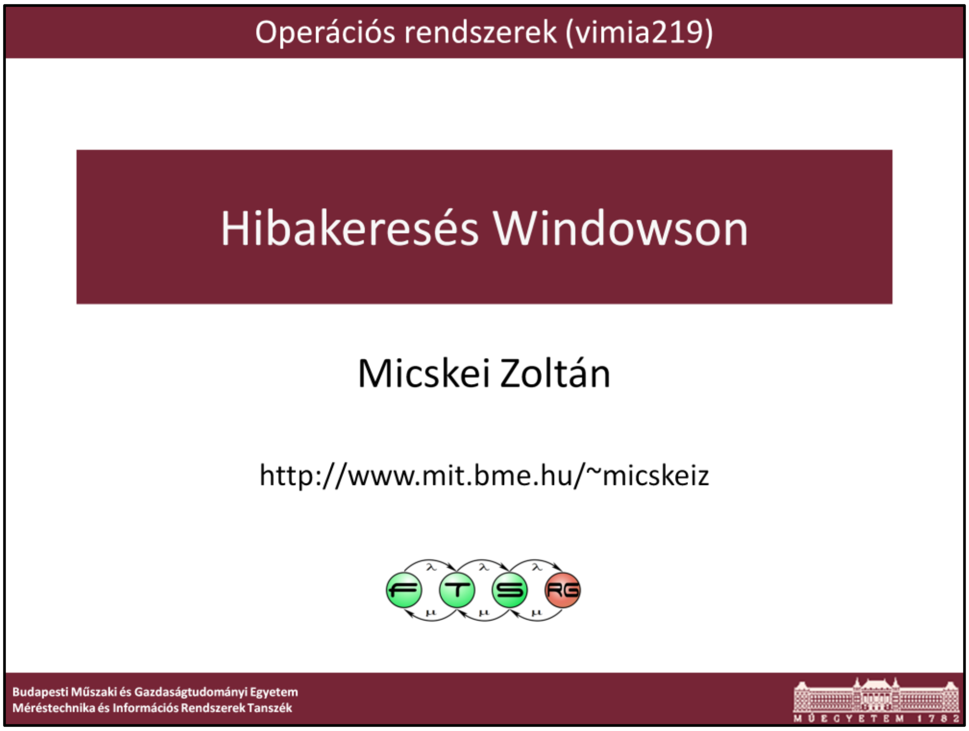


Operációs rendszerek (vimia219)

Hibakeresés Windowson

Micskei Zoltán

http://www.mit.bme.hu/~micskeiz

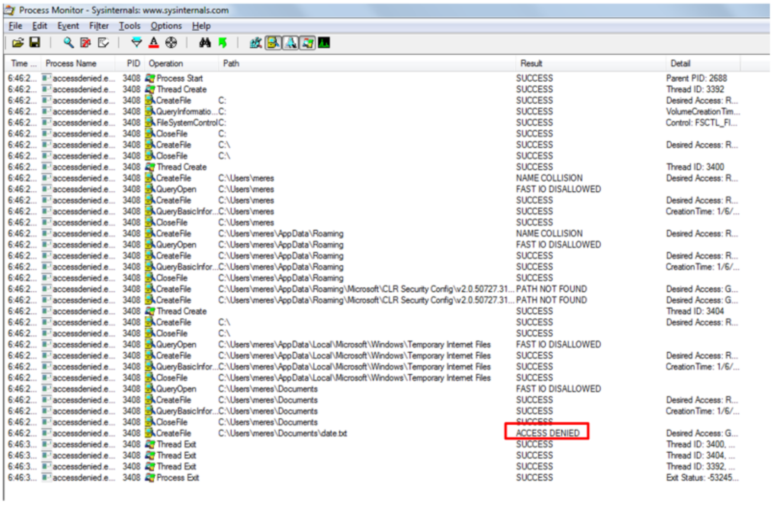
Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

MŰEGYETEM 1782

Utolsó módosítás: 2012. 02. 20.

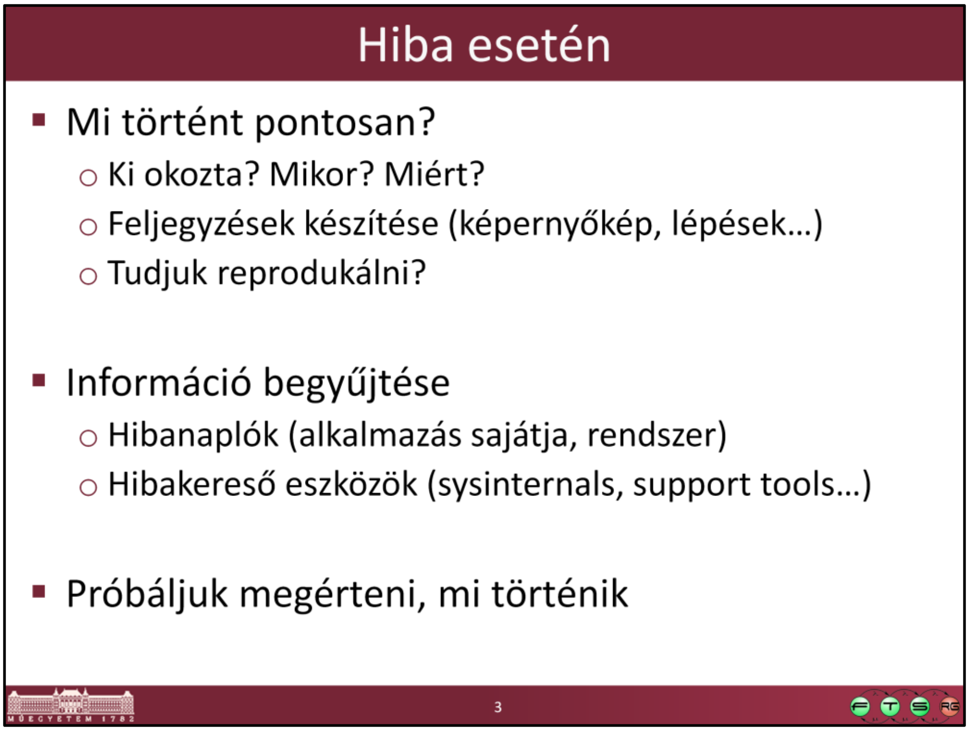
DEMO Hozzáférési hiba megtalálása

- Process Monitor használata:



Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
6:46:2...	accessdenied.e...	3408	Process Start		SUCCESS	Parent PID: 2688
6:46:2...	accessdenied.e...	3408	Thread Create		SUCCESS	Thread ID: 3392
6:46:2...	accessdenied.e...	3408	CreateFile	C:	SUCCESS	Desired Access: R...
6:46:2...	accessdenied.e...	3408	QueryInformatio...	C:	SUCCESS	VolumeCreationTim...
6:46:2...	accessdenied.e...	3408	FileSystemControl	C:	SUCCESS	Control: FSCTL_FI...
6:46:2...	accessdenied.e...	3408	CloseFile	C:	SUCCESS	
6:46:2...	accessdenied.e...	3408	CreateFile	C:\	SUCCESS	Desired Access: R...
6:46:2...	accessdenied.e...	3408	CloseFile	C:\	SUCCESS	
6:46:2...	accessdenied.e...	3408	Thread Create		SUCCESS	Thread ID: 3400
6:46:2...	accessdenied.e...	3408	CreateFile	C:\Users\meres	NAME COLLISION	Desired Access: R...
6:46:2...	accessdenied.e...	3408	QueryOpen	C:\Users\meres	FAST IO DISALLOWED	
6:46:2...	accessdenied.e...	3408	CreateFile	C:\Users\meres	SUCCESS	Desired Access: R...
6:46:2...	accessdenied.e...	3408	QueryBasicInfor...	C:\Users\meres	SUCCESS	CreationTime: 1/6/...
6:46:2...	accessdenied.e...	3408	CloseFile	C:\Users\meres	SUCCESS	
6:46:2...	accessdenied.e...	3408	CreateFile	C:\Users\meres\AppData\Roaming	NAME COLLISION	Desired Access: R...
6:46:2...	accessdenied.e...	3408	QueryOpen	C:\Users\meres\AppData\Roaming	FAST IO DISALLOWED	
6:46:2...	accessdenied.e...	3408	CreateFile	C:\Users\meres\AppData\Roaming	SUCCESS	Desired Access: R...
6:46:2...	accessdenied.e...	3408	QueryBasicInfor...	C:\Users\meres\AppData\Roaming	SUCCESS	CreationTime: 1/6/...
6:46:2...	accessdenied.e...	3408	CloseFile	C:\Users\meres\AppData\Roaming	SUCCESS	
6:46:2...	accessdenied.e...	3408	CreateFile	C:\Users\meres\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.31...	PATH NOT FOUND	Desired Access: G...
6:46:2...	accessdenied.e...	3408	CreateFile	C:\Users\meres\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.31...	PATH NOT FOUND	Desired Access: G...
6:46:2...	accessdenied.e...	3408	Thread Create		SUCCESS	Thread ID: 3404
6:46:2...	accessdenied.e...	3408	CreateFile	C:\	SUCCESS	Desired Access: R...
6:46:2...	accessdenied.e...	3408	CloseFile	C:\	SUCCESS	
6:46:2...	accessdenied.e...	3408	QueryOpen	C:\Users\meres\AppData\Local\Microsoft\Windows\Temporary Internet Files	FAST IO DISALLOWED	
6:46:2...	accessdenied.e...	3408	CreateFile	C:\Users\meres\AppData\Local\Microsoft\Windows\Temporary Internet Files	SUCCESS	Desired Access: R...
6:46:2...	accessdenied.e...	3408	QueryBasicInfor...	C:\Users\meres\AppData\Local\Microsoft\Windows\Temporary Internet Files	SUCCESS	CreationTime: 1/6/...
6:46:2...	accessdenied.e...	3408	CloseFile	C:\Users\meres\AppData\Local\Microsoft\Windows\Temporary Internet Files	SUCCESS	
6:46:2...	accessdenied.e...	3408	QueryOpen	C:\Users\meres\Documents	FAST IO DISALLOWED	
6:46:2...	accessdenied.e...	3408	CreateFile	C:\Users\meres\Documents	SUCCESS	Desired Access: R...
6:46:2...	accessdenied.e...	3408	QueryBasicInfor...	C:\Users\meres\Documents	SUCCESS	CreationTime: 1/6/...
6:46:2...	accessdenied.e...	3408	CloseFile	C:\Users\meres\Documents	SUCCESS	
6:46:2...	accessdenied.e...	3408	CreateFile	C:\Users\meres\Documents\date.txt	ACCESS DENIED	Desired Access: G...
6:46:3...	accessdenied.e...	3408	Thread Exit		SUCCESS	Thread ID: 3400, ...
6:46:3...	accessdenied.e...	3408	Thread Exit		SUCCESS	Thread ID: 3404, ...
6:46:3...	accessdenied.e...	3408	Thread Exit		SUCCESS	Thread ID: 3392, ...
6:46:3...	accessdenied.e...	3408	Process Exit		SUCCESS	Exit Status: -53245...

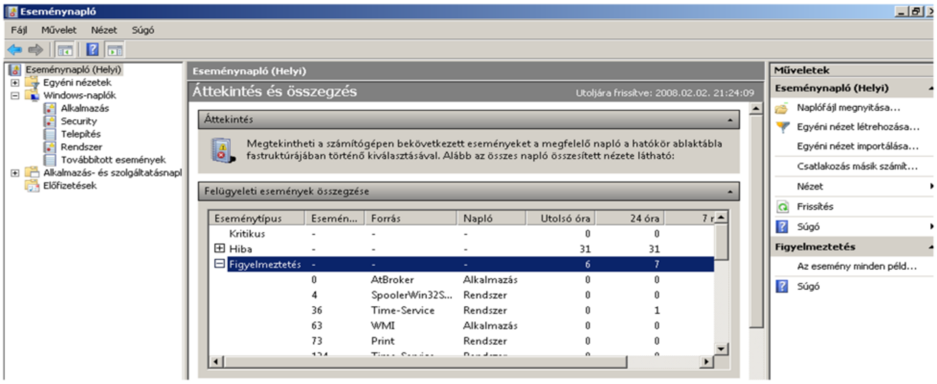


Hiba esetén

- Mi történt pontosan?
  - Ki okozta? Mikor? Miért?
  - Feljegyzések készítése (képernyőkép, lépések…)
  - Tudjuk reprodukálni?
- Információ begyűjtése
  - Hibanaplók (alkalmazás sajátja, rendszer)
  - Hibakereső eszközök (sysinternals, support tools…)
- Próbáljuk megérteni, mi történik

Információ gyűjtés: Eseménynapló

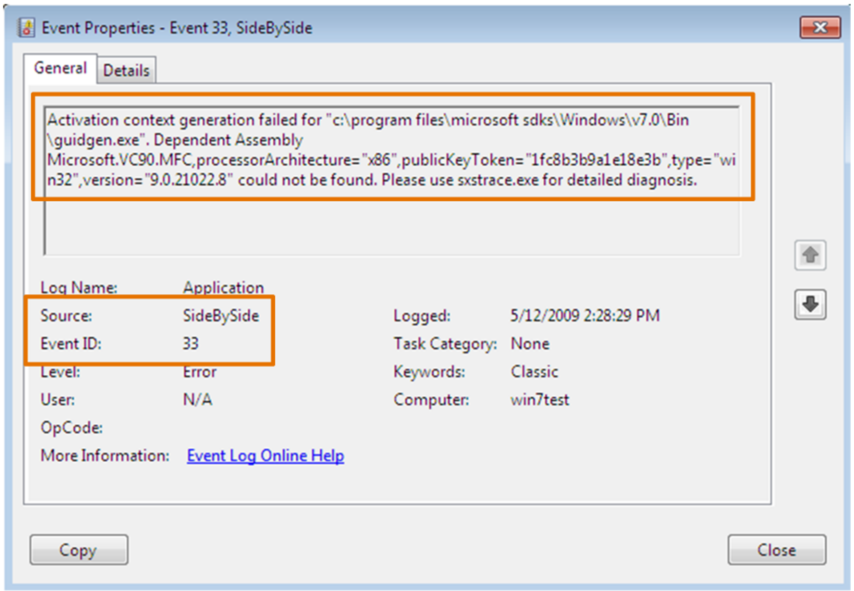
- Eseménynapló megvizsgálása



Megtekintheti a számítógépen bekövetkezett eseményeket a megfelelő napló a hatókör ablaktábla fastruktúrájában történő kiválasztásával. Alább az összes napló összesített nézete látható:

Eseménytípus	Esemén…	Forrás	Napló	Utolsó óra	24 óra	7 r
Kritikus	-	-	-	0	0	
⊞ Hiba	-	-	-	31	31	
⊟ Figyelmeztetés	-	-	-	6	7	
	0	AtBroker	Alkalmazás	0	0	
	4	SpoolerWin32S…	Rendszer	0	0	
	36	Time-Service	Rendszer	0	1	
	63	WMI	Alkalmazás	0	0	
	73	Print	Rendszer	0	0	

Esemény részletei



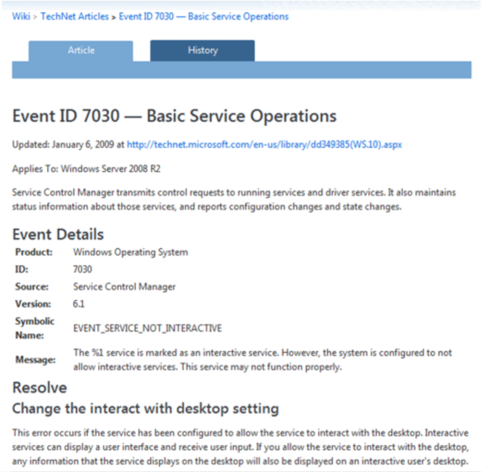
```
Activation context generation failed for "c:\program files\microsoft sdks\Windows\v7.0\Bin
\guidgen.exe". Dependent Assembly
Microsoft.VC90.MFC,processorArchitecture="x86",publicKeyToken="1fc8b3b9a1e18e3b",type="wi
n32",version="9.0.21022.8" could not be found. Please use sxstrace.exe for detailed diagnosis.
```

Log Name:	Application		
Source:	SideBySide	Logged:	5/12/2009 2:28:29 PM
Event ID:	33	Task Category:	None
Level:	Error	Keywords:	Classic
User:	N/A	Computer:	win7test
OpCode:			
More Information:	Event Log Online Help		

Az esemény azonosítása a forrás és az esemény azonosító alapján történhet.

Eventlog Online help

- Keres a forrás + azonosító párosra
- Gyakori hibák esetén megoldás is:



Wiki > TechNet Articles > Event ID 7030 — Basic Service Operations
Article
History

Event ID 7030 — Basic Service Operations

Updated: January 6, 2009 at http://technet.microsoft.com/en-us/library/dd349385(WS.10).aspx

Applies To: Windows Server 2008 R2

Service Control Manager transmits control requests to running services and driver services. It also maintains status information about those services, and reports configuration changes and state changes.

Event Details

Product:	Windows Operating System
ID:	7030
Source:	Service Control Manager
Version:	6.1
Symbolic Name:	EVENT_SERVICE_NOT_INTERACTIVE
Message:	The %1 service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.

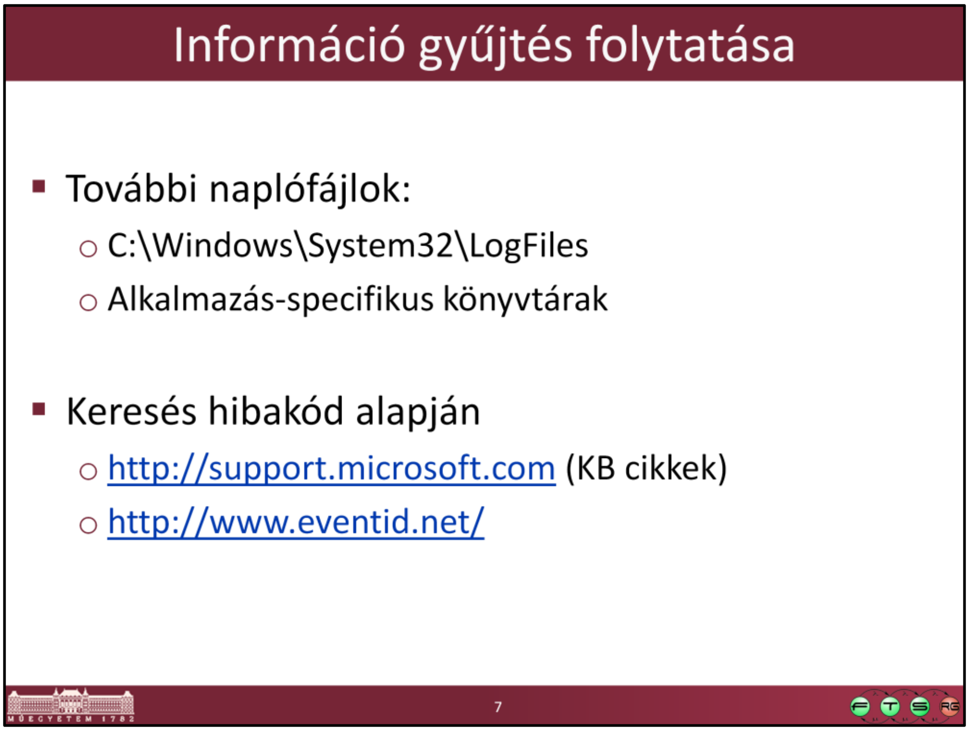
Resolve

Change the interact with desktop setting

This error occurs if the service has been configured to allow the service to interact with the desktop. Interactive services can display a user interface and receive user input. If you allow the service to interact with the desktop, any information that the service displays on the desktop will also be displayed on an interactive user's desktop.

