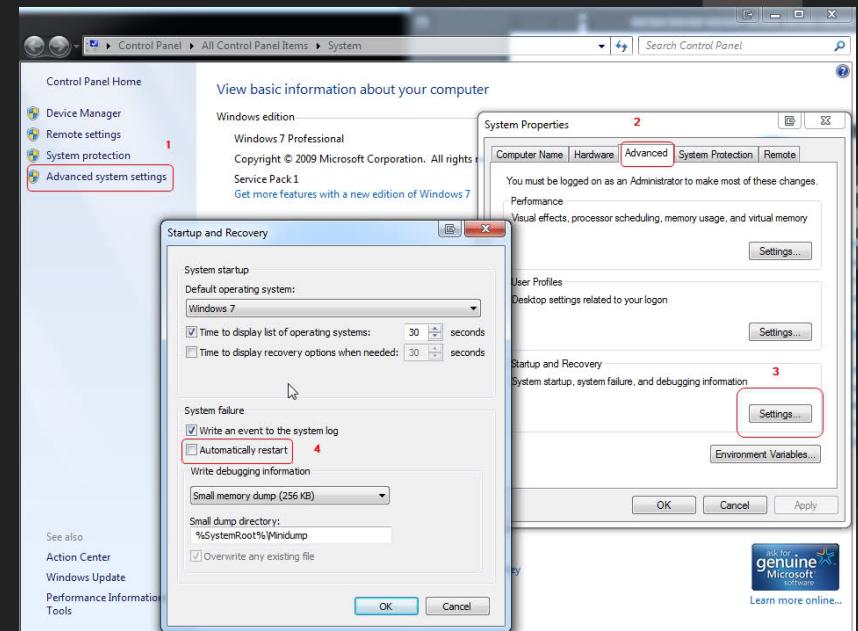
BSODs: Troubleshooting

Εξαιτίας του μεγάλου εύρους των παραγόντων από τους οποίους μπορεί να προκληθεί μια μπλε οθόνη, η χρήση ενός γενικού πλάνου αντιμετώπισης τους, αποτελεί μια καλή αρχή.

Προσπαθούμε να εντοπίσουμε κάτι κοινό στις συνθήκες που επικρατούν στο σύστημα μας πριν την εμφάνιση της μπλε οθόνης

Απενεργοποιούμε την αυτόματη επανεκκίνηση

Φροντίζουμε τη φύλαξη των dumps από προγράμματα τρίτων κατασκευαστών



BSODs: Troubleshooting

Ελέγχουμε τα stop codes: Είναι κοινά για κάθε μπλε οθόνη; Αναφέρεται κάποιος driver; Παραμένει ο ίδιος;

Ναι



Όχι

To [MSDN](#) διαθέτει πληροφορίες για κάθε ένα από τους 265 διαφορετικούς stop codes



A problem has been detected and Windows has been shut down to prevent damage to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS
PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** **SPCMDCON.SYS** - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c

Η μεγάλη ποικιλία stop codes μπορεί να αποτελεί ένδειξη hardware προβλήματος

BSODs: Troubleshooting

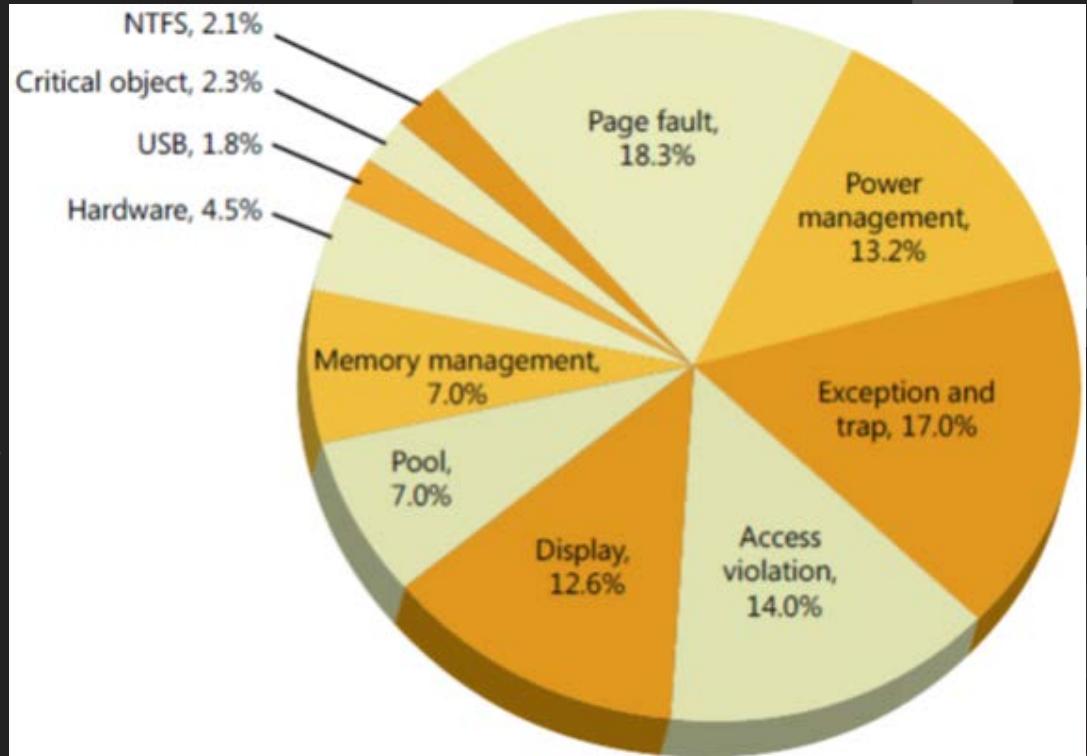
Stop Codes

VIDEO_TDR_FAILURE

MEMORY_MANAGEMENT

DRIVER_IRQL_NOT_LESS_OR_EQUAL

DRIVER_POWER_STATE_FAILURE



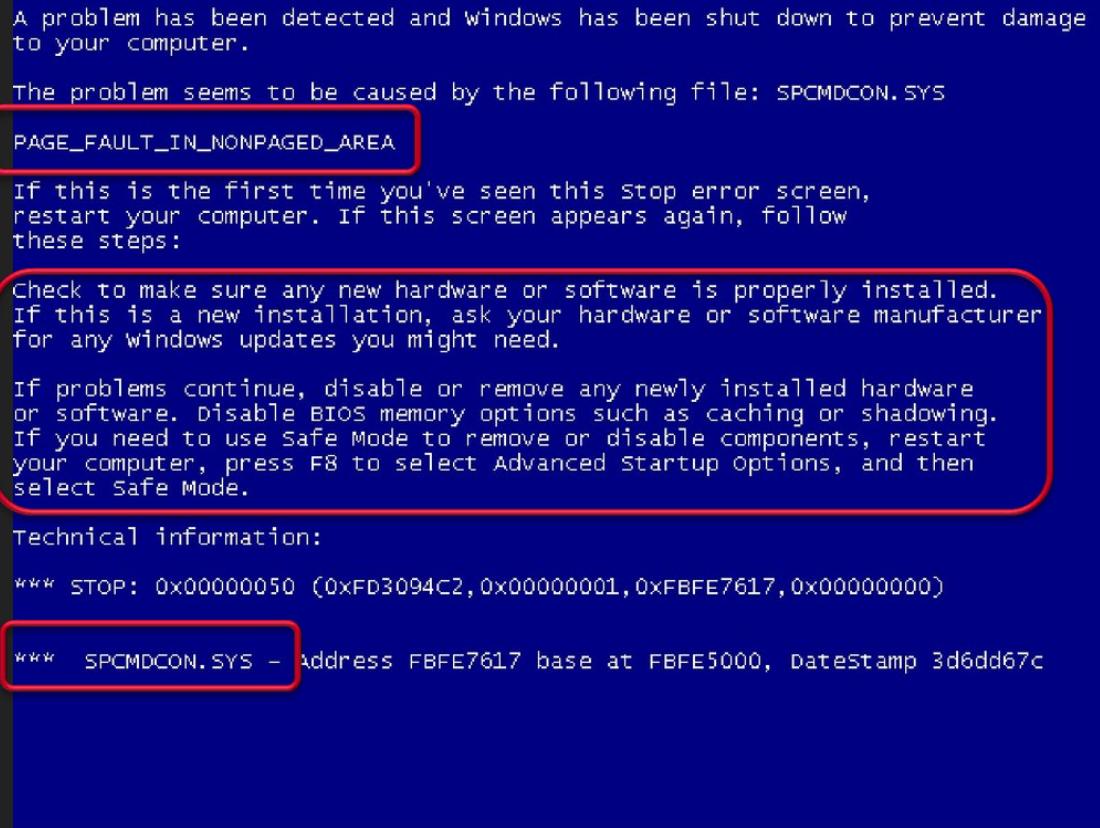
Top stop codes, Windows 7 Μάιος 2012
Windows Internals 6th Edition, Part2

BSODs: Troubleshooting

Έλεγχος του [MSDN](#) για τον stop code

"RTFM" ή στην περίπτωση μας, RTFBSOD

Τι είναι ο SPCMDCON.sys;
Προσοχή σε false positives!



