

Corrupt and Shutdown Dirty EVTX Log Files: A Comparison of Recovery Using the Microsoft Event Viewer Versus Ipswitch's LogHealer Technology

As the Microsoft Windows Vista, Windows Server 2008, and Windows 7 operating systems become increasingly more widely adopted, so too does their new logging format, the EVTX log file. Properly saved EVTX log files can typically be opened without issue in the Microsoft Windows Event Viewer or a third-party tool like WhatsUp Event Analyst or WhatsUp Event Rover. However, corrupt and/or "shutdown dirty" EVTX files raise a serious issue for the network administrator or a forensic examiner tasked to view their contents.

In some, but not all cases, the Microsoft Event Viewer in Windows Vista and Windows Server 2008 can open an EVTX file reclaimed from a shutdown dirty system, such as from a computer where the "plug was pulled" to start a forensic investigation. However, the Microsoft Event Viewer attempts to repair data elements in the file **without prompting or confirming this action with the user of the program.**

🕘 Organize 👻 📗 Views	*							0
Favorite Links Documents Pictures Music Recently Changed Searches Public	Name A O App Dirty	 Date modified 6/16/2009 3:42	PM	Type Saved Ever	t Log	Size 6	8 KB	
Folders 🔥								

This behavior is reproduced readily and shown below in the series of screenshots:

Figure 1 - An application EVTX log from a machine that was shutdown dirty. Notice the date modified timestamp of June 16th, 2009.

🛃 Event Viewer			_ _ X
File Action View Help			
 Free Lines Custom Views Custom Views Custom Views Custom Views Custom Views Security Security Security Security Setup System Forwarded Events Applications and Services Logs DFS Replication Hardware Events Internet Explorer Key Management Service Microsoft Subscriptions 	Event Viewer (Local)	Actions	Lancel

Figure 2 - The Microsoft Event Viewer on Windows Vista has started. The application EVTX log file can now be opened and read by the Microsoft Event Viewer program.

📙 BadE¥TXTest) ×
😋 🕞 🗸 🔸 Local Disk	:(C:) ▼ BadEVTXTest	👻 🔯 Search		2
🕒 Organize 👻 📗 Views	-			0
Favorite Links Documents Fictures Music Recently Changed Searches More >>	App Dirty	Vate modified V Type 7/16/2009 1:02 PM Saved Ever	t Log 68 KB	
Folders I item				

Figure 3 - A return to Windows Explorer shows that the Date Modified timestamp of the file has changed to the current date, July 16th, 2009. The Microsoft Event Viewer modified the EVTX file with no prompting or notice to the administrator!

Obviously, this raises serious implications regarding evidence management and could ultimately compromise an otherwise well-conducted investigation.

Ipswitch has pioneered a new approach to the recovery of corrupt and shutdown dirty EVTX log data that is refered to as LogHealer Technology. WhatsUp Event Rover is the first solution featuring this technology, which is incorporated into other WhatsUp Log Management products.

Rather than attempting to modify the original source file, when LogHealer detects a corruption in an EVTX file, it first prompts the administrator to repair it in a new location, so that the original file remains unmodified. This is shown in the next series of screenshots below:

O	ven	t Ro	ver																		
File	Edi	t Vi	ew.	Opti	ons	Gro	uping	s A	utor	mate	In	icide	nts	He	lp						
	X					÷	₽ taun	¹ 23 123	[-		; <u>-</u>	<u>v</u>	A	0					
					ioosi Oper File:	eaP naPi	revi eviou	ousl isly <u>S</u> idEV1	y S a ave	a ve ed Ev	d Ev vent l	ent Log- Dirtu	Log	to	Ope	n					
					- Iype:	ri 7 :	Applic	ation	1 les/i	meta	udata	from	r IV	IST	ΔΝΠ	TEX					
						Quicł	Filte	r This	s Lo	g By	Eve	nt ID									
																		ОК		Can	cel

Figure 4 – WhatsUp Event Rover is preparing to load the shutdown dirty Application EVTX file into memory. Because the log file is from a foreign network, we are electing to load log metadata from an alternate computer.



Figure 5 - LogHealer detects corruption in the EVTX file, and is prompting the administrator to perform a repair into a new file, leaving the original file unmodified.

Event Roy	ver D
1	Congratulations! The corrupt log file has been repaired and saved to a new file: C:\BadEVTXTest\App Dirty_repaired.evtx. Event Rover will now open the repaired file.
	ОК

Figure 6 - LogHealer makes the repairs in a new file on disk, and WhatsUp Event Rover now loads log records from the repaired file into memory.

📕 BadEVTXTest			_ 🗆 🗙
G 🕞 🗸 🕹 🗸 Local Dis	k(C:) ▼ BadEVTXTest	👻 🚱 Search	
🔄 Organize 👻 📗 Views	•		0
Favorite Links Documents Fictures Music Searches More >>	Name App Dirty App Dirty_repaired	• Date modified • Type • Size • 6/16/2009 3:42 PM Saved Event Log 68 KB 7/16/2009 1:12 PM Saved Event Log 68 KB 7/16/2009 1:13 PM HTML Document 4 KB	
Folders 🔨			
3 items			

Figure 7 - Windows Explorer shows the original file's Date Modified timestamp unchanged, with the new repaired version next to it in the same folder.

In some cases, Microsoft Event Viewer cannot open a corrupted log file, and instead displays the following dialog:

.og	
C:\BadEVTXTe	est\Othe The event log file is corrupted

While LogHealer technology remains in its infancy, we are pleased with its current ability to repair some log files that the Microsoft Event Viewer cannot, as well its ability to do so in a non-destructive manner. As the EVTX logging format becomes more widely adopted, we look forward to working with end users, network professionals, and forensic examiners to expand and improve upon this technology. Correspondence with Ipswitch's support and development team, as well as the submission of corrupt log files, are always welcome at http://www.whatsupgold.com/support.