DEMO

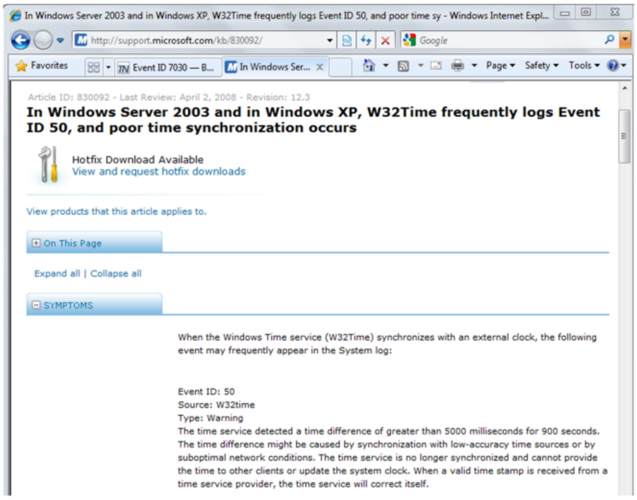
Forrás: http://social.technet.microsoft.com/wiki/contents/articles/event-id-7030-basic-service-operations.aspx



Információ gyűjtés folytatása

- További naplófájlok:
  - C:\Windows\System32\LogFiles
  - Alkalmazás-specifikus könyvtárak
- Keresés hibakód alapján
  - http://support.microsoft.com (KB cikkek)
  - http://www.eventid.net/

MS Knowledge Base cikkek


In Windows Server 2003 and in Windows XP, W32Time frequently logs Event ID 50, and poor time sy - Windows Internet Expl...
http://support.microsoft.com/kb/830092/
Google
Favorites
Event ID 7030 — B...
In Windows Ser...
Page
Safety
Tools

Article ID: 830092 - Last Review: April 2, 2008 - Revision: 12.3

In Windows Server 2003 and in Windows XP, W32Time frequently logs Event ID 50, and poor time synchronization occurs

Hotfix Download Available
View and request hotfix downloads

View products that this article applies to.

⊞ On This Page

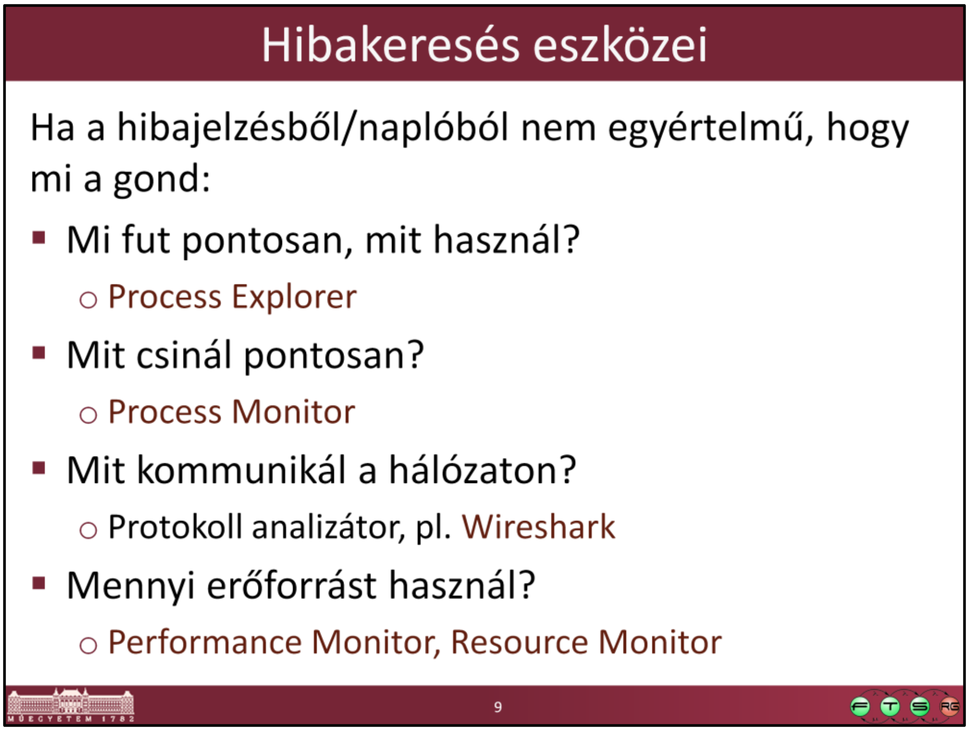
Expand all | Collapse all

⊟ SYMPTOMS

When the Windows Time service (W32Time) synchronizes with an external clock, the following event may frequently appear in the System log:

```
Event ID: 50
Source: W32time
Type: Warning
The time service detected a time difference of greater than 5000 milliseconds for 900 seconds.
The time difference might be caused by synchronization with low-accuracy time sources or by
suboptimal network conditions. The time service is no longer synchronized and cannot provide
the time to other clients or update the system clock. When a valid time stamp is received from a
time service provider, the time service will correct itself.
```

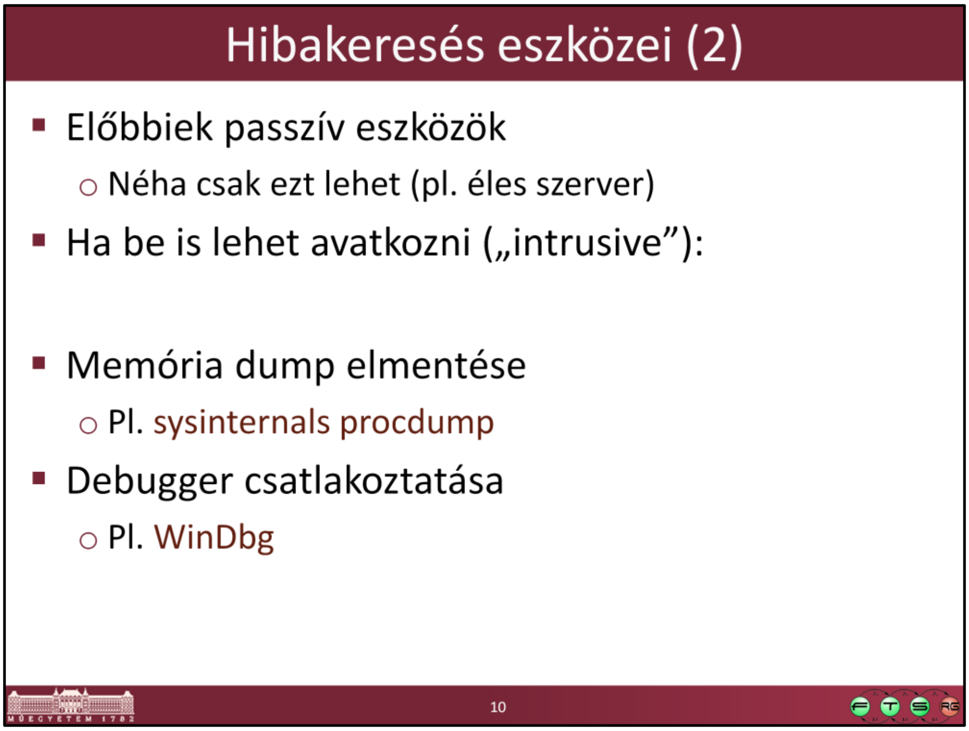
- Hibajelenség
- Megoldások:
  - Hotfix
  - Workaround
  - Ismert hiba
  - …



Hibakeresés eszközei

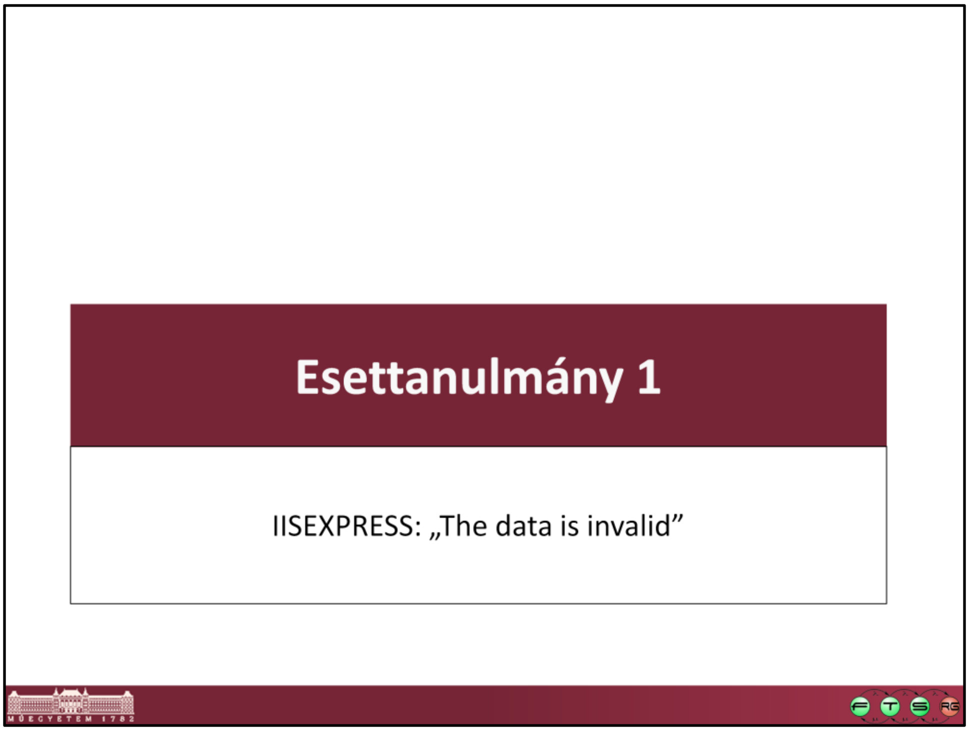
Ha a hibajelzésből/naplóból nem egyértelmű, hogy mi a gond:

- Mi fut pontosan, mit használ?
  - Process Explorer
- Mit csinál pontosan?
  - Process Monitor
- Mit kommunikál a hálózaton?
  - Protokoll analizátor, pl. Wireshark
- Mennyi erőforrást használ?
  - Performance Monitor, Resource Monitor



Hibakeresés eszközei (2)

- Előbbiek passzív eszközök
  - Néha csak ezt lehet (pl. éles szerver)
- Ha be is lehet avatkozni („intrusive”):
- Memória dump elmentése
  - Pl. sysinternals procdump
- Debugger csatlakoztatása
  - Pl. WinDbg



Esettanulmány 1

IISEXPRESS: „The data is invalid”

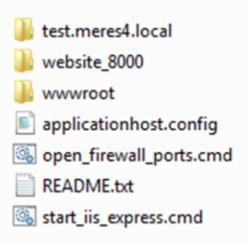
IIS Express

- IIS Express: web szerver fejlesztői változata

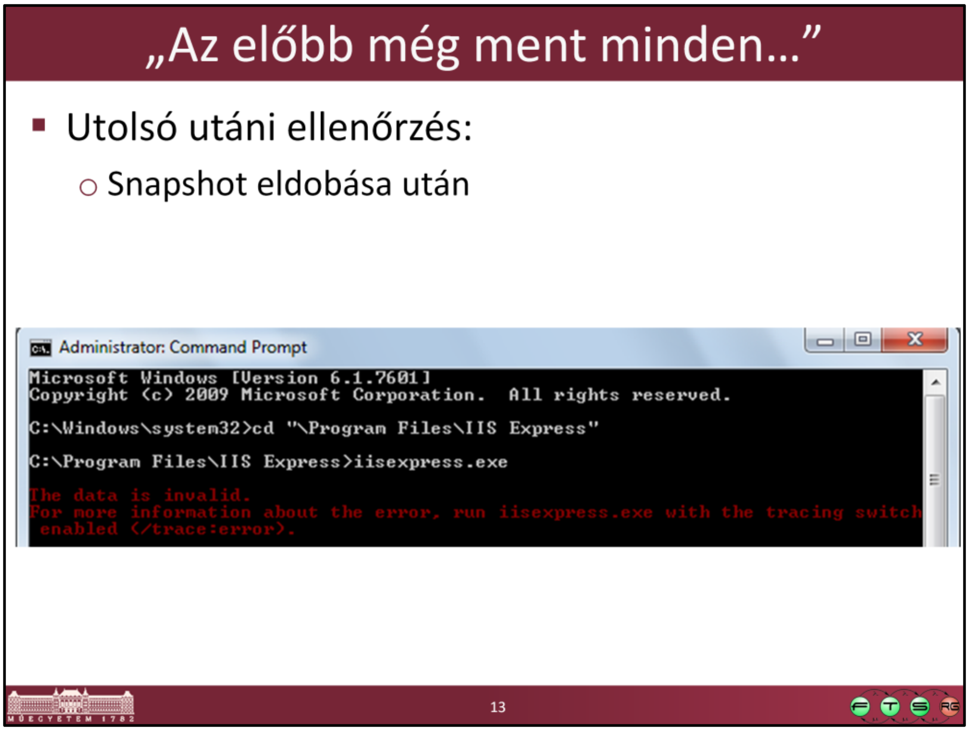
IIS7
internet information services

- Mérés labor 4:
  - Példa webszerver HTTP kérésekhez
  - Windows 7 virtuális gépben

- Félévkezdés előtt: minden megy a
  - saját gépemen,
  - végleges környezetben is



```
test.meres4.local
website_8000
wwwroot
applicationhost.config
open_firewall_ports.cmd
README.txt
start_iis_express.cmd
```

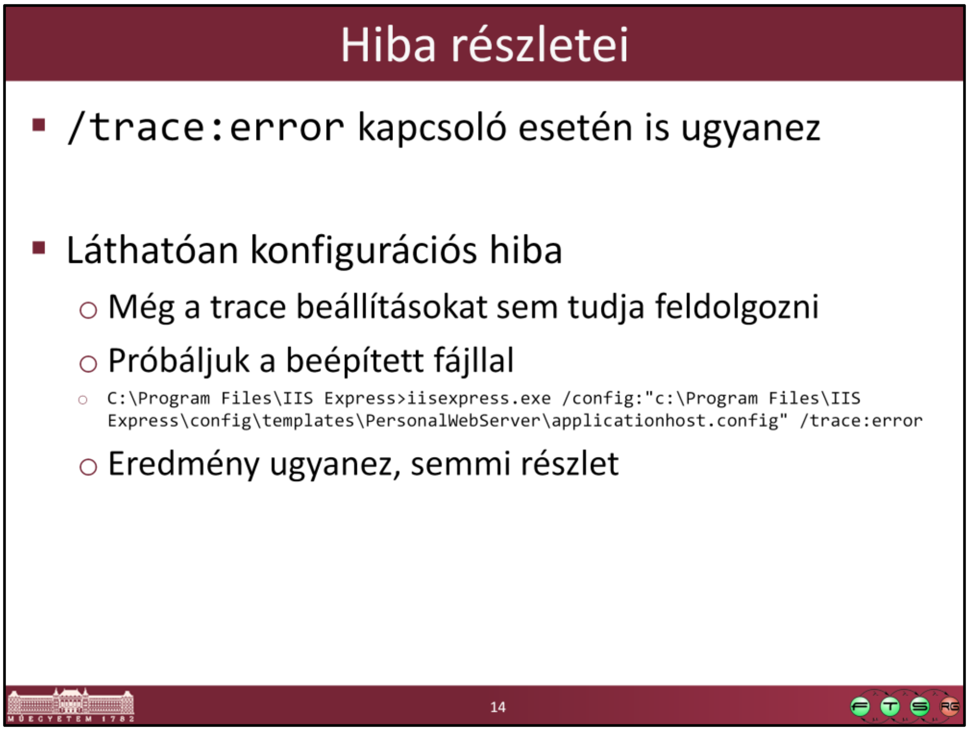


„Az előbb még ment minden…”

- Utolsó utáni ellenőrzés:
  - Snapshot eldobása után

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd "\Program Files\IIS Express"

C:\Program Files\IIS Express>iisexpress.exe

The data is invalid.
For more information about the error, run iisexpress.exe with the tracing switch
 enabled (/trace:error).
```

C:\Program Files\IIS Express>iisexpress.exe
The data is invalid.For more information about the error, run iisexpress.exe with the tracing switch enabled (/trace:error).



Hiba részletei

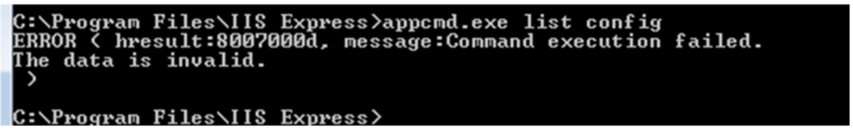
- `/trace:error` kapcsoló esetén is ugyanez

- Láthatóan konfigurációs hiba
  - Még a trace beállításokat sem tudja feldolgozni
  - Próbáljuk a beépített fájllal

  -
    ```
    C:\Program Files\IIS Express>iisexpress.exe /config:"c:\Program Files\IIS Express\config\templates\PersonalWebServer\applicationhost.config" /trace:error
    ```
  - Eredmény ugyanez, semmi részlet

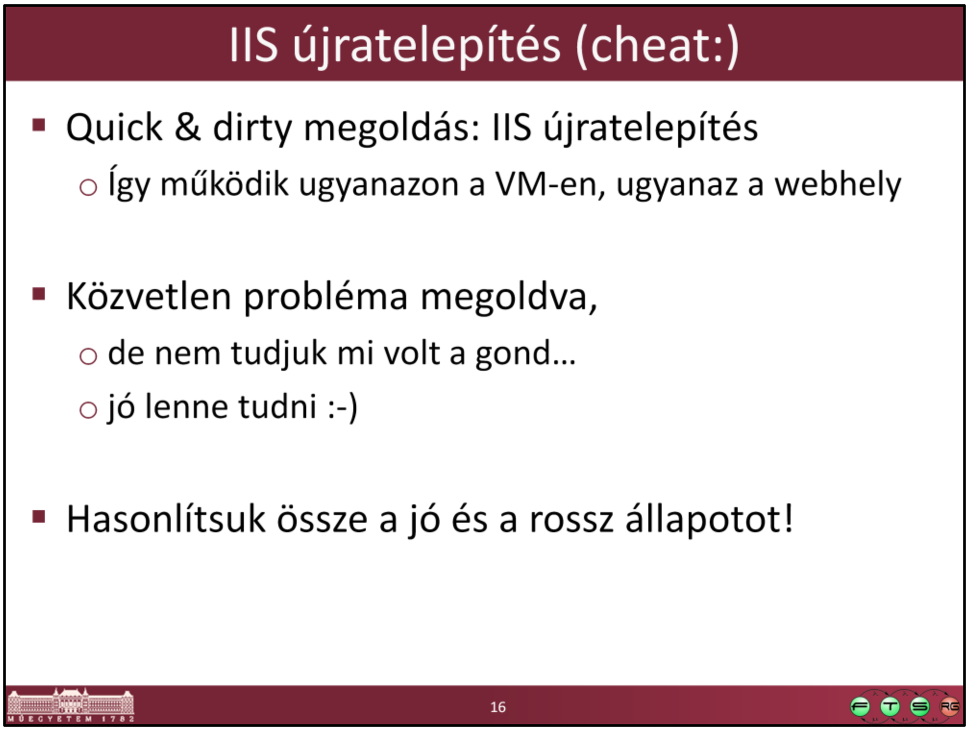
Hiba részletei (2)

- Kimerítő keresés az indítási módok között
  - `iisexpress.exe`-nek nem maradt több kapcsolója
- `appcmd.exe`: parancssori felület



```
C:\Program Files\IIS Express>appcmd.exe list config
ERROR ( hresult:8007000d, message:Command execution failed.
The data is invalid.
 )

C:\Program Files\IIS Express>
```

- Végre van egy hibakódunk!
  - gg: 8007000d → főleg Windows Update hibák
  - gg: 8007000d iis → web.config hiba, nem telepített modulok | nálunk ez nem lehet, hisz ez a config eddig ment



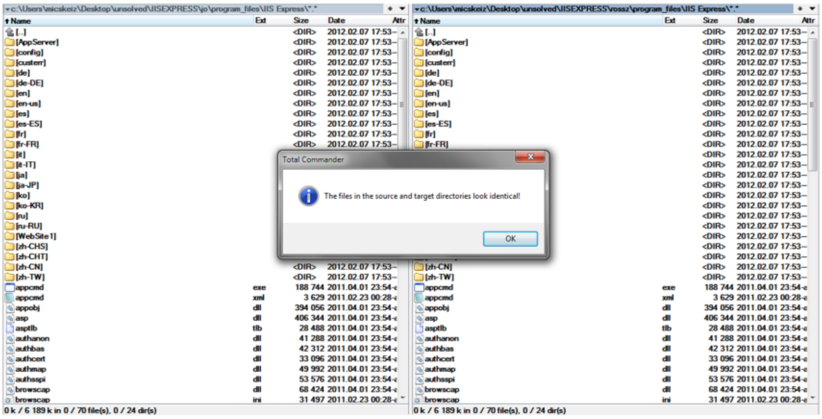
IIS újratelepítés (cheat:)

- Quick & dirty megoldás: IIS újratelepítés
  - Így működik ugyanazon a VM-en, ugyanaz a webhely
- Közvetlen probléma megoldva,
  - de nem tudjuk mi volt a gond…
  - jó lenne tudni :-)
- Hasonlítsuk össze a jó és a rossz állapotot!

