

How to Read a Windows SPK Crash Report

in less than 1 minute

Resolving system level crashes (aka: blue screens) under Windows has been difficult, if not impossible, for most users. This is because the data needed to resolve crashes, as with all operating systems, is cryptic, cumbersome, and few are trained to interpret it. The Alexander SPK for Windows automates the recovery of the system following the crash, analyzes the event, and reports the event and cause to one or more systems administrators. All the administrator needs to do is to read the crash file to see the faulty driver clearly identified.

The following pages will walk you through some of the data presented in the SPK Crash Reports.

Trademarks property of their respective owners.

The screenshot shows the Alexander SPK Manager Console interface. The main window is titled 'Crash Report' and displays the following information:

- SPK Station: Import
- SPK Center: scott
- Administrator: Nick Charles
- Date/Time: Thu May 23 07:11:38 2002
- Downtime: 3 min, 52 sec
- Application: product3.exe
- Crash Driver: driver1.sys (driver1+257c8)

The 'Crash Driver' field is highlighted with a blue box and an arrow pointing to it from the 'Application' box. Below the 'Crash Driver' field, the 'Report Summary' section contains the following text:

SPK Station name "Import" which reports Center "scott", crashed on Thu May 23 07:11:38 2002 while executing "product3.exe".

The fact that driver "driver1.sys" (driver1+257c8) was in control of the processor at the exact time of the crash makes it the primary suspect.

Brief analysis:

Options: Make Report Contact I

SPK Log

Reading in report 20020523122318.axd... Done
Reading in report Sample SPK Report 1.axd... Done

Application

The **Application** is what product was running in **User Mode**. This could be a word processor or any such application with direct access by the end user. User Mode applications do not directly cause system failures. For that, move down to the **Crash Driver**.

Crash Driver

The Crash Driver window displays the name of the driver that failed while in control of the processor. Since the system crashed running code belonging to this driver, it becomes the #1 suspect. If it is a 3rd party product, it is even more likely to be responsible.

In this example, **driver1.sys** is identified (Please note that this is a report from a real-world crash event, however, many actual product and company names were changed to more generic vendor(n), product(n), etc.)

Most often, the driver reported in this window is a 3rd party driver, however, if a Microsoft® driver is listed, then look at the stack information to see if any third party drivers are listed there (information on how to do this appears further down in this report). It is rare that the system will crash in an MS driver.

Remember that drivers operate in **Kernel Mode** and Kernel Mode (as opposed to User Mode which is where a word processor would run) problems can cause complete system failures. Even in the unusual case where it (Crash Driver) turns out not to be the cause, it remains that it was the code that actually failed.

Alexander SPK™ System Protection Kit™
for Windows Servers and PCs

Support User Guide Copyright 1995-2002 Alexander LAN, Inc.
Version 5.00 (Build 60)

SPK Center
scott

Add Edit Delete

SPK Station
Import
SCOTT

Crash Report #Sample SPK Report

SPK Station: Import
SPK Center: scott
Administrator: Nick Charles
Date/Time: Thu May 23 07:11:58 2002
Downtime: 3 min, 52 sec
Application: product3.exe
Crash Driver: \\??C:\PROGRAM~1\COMMON~1\vendor1\20020521.016
\\driver1.sys
Timestamp: Tue Feb 26 14:38:48 2002 (3C79E449)

Crash Driver Information

By scrolling through the window you will also see the exact location on the hard drive where the driver is stored which will usually also tell you the vendor name (in this case a company called **vendor1**) and what date stamp it has.