BSODs: Troubleshooting

Τι κάνουμε σε περίπτωση μιας τέτοιας μπλε οθόνης;

«*This indicates that an exception happened while executing a routine that transitions from non-privileged code to privileged code. A hardware device, its driver, or related software might have caused this error*»

[MSDN](#)

Dxgkrnl.sys



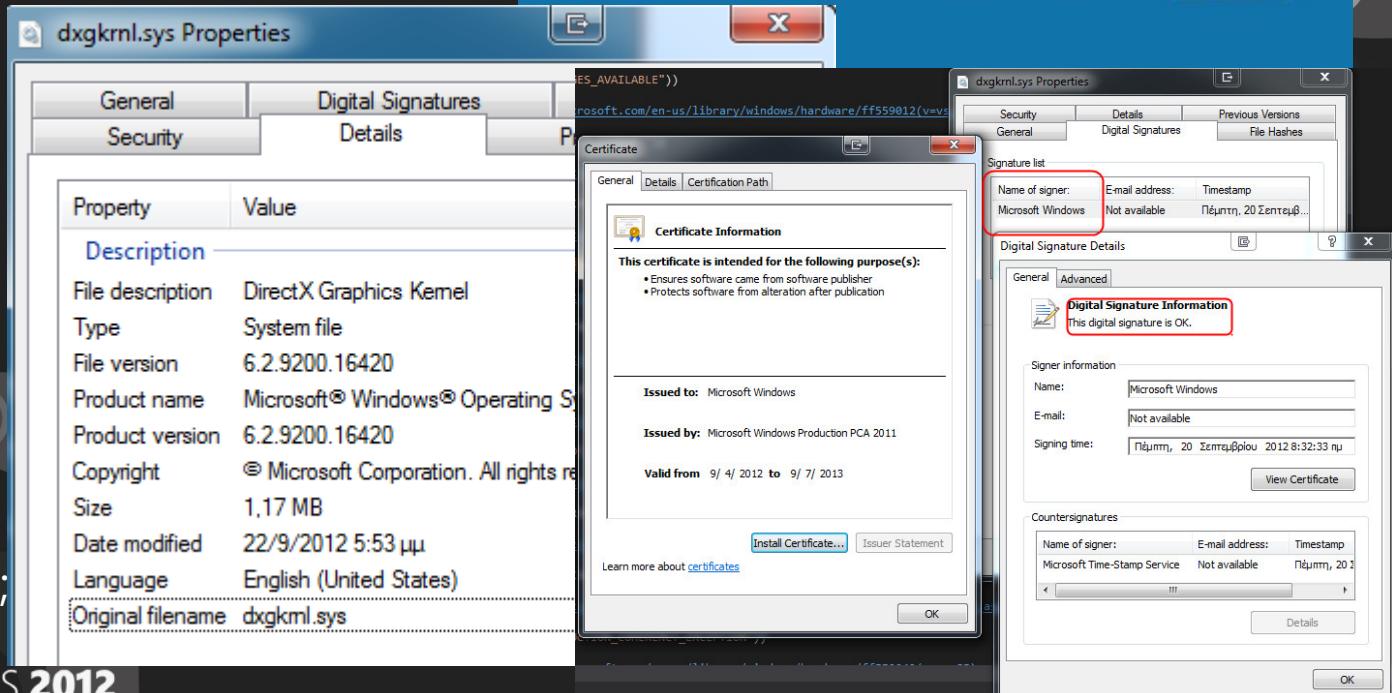
DirectX



Microsoft code



Σίγουρα:::



BSODs: Troubleshooting

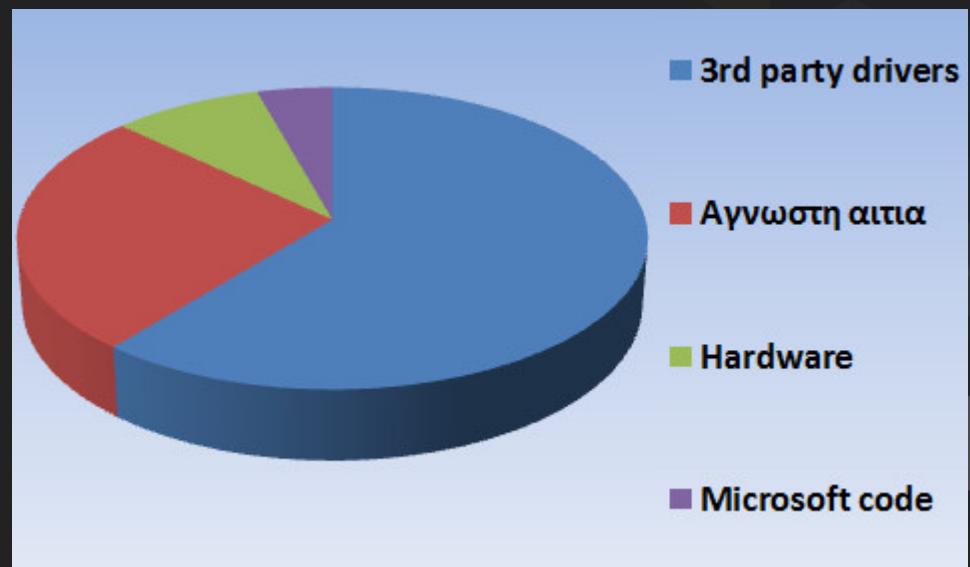
Μήπως όντως φταίει ο dxgkrnl.sys;  Σχεδόν αποκλείεται!

Drivers της Microsoft σπανίως είναι υπεύθυνοι για μπλε οθόνες

To 2004 υπήρχαν 55.000 διαφορετικοί 3rd party drivers, 24 νέοι/μέρα

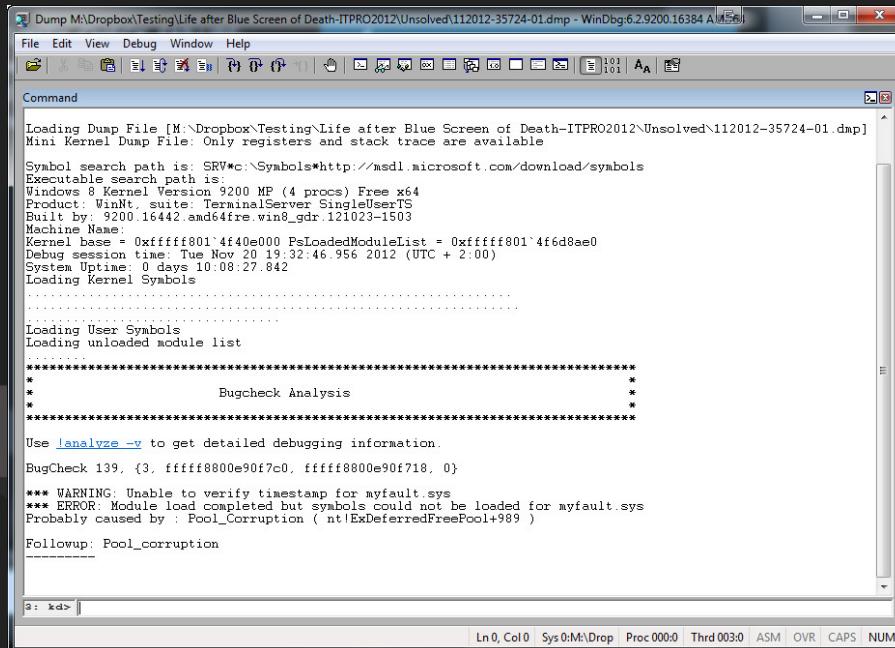
Microsoft's crash dump analysis:

- 70% από 3rd party drivers
- 15% από άγνωστη αιτία
- 10% hardware
- 5% Microsoft code



BSODs: Troubleshooting

KERNEL_SECURITY_CHECK_FAILURE:
«*This bug check indicates that the kernel has detected the corruption of a critical data structure»*



Dump M:\Dropbox\Testing\Life after Blue Screen of Death-ITPRO2012\Unsolved\112012-35724-01.dmp - WinDbg 6.2.9200.16384 A[...]