Fájlok összehasonlítása

Fájlok megegyeznek:

- ○ C:\program files\iis express; Documents\IISExpress; C:\inetpub; .NET FW\config

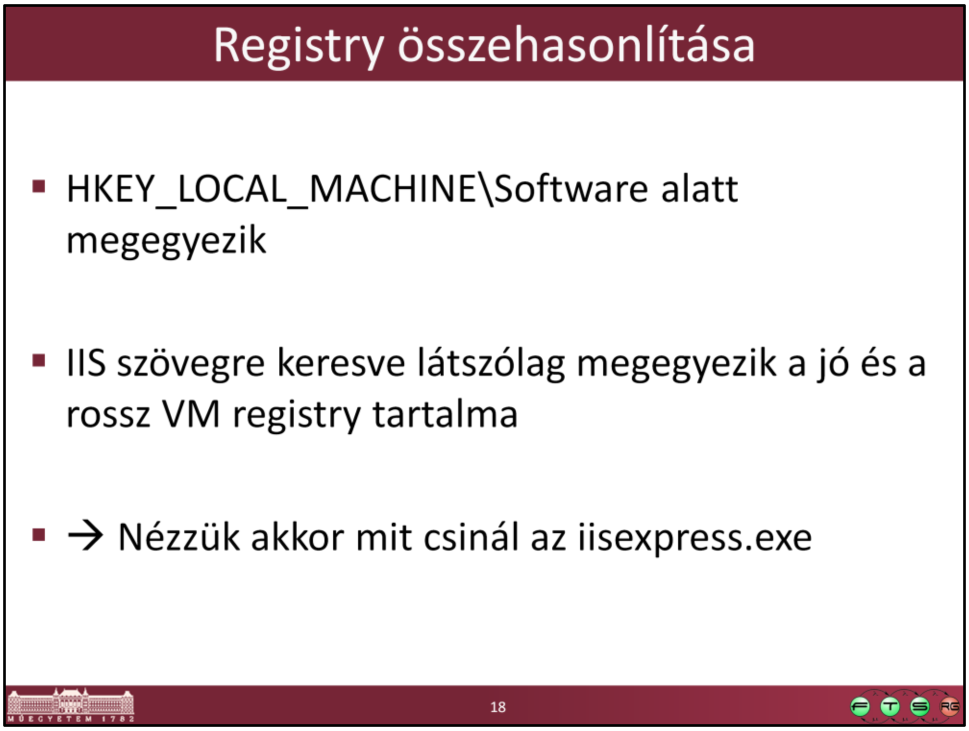


```
c:\Users\micskeiz\Desktop\unsolved\IISEXPRESS\jo\program_files\IIS Express\*.*
Name                Ext    Size      Date              Attr
[..]                       <DIR>     2012.02.07 17:53—
[AppServer]                <DIR>     2012.02.07 17:53—
[config]                   <DIR>     2012.02.07 17:53—
[custerr]                  <DIR>     2012.02.07 17:53—
[de]                       <DIR>     2012.02.07 17:53—
[de-DE]                    <DIR>     2012.02.07 17:53—
[en]                       <DIR>     2012.02.07 17:53—
[en-us]                    <DIR>     2012.02.07 17:53—
[es]                       <DIR>     2012.02.07 17:53—
[es-ES]                    <DIR>     2012.02.07 17:53—
[fr]                       <DIR>     2012.02.07 17:53—
[fr-FR]                    <DIR>     2012.02.07 17:53—
[it]
[it-IT]
[ja]
[ja-JP]
[ko]
[ko-KR]
[ru]
[ru-RU]
[WebSite1]
[zh-CHS]
[zh-CHT]
[zh-CN]                    <DIR>     2012.02.07 17:53—
[zh-TW]                    <DIR>     2012.02.07 17:53—
appcmd              exe    188 744   2011.04.01 23:54-a
appcmd              xml      3 629   2011.02.23 00:28-a
appobj              dll    394 056   2011.04.01 23:54-a
asp                 dll    406 344   2011.04.01 23:54-a
asptlb              tlb     28 488   2011.04.01 23:54-a
authanon            dll     41 288   2011.04.01 23:54-a
authbas             dll     42 312   2011.04.01 23:54-a
authcert            dll     33 096   2011.04.01 23:54-a
authmap             dll     49 992   2011.04.01 23:54-a
authsspi            dll     53 576   2011.04.01 23:54-a
browscap            dll     68 424   2011.04.01 23:54-a
browscap            ini     31 497   2011.02.23 00:28-a
0 k / 6 189 k in 0 / 70 file(s), 0 / 24 dir(s)
```

```
c:\Users\micskeiz\Desktop\unsolved\IISEXPRESS\rossz\program_files\IIS Express\*.*
Name                Ext    Size      Date              Attr
[..]                       <DIR>     2012.02.07 17:53—
[AppServer]                <DIR>     2012.02.07 17:53—
[config]                   <DIR>     2012.02.07 17:53—
[custerr]                  <DIR>     2012.02.07 17:53—
[de]                       <DIR>     2012.02.07 17:53—
[de-DE]                    <DIR>     2012.02.07 17:53—
[en]                       <DIR>     2012.02.07 17:53—
[en-us]                    <DIR>     2012.02.07 17:53—
[es]                       <DIR>     2012.02.07 17:53—
[es-ES]                    <DIR>     2012.02.07 17:53—
[fr]                       <DIR>     2012.02.07 17:53—
[fr-FR]                    <DIR>     2012.02.07 17:53—
                           <DIR>     2012.02.07 17:53—
                           <DIR>     2012.02.07 17:53—
                           <DIR>     2012.02.07 17:53—
                           <DIR>     2012.02.07 17:53—
                           <DIR>     2012.02.07 17:53—
                           <DIR>     2012.02.07 17:53—
                           <DIR>     2012.02.07 17:53—
                           <DIR>     2012.02.07 17:53—
                           <DIR>     2012.02.07 17:53—
                           <DIR>     2012.02.07 17:53—
                           <DIR>     2012.02.07 17:53—
[zh-CN]                    <DIR>     2012.02.07 17:53—
[zh-TW]                    <DIR>     2012.02.07 17:53—
appcmd              exe    188 744   2011.04.01 23:54-a
appcmd              xml      3 629   2011.02.23 00:28-a
appobj              dll    394 056   2011.04.01 23:54-a
asp                 dll    406 344   2011.04.01 23:54-a
asptlb              tlb     28 488   2011.04.01 23:54-a
authanon            dll     41 288   2011.04.01 23:54-a
authbas             dll     42 312   2011.04.01 23:54-a
authcert            dll     33 096   2011.04.01 23:54-a
authmap             dll     49 992   2011.04.01 23:54-a
authsspi            dll     53 576   2011.04.01 23:54-a
browscap            dll     68 424   2011.04.01 23:54-a
browscap            ini     31 497   2011.02.23 00:28-a
0 k / 6 189 k in 0 / 70 file(s), 0 / 24 dir(s)
```

Total Commander

The files in the source and target directories look identical!

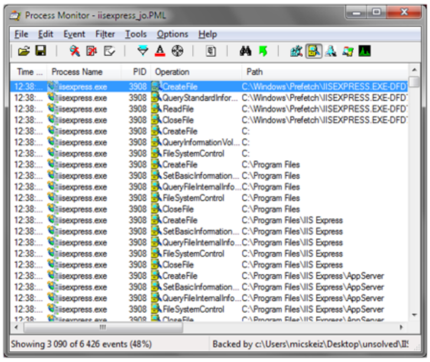


Registry összehasonlítása

- HKEY_LOCAL_MACHINE\Software alatt megegyezik
- IIS szövegre keresve látszólag megegyezik a jó és a rossz VM registry tartalma
- → Nézzük akkor mit csinál az iisexpress.exe

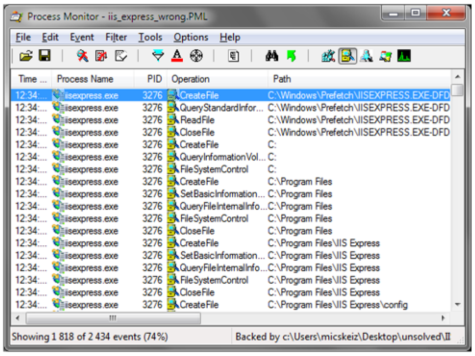
Futások összehasonlítása

- Fájl, registry kérések elkapása (Process Monitor)
- Események: 3090 (jó) vs. 1818 (rossz)



Time ...	Process Name	PID	Operation	Path
12:38:...	iisexpress.exe	3908	CreateFile	C:\Windows\Prefetch\IISEXPRESS.EXE-DFD
12:38:...	iisexpress.exe	3908	QueryStandardInfor...	C:\Windows\Prefetch\IISEXPRESS.EXE-DFD
12:38:...	iisexpress.exe	3908	ReadFile	C:\Windows\Prefetch\IISEXPRESS.EXE-DFD
12:38:...	iisexpress.exe	3908	CloseFile	C:\Windows\Prefetch\IISEXPRESS.EXE-DFD
12:38:...	iisexpress.exe	3908	CreateFile	C:
12:38:...	iisexpress.exe	3908	QueryInformationVol...	C:
12:38:...	iisexpress.exe	3908	FileSystemControl	C:
12:38:...	iisexpress.exe	3908	CreateFile	C:\Program Files
12:38:...	iisexpress.exe	3908	SetBasicInformation...	C:\Program Files
12:38:...	iisexpress.exe	3908	QueryFileInternalInfo...	C:\Program Files
12:38:...	iisexpress.exe	3908	FileSystemControl	C:\Program Files
12:38:...	iisexpress.exe	3908	CloseFile	C:\Program Files
12:38:...	iisexpress.exe	3908	CreateFile	C:\Program Files\IIS Express
12:38:...	iisexpress.exe	3908	SetBasicInformation...	C:\Program Files\IIS Express
12:38:...	iisexpress.exe	3908	QueryFileInternalInfo...	C:\Program Files\IIS Express
12:38:...	iisexpress.exe	3908	FileSystemControl	C:\Program Files\IIS Express
12:38:...	iisexpress.exe	3908	CloseFile	C:\Program Files\IIS Express
12:38:...	iisexpress.exe	3908	CreateFile	C:\Program Files\IIS Express\AppServer
12:38:...	iisexpress.exe	3908	SetBasicInformation...	C:\Program Files\IIS Express\AppServer
12:38:...	iisexpress.exe	3908	QueryFileInternalInfo...	C:\Program Files\IIS Express\AppServer
12:38:...	iisexpress.exe	3908	FileSystemControl	C:\Program Files\IIS Express\AppServer
12:38:...	iisexpress.exe	3908	CloseFile	C:\Program Files\IIS Express\AppServer

Showing 3 090 of 6 426 events (48%) Backed by c:\Users\micskeiz\Desktop\unsolved\II!



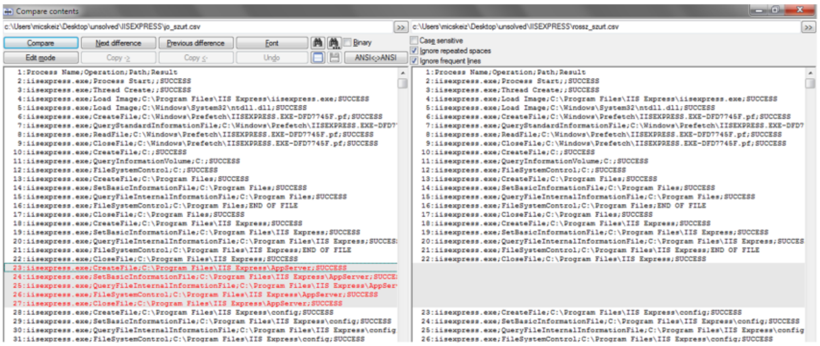
Time ...	Process Name	PID	Operation	Path
12:34:...	iisexpress.exe	3276	CreateFile	C:\Windows\Prefetch\IISEXPRESS.EXE-DFD
12:34:...	iisexpress.exe	3276	QueryStandardInfor...	C:\Windows\Prefetch\IISEXPRESS.EXE-DFD
12:34:...	iisexpress.exe	3276	ReadFile	C:\Windows\Prefetch\IISEXPRESS.EXE-DFD
12:34:...	iisexpress.exe	3276	CloseFile	C:\Windows\Prefetch\IISEXPRESS.EXE-DFD
12:34:...	iisexpress.exe	3276	CreateFile	C:
12:34:...	iisexpress.exe	3276	QueryInformationVol...	C:
12:34:...	iisexpress.exe	3276	FileSystemControl	C:
12:34:...	iisexpress.exe	3276	CreateFile	C:\Program Files
12:34:...	iisexpress.exe	3276	SetBasicInformation...	C:\Program Files
12:34:...	iisexpress.exe	3276	QueryFileInternalInfo...	C:\Program Files
12:34:...	iisexpress.exe	3276	FileSystemControl	C:\Program Files
12:34:...	iisexpress.exe	3276	CloseFile	C:\Program Files
12:34:...	iisexpress.exe	3276	CreateFile	C:\Program Files\IIS Express
12:34:...	iisexpress.exe	3276	SetBasicInformation...	C:\Program Files\IIS Express
12:34:...	iisexpress.exe	3276	QueryFileInternalInfo...	C:\Program Files\IIS Express
12:34:...	iisexpress.exe	3276	FileSystemControl	C:\Program Files\IIS Express
12:34:...	iisexpress.exe	3276	CloseFile	C:\Program Files\IIS Express
12:34:...	iisexpress.exe	3276	CreateFile	C:\Program Files\IIS Express\config

Showing 1 818 of 2 434 events (74%) Backed by c:\Users\micskeiz\Desktop\unsolved\II

- Nehéz meglátni a különbséget

Futások összehasonlítása (2)

- Futás exportálása CSV-be
- Operation, Path, Result mezők megtartása



c:\Users\micskeiz\Desktop\unsolved\IISEXPRESS\jo_szurt.csv

c:\Users\micskeiz\Desktop\unsolved\IISEXPRESS\rossz_szurt.csv

□ Binary

□ Case sensitive

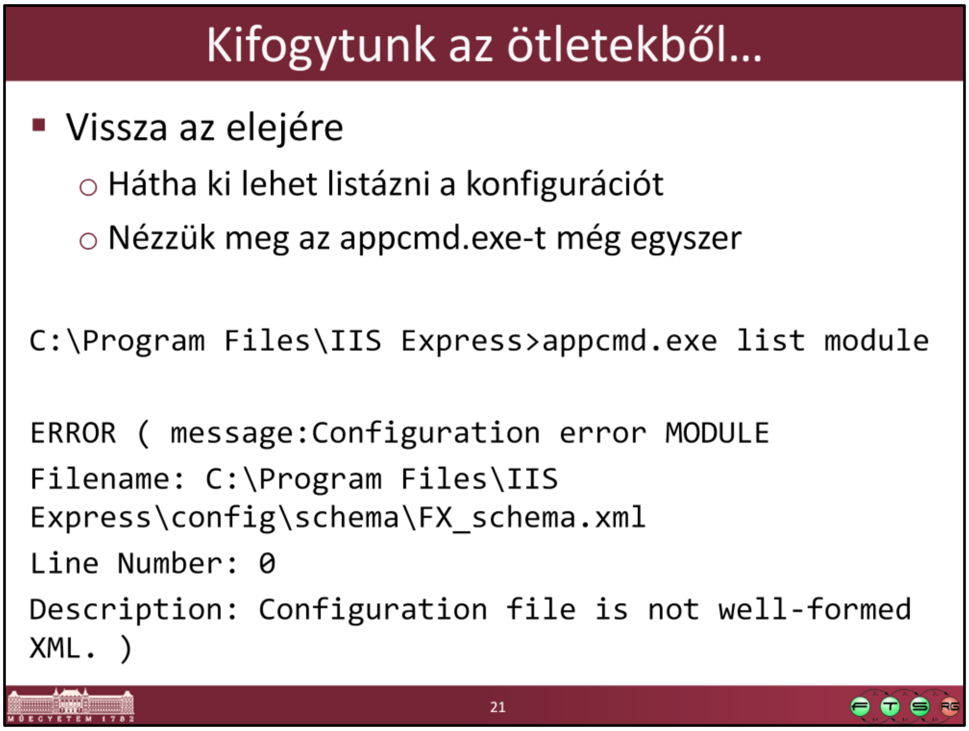
☑ Ignore repeated spaces

☑ Ignore frequent lines

```
 1:Process Name;Operation;Path;Result
 2:iisexpress.exe;Process Start;;SUCCESS
 3:iisexpress.exe;Thread Create;;SUCCESS
 4:iisexpress.exe;Load Image;C:\Program Files\IIS Express\iisexpress.exe;SUCCESS
 5:iisexpress.exe;Load Image;C:\Windows\System32\ntdll.dll;SUCCESS
 6:iisexpress.exe;CreateFile;C:\Windows\Prefetch\IISEXPRESS.EXE-DFD7745F.pf;SUCCESS
 7:iisexpress.exe;QueryStandardInformationFile;C:\Windows\Prefetch\IISEXPRESS.EXE-DFD7
 8:iisexpress.exe;ReadFile;C:\Windows\Prefetch\IISEXPRESS.EXE-DFD7745F.pf;SUCCESS
 9:iisexpress.exe;CloseFile;C:\Windows\Prefetch\IISEXPRESS.EXE-DFD7745F.pf;SUCCESS
10:iisexpress.exe;CreateFile;C:;SUCCESS
11:iisexpress.exe;QueryInformationVolume;C:;SUCCESS
12:iisexpress.exe;FileSystemControl;C:;SUCCESS
13:iisexpress.exe;CreateFile;C:\Program Files;SUCCESS
14:iisexpress.exe;SetBasicInformationFile;C:\Program Files;SUCCESS
15:iisexpress.exe;QueryFileInternalInformationFile;C:\Program Files;SUCCESS
16:iisexpress.exe;FileSystemControl;C:\Program Files;END OF FILE
17:iisexpress.exe;CloseFile;C:\Program Files;SUCCESS
18:iisexpress.exe;CreateFile;C:\Program Files\IIS Express;SUCCESS
19:iisexpress.exe;SetBasicInformationFile;C:\Program Files\IIS Express;SUCCESS
20:iisexpress.exe;QueryFileInternalInformationFile;C:\Program Files\IIS Express;SUCCES
21:iisexpress.exe;FileSystemControl;C:\Program Files\IIS Express;END OF FILE
22:iisexpress.exe;CloseFile;C:\Program Files\IIS Express;SUCCESS
23:iisexpress.exe;CreateFile;C:\Program Files\IIS Express\AppServer;SUCCESS
24:iisexpress.exe;SetBasicInformationFile;C:\Program Files\IIS Express\AppServer;SUCCE
25:iisexpress.exe;QueryFileInternalInformationFile;C:\Program Files\IIS Express\AppSer
26:iisexpress.exe;FileSystemControl;C:\Program Files\IIS Express\AppServer;SUCCESS
27:iisexpress.exe;CloseFile;C:\Program Files\IIS Express\AppServer;SUCCESS
28:iisexpress.exe;CreateFile;C:\Program Files\IIS Express\config;SUCCESS
29:iisexpress.exe;SetBasicInformationFile;C:\Program Files\IIS Express\config;SUCCESS
30:iisexpress.exe;QueryFileInternalInformationFile;C:\Program Files\IIS Express\config
31:iisexpress.exe;FileSystemControl;C:\Program Files\IIS Express\config;SUCCESS
```

```
 1:Process Name;Operation;Path;Result
 2:iisexpress.exe;Process Start;;SUCCESS
 3:iisexpress.exe;Thread Create;;SUCCESS
 4:iisexpress.exe;Load Image;C:\Program Files\IIS Express\iisexpress.exe;SUCCESS
 5:iisexpress.exe;Load Image;C:\Windows\System32\ntdll.dll;SUCCESS
 6:iisexpress.exe;CreateFile;C:\Windows\Prefetch\IISEXPRESS.EXE-DFD7745F.pf;SUCCESS
 7:iisexpress.exe;QueryStandardInformationFile;C:\Windows\Prefetch\IISEXPRESS.EXE-DFD7
 8:iisexpress.exe;ReadFile;C:\Windows\Prefetch\IISEXPRESS.EXE-DFD7745F.pf;SUCCESS
 9:iisexpress.exe;CloseFile;C:\Windows\Prefetch\IISEXPRESS.EXE-DFD7745F.pf;SUCCESS
10:iisexpress.exe;CreateFile;C:;SUCCESS
11:iisexpress.exe;QueryInformationVolume;C:;SUCCESS
12:iisexpress.exe;FileSystemControl;C:;SUCCESS
13:iisexpress.exe;CreateFile;C:\Program Files;SUCCESS
14:iisexpress.exe;SetBasicInformationFile;C:\Program Files;SUCCESS
15:iisexpress.exe;QueryFileInternalInformationFile;C:\Program Files;SUCCESS
16:iisexpress.exe;FileSystemControl;C:\Program Files;END OF FILE
17:iisexpress.exe;CloseFile;C:\Program Files;SUCCESS
18:iisexpress.exe;CreateFile;C:\Program Files\IIS Express;SUCCESS
19:iisexpress.exe;SetBasicInformationFile;C:\Program Files\IIS Express;SUCCESS
20:iisexpress.exe;QueryFileInternalInformationFile;C:\Program Files\IIS Express;SUCCES
21:iisexpress.exe;FileSystemControl;C:\Program Files\IIS Express;END OF FILE
22:iisexpress.exe;CloseFile;C:\Program Files\IIS Express;SUCCESS





23:iisexpress.exe;CreateFile;C:\Program Files\IIS Express\config;SUCCESS
24:iisexpress.exe;SetBasicInformationFile;C:\Program Files\IIS Express\config;SUCCESS
25:iisexpress.exe;QueryFileInternalInformationFile;C:\Program Files\IIS Express\config
26:iisexpress.exe;FileSystemControl;C:\Program Files\IIS Express\config;SUCCESS
```