Report Summary:
SPK Station named "Import" which reports to SPK Center "scott", crashed on Thu May 23 07:11:58 2002 while executing "product3.exe".
The fact that driver "driver1.sys (driver1+257)" was in control of the processor at the exact time of the crash makes it the primary suspect.
Brief analysis:

Options: Make Report Contact Info Show Details

SPK Log
Reading in report 20020523122318.axd... Done
Reading in report Sample SPK Report 1.axd... Done

Guide
This window displays the names of the reports that pertain to the selected SPK Station. The numeric string is based upon the date and time of the crash event, thus, 20020523122318 represents the year 2002, May 23, at 12:23:18.
To view a Crash Report, click on one of the files and the SPK Manager's central working area will change from switch settings to crash report, displaying the

The screenshot shows the Alexander SPK Manager Console interface. The main window is titled "Alexander SPK™ System Protection Kit™ for Windows Servers and PCs". It includes a "Support" and "User Guide" button, and a copyright notice for 1995-2002 Alexander LAN, Inc. The version is 5.00 (Build 60).

The interface is divided into several panes:

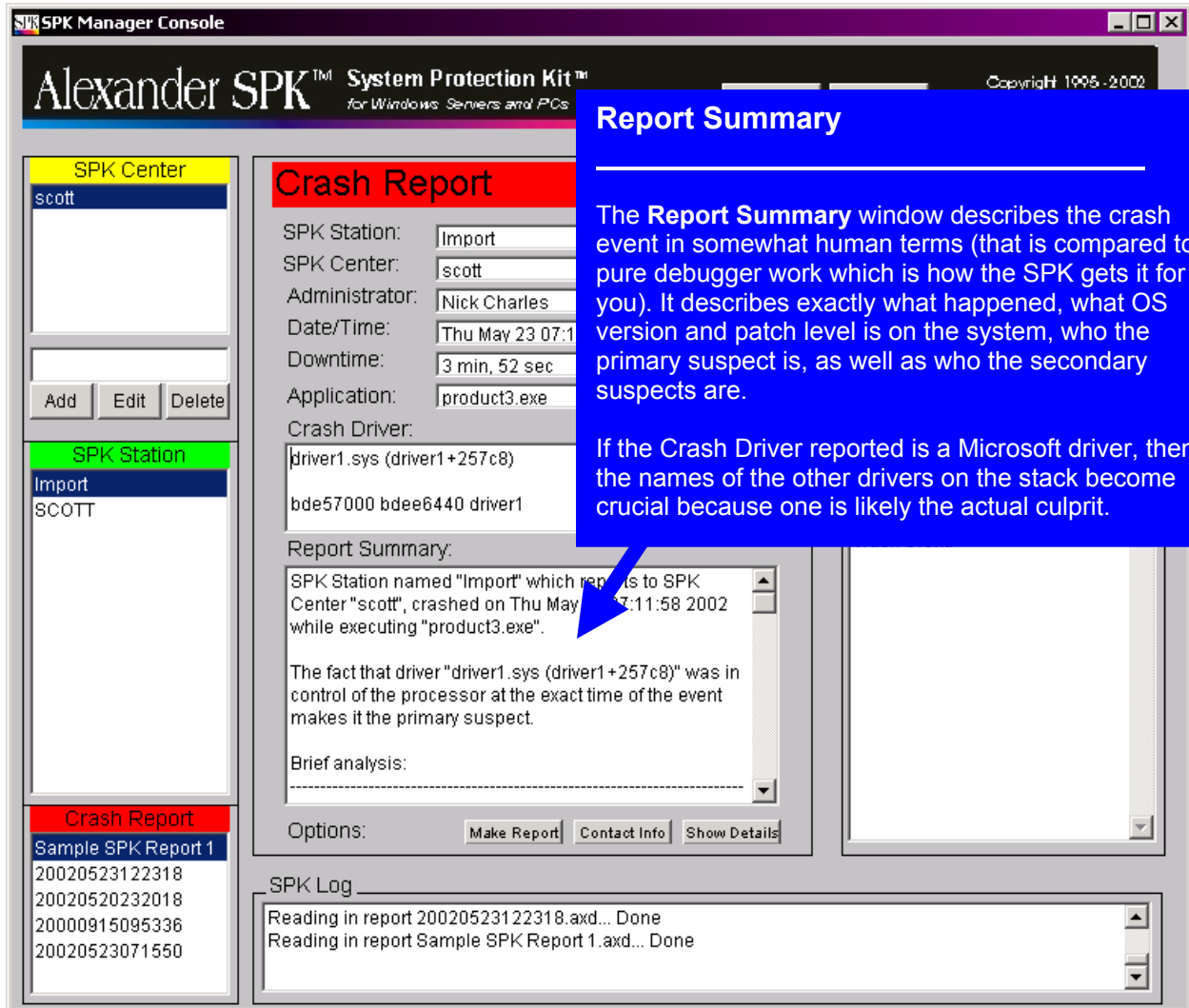
- SPK Center:** Lists the center name "scott" and has "Add", "Edit", and "Delete" buttons.
- SPK Station:** Lists stations "Import" and "SCOTT".
- Crash Report:** Displays details for a crash event. A blue arrow points to the "Image path" field, which contains the text: `\\?\C:\PROGRAM~1\COMMON~1\vendor1\20020521.016\driver1.sys`. The "Report Summary" section states: "SPK Station named 'Import' which reports to SPK Center 'scott', crashed on Thu May 23 07:11:58 2002 while executing 'product3.exe'."
- Guide:** Provides instructions on how to view a crash report.
- Crash Report List:** A table listing report IDs: "Sample SPK Report 1", "20020523122318", "20020520232018", "20000915095336", and "20020523071550".