File Edit View Debug Window Help

Command

```
Loading Dump File [M:\Dropbox\Testing\Life after Blue Screen of Death-ITPRO2012\Unsolved\112012-35724-01.dmp]
Mini Kernel Dump File: Only registers and stack trace are available

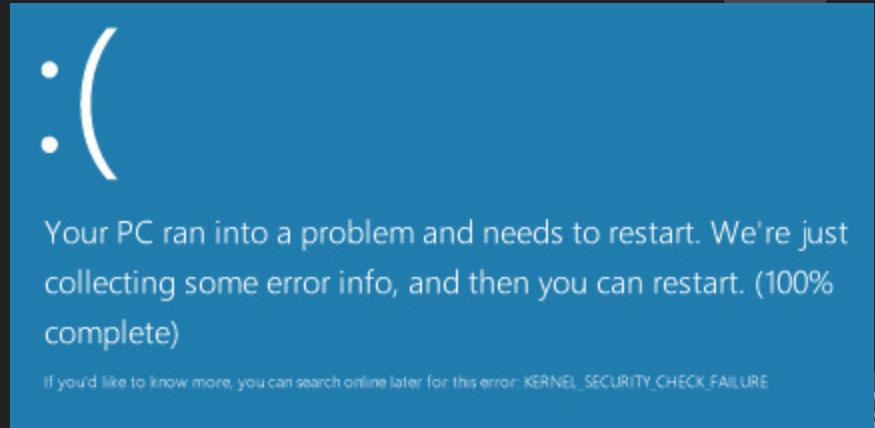
Symbol search path is: SRV*c:\Symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows 8 Kernel Version 9200 MP (4 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 9200_16442_amd64fre_win8_gdr_121023-1503
Machine Name:
Kernel base = 0xfffff801`4f40e000 PsLoadedModuleList = 0xfffff801`4f6d8ae0
Debug session time: Tue Nov 20 19:32:46.956 2012 (UTC + 2:00)
System Uptime: 0 days 10:08:27.842
Loading Kernel Symbols
.....
Loading User Symbols
Loading unloaded module list
*****
*           Bugcheck Analysis
*
*****
Use !analyze -v to get detailed debugging information.
BugCheck 139, {3, fffff8800e90f7c0, fffff8800e90f718, 0}

*** WARNING: Unable to verify timestamp for myfault.sys
*** ERROR: Module load completed but symbols could not be loaded for myfault.sys
Probably caused by : Pool_Corruption ( nt!ExDeferredFreePool+909 )

Followup: Pool_corruption
-----
```

2: kd> |

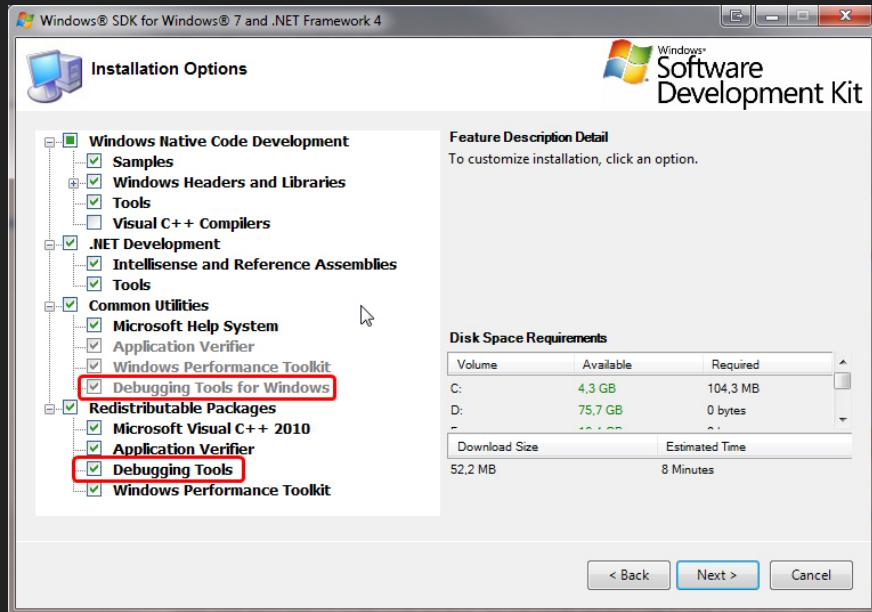
Ln 0, Col 0 Sys 0:M:\Drop Proc 000:0 Thrd 003:0 ASM OVR CAPS NUM



Windows Debugger (WinDbg)

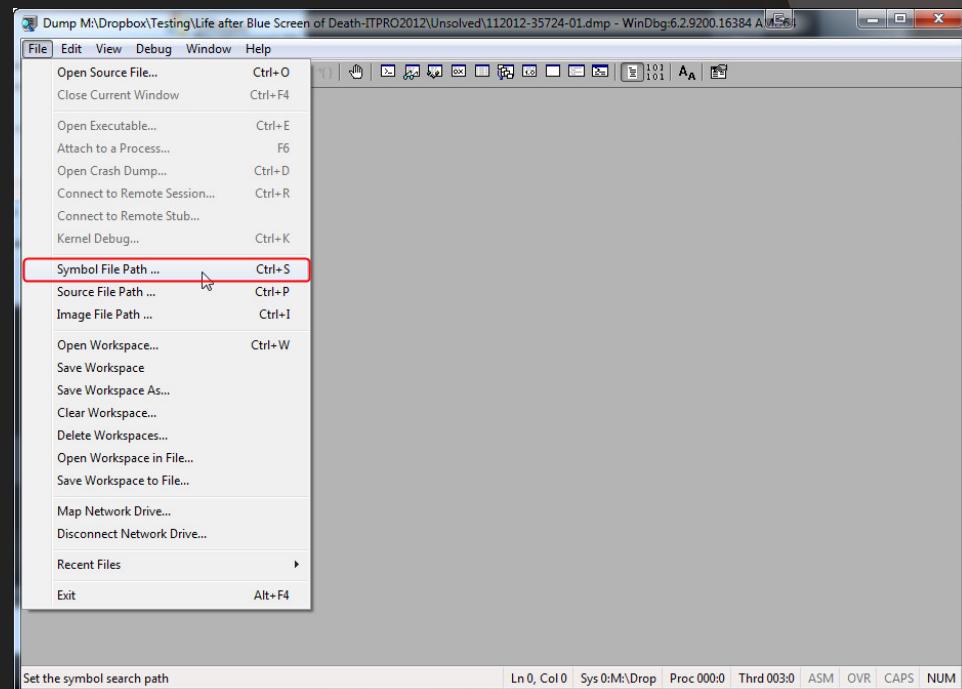
- Windows Driver Kit (WDK)
- Windows SDK

BSODs: Troubleshooting

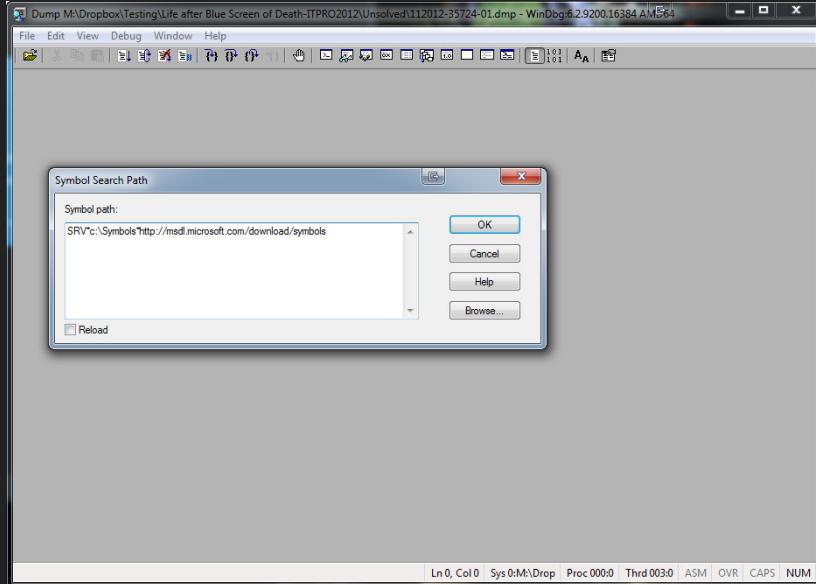


Εγκατάσταση του WinDbg μέσω του Windows SDK

Ρυθμίζουμε τον WinDbg να επικοινωνεί με τον Symbol Server της Microsoft και να διατηρεί μια cache σε φάκελο της επιλογής μας