- 59 helyen különbözik, látszólag ugyanolyan visszatérési érték után tér el



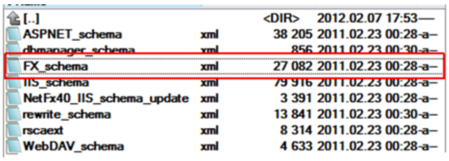
Kifogytunk az ötletekből…

- Vissza az elejére
  - Hátha ki lehet listázni a konfigurációt
  - Nézzük meg az appcmd.exe-t még egyszer

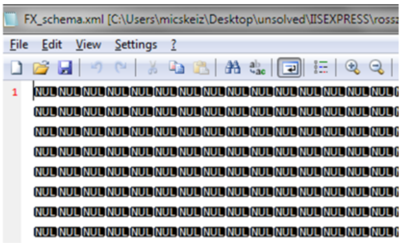
```
C:\Program Files\IIS Express>appcmd.exe list module

ERROR ( message:Configuration error MODULE
Filename: C:\Program Files\IIS
Express\config\schema\FX_schema.xml
Line Number: 0
Description: Configuration file is not well-formed
XML. )
```

Nyertünk: FX_schema.xml

- Mi van az FX_schema.xml-ben?



```
[..]                                <DIR>  2012.02.07 17:53—
ASPNET_schema              xml     38 205 2011.02.23 00:28-a–
dbmanager_schema           xml        856 2011.02.23 00:30-a–
FX_schema                  xml     27 082 2011.02.23 00:28-a–
IIS_schema                 xml     79 916 2011.02.23 00:28-a–
NetFx40_IIS_schema_update  xml      3 391 2011.02.23 00:28-a–
rewrite_schema             xml     13 841 2011.02.23 00:30-a–
rscaext                    xml      8 314 2011.02.23 00:28-a–
WebDAV_schema              xml      4 633 2011.02.23 00:28-a–
```

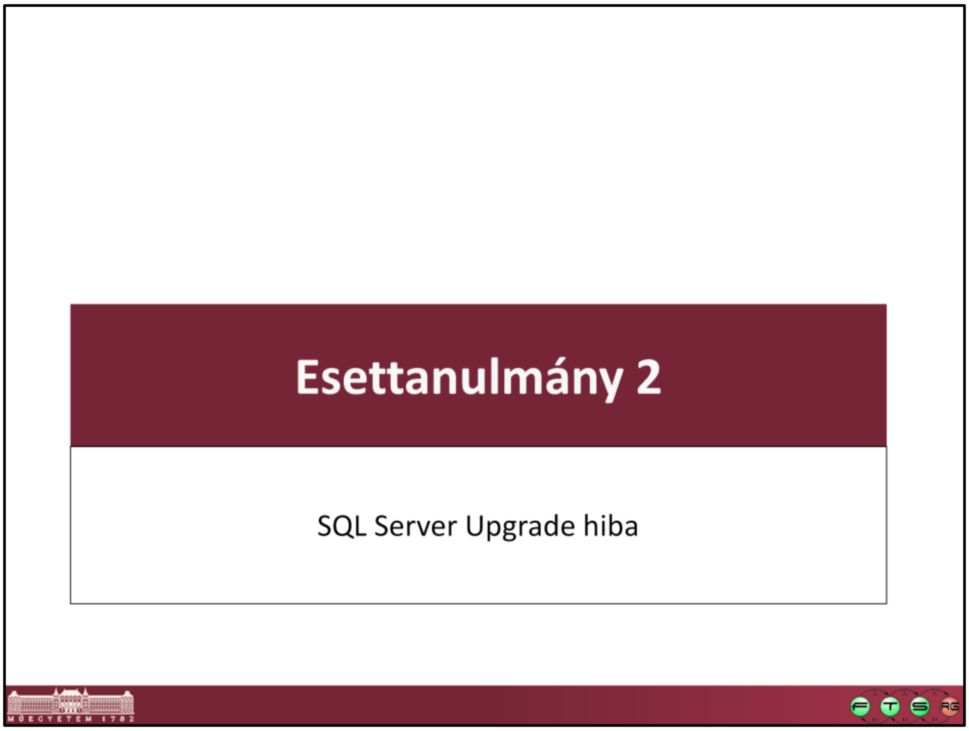


FX_schema.xml [C:\Users\micskeiz\Desktop\unsolved\IISEXPRESS\rossz
File Edit View Settings ?

```
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
```

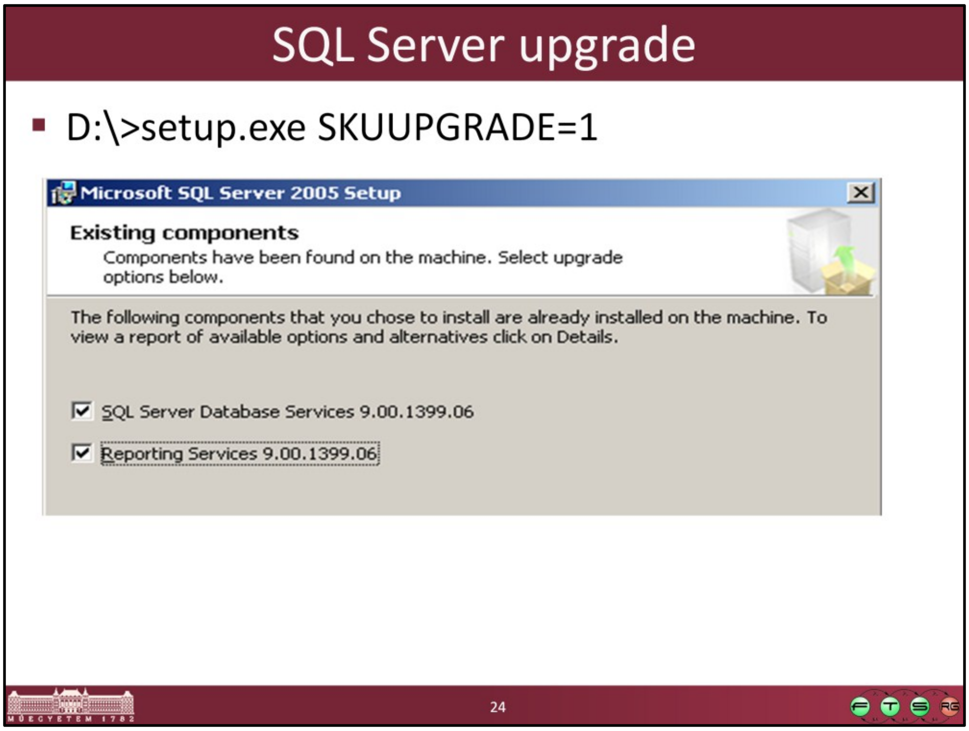
- A fájl látszólag megvan, de csupa NUL a tartalma

- (Snapshot eldobása közben sérült meg?)



Esettanulmány 2

SQL Server Upgrade hiba



SQL Server upgrade

- D:\>setup.exe SKUUPGRADE=1

Microsoft SQL Server 2005 Setup

Existing components

Components have been found on the machine. Select upgrade options below.

The following components that you chose to install are already installed on the machine. To view a report of available options and alternatives click on Details.

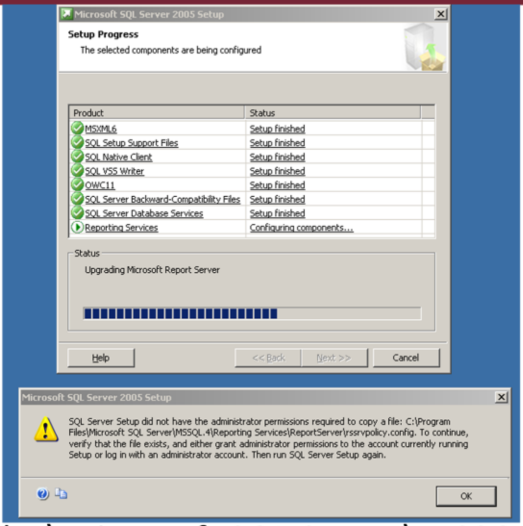
☑ SQL Server Database Services 9.00.1399.06

☑ Reporting Services 9.00.1399.06

Leírás: **SKUUPGRADE of Reporting Services fails with could not write rssrvpolicy.config,** http://social.technet.microsoft.com/Forums/en/sqlsetupandupgrade/thread/c75f35c7-f00d-45df-bdba-464ca5bd011a

Vagy magyarul: **SCE 2007 vs. SQL 2005 Express** http://micskeiz.wordpress.com/2007/08/27/sce-2007-vs-sql-2005-express/

Hiba a telepítés során



Microsoft SQL Server 2005 Setup

Setup Progress

The selected components are being configured

Product	Status
MSXML6	Setup finished
SQL Setup Support Files	Setup finished
SQL Native Client	Setup finished
SQL VSS Writer	Setup finished
OWC11	Setup finished
SQL Server Backward-Compatibility Files	Setup finished
SQL Server Database Services	Setup finished
Reporting Services	Configuring components...

Status

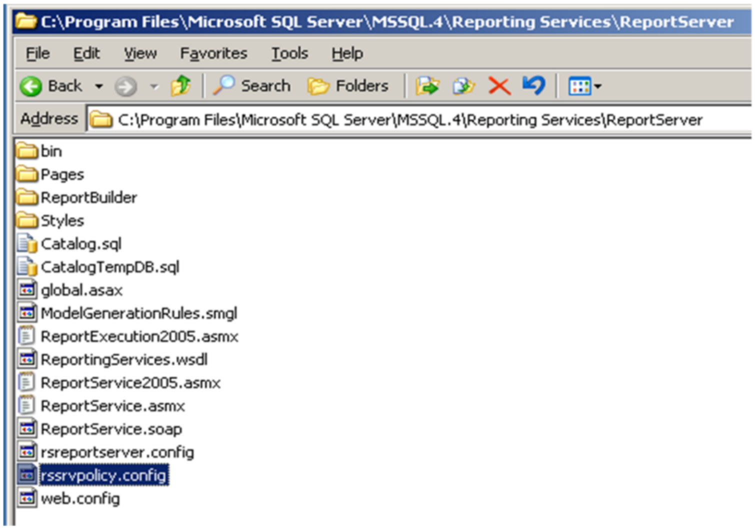
Upgrading Microsoft Report Server

Microsoft SQL Server 2005 Setup

SQL Server Setup did not have the administrator permissions required to copy a file: C:\Program Files\Microsoft SQL Server\MSSQL.4\Reporting Services\ReportServer\rssrvpolicy.config. To continue, verify that the file exists, and either grant administrator permissions to the account currently running Setup or log in with an administrator account. Then run SQL Server Setup again.

C:\Program Files\Microsoft SQL Server\MSSQL.4
\Reporting Services\ReportServer\rssrvpolicy.config

A fájl pedig létezik…



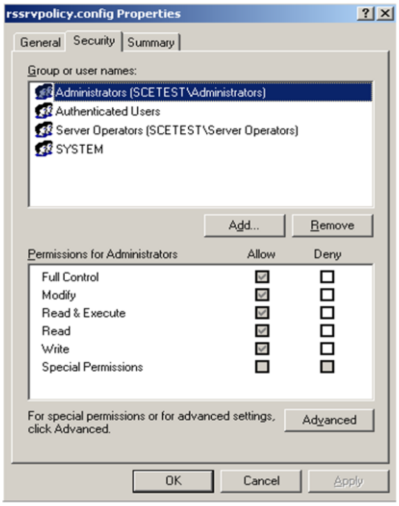
C:\Program Files\Microsoft SQL Server\MSSQL.4\Reporting Services\ReportServer

C:\Program Files\Microsoft SQL Server\MSSQL.4\Reporting Services\ReportServer

- bin
- Pages
- ReportBuilder
- Styles
- Catalog.sql
- CatalogTempDB.sql
- global.asax
- ModelGenerationRules.smgl
- ReportExecution2005.asmx
- ReportingServices.wsdl
- ReportService2005.asmx
- ReportService.asmx
- ReportService.soap
- rsreportserver.config
- rssrvpolicy.config
- web.config

És van hozzá jogosultságunk is… ??

- A Rendszergazda felhasználó nevében ment a telepítő
- De a hibaüzenet szerint jogosultsági gond lehet



Group or user names:

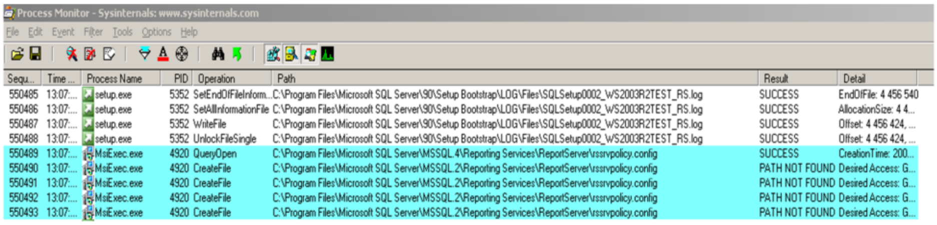
- Administrators (SCETEST\Administrators)
- Authenticated Users
- Server Operators (SCETEST\Server Operators)
- SYSTEM

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

Process Monitor

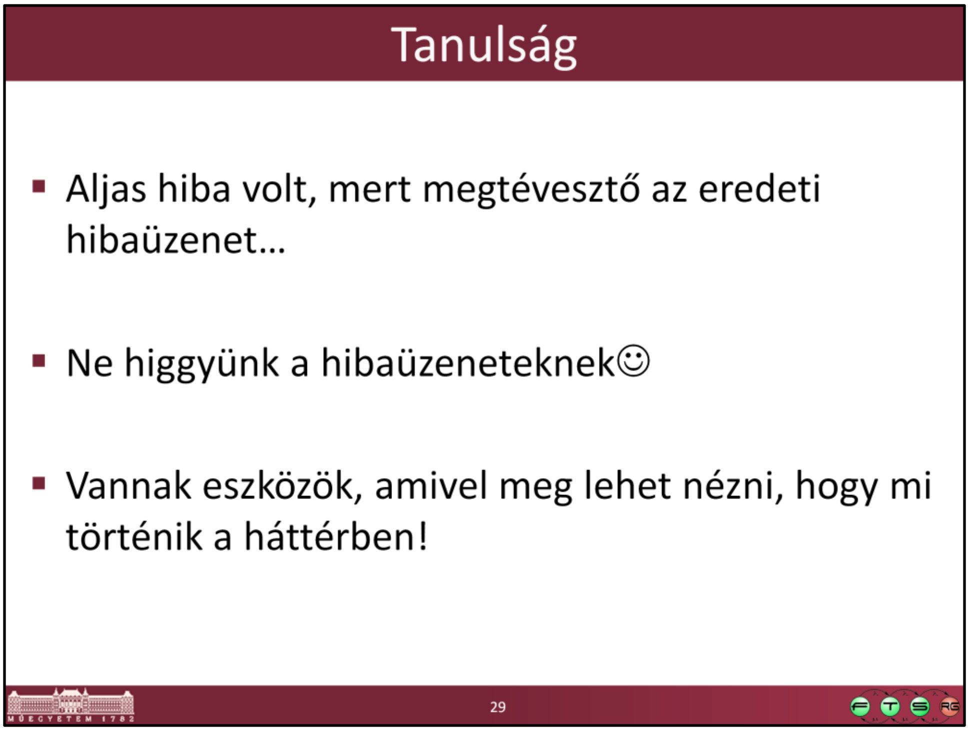
- Pár százezer esemény közül kikeressük a relevánsakat:


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Sequ...	Time ...	Process Name	PID	Operation	Path	Result	Detail
550485	13:07:...	setup.exe	5352	SetEndOfFileInform...	C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\Files\SQLSetup0002_WS2003R2TEST_RS.log	SUCCESS	EndOfFile: 4 456 540
550486	13:07:...	setup.exe	5352	SetAllInformationFile	C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\Files\SQLSetup0002_WS2003R2TEST_RS.log	SUCCESS	AllocationSize: 4 4...
550487	13:07:...	setup.exe	5352	WriteFile	C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\Files\SQLSetup0002_WS2003R2TEST_RS.log	SUCCESS	Offset: 4 456 424, ...
550488	13:07:...	setup.exe	5352	UnlockFileSingle	C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\Files\SQLSetup0002_WS2003R2TEST_RS.log	SUCCESS	Offset: 4 456 424, ...
550489	13:07:...	MsiExec.exe	4920	QueryOpen	C:\Program Files\Microsoft SQL Server\MSSQL.4\Reporting Services\ReportServer\rssrvpolicy.config	SUCCESS	CreationTime: 200...
550490	13:07:...	MsiExec.exe	4920	CreateFile	C:\Program Files\Microsoft SQL Server\MSSQL.2\Reporting Services\ReportServer\rssrvpolicy.config	PATH NOT FOUND	Desired Access: G...
550491	13:07:...	MsiExec.exe	4920	CreateFile	C:\Program Files\Microsoft SQL Server\MSSQL.2\Reporting Services\ReportServer\rssrvpolicy.config	PATH NOT FOUND	Desired Access: G...
550492	13:07:...	MsiExec.exe	4920	CreateFile	C:\Program Files\Microsoft SQL Server\MSSQL.2\Reporting Services\ReportServer\rssrvpolicy.config	PATH NOT FOUND	Desired Access: G...
550493	13:07:...	MsiExec.exe	4920	CreateFile	C:\Program Files\Microsoft SQL Server\MSSQL.2\Reporting Services\ReportServer\rssrvpolicy.config	PATH NOT FOUND	Desired Access: G...

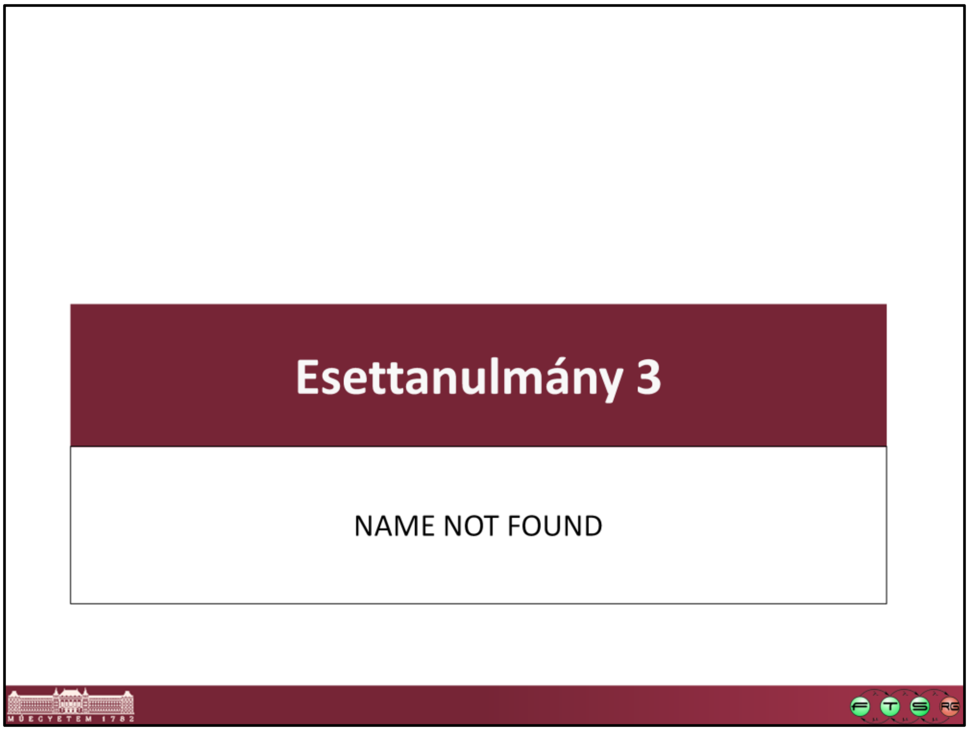
- Ki látja mi a hiba?☺

Nem az a gondja, hogy MSSQL.4-ben lévő cél fájlt nem tudja írni, hanem az MSSQL.2-ben lévő forrásfájlt nem találja (persze, mert nem is abban a könyvtárban kéne keresnie!)