Vendor Information

This is where the driver that crashed resides on the machine. You will notice the vendor name **vendor1**. If this is a 3rd party vendor, then these are the people to report to. In the case of every third party driver, they are almost guaranteed to be at fault. The likelihood that they can prove their innocence is low, especially in light of the incriminating data presented in your crash report.

They would be hard pressed to argue with you because this data is based upon debugging level technology: it's like trying to argue against a photograph of their hands in the cookie jar. Actually, 3rd party vendors like seeing these reports because it greatly simplifies bug resolution.

You will find that most crash events will look like this.



Alexander SPK™ System Protection Kit™
for Windows Servers and PCs

Support User Guide
Copyright 1995-2002 Alexander LAN, Inc.
Version 5.00 (Build 60)

SPK Center
scott

Add Edit Delete

SPK Station
Import
SCOTT

Crash Report
Sample SPK Report 1
20020523122318
20020520232018
20000915095336
20020523071550

Stack Report

```
Module "driver2" before "0x257c8"  
Module "driver2" before "0x262f4"  
Module "driver2" before "0x1bb5b"  
Module "driver2" before "0x15191"  
Module "driver2" before "0xa9e"  
Module "driver1" before "0x70e6"  
Module "driver1" before "0x1dbc9"  
Module "driver1" before "0x1e0ab"  
Module "driver1" before "0x1d375"  
Module "driver1" before "0x1d1e2"  
Module "driver1" before "0x852"  
Module "driver1" before "0x2426"  
Module "driver1" before "0x90b"  
Module "driver1" before "0x1cd95"  
Module "driver7" before "EventObject"
```

ChildEBP	RetAddr	Args to Child
870cd630	804689af	00000000 e5b3e043 0
870cd630	bde7c7c8	00000000 e5b3e043 0
870cd6ec	bde7d2f4	e5b3d6b4 870cd76c e
870cd730	bde72b5b	870cd76c 00000000 8
870cd750	bde6c191	870cd76c e2279fec 8
870cd7bc	bde57a9e	bdff0ca90 00000170 e

Options: Make Report Contact Info

SPK Log
Reading in report 20020523122318.axd... Done
Reading in report Sample SPK Report 1.axd... Done

Stack Information

By scrolling through this screen you will see all drivers that were on the stack at the time of the crash. In this case, driver2, driver1, and then driver7 were active on the stack. In the actual crash event that this report was taken from, all three of the drivers listed here were from the same vendor and were part of the same product.

