



# Debugging.TV

Frame 0x14

Presenter: Dmitry Vostokov

MEMORY DUMP ANALYSIS SERVICES

[DumpAnalysis.com](http://DumpAnalysis.com)

Including Crash and Hang Analysis Audit, Training and Seminars

Sponsors

**OPENTASK**

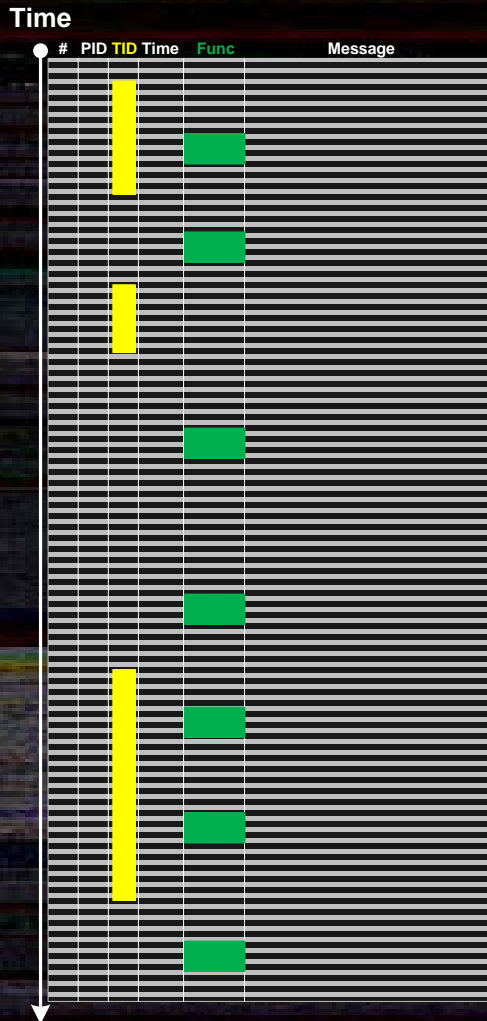
Iterative and Incremental Publishing

# Topics

- Thread
- Adjoint Thread
- Software Trace Analysis Patterns
- Examples (Procmon, CDFAnalyzer, Excel)



# Adjoint Thread

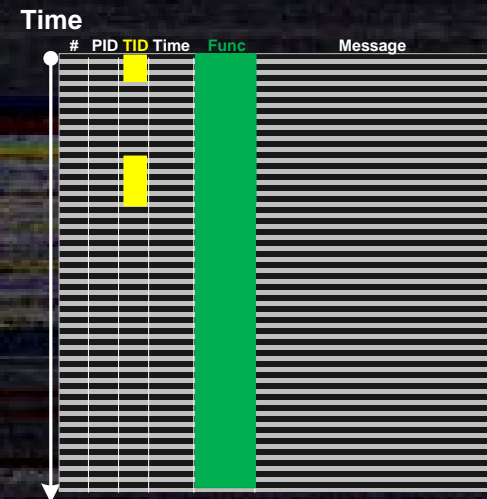


{ msg | Func = 'Text' }

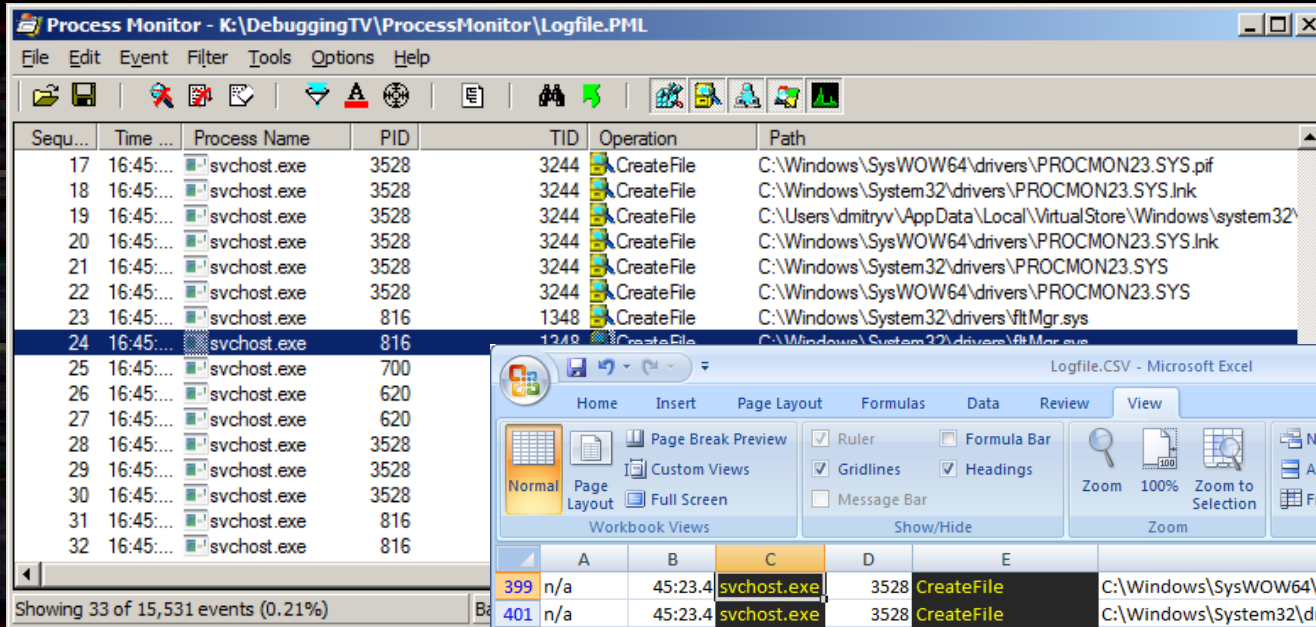
```
SELECT * FROM Messages
WHERE Messages.Func = 'CreateProcess'
```