Tanulság

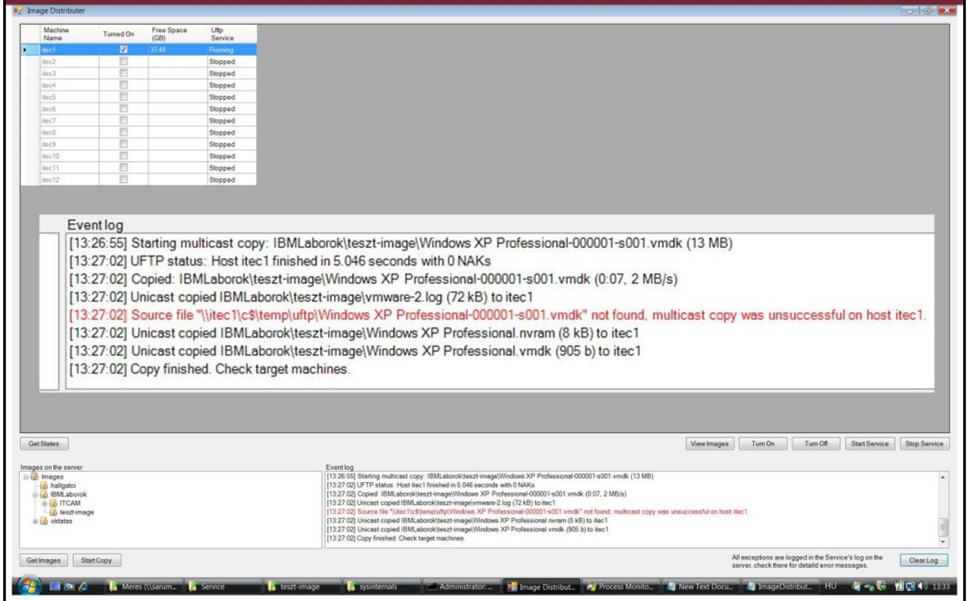
- Aljas hiba volt, mert megtévesztő az eredeti hibaüzenet…
- Ne higgyünk a hibaüzeneteknek☺
- Vannak eszközök, amivel meg lehet nézni, hogy mi történik a háttérben!



Esettanulmány 3

NAME NOT FOUND

„File not found” hiba



	Machine Name	Turned On	Free Space (GB)	Uftp Service
▸	itec1	☑	37.48	Running
	itec2	☐		Stopped
	itec3	☐		Stopped
	itec4	☐		Stopped
	itec5	☐		Stopped
	itec6	☐		Stopped
	itec7	☐		Stopped
	itec8	☐		Stopped
	itec9	☐		Stopped
	itec10	☐		Stopped
	itec11	☐		Stopped
	itec12	☐		Stopped

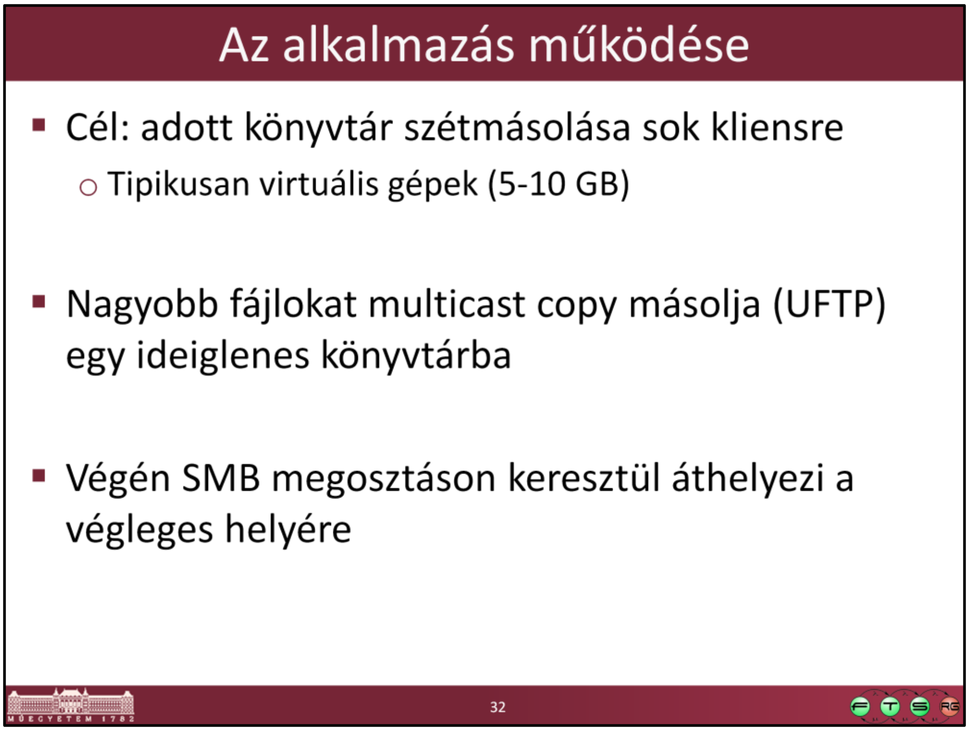
Event log

```
[13:26:55] Starting multicast copy: IBMLaborok\teszt-image\Windows XP Professional-000001-s001.vmdk (13 MB)
[13:27:02] UFTP status: Host itec1 finished in 5.046 seconds with 0 NAKs
[13:27:02] Copied: IBMLaborok\teszt-image\Windows XP Professional-000001-s001.vmdk (0:07, 2 MB/s)
[13:27:02] Unicast copied IBMLaborok\teszt-image\vmware-2.log (72 kB) to itec1
[13:27:02] Source file "\\itec1\c$\temp\uftp\Windows XP Professional-000001-s001.vmdk" not found, multicast copy was unsuccessful on host itec1.
[13:27:02] Unicast copied IBMLaborok\teszt-image\Windows XP Professional.nvram (8 kB) to itec1
[13:27:02] Unicast copied IBMLaborok\teszt-image\Windows XP Professional.vmdk (905 b) to itec1
[13:27:02] Copy finished. Check target machines.
```

```
[13:26:55] Starting multicast copy: IBMLaborok\teszt-image\Windows XP Professional-000001-s001.vmdk (13 MB)
[13:27:02] UFTP status: Host itec1 finished in 5.046 seconds with 0 NAKs
[13:27:02] Copied: IBMLaborok\teszt-image\Windows XP Professional-000001-s001.vmdk (0:07, 2 MB/s)
[13:27:02] Unicast copied IBMLaborok\teszt-image\vmware-2.log (72 kB) to itec1
[13:27:02] Source file "\\itec1\c$\temp\uftp\Windows XP Professional-000001-s001.vmdk" not found, multicast copy was unsuccessful on host itec1.
[13:27:02] Unicast copied IBMLaborok\teszt-image\Windows XP Professional.nvram (8 kB) to itec1
[13:27:02] Unicast copied IBMLaborok\teszt-image\Windows XP Professional.vmdk (905 b) to itec1
[13:27:02] Copy finished. Check target machines.
```

All exceptions are logged in the Service's log on the server, check there for detaild error messages.

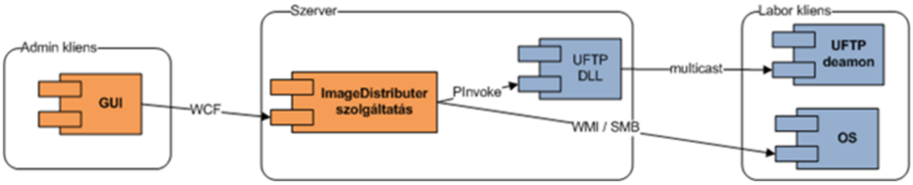
Részletes leírás:http://micskeiz.wordpress.com/2009/09/24/name-not-found-%E2%80%93-egy-furcsa-fajl-hozzaferesi-hiba/

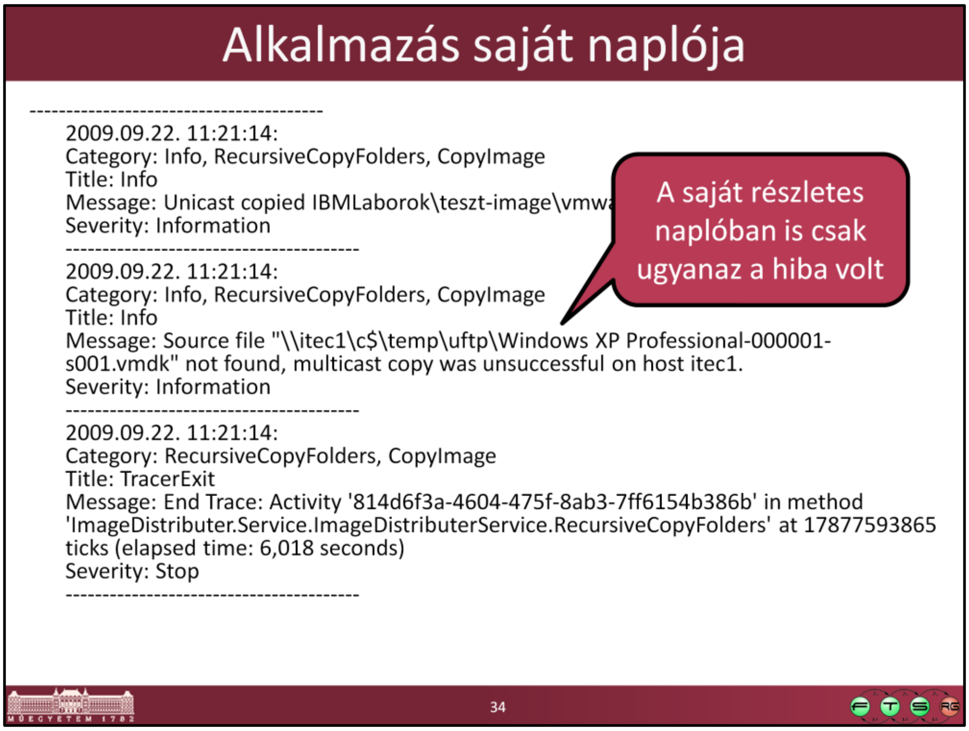


Az alkalmazás működése

- Cél: adott könyvtár szétmásolása sok kliensre
  - Tipikusan virtuális gépek (5-10 GB)
- Nagyobb fájlokat multicast copy másolja (UFTP) egy ideiglenes könyvtárba
- Végén SMB megosztáson keresztül áthelyezi a végleges helyére

Az alkalmazás



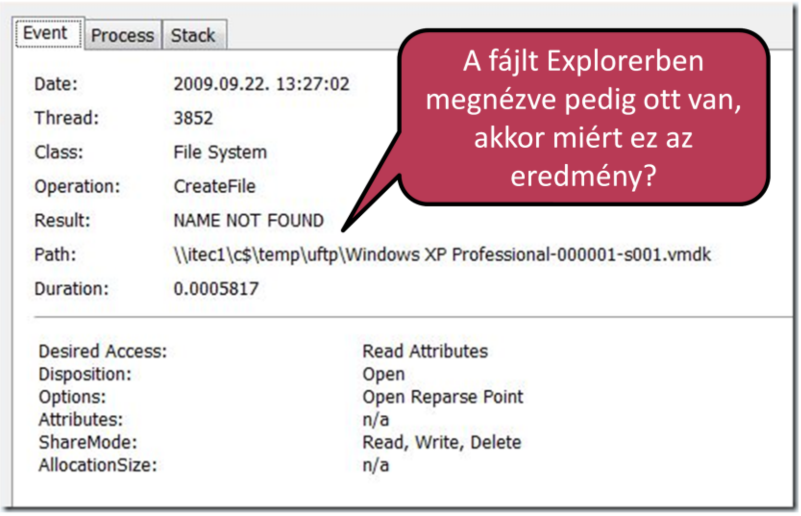


Alkalmazás saját naplója

```
----------------------------------------
    2009.09.22. 11:21:14:
    Category: Info, RecursiveCopyFolders, CopyImage
    Title: Info
    Message: Unicast copied IBMLaborok\teszt-image\vmwa
    Severity: Information
    ----------------------------------------
    2009.09.22. 11:21:14:
    Category: Info, RecursiveCopyFolders, CopyImage
    Title: Info
    Message: Source file "\\itec1\c$\temp\uftp\Windows XP Professional-000001-
    s001.vmdk" not found, multicast copy was unsuccessful on host itec1.
    Severity: Information
    ----------------------------------------
    2009.09.22. 11:21:14:
    Category: RecursiveCopyFolders, CopyImage
    Title: TracerExit
    Message: End Trace: Activity '814d6f3a-4604-475f-8ab3-7ff6154b386b' in method
    'ImageDistributer.Service.ImageDistributerService.RecursiveCopyFolders' at 17877593865
    ticks (elapsed time: 6,018 seconds)
    Severity: Stop
    ----------------------------------------
```

A saját részletes naplóban is csak ugyanaz a hiba volt

A fájl hozzáférés Process Monitorban

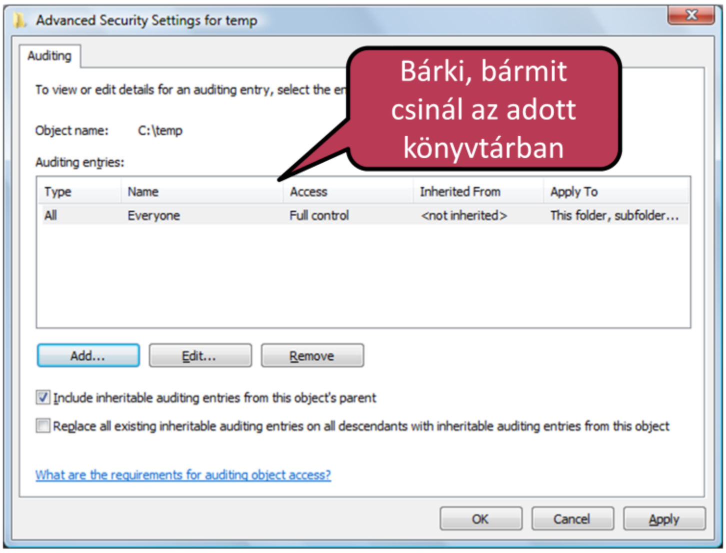


Date:	2009.09.22. 13:27:02
Thread:	3852
Class:	File System
Operation:	CreateFile
Result:	NAME NOT FOUND
Path:	\\itec1\c$\temp\uftp\Windows XP Professional-000001-s001.vmdk
Duration:	0.0005817

Desired Access:	Read Attributes
Disposition:	Open
Options:	Open Reparse Point
Attributes:	n/a
ShareMode:	Read, Write, Delete
AllocationSize:	n/a

A fájlt Explorerben megnézve pedig ott van, akkor miért ez az eredmény?

NTFS szintű naplózás beállítása (SACL)



Advanced Security Settings for temp

Auditing

To view or edit details for an auditing entry, select the en

Object name: C:\temp

Auditing entries:

Type	Name	Access	Inherited From	Apply To
All	Everyone	Full control	<not inherited>	This folder, subfolder...

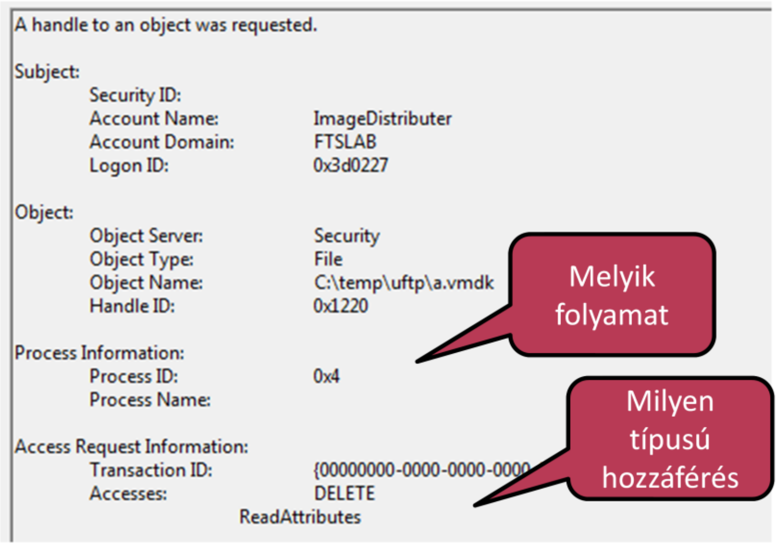
☑ Include inheritable auditing entries from this object's parent

□ Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object

What are the requirements for auditing object access?

Bárki, bármit csinál az adott könyvtárban

Bejegyzés a biztonsági naplóban

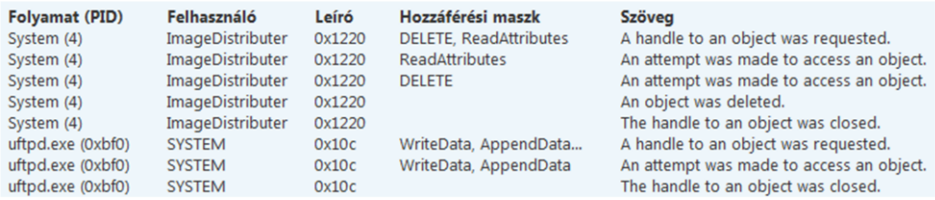


```
A handle to an object was requested.

Subject:
          Security ID:
          Account Name:          ImageDistributer
          Account Domain:        FTSLAB
          Logon ID:              0x3d0227

Object:
          Object Server:         Security
          Object Type:           File
          Object Name:           C:\temp\uftp\a.vmdk
          Handle ID:             0x1220

Process Information:
          Process ID:            0x4
          Process Name:

Access Request Information:
          Transaction ID:        {00000000-0000-0000-0000
          Accesses:              DELETE
                       ReadAttributes
```

Melyik folyamat

Milyen típusú hozzáférés

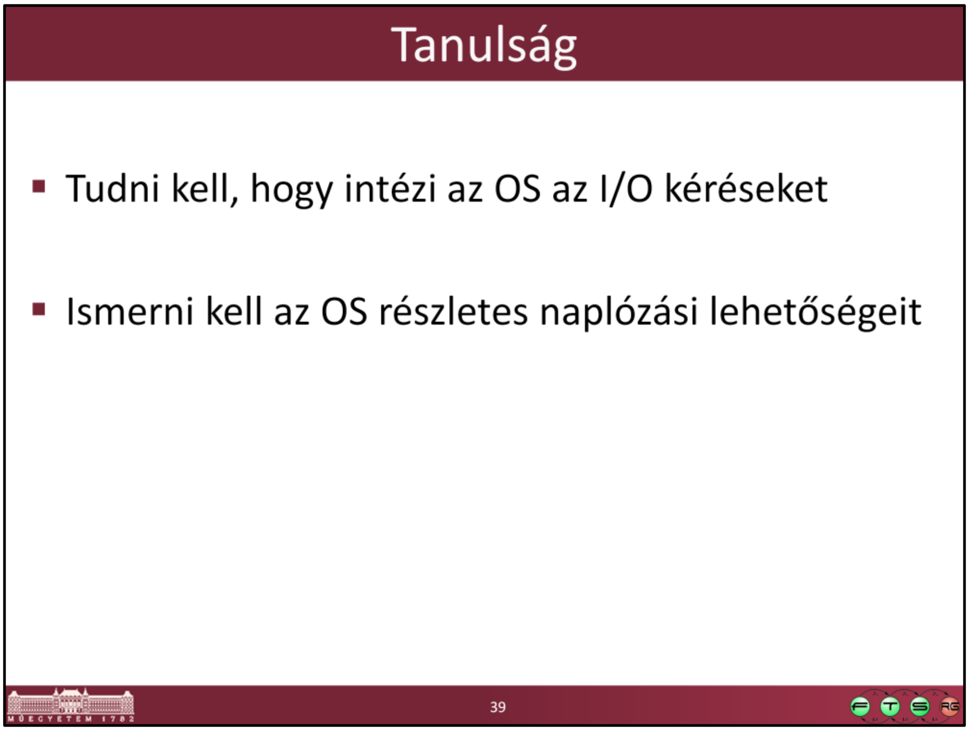
Fájl hozzáférések sorrendje



Folyamat (PID)	Felhasználó	Leíró	Hozzáférési maszk	Szöveg
System (4)	ImageDistributer	0x1220	DELETE, ReadAttributes	A handle to an object was requested.
System (4)	ImageDistributer	0x1220	ReadAttributes	An attempt was made to access an object.
System (4)	ImageDistributer	0x1220	DELETE	An attempt was made to access an object.
System (4)	ImageDistributer	0x1220		An object was deleted.
System (4)	ImageDistributer	0x1220		The handle to an object was closed.
uftpd.exe (0xbf0)	SYSTEM	0x10c	WriteData, AppendData...	A handle to an object was requested.
uftpd.exe (0xbf0)	SYSTEM	0x10c	WriteData, AppendData	An attempt was made to access an object.
uftpd.exe (0xbf0)	SYSTEM	0x10c		The handle to an object was closed.

