Rescuing a corrupt NTFS partition (and giving Linux an n-th chance)

Alexander Sklar 12 Jul 2011 10:41 PM 2

A little while ago, I started getting bugchecks (BSOD). At first I didn't pay much attention to them, but as they started to occur more frequently I guess the writing was on the wall. The bugcheck code in question was STOP 0x7A - KERNEL_DATA_INPAGE_ERROR. Well, what the heck does that mean, you say?

From MSDN:

> This Stop message indicates that the requested page of kernel data from the paging file could not be read into memory. This Stop message is usually caused by a bad block (sector) in a paging file, a virus, a disk controller error, or failing RAM. In rare cases, it is caused when nonpaged pool resources run out. It is also caused by defective hardware.

Uh-oh, that can't be good. Either I had been pwned, or I would have had to replace my hard drive, hdd controller or my memory. That sounds like it costs more than 0 dollars. A virus seemed unlikely as I always run Forefront Client Security. At that point I thought, "what the hay, it's Friday night, let's run `chkdsk /f /r` on this partition and see what it comes up with". Bad idea.

After grinding away for longer than I could stay awake, chkdsk had done "something" and happily rebooted (so when I woke up, the error message from chkdsk, ***if*** it existed, was no longer there). What I found when I went to check on the fruits of cutting-edge file-system checking utilities, were the most terrifying words, written in plain 80x25 text-mode:

> "Device I/O Error. Press Ctrl+Alt+Del to reboot"

"Um…yeah…can we go back to when things were kind of ok and I could access my files? that'd be great, kthxbai" - I thought to myself. Alas, the damage was done. It was not well. I went to a not-so-local electronics store and got myself a Seagate Momentus XT 500 GB hybrid SSD. Cool stuff. I also got a 2.5" HDD enclosure to connect my failing drive through USB for $6, quite a bargain methinks.

With some bing-ing and the helpful assistance of some of my coworkers, I was referred to ddrescue. It is essentially tool that will take a byte-for-byte image of your disk/partition, ignoring whatever filesystem inconsistencies the volume might have. The output of that process is a huge binary file (as big as the partition you're trying to recover, which in my case was ~300 GB) containing the volume's raw data. Easy enough, right? maybe, but definitely not for the average home user. First, you need to boot into Linux ("WTF, I thought you worked for Micro$0ft". Yeah, I do, get over it). To me that meant running Linux from a USB thumb drive (I couldn't be bothered to install Linux on my machine if I'm only going to use it to get my data out,).

So after a quick visit to PenDriveLinux.com and borrowing a thumb drive from the Development Lead responsible for Storage and File systems (hey, if there's anybody who can communicate with ~~the dead~~ NTFS, it must be him!), I had a Ubuntu "LiveCD" USB drive.

I booted into Linux, and at first the graphical environment did not appear. I remembered from my Unix Sysadmin days that ctrl+Alt+Backspace takes you back and from the console, where the window system is still spewing a bunch of info. Well, it seems Linux wanted to read from my attached failing drive. "Fine, here, I'll disconnect it", and X Window system resumed doing actual useful stuff. I was then presented with a minimalist but functional desktop, complete with Wi-Fi connectivity, Firefox ("ew"), etc. One of the things I did not get used to (read: hated) during my stay on Ubuntu was the fact that the window controls (maximize, minimize, close) are on the left of the application title bar. Apparently Apple is an easier virus to catch than I had thought.

Anyway, I went on to the ddrescue website to download it. But wait, this is Linux, you don't download an installer or anything like that. No, you download a .tar.gz file, open a console window, run *gunzip* and *tar xvf* on it (good thing I have a good memory and remembered this crap after 5+ years…). You are then left with a source tree. You run ./configure and make to actually get something useful you can execute. Then you read ddrescue's help file that describes how to use it. If No average Joe will be able to figure this out.

Anyway, back to the car chase. I also ran testdisk which is said to be able to restore partition tables, MFTs, etc. No such luck, it just told me that the MFT and the MFT mirror were both corrupt or something like that. No dice.

I then figure, I have an image of the faulty partition, might as well try to mount it from Linux. Linux tells me it hates me and that it can't/won't mount the partition because there are filesystem errors, and that I should run chkdsk from Windows. Seriously?

So, "whatever", I will try to mount it from Windows. I bing some more and find this little gem called Mount Image Pro (free trial for 14 days). This app installs a filesystem driver that essentially shows you a drive letter that mirrors the content of the image file you created with ddrescue. While it wasn't able to show me files at the root of the partition (since my MFT was hosed), it did show me a folder it called "Lost and Found". I went into that folder and lo and behold, 95% of the content I care about is there. Some files and folders have corrupt names, etc., but for the most part, my data is still there!

Now, on to double triple backup this stuff while I still have access to it.

Disclaimer: I do not receive any sort of payment for mentioning the software above, it just worked for me so I figured I'd share the data.

Comments

Joshua
14 Jul 2011 8:42 AM

Well since you had a Ubuntu live image, apt-get install ddrescue would have gotten it a lot faster than the source tarball. Ah well.

Alexander Sklar
14 Jul 2011 8:27 PM

@Joshua: yes, and the average Joe will likely not know how to do this either :)