$\langle T|A \rangle \leftrightarrow \langle A|T \rangle$

From mathematics: Adjoint



# Log Analysis Patterns

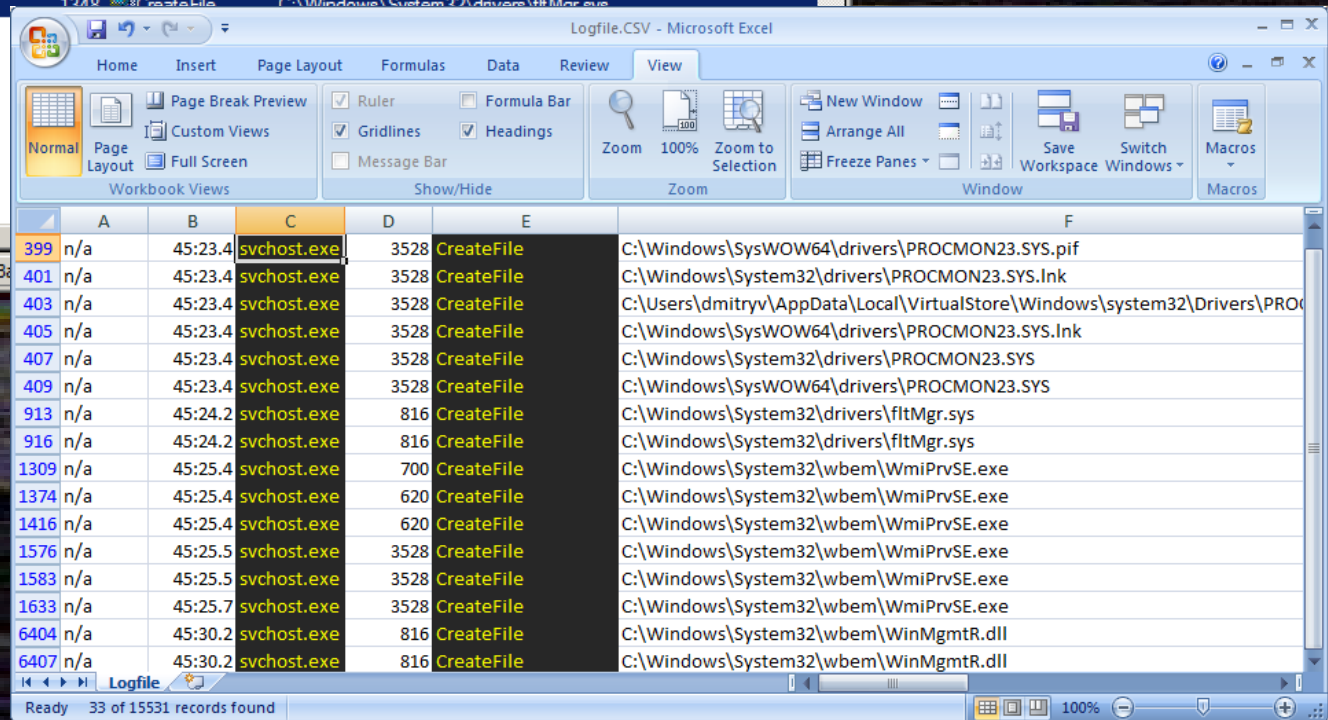


Process Monitor - K:\DebuggingTV\ProcessMonitor\Logfile.PML

Sequ...	Time ...	Process Name	PID	TID	Operation	Path
17	16:45:...	svchost.exe	3528	3244	CreateFile	C:\Windows\SysWOW64\drivers\PROCMON23.SYS.pif
18	16:45:...	svchost.exe	3528	3244	CreateFile	C:\Windows\System32\drivers\PROCMON23.SYS.Ink
19	16:45:...	svchost.exe	3528	3244	CreateFile	C:\Users\dmitryv\AppData\Local\VirtualStore\Windows\system32\
20	16:45:...	svchost.exe	3528	3244	CreateFile	C:\Windows\SysWOW64\drivers\PROCMON23.SYS.Ink
21	16:45:...	svchost.exe	3528	3244	CreateFile	C:\Windows\System32\drivers\PROCMON23.SYS
22	16:45:...	svchost.exe	3528	3244	CreateFile	C:\Windows\SysWOW64\drivers\PROCMON23.SYS
23	16:45:...	svchost.exe	816	1348	CreateFile	C:\Windows\System32\drivers\fltMgr.sys
24	16:45:...	svchost.exe	816	1248	CreateFile	C:\Windows\System32\drivers\fltMgr.sys
25	16:45:...	svchost.exe	700			
26	16:45:...	svchost.exe	620			
27	16:45:...	svchost.exe	620			
28	16:45:...	svchost.exe	3528			
29	16:45:...	svchost.exe	3528			
30	16:45:...	svchost.exe	3528			
31	16:45:...	svchost.exe	816			
32	16:45:...	svchost.exe	816			

Showing 33 of 15,531 events (0.21%)

- Discontinuity
- Time Delta
- Anchor Messages
- Fiber Bundle



Logfile.CSV - Microsoft Excel

	A	B	C	D	E	F
399	n/a	45:23.4	svchost.exe	3528	CreateFile	C:\Windows\SysWOW64\drivers\PROCMON23.SYS.pif
401	n/a	45:23.4	svchost.exe	3528	CreateFile	C:\Windows\System32\drivers\PROCMON23.SYS.Ink
403	n/a	45:23.4	svchost.exe	3528	CreateFile	C:\Users\dmitryv\AppData\Local\VirtualStore\Windows\system32\Drivers\PRO
405	n/a	45:23.4	svchost.exe	3528	CreateFile	C:\Windows\SysWOW64\drivers\PROCMON23.SYS.Ink