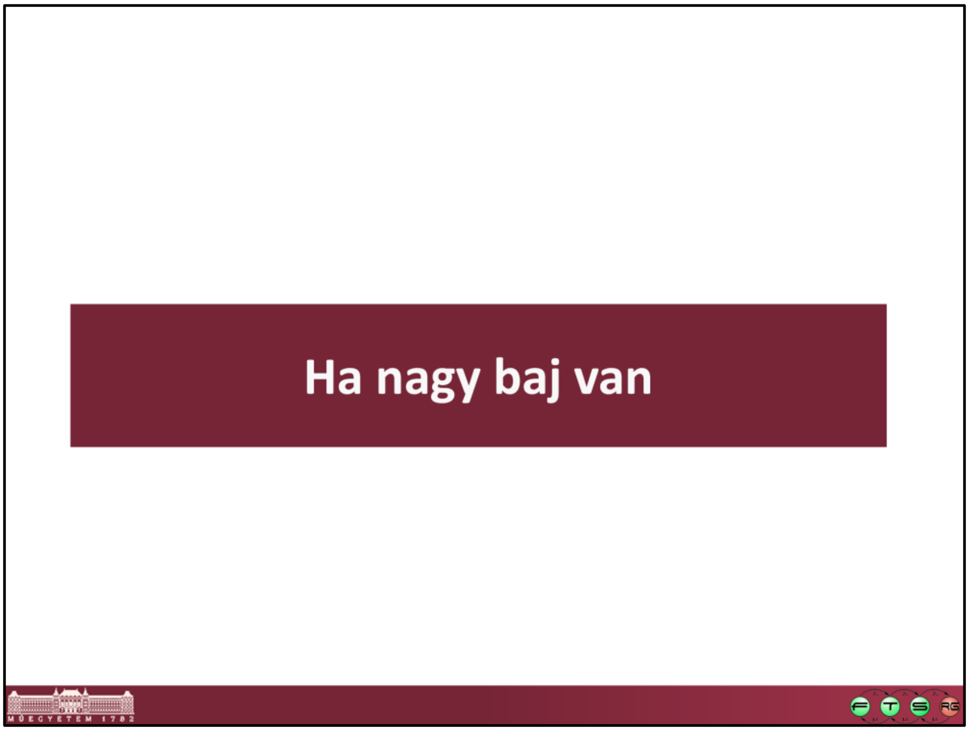
Megoldás:

- Az uftd.exe még írni akarta és fogta a fájlt az ImageDistributer hozzáférése előtt

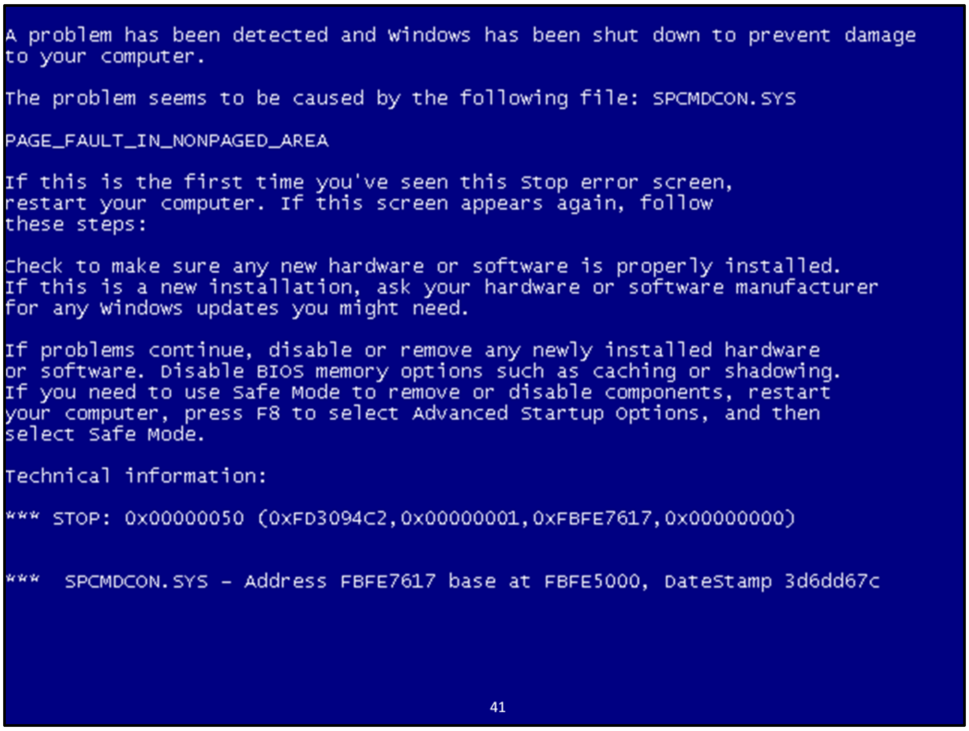


Tanulság

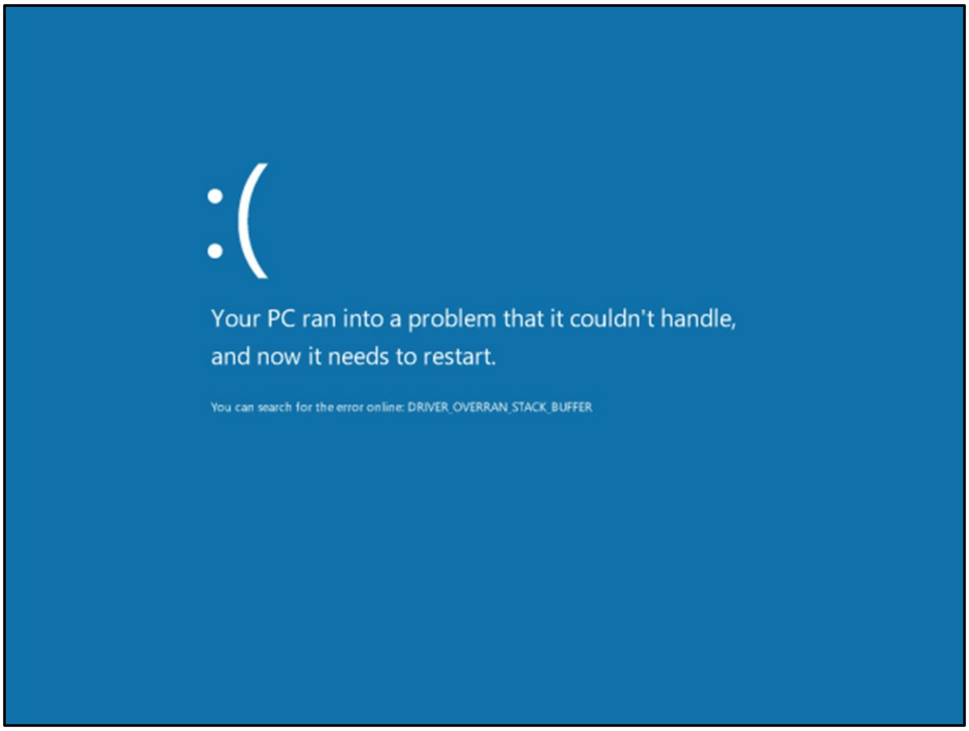
- Tudni kell, hogy intézi az OS az I/O kéréseket
- Ismerni kell az OS részletes naplózási lehetőségeit



Ha nagy baj van



```
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
```

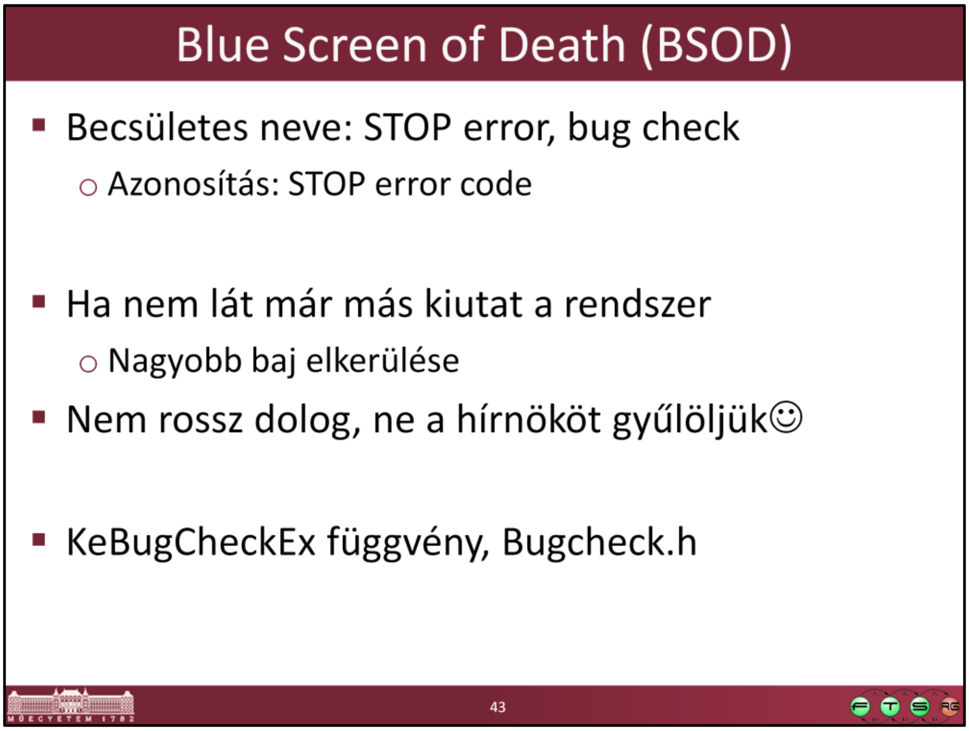


:(

Your PC ran into a problem that it couldn't handle, and now it needs to restart.

You can search for the error online: DRIVER_OVERRAN_STACK_BUFFER

Windows 8-ban bevezetett új BSOD

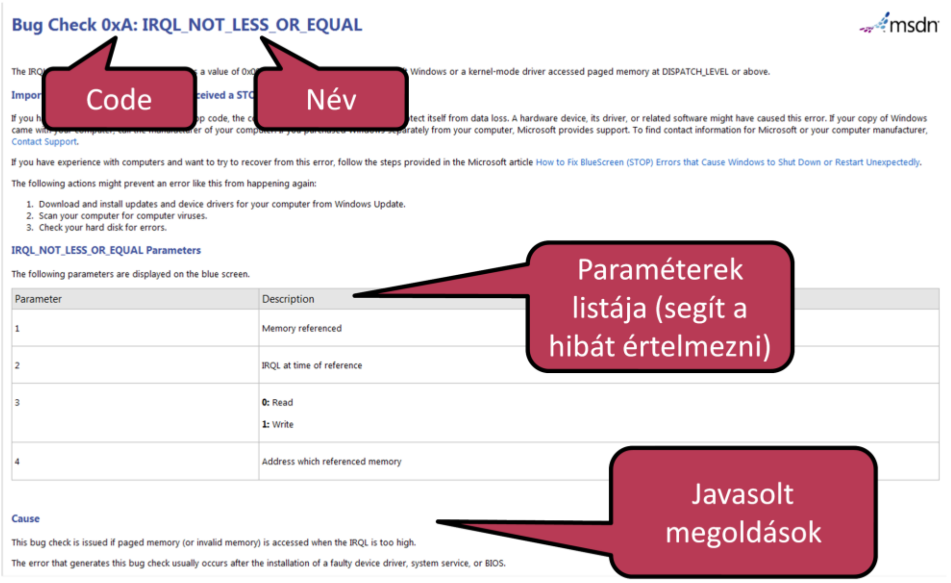


Blue Screen of Death (BSOD)

- Becsületes neve: STOP error, bug check
  - Azonosítás: STOP error code
- Ha nem lát már más kiutat a rendszer
  - Nagyobb baj elkerülése
- Nem rossz dolog, ne a hírnököt gyűlöljük☺
- KeBugCheckEx függvény, Bugcheck.h

Bug Check Codes, http://msdn.microsoft.com/en-us/library/hh406232.aspx

Példa bug check (MSDN)



Bug Check 0xA: IRQL_NOT_LESS_OR_EQUAL

msdn

The IRQ a value of 0x0 Windows or a kernel-mode driver accessed paged memory at DISPATCH_LEVEL or above.

Impor ceived a STO

If you h p code, the c tect itself from data loss. A hardware device, its driver, or related software might have caused this error. If your copy of Windows came wi er of your comp arately from your computer, Microsoft provides support. To find contact information for Microsoft or your computer manufacturer, Contact Support.

If you have experience with computers and want to try to recover from this error, follow the steps provided in the Microsoft article How to Fix BlueScreen (STOP) Errors that Cause Windows to Shut Down or Restart Unexpectedly.

The following actions might prevent an error like this from happening again:

1. Download and install updates and device drivers for your computer from Windows Update.
2. Scan your computer for computer viruses.
3. Check your hard disk for errors.

IRQL_NOT_LESS_OR_EQUAL Parameters

The following parameters are displayed on the blue screen.

Parameter	Description
1	Memory referenced
2	IRQL at time of reference
3	**0:** Read **1:** Write
4	Address which referenced memory

Cause

This bug check is issued if paged memory (or invalid memory) is accessed when the IRQL is too high.

The error that generates this bug check usually occurs after the installation of a faulty device driver, system service, or BIOS.

Code

Név

Paraméterek listája (segít a hibát értelmezni)

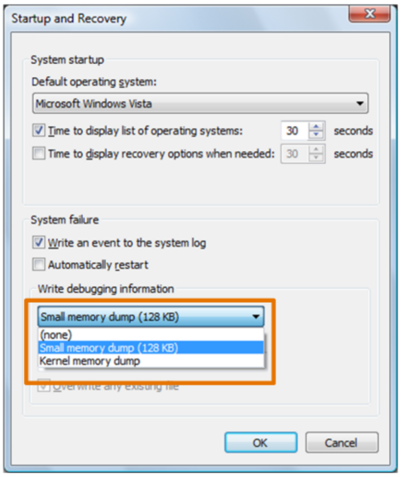
Javasolt megoldások

Forrás: http://msdn.microsoft.com/en-us/library/ff560129(v=VS.85).aspx

Crash dump

- Memória részlet és CPU állapot elmentése
- Lapozófájlba írja ki ideiglenesen

- Fajtái:
  - Small memory dump
  - Kernel memory dump
  - Full memory dump



Startup and Recovery

System startup

Default operating system:

Microsoft Windows Vista

☑ Time to display list of operating systems: 30 seconds

☐ Time to display recovery options when needed: 30 seconds

System failure

☑ Write an event to the system log

☐ Automatically restart

Write debugging information

Small memory dump (128 KB)

(none)

Small memory dump (128 KB)

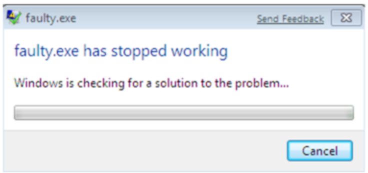
Kernel memory dump

☑ Overwrite any existing file

MSDN. **Crash Dump Files,** http://msdn.microsoft.com/en-us/library/ff539316.aspx

Crash dump elemzése

- Microsoft Error Reporting
  - MS szerverének elküldi
  - Elemzés, összehasonlítás
  - Visszajelzés, esetleg megoldás

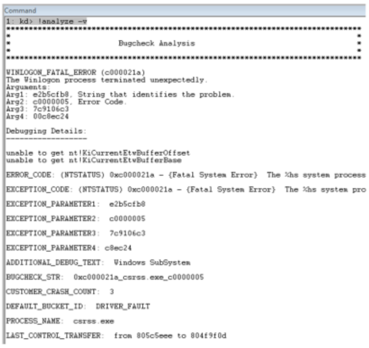


faulty.exe

faulty.exe has stopped working

Windows is checking for a solution to the problem...

- Saját magunk:
  - WinDbg
  - !analyze –v parancs
  - Hibázó modul azonosítása



```
1: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

WINLOGON_FATAL_ERROR (c000021a)
The Winlogon process terminated unexpectedly.
Arguments:
Arg1: e2b5cfb8, String that identifies the problem.
Arg2: c0000005, Error Code.
Arg3: 7c9106c3
Arg4: 00c8ec24

Debugging Details:
------------------

unable to get nt!KiCurrentEtwBufferOffset
unable to get nt!KiCurrentEtwBufferBase

ERROR_CODE: (NTSTATUS) 0xc000021a - {Fatal System Error}  The %hs system process

EXCEPTION_CODE: (NTSTATUS) 0xc000021a - {Fatal System Error}  The %hs system pro

EXCEPTION_PARAMETER1:  e2b5cfb8

EXCEPTION_PARAMETER2:  c0000005

EXCEPTION_PARAMETER3:  7c9106c3

EXCEPTION_PARAMETER4: c8ec24

ADDITIONAL_DEBUG_TEXT:  Windows SubSystem

BUGCHECK_STR:  0xc000021a_csrss.exe_c0000005

CUSTOMER_CRASH_COUNT:  3

DEFAULT_BUCKET_ID:  DRIVER_FAULT

PROCESS_NAME:  csrss.exe

LAST_CONTROL_TRANSFER:  from 805c5eee to 804f9f0d
```

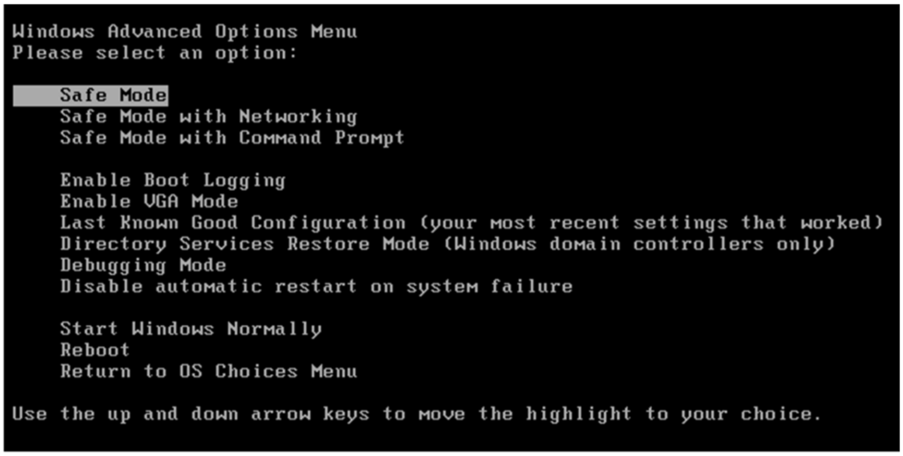
How to read the small memory dump files that Windows creates for debugging, http://support.microsoft.com/kb/315263/en-us

DEMO Blue Screen of Death (BSOD)

- Hibajelentés küldése (Error reporting)
- Memory dump készítése
- Minidump elemzése WinDgb-ben