If the main SPK Crash Report Window listed a Windows module as causing the crash, and this Stack Report Window showed more of the same, then it becomes crucial to see any 3rd party drivers that were active on the stack. Note that the stack grew downwards, therefore driver7 was active after driver1 and driver2.

Alexander SPK™ System Protection Kit™
for Windows Servers and PCs

Support User Guide Copyright 1995-2002 Alexander LAN, Inc. Version 5.00 (Build 60)

SPK Center
scott

SPK Station
Import
SCOTT

Crash Report
Sample SPK Report 1
20020523122318
20020520232018
20000915095336
20020523071550

Drivers and Processes Report

System Driver and Image Summary

Base	Code Size	Data Size	Image Name	Creation Time
80400000	13d7c0 (1270 k)	5d900 (375 k)	ntoskrnl.exe	Fri Apr 13 18:06:33 2001
80062000	101e0 (65 k)	3dc0 (16 k)	hal.dll	Tue Nov 28 23:34:11 2000
f6810000	1760 (6 k)	1000 (4 k)	BOOTVID.dll	Wed Nov 03 20:24:33 1999
bffd8000	21f00 (136 k)	59a0 (23 k)	ACPI.sys	Wed Oct 25 16:59:00 2000
f69c8000	740 (2 k)	560 (2 k)	WMILIB.SYS	Sat Sep 25 14:36:47 1999
f6400000	bf40 (48 k)	22e0 (9 k)	pci.sys	Thu Mar 01 19:38:34 2001
f6410000	9aa0 (39 k)	1900 (7 k)	isapnp.sys	Mon Aug 28 01:40:00 2000
f69c9000	320 (1 k)	520 (2 k)	pciide.sys	Mon Aug 28 01:39:25 2000
f6680000	42e0 (17 k)	e80 (4 k)	PCIINDEX.SYS	Mon Aug 28 01:39:25 2000
f6688000	64e0 (26 k)	a40 (3 k)	MountMgr.sys	Mon Aug 28 01:42:41 2000
bffbb000	192c0 (101 k)	2b00 (11 k)	ftdisk.sys	Mon Nov 22 14:36:23 1999
f6900000	12e0 (5 k)	640 (2 k)	Diskperf.sys	Thu Sep 30 20:30:40 1999
f6902000	d80 (4 k)	b40 (3 k)	dmload.sys	Mon Aug 28 01:42:29 2000
bff99000	1a720 (106 k)	6c40 (28 k)	dmio.sys	Mon Aug 28 01:42:30 2000
f6814000	21a0 (9 k)	720 (2 k)	PartMgr.sys	Thu Oct 14 20:59:16 1999
f6818000	30e0 (13 k)	a20 (3 k)	cpqarray.sys	Wed Feb 07 14:49:28 2001
bff87000	f420 (62 k)	23a0 (9 k)	SCSIPORT.SYS	Fri Nov 10 21:52:30 2000
bff72000	11c80 (72 k)	2c20 (12 k)	atapi.sys	Thu Sep 14 22:18:07 2000
f681c000	3120 (13 k)	c00 (3 k)	symc810.sys	Sat Sep 25 15:11:49 1999
f6420000	bd00 (48 k)	3c40 (16 k)	cpq32fs2.sys	Mon Nov 05 16:47:06 2001
f6430000	74e0 (30 k)	980 (3 k)	lp6nds35.sys	Mon Aug 28 04:01:34 2000
f6690000	45e0 (18 k)	1a80 (7 k)	symc8xx.sys	Fri Mar 30 12:01:54 2001
f6698000	3e20 (16 k)	10a0 (5 k)	sym_hi.sys	Sat Sep 25 15:11:49 1999

Options:

SPK Log
Reading in report 20020523122318.axd... Done
Reading in report Sample SPK Report 1.axd... Done

Drivers and Process Report

This report shows all drivers and processes that were active when the system crash occurred. Details include memory address, code size, data size, driver name, as well as the date and time stamp.