407	n/a	45:23.4	svchost.exe	3528	CreateFile	C:\Windows\System32\drivers\PROCMON23.SYS
409	n/a	45:23.4	svchost.exe	3528	CreateFile	C:\Windows\SysWOW64\drivers\PROCMON23.SYS
913	n/a	45:24.2	svchost.exe	816	CreateFile	C:\Windows\System32\drivers\fltMgr.sys
916	n/a	45:24.2	svchost.exe	816	CreateFile	C:\Windows\System32\drivers\fltMgr.sys
1309	n/a	45:25.4	svchost.exe	700	CreateFile	C:\Windows\System32\wbem\WmiPrvSE.exe
1374	n/a	45:25.4	svchost.exe	620	CreateFile	C:\Windows\System32\wbem\WmiPrvSE.exe
1416	n/a	45:25.4	svchost.exe	620	CreateFile	C:\Windows\System32\wbem\WmiPrvSE.exe
1576	n/a	45:25.5	svchost.exe	3528	CreateFile	C:\Windows\System32\wbem\WmiPrvSE.exe
1583	n/a	45:25.5	svchost.exe	3528	CreateFile	C:\Windows\System32\wbem\WmiPrvSE.exe
1633	n/a	45:25.7	svchost.exe	3528	CreateFile	C:\Windows\System32\wbem\WmiPrvSE.exe
6404	n/a	45:30.2	svchost.exe	816	CreateFile	C:\Windows\System32\wbem\WinMgmtR.dll
6407	n/a	45:30.2	svchost.exe	816	CreateFile	C:\Windows\System32\wbem\WinMgmtR.dll

Ready 33 of 15531 records found

Complex adjoint  
threads:  
nested filtering

# Suggested Reading

Articles on adjoint threading:

- [Extending Multithreading to Multibraiding](#)
- [What is an Adjoint Thread?](#)

Tools supporting adjoint threading:

- [Process Monitor](#)
- [Citrix CDFAnalyzer](#)

# !Ad Hardcore Software Support Training

November 2-5, 2012	<u>Accelerated Windows Software Trace Analysis</u>
November 16-26, 2012	<u>Accelerated Windows Memory Dump Analysis</u>
December 7-10, 2012	<u>Accelerated Windows Malware Analysis</u>
December 17, 2012	<u>Philosophy of Software Diagnostics</u> (FREE)
Early 2013	The New Old Debugging

# Debugging<sup>3</sup>

Coming soon

# Debugging.TV

Now on YouTube!

<http://www.youtube.com/DebuggingTV>