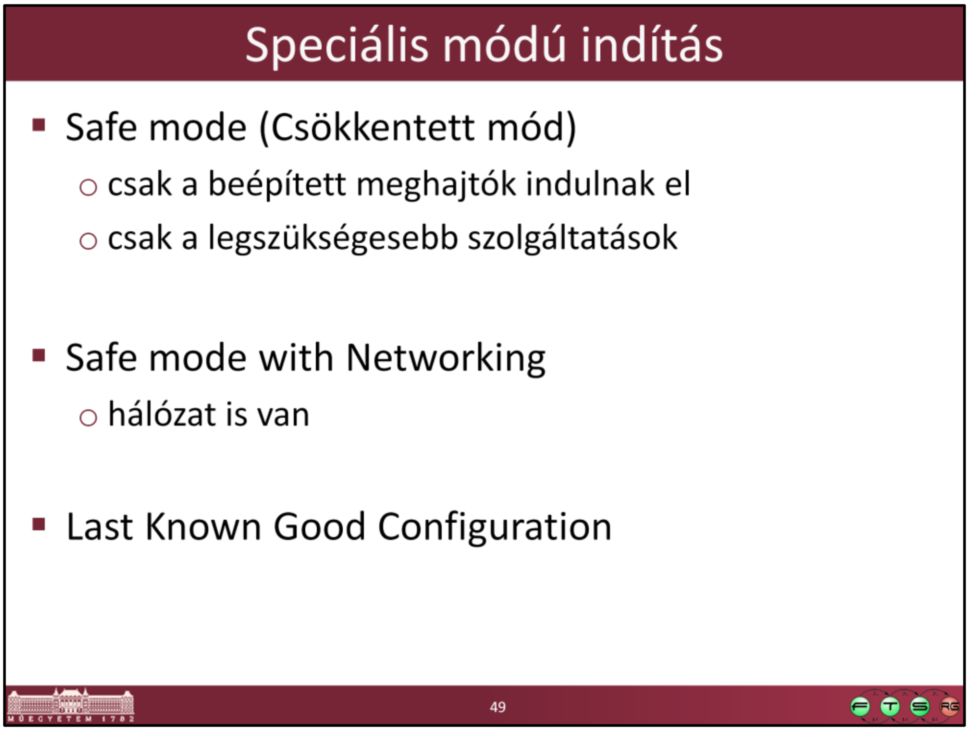
Speciális módú indítás

- F8 a Windows logó előtt



```
Windows Advanced Options Menu
Please select an option:

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable VGA Mode
    Last Known Good Configuration (your most recent settings that worked)
    Directory Services Restore Mode (Windows domain controllers only)
    Debugging Mode
    Disable automatic restart on system failure

    Start Windows Normally
    Reboot
    Return to OS Choices Menu

Use the up and down arrow keys to move the highlight to your choice.
```

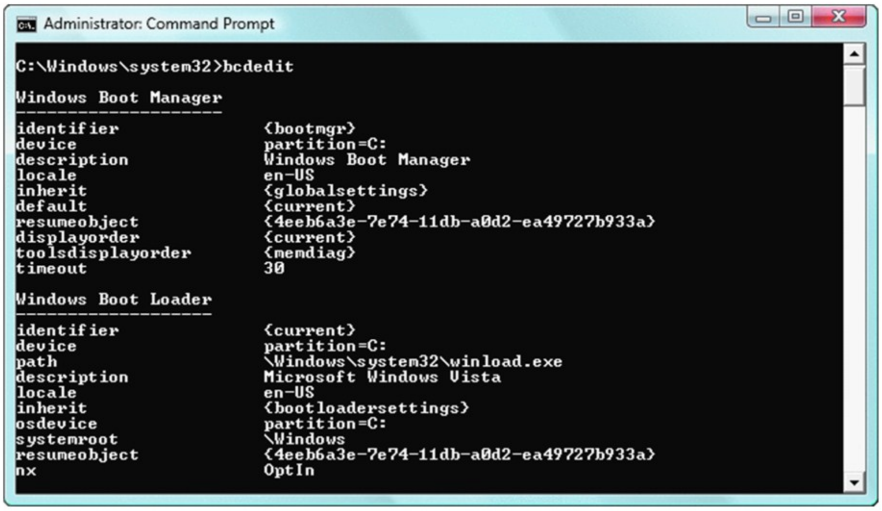
A description of the Safe Mode Boot options in Windows XP
http://support.microsoft.com/default.aspx?scid=kb;en-us;315222



Speciális módú indítás

- Safe mode (Csökkentett mód)
  - csak a beépített meghajtók indulnak el
  - csak a legszükségesebb szolgáltatások
- Safe mode with Networking
  - hálózat is van
- Last Known Good Configuration

Boot Configuration Database



```
C:\Windows\system32>bcdedit

Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=C:
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
default                 {current}
resumeobject            {4eeb6a3e-7e74-11db-a0d2-ea49727b933a}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             Microsoft Windows Vista
locale                  en-US
inherit                 {bootloadersettings}
osdevice                partition=C:
systemroot              \Windows
resumeobject            {4eeb6a3e-7e74-11db-a0d2-ea49727b933a}
nx                      OptIn
```

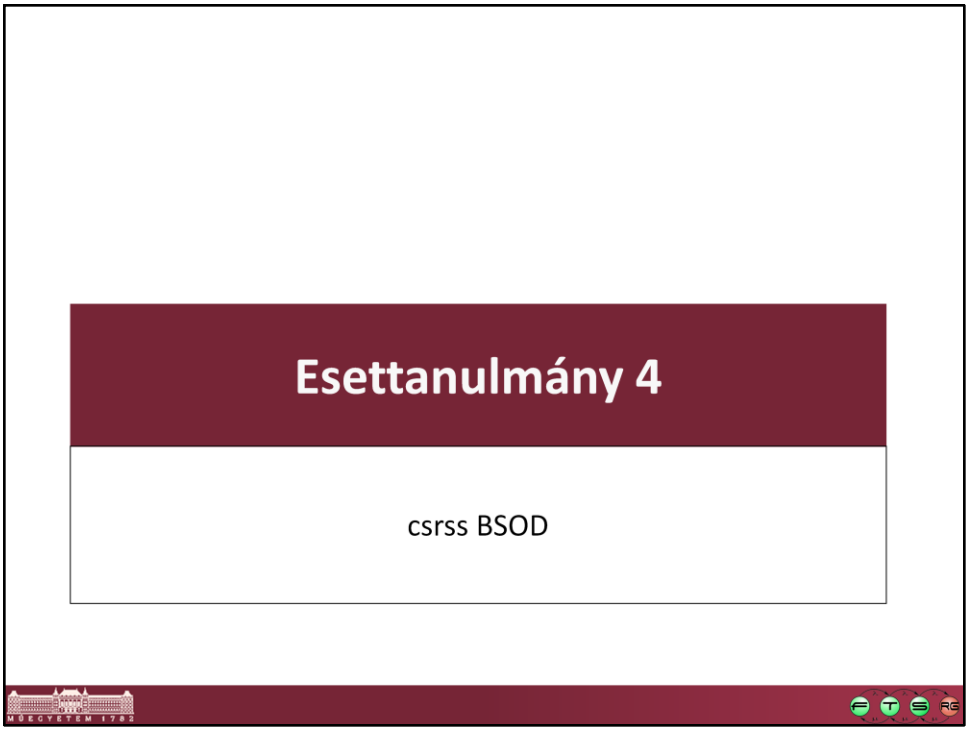
- GUI eszköz: *msconfig.exe*

DEMO

Forrás: Mark Russinovich: Inside the Windows Vista kernel: Part 2, Technet Magazine

„Windows Vista has enhanced several aspects of startup and shutdown. Startup has improved with the introduction of the Boot Configuration Database (BCD) for storing system and OS startup configuration, a new flow and organization of system startup processes, new logon architecture, and support for delayed-autostart services. Windows Vista shutdown changes include pre-shutdown notification for Windows services, Windows services shutdown ordering, and a significant change to the way the OS manages power state transitions.
One of the most visible changes to the startup process is the absence of Boot.ini from the root of the system volume. That's because the boot configuration, which on previous versions of Windows was stored in the Boot.ini text file, is now stored in the BCD. One of the reasons Windows Vista uses the BCD is that it unifies the two current boot architectures supported by Windows: Master Boot Record (MBR) and Extensible Firmware Interface (EFI). MBR is generally used by x86 and x64 desktop systems, while EFI is used by Itanium-based systems (though desktop PCs are likely to ship with EFI support in the near future). The BCD abstracts the firmware and has other advantages over Boot.ini, like its support for Unicode strings and alternate pre-boot executables.
The BCD is actually stored on disk in a registry hive that loads into the Windows registry for access via registry APIs. On PCs, Windows stores it in \Boot\Bcd on the system volume. On EFI systems, it's on the EFI system partition. When the hive is loaded, it appears under HKLM\Bcd00000000, but its internal format is undocumented so editing it requires the use of a tool like %SystemRoot%\System32\Bcdedit.exe. Interfaces for manipulating the BCD are also made available for scripts and custom editors through Windows Management Instrumentation (WMI) and you can use the Windows System Configuration Utility (%SystemRoot%\System32\Msconfig.exe) to edit or add basic parameters, like kernel debugging options.
The BCD divides platform-wide boot settings, like the default OS selection and the boot menu timeout, from OS-specific settings such as OS boot options and the path to the OS boot loader. For example, Figure 3 shows that when you run Bcdedit with no command-line options, it displays platform settings in the Windows Boot Manager section at the top of the output, followed by OS-specific settings in the Windows Boot Loader section.

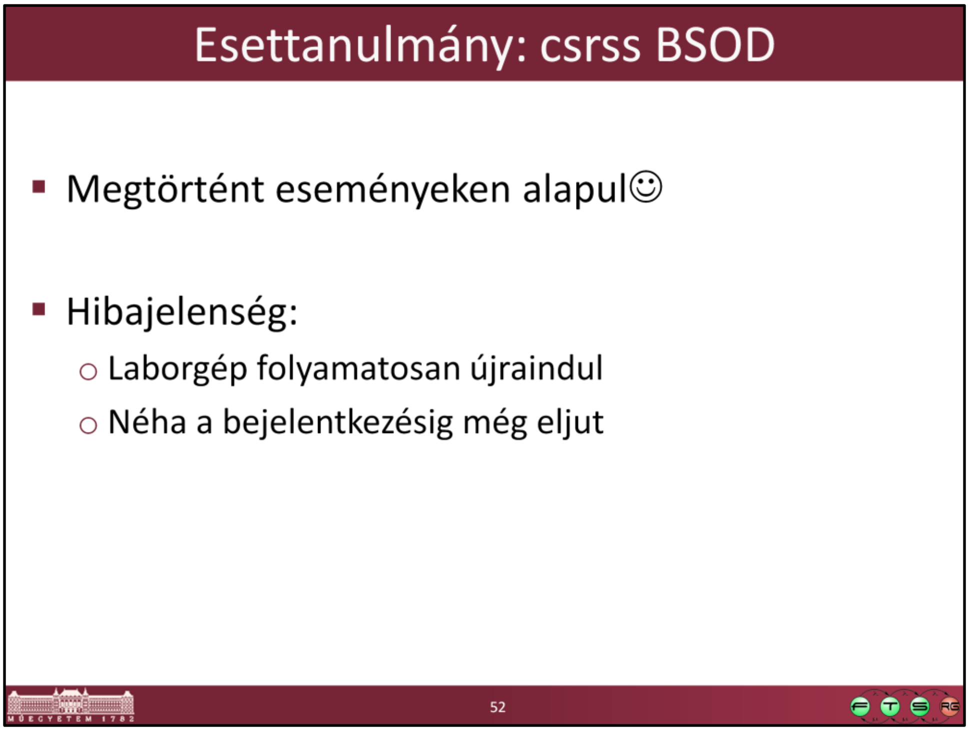
When you boot a Windows Vista installation, this new scheme divides the tasks that were handled by the operating system loader (Ntldr) on previous versions of Windows into two different executables: \BootMgr and %SystemRoot%\System32\Winload.exe. Bootmgr reads the BCD and displays the OS boot menu, while Winload.exe handles operating-system loading. If you're performing a clean boot, Winload.exe loads boot-start device drivers and core operating system files, including Ntoskrnl.exe, and transfers control to the operating system; if the system is resuming from hibernation, then it executes %SystemRoot%\System32\Winresume.exe to load the hibernation data into memory and resume the OS. Bootmgr also includes support for additional pre-boot executables. Windows Vista comes with the Windows Memory Diagnostic (\Boot\Memtest.exe) pre-configured as an option for checking the health of RAM, but third parties can add their own pre-boot executables as options that will display in Bootmgr's boot menu.”



Esettanulmány 4

csrss BSOD

MŰEGYETEM 1782



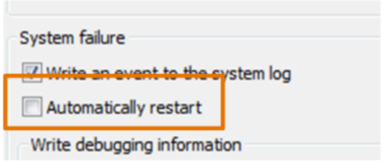
Esettanulmány: csrss BSOD

- Megtörtént eseményeken alapul☺
- Hibajelenség:
  - Laborgép folyamatosan újraindul
  - Néha a bejelentkezésig még eljut

Részletes leírás: **0xC000021A: csrss kék halál a laborban**,
http://micskeiz.wordpress.com/2009/05/21/0xc000021a-csrss-kek-halal-a-laborban/

Első lépések

- Automatikus újraindítás kikapcsolása



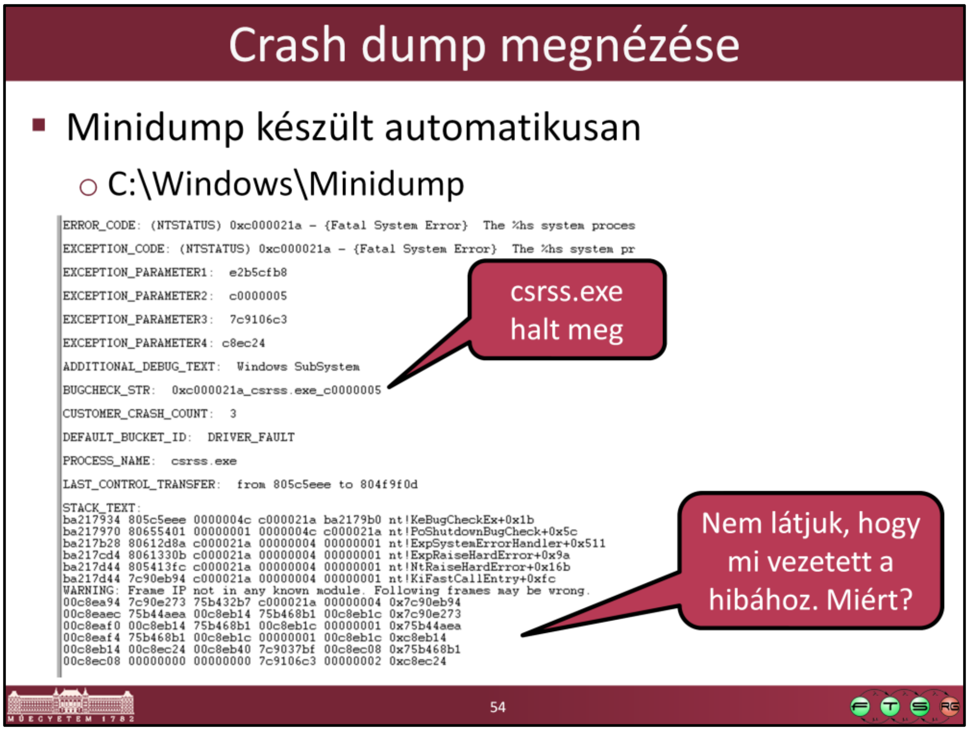
System failure

☑ Write an event to the system log

□ Automatically restart

Write debugging information

- STOP hibakód így kiderül:
  - C000021A, {e2a5ee98, c0000005, 7c9106c3, 69ec24}
  - MSDN dokumentáció: Bug Checks
    - 0xC000021A: STATUS_SYSTEM_PROCESS_TERMINATED



Crash dump megnézése

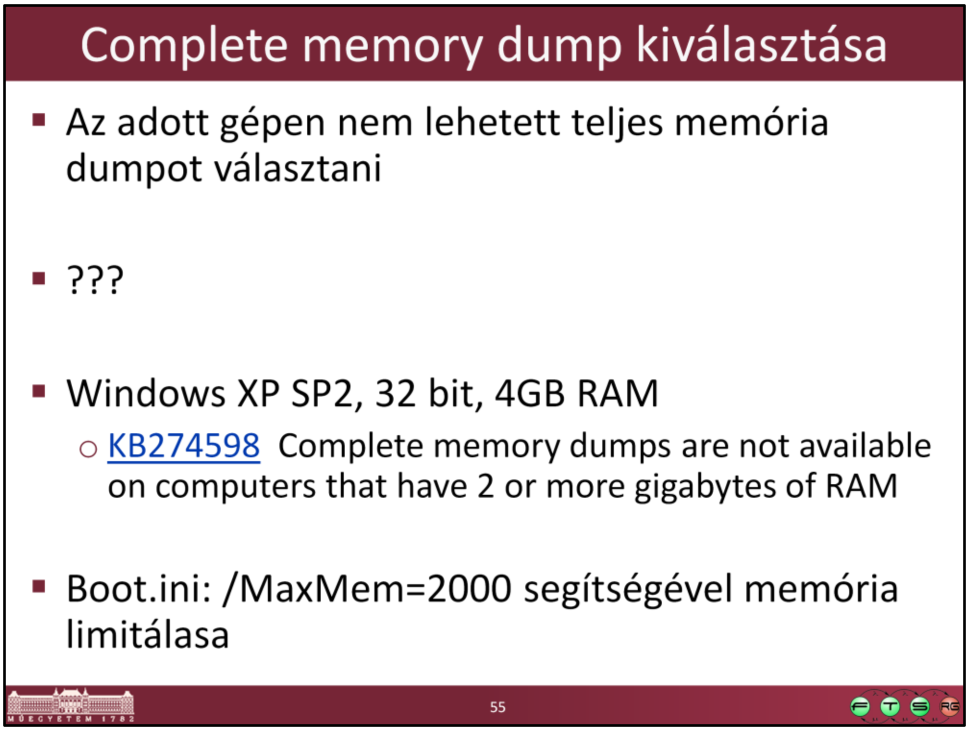
- Minidump készült automatikusan
  - C:\Windows\Minidump

```
ERROR_CODE: (NTSTATUS) 0xc000021a - {Fatal System Error}  The %hs system proces

EXCEPTION_CODE: (NTSTATUS) 0xc000021a - {Fatal System Error}  The %hs system pr

EXCEPTION_PARAMETER1:  e2b5cfb8

EXCEPTION_PARAMETER2:  c0000005

EXCEPTION_PARAMETER3:  7c9106c3

EXCEPTION_PARAMETER4: c8ec24

ADDITIONAL_DEBUG_TEXT:  Windows SubSystem

BUGCHECK_STR:  0xc000021a_csrss.exe_c0000005

CUSTOMER_CRASH_COUNT:  3

DEFAULT_BUCKET_ID:  DRIVER_FAULT

PROCESS_NAME:  csrss.exe

LAST_CONTROL_TRANSFER:  from 805c5eee to 804f9f0d

STACK_TEXT:
ba217934 805c5eee 0000004c c000021a ba2179b0 nt!KeBugCheckEx+0x1b
ba217970 80655401 00000001 0000004c c000021a nt!PoShutdownBugCheck+0x5c
ba217b28 80612d8a c000021a 00000004 00000001 nt!ExpSystemErrorHandler+0x511
ba217cd4 8061330b c000021a 00000004 00000001 nt!ExpRaiseHardError+0x9a
ba217d44 805413fc c000021a 00000004 00000001 nt!NtRaiseHardError+0x16b
ba217d44 7c90eb94 c000021a 00000004 00000001 nt!KiFastCallEntry+0xfc
WARNING: Frame IP not in any known module. Following frames may be wrong.
00c8ea94 7c90e273 75b432b7 c000021a 00000004 0x7c90eb94
00c8eaec 75b44aea 00c8eb14 75b468b1 00c8eb1c 0x7c90e273
00c8eaf0 00c8eb14 75b468b1 00c8eb1c 00000001 0x75b44aea
00c8eaf4 75b468b1 00c8eb1c 00000001 00c8eb1c 0xc8eb14
00c8eb14 00c8ec24 00c8eb40 7c9037bf 00c8ec08 0x75b468b1
00c8ec08 00000000 00000000 7c9106c3 00000002 0xc8ec24
```

csrss.exe halt meg

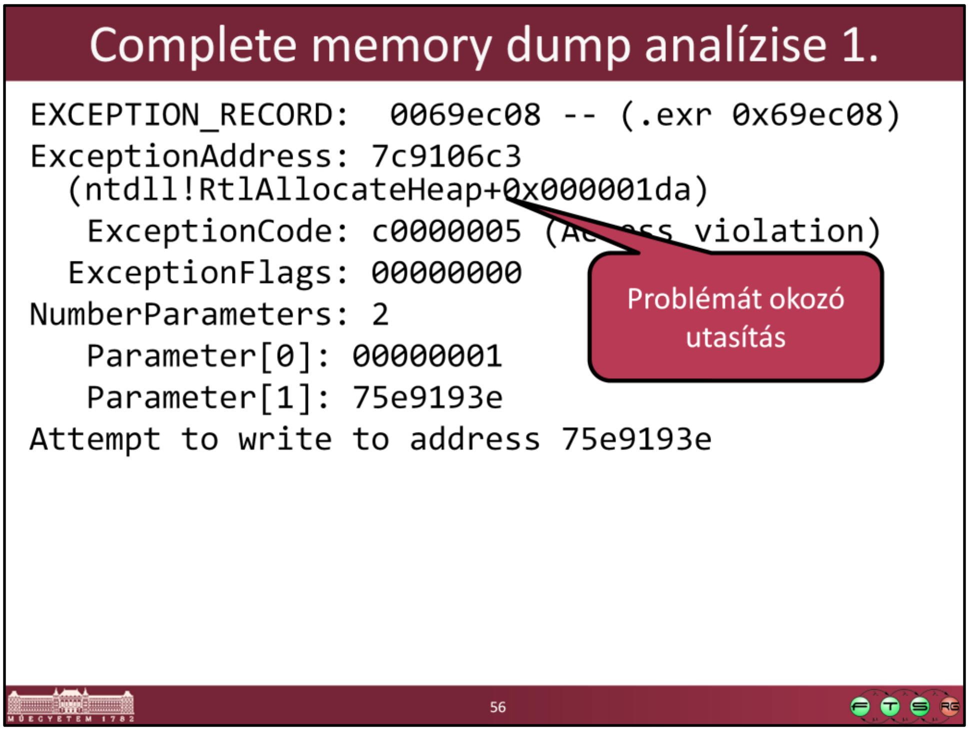
Nem látjuk, hogy mi vezetett a hibához. Miért?