BSODs: Troubleshooting



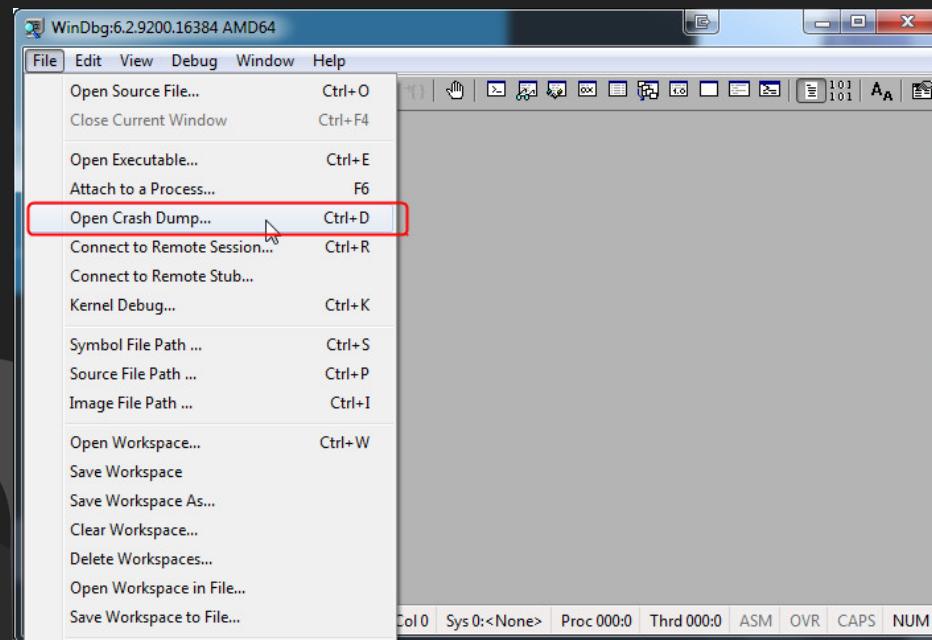
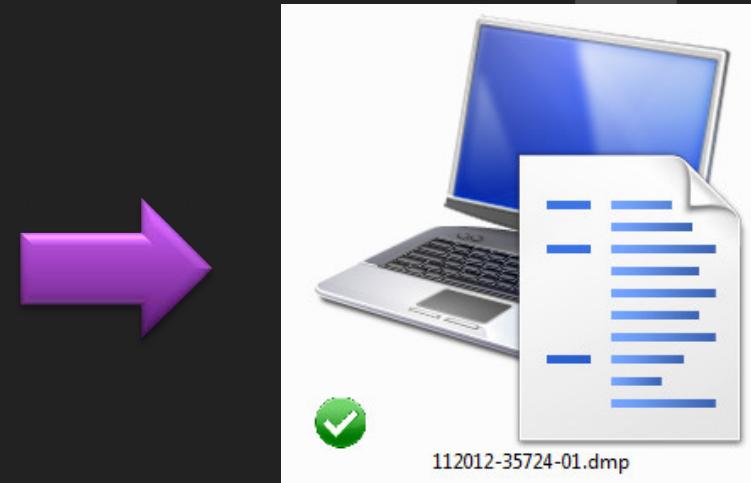
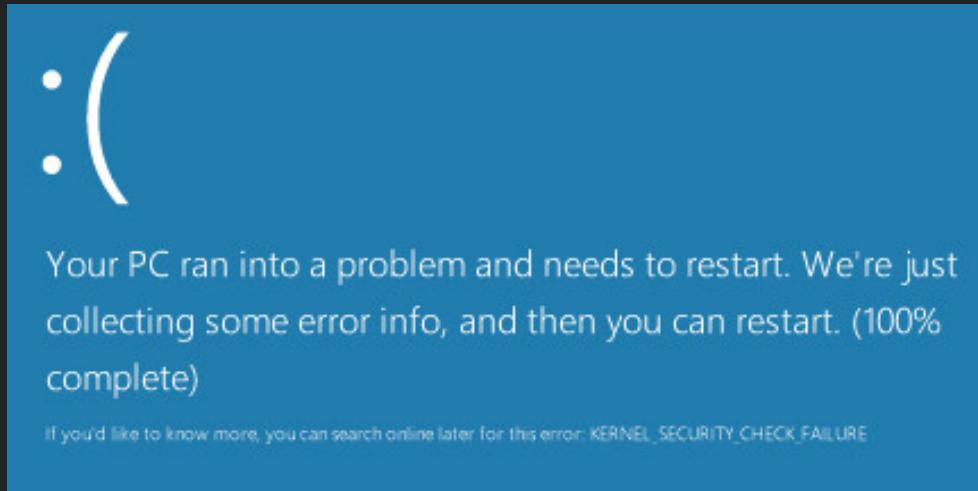
Ρυθμίζουμε τον WinDbg να χρησιμοποιεί τον Symbol Server και δηλώνουμε τον φάκελο C:\Symbols ως την cache τους:

SRV*c:\Symbols*http://msdl.microsoft.com/download/symbols

Symbol files

- Έχουν κατάληξη .pdb (παλαιότερες εκδόσεις χρησιμοποιούν την .dbg)
- Χωρίς αυτά ένα dump είναι απλά μια αλληλουχία αριθμών χωρίς νόημα
- Τα χρησιμοποιούμε για να μετατρέψουμε τα dumps σε ευανάγνωστη μορφή

BSODs: Troubleshooting



BSODs: Troubleshooting

Microsoft (R) Windows Debugger Version 6.2.9200.16384 AMD64

Copyright (c) Microsoft Corporation. All rights reserved.

Loading Dump File [M:\Dropbox\Testing\Life after Blue Screen of Death-ITPRO2012\Unsolved\112012-35724-01.dmp]

Mini Kernel Dump File: Only registers and stack trace are available

Symbol search path is: SRV*c:\Symbols*http://msdl.microsoft.com/download/symbols

Executable search path is:

Windows 8 Kernel Version 9200 MP (4 procs) Free x64

Product: WinNt, suite: TerminalServer SingleUserTS

Built by: 9200.16442.amd64fre.win8_gdr.121023-1503

Machine Name:

Kernel base = 0xfffffff801`4f40e000 PsLoadedModuleList = 0xfffffff801`4f6d8ae0

Debug session time: Tue Nov 20 19:32:46.956 2012 (UTC + 2:00)

System Uptime: 0 days 10:08:27.842

Loading Kernel Symbols

.....

Loading User Symbols

Loading unloaded module list

* * * * *
* Bugcheck Analysis *
* * * * *

Use !analyze -v to get detailed debugging information.

BugCheck 139, {3, tffff8800e9017c0, tffff8800e901718, 0}

*** WARNING: Unable to verify timestamp for myfault.sys

*** ERROR: Module load completed but symbols could not be loaded for myfault.sys

Probably caused by : Pool_Corruption (nt!ExDeferredFreePool+989)

Followup: Pool_corruption

BSODs: Troubleshooting

3: kd> !analyze -v

```
*****
```

*

*

Bugcheck Analysis

*

*

```
*****
```

KERNEL_SECURITY_CHECK_FAILURE (139)

```
*****
```

A kernel component has corrupted a critical data structure. The corruption could potentially allow a malicious user to gain control of this machine.

Arguments:

Arg1: 0000000000000003, A LIST_ENTRY has been corrupted (i.e. double remove).

Arg2: fffff8800e90f7c0, Address of the trap frame for the exception that caused the bugcheck

Arg3: fffff8800e90f718, Address of the exception record for the exception that caused the bugcheck

Arg4: 0000000000000000, Reserved

Debugging Details:

TRAP_FRAME: fffff8800e90f7c0 -- (.trap 0xfffff8800e90f7c0)

NOTE: The trap frame does not contain all registers.