Mert ez minidump, csak a kernel legfontosabb adatstruktúrái vannak benne. De nincs benne felhasználói módú memóriaterület, így a felhasználói módú veremtartalom sem.



Complete memory dump kiválasztása

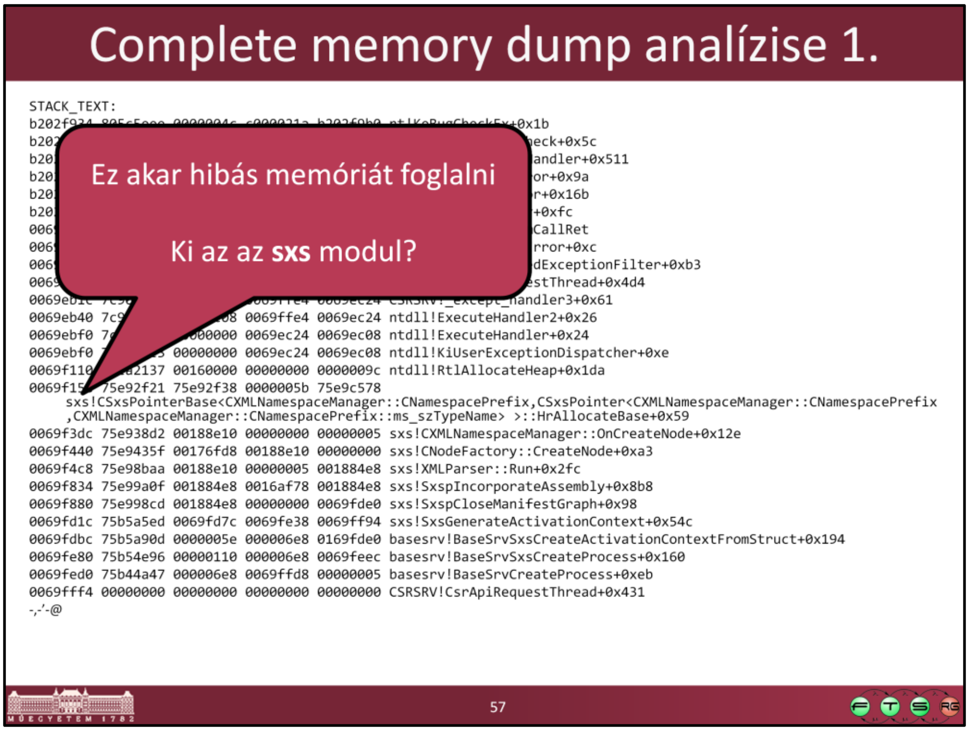
- Az adott gépen nem lehetett teljes memória dumpot választani
- ???
- Windows XP SP2, 32 bit, 4GB RAM
  - KB274598 Complete memory dumps are not available on computers that have 2 or more gigabytes of RAM
- Boot.ini: /MaxMem=2000 segítségével memória limitálása



Complete memory dump analízise 1.

```
EXCEPTION_RECORD:  0069ec08 -- (.exr 0x69ec08)
ExceptionAddress: 7c9106c3
  (ntdll!RtlAllocateHeap+0x000001da)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 00000001
   Parameter[1]: 75e9193e
Attempt to write to address 75e9193e
```

Problémát okozó utasítás

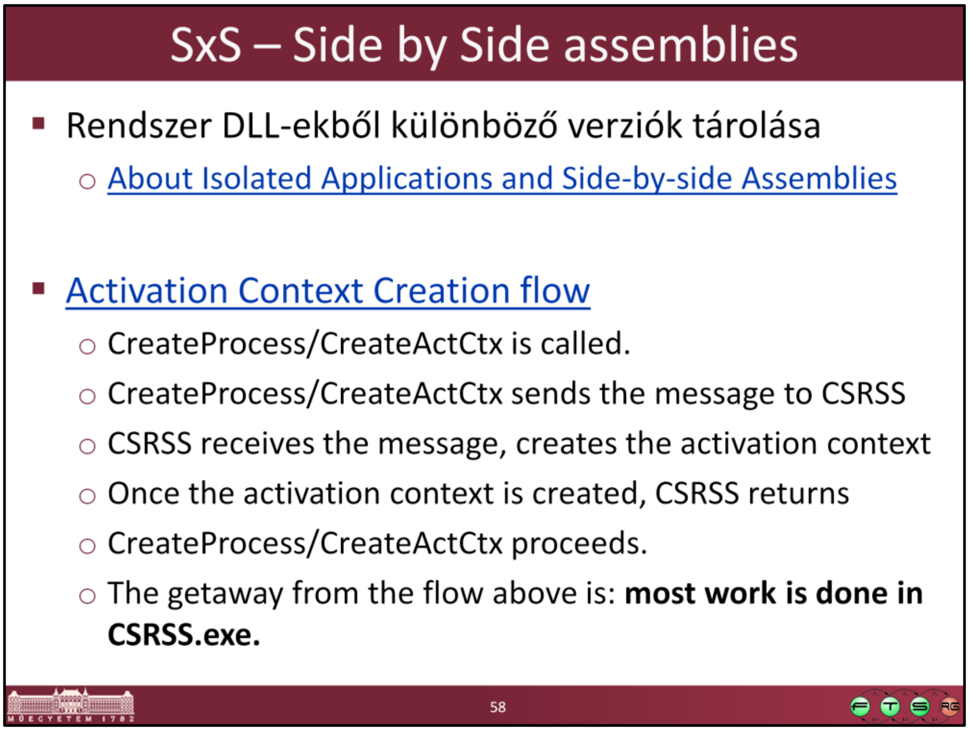


Complete memory dump analízise 1.

```
STACK_TEXT:
b202f934 805c5eee 0000004c c000021a b202f9b0 nt!KeBugCheckEx+0x1b
b202                                          eck+0x5c
b20                                           andler+0x511
b20                                           or+0x9a
b20                                           r+0x16b
b20                                           +0xfc
006                                           CallRet
006                                           rror+0xc
006                                           dExceptionFilter+0xb3
0069                                          estThread+0x4d4
0069eb1c 7c9              0069ffe4 0069ec24 CSRSRV!_except_handler3+0x61
0069eb40 7c9           08 0069ffe4 0069ec24 ntdll!ExecuteHandler2+0x26
0069ebf0 7c      00000000 0069ec24 0069ec08 ntdll!ExecuteHandler+0x24
0069ebf0 7      3 00000000 0069ec24 0069ec08 ntdll!KiUserExceptionDispatcher+0xe
0069f110   a2137 00160000 00000000 0000009c ntdll!RtlAllocateHeap+0x1da
0069f15  75e92f21 75e92f38 0000005b 75e9c578
     sxs!CSxsPointerBase<CXMLNamespaceManager::CNamespacePrefix,CSxsPointer<CXMLNamespaceManager::CNamespacePrefix
     ,CXMLNamespaceManager::CNamespacePrefix::ms_szTypeName> >::HrAllocateBase+0x59
0069f3dc 75e938d2 00188e10 00000000 00000005 sxs!CXMLNamespaceManager::OnCreateNode+0x12e
0069f440 75e9435f 00176fd8 00188e10 00000000 sxs!CNodeFactory::CreateNode+0xa3
0069f4c8 75e98baa 00188e10 00000005 001884e8 sxs!XMLParser::Run+0x2fc
0069f834 75e99a0f 001884e8 0016af78 001884e8 sxs!SxspIncorporateAssembly+0x8b8
0069f880 75e998cd 001884e8 00000000 0069fde0 sxs!SxspCloseManifestGraph+0x98
0069fd1c 75b5a5ed 0069fd7c 0069fe38 0069ff94 sxs!SxsGenerateActivationContext+0x54c
0069fdbc 75b5a90d 0000005e 000006e8 0169fde0 basesrv!BaseSrvSxsCreateActivationContextFromStruct+0x194
0069fe80 75b54e96 00000110 000006e8 0069feec basesrv!BaseSrvSxsCreateProcess+0x160
0069fed0 75b44a47 000006e8 0069ffd8 00000005 basesrv!BaseSrvCreateProcess+0xeb
0069fff4 00000000 00000000 00000000 00000000 CSRSRV!CsrApiRequestThread+0x431
-,-'-@
```

Ez akar hibás memóriát foglalni

Ki az az **sxs** modul?



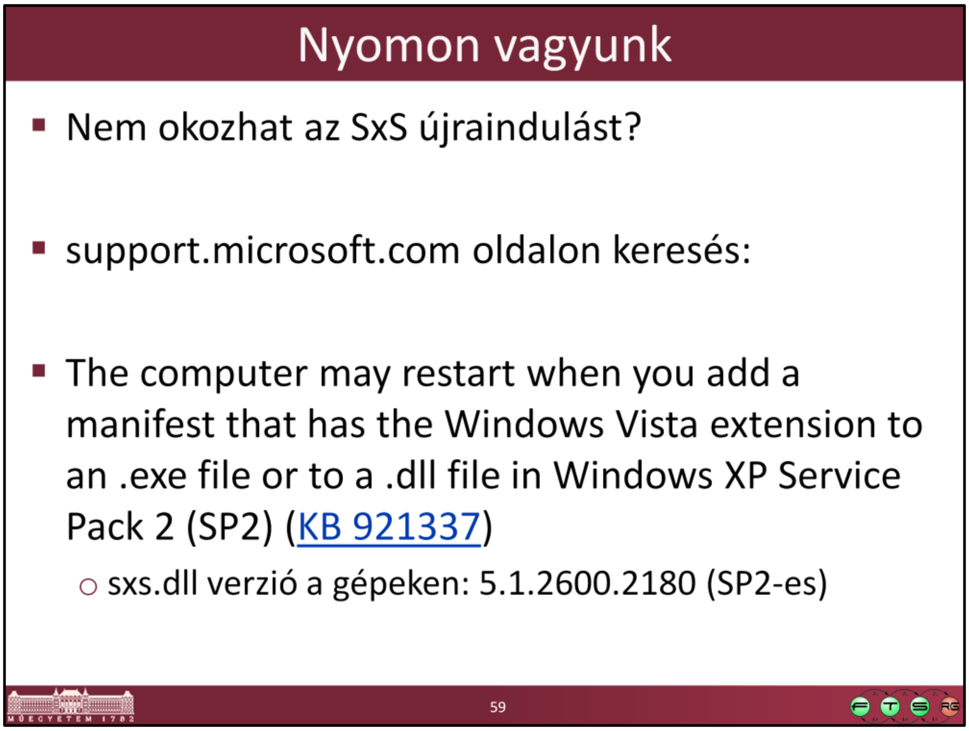
SxS – Side by Side assemblies

- Rendszer DLL-ekből különböző verziók tárolása
  - About Isolated Applications and Side-by-side Assemblies
- Activation Context Creation flow
  - CreateProcess/CreateActCtx is called.
  - CreateProcess/CreateActCtx sends the message to CSRSS
  - CSRSS receives the message, creates the activation context
  - Once the activation context is created, CSRSS returns
  - CreateProcess/CreateActCtx proceeds.
  - The getaway from the flow above is: **most work is done in CSRSS.exe.**

58

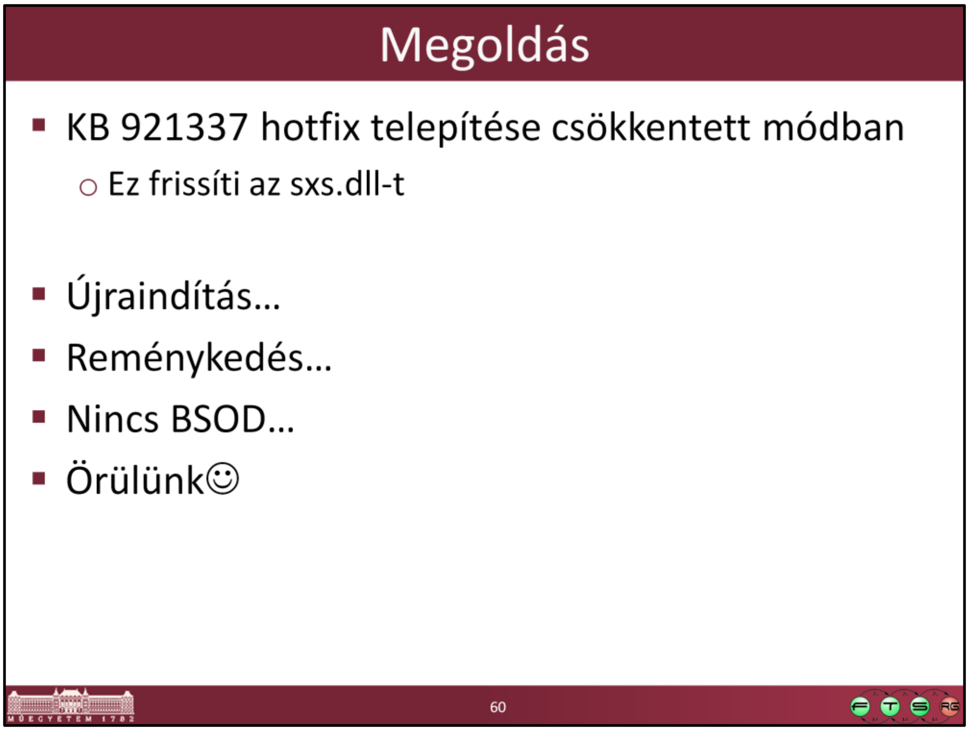
MSDN. „**About Isolated Applications and Side-by-side Assemblies**”, URL: http://msdn.microsoft.com/en-us/library/aa374029%28v=vs.85%29.aspx

Junfeng Zhang's Windows Programming Notes. „**Activation Context Creation flow**”, 12 Jun 2007. URL: http://blogs.msdn.com/b/junfeng/archive/2007/06/12/activation-context-creation-flow.aspx



Nyomon vagyunk

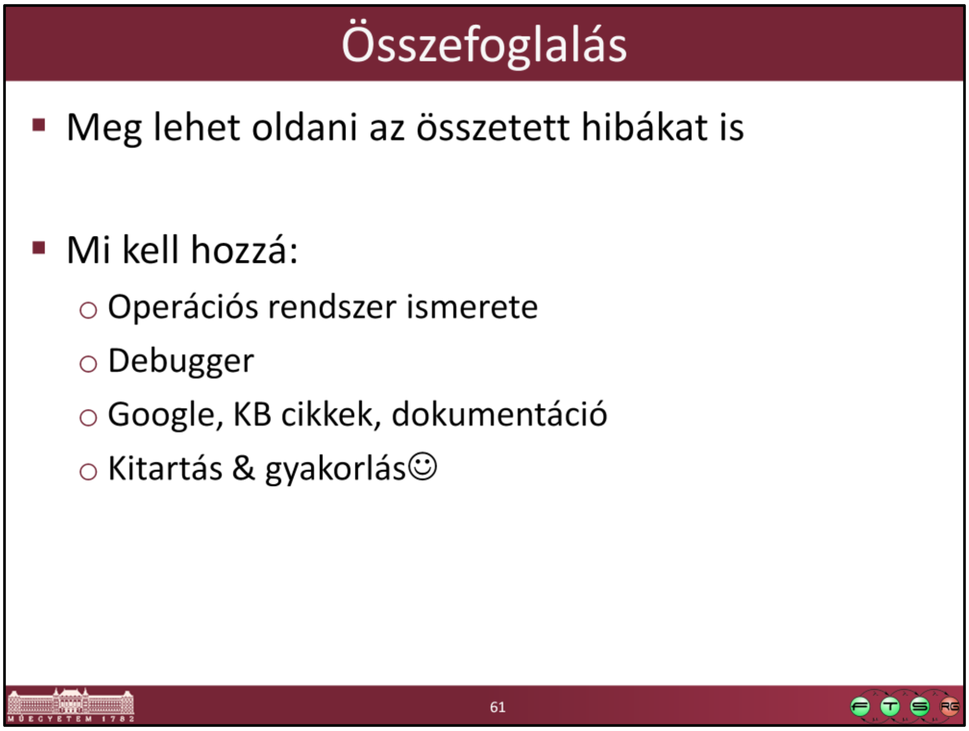
- Nem okozhat az SxS újraindulást?
- support.microsoft.com oldalon keresés:
- The computer may restart when you add a manifest that has the Windows Vista extension to an .exe file or to a .dll file in Windows XP Service Pack 2 (SP2) (KB 921337)
  - sxs.dll verzió a gépeken: 5.1.2600.2180 (SP2-es)



Megoldás

- KB 921337 hotfix telepítése csökkentett módban
  - Ez frissíti az sxs.dll-t

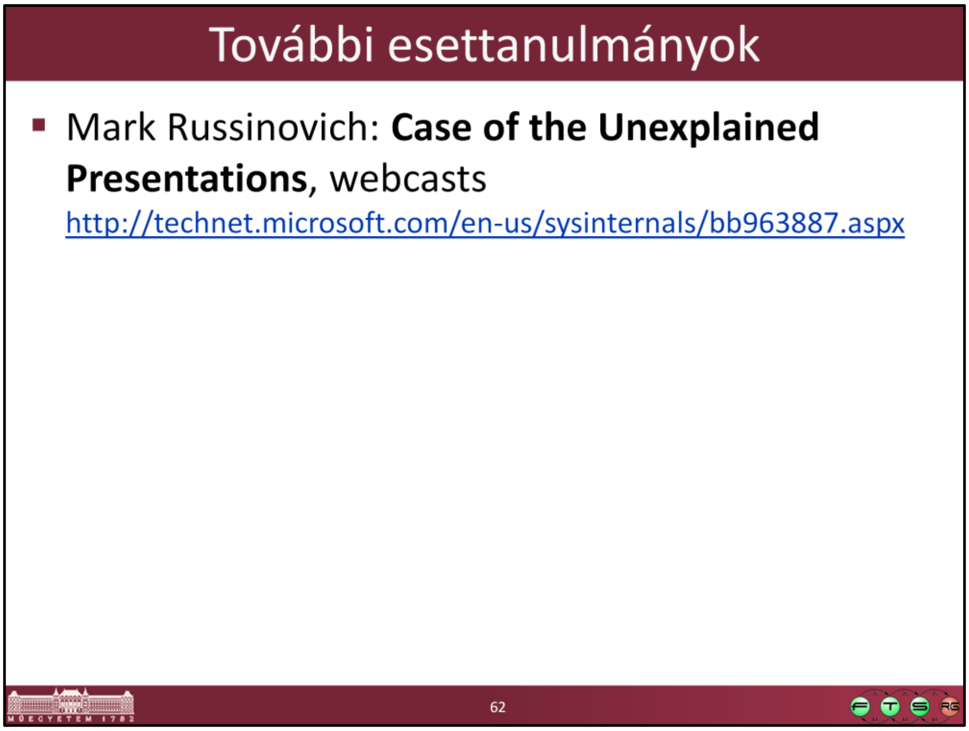
- Újraindítás…
- Reménykedés…
- Nincs BSOD…
- Örülünk☺



Összefoglalás

- Meg lehet oldani az összetett hibákat is

- Mi kell hozzá:
  - Operációs rendszer ismerete
  - Debugger
  - Google, KB cikkek, dokumentáció
  - Kitartás & gyakorlás☺



További esettanulmányok

- Mark Russinovich: **Case of the Unexplained Presentations**, webcasts
  http://technet.microsoft.com/en-us/sysinternals/bb963887.aspx