Some register values may be zeroed or incorrect.

rax=fffffa8030e09820 rbx=0000000000000000 rcx=0000000000000003

rdx=0000000000000000 rsi=0000000000000000 rdi=0000000000000000

rip=fffff8014f67e5c6 rsp=fffff8800e90f950 rbp=fffff8014f699bc0

r8=fffffa8030e08010 r9=72a0e3bd9d3fa24c r10=fffffa8030c19c10

r11=0000000000000000 r12=0000000000000000 r13=0000000000000000

r14=0000000000000000 r15=0000000000000000

iopl=0 nv up ei pl nz na po cy

nt!ExDeferredFreePool+0x989:

fffff801`4f67e5c6 cd29 int 29h

Resetting default scope

BSODs: Troubleshooting

[snip]

CUSTOMER_CRASH_COUNT: 1
DEFAULT_BUCKET_ID: LIST_ENTRY_CORRUPT
BUGCHECK_STR: 0x139

PROCESS_NAME: NotMyfault.exe

CURRENT_IRQL: 2

ERROR_CODE: (NTSTATUS) 0xc0000409 - The system detected an overrun of a stack-based buffer in this application. This overrun could potentially allow a malicious user to gain control of this application.

EXCEPTION_CODE: (NTSTATUS) 0xc0000409 - The system detected an overrun of a stack-based buffer in this application. This overrun could potentially allow a malicious user to gain control of this application.

EXCEPTION_PARAMETER1: 0000000000000000

LAST_CONTROL_TRANSFER: from fffff8014f487a69 to fffff8014f488740

STACK_TEXT:

fffff880`0e90f498 fffff801`4f487a69 : 00000000`00000139 00000000`00000003 fffff880`0e90f7c0 fffff880`0e90f718 : nt!KeBugCheckEx
fffff880`0e90f4a0 fffff801`4f487d90 : fffffa80`31bc9040 fffff880`0e90f6c9 00000000`00000006 00000000`00000002 : nt!KiBugCheckDispatch+0x69
fffff880`0e90f5e0 fffff801`4f486ff4 : 00000000`0057e8b8 00000000`0057e830 fffff880`0e90fcf0 00000000`00000030 : nt!KiFastFailDispatch+0xd0
fffff880`0e90f7c0 fffff801`4f67e5c6 : 00000000`00000000 00000000`00001000 fffff801`4f69ad00 000007f6`320cd800 : nt!KiRaiseSecurityCheckFailure+0xf4
fffff880`0e90f950 fffff880`0da804d4 : 00000000`00000000 fffff880`0e90fec0 fffff901`022abb90 00000000`00000000 : nt!ExDeferredFreePool+0x989
fffff880`0e90fa20 00000000`00000000 : fffff880`0e90fec0 fffff901`022abb90 00000000`00000000 00000000`00000000 : myfault+0x14d4

STACK_COMMAND: kb

FOLLOWUP_IP:

nt!ExDeferredFreePool+989

fffff801`4f67e5c6 cd29 int 29h

SYMBOL_STACK_INDEX: 4

SYMBOL_NAME: nt!ExDeferredFreePool+989

FOLLOWUP_NAME: Pool_corruption

IMAGE_NAME: Pool_Corruption

DEBUG_FLR_IMAGE_TIMESTAMP: 0

MODULE_NAME: Pool_Corruption

BUCKET_ID_FUNC_OFFSET: 989

FAILURE_BUCKET_ID: 0x139_3_nt!ExDeferredFreePool

BUCKET_ID: 0x139_3_nt!ExDeferredFreePool

Followup: Pool_corruption

BSODs: Troubleshooting

Χρήσιμες εντολές του WinDbg

!m : Λίστα των modules [v | l | k | u | f]

!vm : Πληροφορίες σχετικά με τη μνήμη. *Tip: 0x21*

!vertarget : Πληροφορίες σχετικά με το σύστημα (έκδοση Windows, SP, uptime, κλπ)

!sysinfo : [cpuinfo | cpumicrocode | cpuspeed | gbl | machineid
registers | smbios] [-csv | - noheaders]

!mv m {driver} : Πληροφορίες σχετικά με ένα συγκεκριμένο driver

!running : Πληροφορίες σχετικά με κάθε thread που τρέχει στη cput (kernel dump)

-logo {c:\mylogfile.txt} : Αποθήκευση log σε θέση της επιλογής μας

BSODs: Troubleshooting

Άλλοι debuggers που μπορούν να χρησιμοποιηθούν για την ανάλυση
crash dumps

kd.exe : Kernel-mode debugger with a console interface.

cdb.exe και Ntsd.exe : User-mode debugger with a console interface

Τυπική ανάλυση ενός minidump, με export των drivers, δημιουργία log file, κλείσιμο αυτού, σύνδεση με τον symbol server και αποθήκευση των .pdb σε cache:

```
1
2 C:\Program Files (x86)>"Windows Kits\8.0\Debuggers\x64\kd.exe -logo c:\FullAnalysis.txt -c "!analyze -v;r;kv;lmtn;.logclose;q" -y "SRV*c:\Symbols*http://msdl.microsoft.com/download/symbols" -z "M:\Minidumps\100512-12312-01.dmp"
```

BSODs: Troubleshooting

Τι μπορούμε να κάνουμε όταν :

- Ο windbg επιμένει να μας ενημερώνει πως για τη μπλε οθόνη φταίει το ntoskrnl.exe (kernel image των Windows)
- Αντί για μπλε οθόνη, το σύστημα μας παγώνει (hang Vs crash)
- Δεν παίρνουμε crash dump, παρόλου που το page file είναι ενεργό
- Έχουμε ελέγξει διεξοδικά το hardware, χωρίς αποτέλεσμα
- Η stack είναι της μορφής

nt!KeBugCheckEx
nt!MiBadShareCount+0x4c
nt! ?? ::FNODOBFM::`string'+0x31f4a
nt!MiDeleteVirtualAddresses+0x408
nt!MiRemoveMappedView+0xd9
nt!MiUnmapViewOfSection+0x1b0
nt!NtUnmapViewOfSection+0x5f
nt!KiSystemServiceCopyEnd+0x13

BSODs: Troubleshooting

Driver Verifier

Είναι ενσωματωμένος στα Windows (2000, XP, Server 2003, Vista, Server 2008, Server 2008 R2, 7, Server 2012, 8)

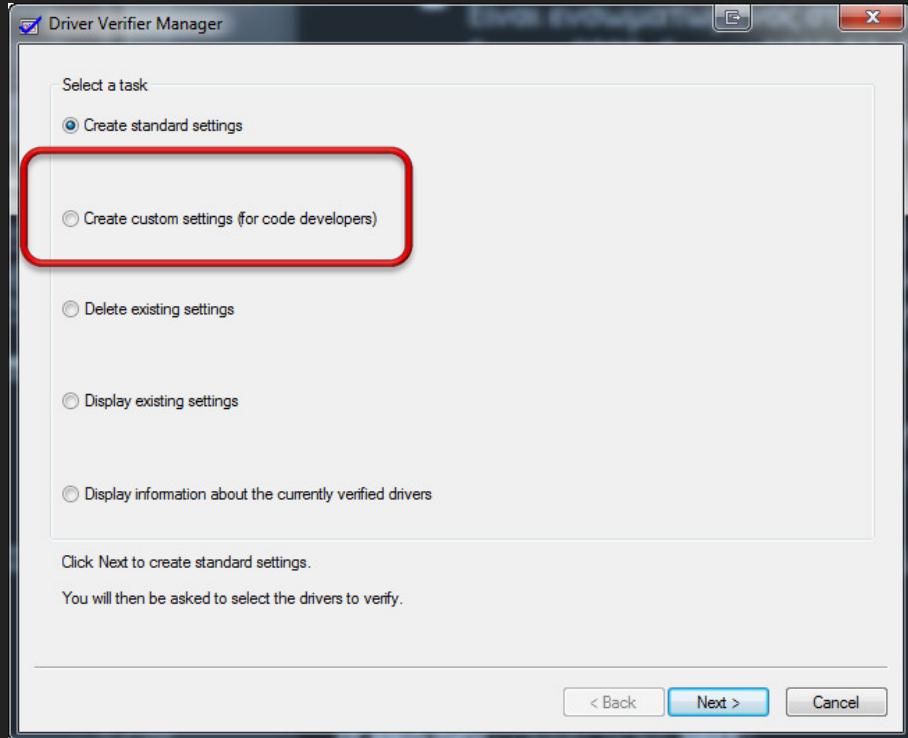
Χρησιμοποιείται για την αντιμετώπιση και τον εντοπισμό προβληματικών drivers

Μπορεί να ενεργοποιηθεί με δυο τρόπους:

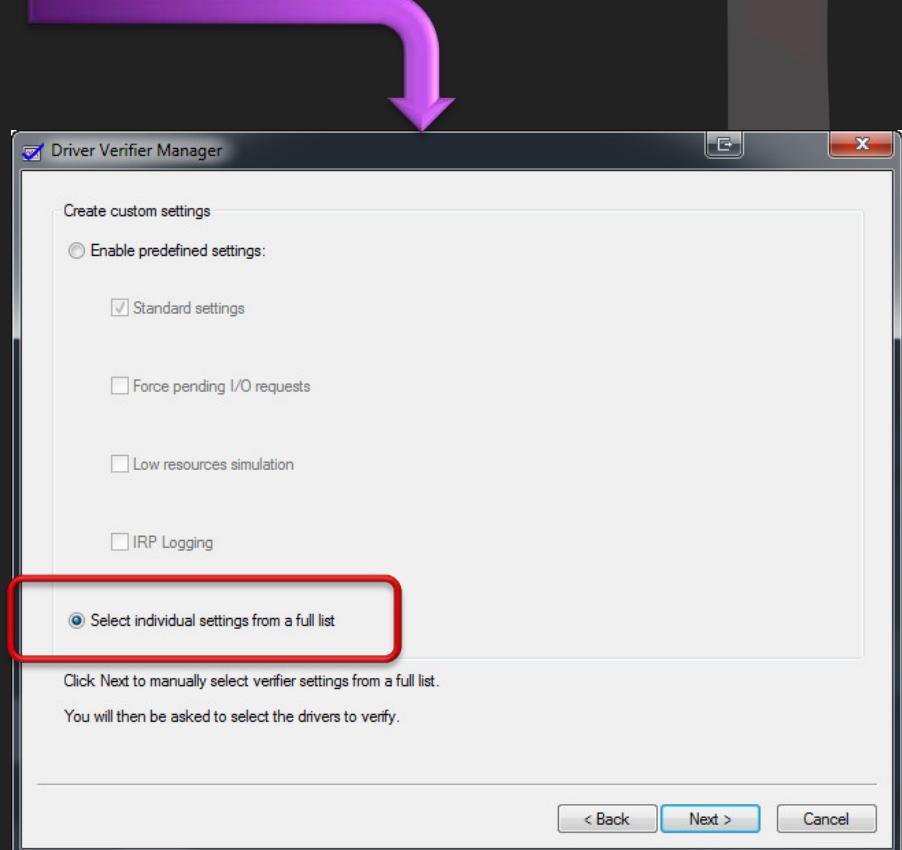
- Μέσω της Registry και των κλειδίων
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
Session Manager\Memory Management\VerifyDrivers
και
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
Session Manager\Memory Management\ VerifyDriverLevel
- Μέσω της Εκτέλεσης (Run), δίνοντας verifier.exe

BSODs: Troubleshooting

Driver Verifier



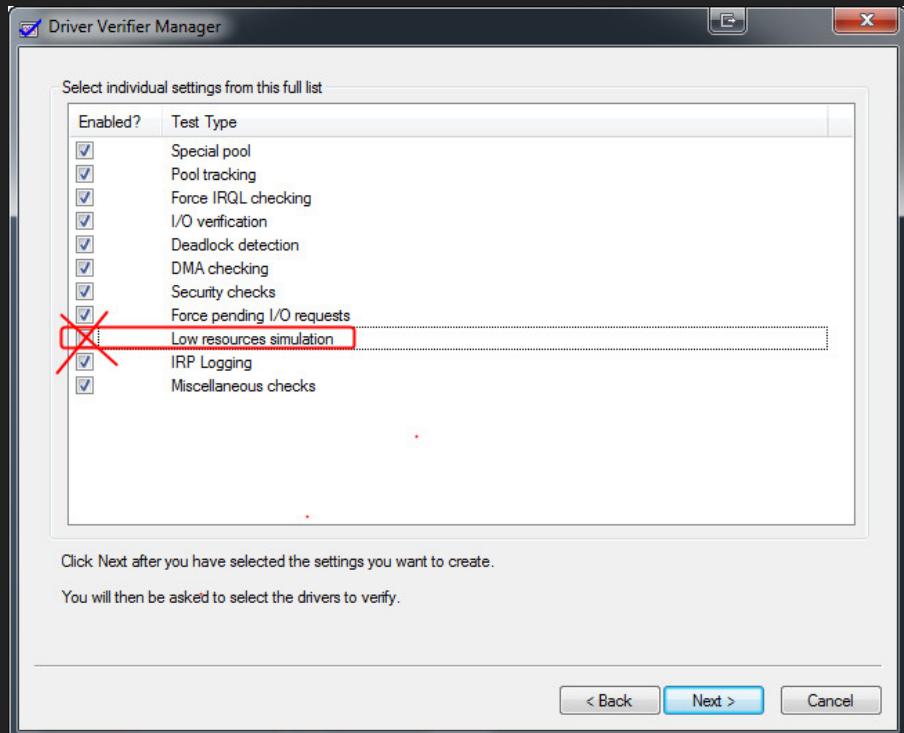
«Create custom settings (for code developers)»



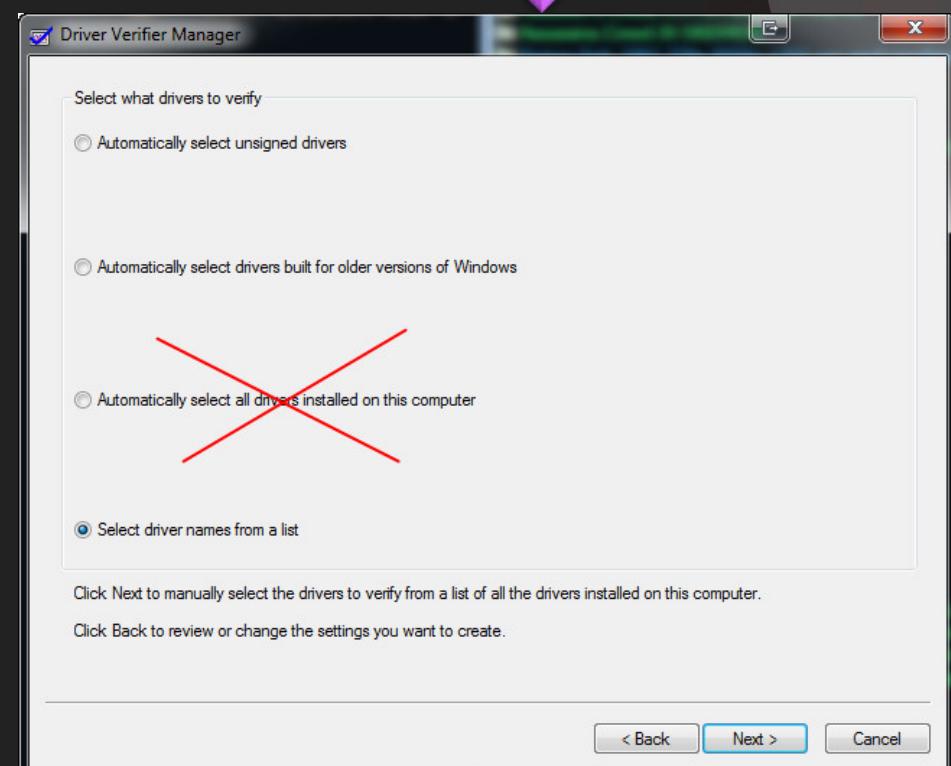
«Select individual settings from full list»

BSODs: Troubleshooting

Driver Verifier



Επιλεγούμε όλα τα διαγνωστικά εκτός από το «Low resources simulation»



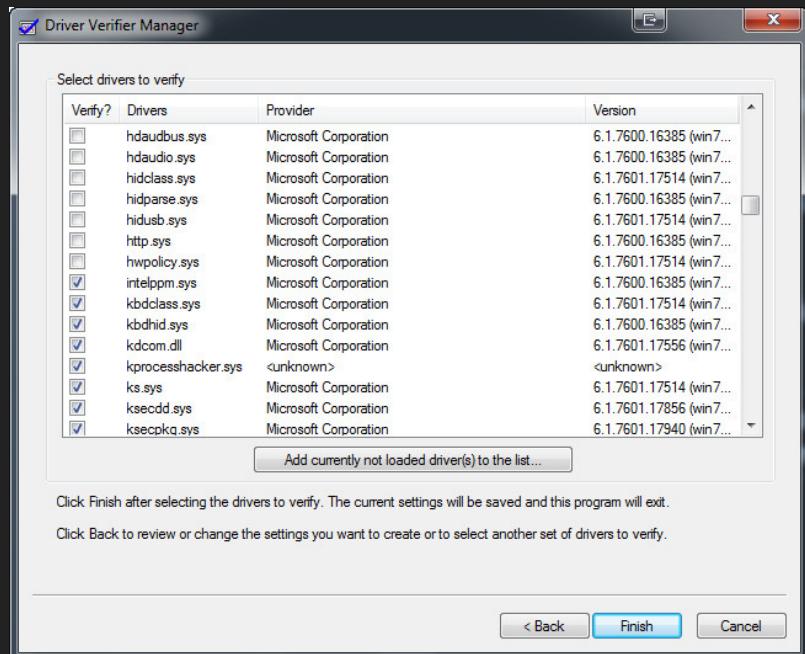
Δεν επιλεγούμε όλους τους drivers:

- Επιβαρύνουμε το σύστημα
- Μειώνουμε την αποδοτικότητα του verifier

BSODs: Troubleshooting

Driver Verifier

Συνταγή επιλογής drivers



Unsigned drivers. Σε x64 συστήματα το πιο πιθανόν είναι να μην βρείτε κανένα τέτοιο

Οι signed drivers δεν είναι απαραίτητα «αθώοι»

Επιλεγούμε μικρές ομάδες drivers,
5-6/έλεγχο

Οι πιο πρόσφατα εγκατεστημένοι drivers
είναι οι πρώτοι υποψήφιοι

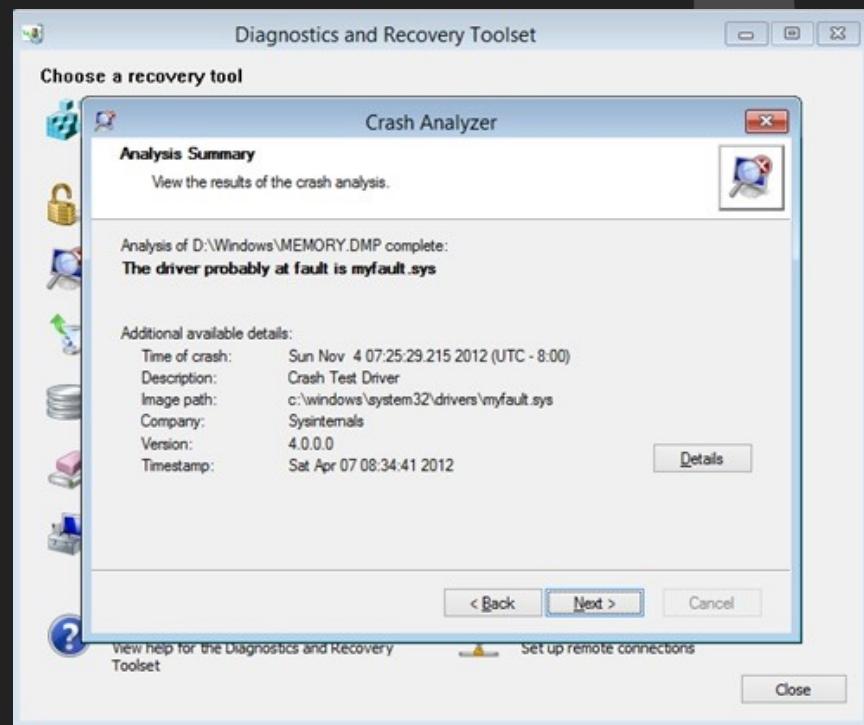
Έως ύστατο μετρό χρησιμοποιείστε ομάδες
10 drivers

BSODs: Troubleshooting Software

Αυτοματοποιημένες λύσεις

[Microsoft Diagnostics and Recovery Toolset \(DaRT\)](#), μέρος του Microsoft Desktop Optimization Pack.

- Χρειάζεται τα debugging tools για να λειτουργήσει
- Χρησιμοποιεί τον symbol server της Microsoft
- Μπορεί να αναλύσει ένα crash dump κάθε φορά
- Το log file θα πρέπει να εξαχθεί χειροκίνητα (copy-paste)
- Η έκδοση 7 είναι σε beta μορφή
- Δεν είναι δωρεάν

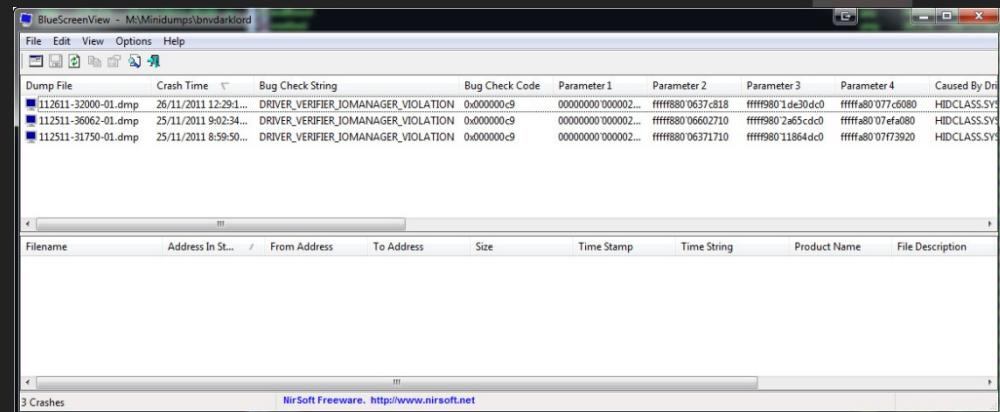


BSODs: Troubleshooting Software

Αυτοματοποιημένες λύσεις

Nirsoft BlueScreenView v1.46

- Κάνει χρήση του Dumpchk.exe, ένα command line πρόγραμμα των Windows, το οποίο ελέγχει την ακεραιότητα των crash dumps
- Δεν χρησιμοποιεί τον Symbol server
- Δεν αναλύει τα dumps όπως κάνει ο Windbg, ο kd, ο cdb, κλπ
- Δυνατότητα επιλογής φακέλου, πέρα του C:\Windows\minidump
- Freeware

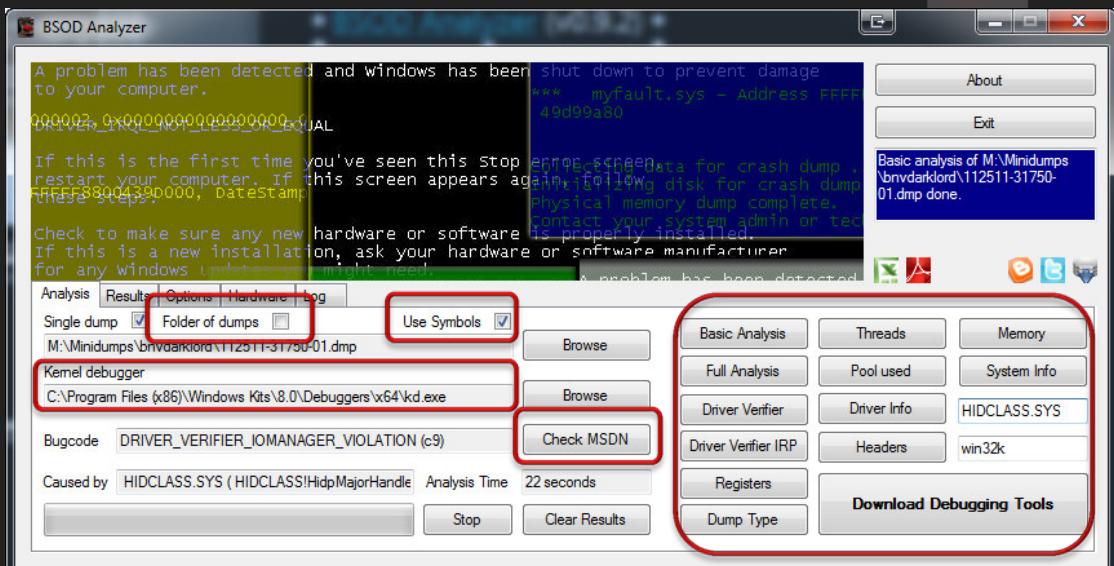


BSODs: Troubleshooting Software

Αυτοματοποιημένες λύσεις

BSOD Analyzer (v0.9.2)

- Χρειάζεται τα debugging tools για να λειτουργήσει
- Χρησιμοποιεί τον Symbol server εάν το επιλέξει ο χρήστης
- Άμεση πρόσβαση στο MSDN για αναζήτηση του stop code
- Δυνατότητα επιλογής φάκελου με crash dumps και αυτόματη ανάλυση αυτών
- Δέκα επιπλέον αυτοματοποιημένες αναλύσεις σε σχέση με το DaRT

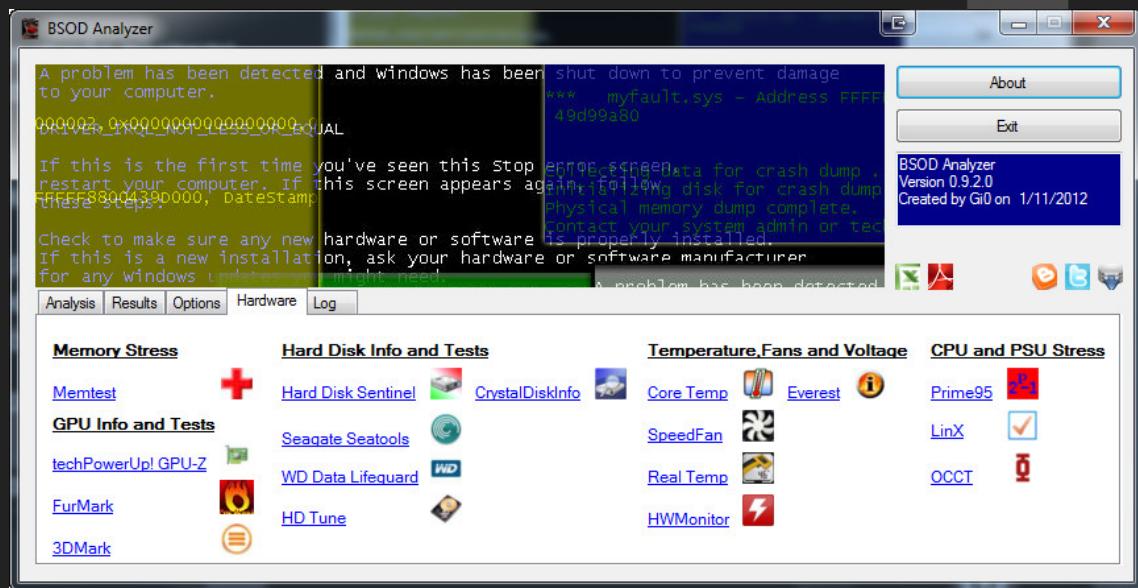


BSODs: Troubleshooting Software

Αυτοματοποιημένες λύσεις

BSOD Analyzer (v0.9.2)

- Συγκεντρωτικός πίνακας αποτελεσμάτων
- Εξαγωγή των αποτελεσμάτων σε xls και pdf
- Άμεση πρόσβαση σε ρυθμίσεις των Windows σχετικά με τις μπλε οθόνες
- Ενεργοποίηση και απενεργοποίηση του Driver verifier για μέχρι 6 drivers
- Links με hardware tests και diagnostics, για κάθε κατηγορία hardware
- Freeware



BSODs: Troubleshooting Software

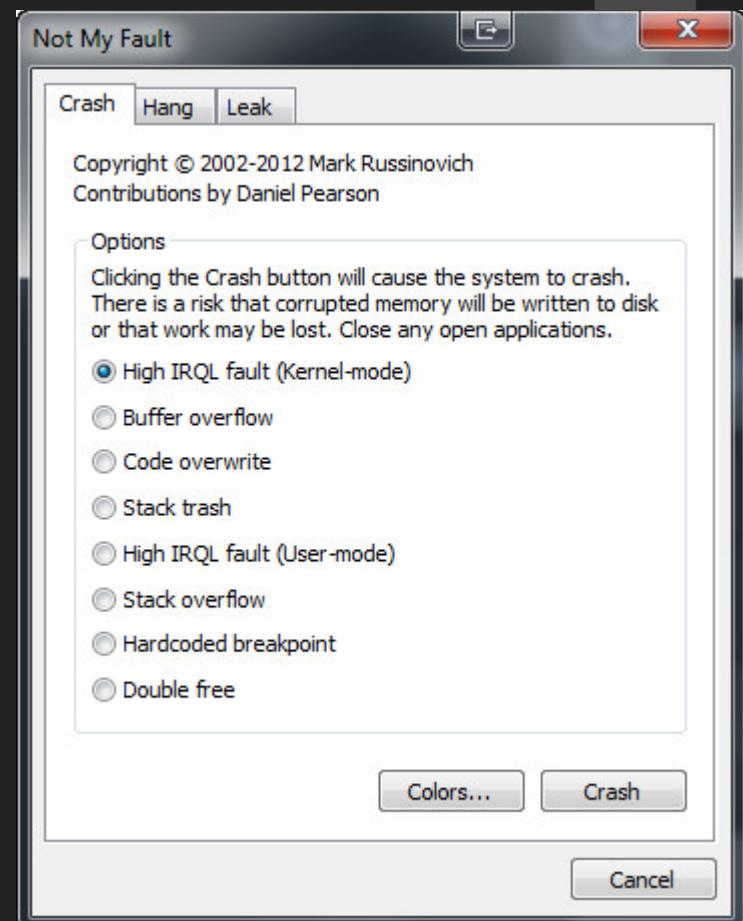
Εξάσκηση / Πειραματισμοί

[Mark Russinovich's Not My Fault](#)

Οκτώ διαφορετικοί τρόποι για να προκαλέσετε
ένα crash

Τρεις τρόποι για να «κολλήσετε» το
σύστημα σας

Memory Leaks



BSODs: Last but not least

- Υπάρχουν crash dumps που παρά τις προσπάθειες μας δεν διαθέτουν αρκετά στοιχειά για να λυθούν
- Ακόμα και αν μια στις πέντε μπλε οθόνες που αντιμετωπίζετε μπορεί να λυθεί με κάποιον από τους προαναφερθείς τρόπους, αξίζει τον κόπο να δοκιμάσετε
- Την επομένη φορά που θα κάνετε reboot μετά από μπλε οθόνη, αφήστε τα Windows να «δώσουν αναφορά» στην Microsoft ☺

Your PC ran into a problem

This problem caused your PC to restart. You can send info to Microsoft about what went wrong to help us improve Windows.

Files that will be sent to Microsoft

C:\Windows\Minidump\111812-23212-01.dmp
C:\Users\Administrator\AppData\Local\Temp\WER-54647-0.sysdata.xml
C:\Windows\MEMORY.DMP

For your convenience, here is the text of the privacy statement for the Microsoft Error Reporting Service. To see the latest version, please visit the online version of this privacy statement at <http://go.microsoft.com/fwlink/?LinkId=190175>.

Privacy Statement for the Microsoft Error Reporting Service

Last updated: June 2011

Microsoft is committed to helping protect your privacy. This statement explains how the Microsoft Error Reporting (MER) service collects information and how the information can be used. This statement does not apply to other online or offline Microsoft websites, software, or services.

Why does Microsoft collect information about errors and problems?

The information helps Microsoft and Microsoft partners diagnose problems in the software you use and provide solutions. Not all problems have solutions but when solutions are available, they are offered as updates to install or steps for solving a problem you've reported. To help prevent problems and make software more reliable, some solutions are also included in service packs and future versions of the software.

How is information collected?

Many third-party and Microsoft software programs, including some Windows operating systems, are designed to work with the MER service. If a problem occurs in one of these software programs, you might be asked if you want to report it. You can view the details of the report before sending it, although some files might not be in a readable format.

Some software also allows you to report problems automatically instead of requesting your consent each time a problem occurs. If you use automatic reporting, you're not prompted to review the information in a report before it is sent. However, no information is collected unless you (or your system or network administrator) choose to report problems. You can choose to stop reporting problems at any time.

Enterprise customers can use the Microsoft System Center Desktop Error Monitoring (<http://go.microsoft.com/fwlink/?LinkId=190175>)

BSODs: References

Vostokov, D. (2008). Memory Dump Analysis Anthology, OpenTask.

Russinovich, M. E. and D. A. Solomon (2009). Windows® Internals, Microsoft Press.

<http://blogs.technet.com/b/jeffa36/archive/2007/04/22/big-invite-may-user-group-meeting.aspx>

<http://blogs.msdn.com/b/ntdebugging/archive/2010/04/02/how-to-use-the-dedicateddumpfile-registry-value-to-overcome-space-limitations-on-the-system-drive-when-capturing-a-system-memory-dump.aspx>

<http://windbg.info/doc/1-common-cmds.html>

<http://gi0.blogspot.gr/search/label/bsod>

<http://support.microsoft.com/kb/244617>

**Thank you,
fill in your evaluation sheets!**

