Alternate Data Streams in NTFS

By kexugit

Archived: 2026-04-05 16:18:33 UTC

This blog has been a long time coming. There is a bit of confusion about the subject of ***alternate data streams*** (ADS) and no small amount of suspicion. So I want to take a few minutes to set the record straight on ADS.

A couple years ago I wrote a blog on NTFS attributes.

https://blogs.technet.com/b/askcore/archive/2010/08/25/ntfs-file-attributes.aspx

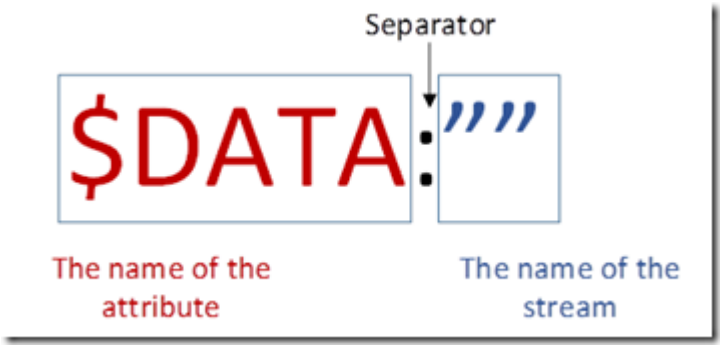
You might want to review that blog before continuing. I'll wait….

Welcome back.

One of the common questions I get is, "Robert. What is an alternate data stream?"

My reply is always the same, "It is a data stream that is alternate".

I don't mean to be smart aleck about it…but that's what it is. We know from my older blog that a file is divided up into 'attributes' and one of these attributes is $DATA or simply called the data attribute. It is the part of the file we put data into. So if I have a text file that says, "This is my text", then if I look at the data attribute, it will contain a stream of data that reads, "This is my text". However, this is the normal data stream, sometimes called the primary data stream, but more accurately it is called the ***unnamed data stream***. Why? Because it is a data stream that has no name. In the jolly land of programming it is referred to as $DATA:""



The name of the stream will appear between the quotes. Since this is an unnamed data stream, there isn't anything there.

Now that we know what the unnamed data stream looks like, we can start thinking in terms of alternates. Knowing that the place we normally store data is the unnamed data stream, if a stream has a name, it is alternate. So if I had a file with an ADS named SecondStream, its full name would be, $DATA:"SecondStream"

image

This is all good and fine, but unlike the unnamed data stream, we can't see the ADS. Or can we? The answer is, yes we can. But you have to use a method different than just opening the file in NotePad.

There are a number of tools out there that will allow you to view and manipulate ADS. One that Microsoft has provided for years is called STREAMS.EXE.

https://technet.microsoft.com/en-us/sysinternals/bb897440.aspx

STREAMS.EXE will display any ADS the file has.

```
C:\Tools\DiskTools\Streams>streams c:\test\TestFile2.txt

Streams v1.56 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\test\TestFile2.txt:
    :SecondStream:$DATA 27
```

The formatting is a little different.

image

STREAMS.EXE is fine, and I've used it for years, but with the release of Win8/Server 2012, I've discovered a new way of dealing with ADS….Windows PowerShell. Using the cmdlet, Get-Item, I can get more information than I did with STREAM.EXE.

clip_image008

The output shows not only the name of the ADS and its size, but also the unnamed data stream and its size is also listed (shown as :$DATA). And now that I know the name of the ADS, I can use the Get-Content cmdlet to query its contents.

```
PS C:\windows\system32> Get-Content -Path C:\test\TestFile2.txt -Stream SecondStream
This is the second stream
```

STREAM.EXE can't display what's actually in an ADS. Here's another trick that STREAM.EXE can't do….create data streams. Using Set-Content, I'll create a second ADS in the same file and add a line of text.

clip_image010

And again, we can query for the streams using Get-Item.

clip_image011

And finally, we can remove an ADS using the Remove-Item cmdlet.

clip_image012

Now we know what ADS is, how to query for ADS, how to create ADS, and how to delete ADS. So what is the big deal?

The big deal is that since ADS isn't easily visible, it has become a cute way to hide data. Unfortunately it has also been used in the past to hide malicious code. This is how ADS got a bad name. In fact, a number of people that approach me about ADS already know that they have files with alternate data streams and they think they are infected with viruses.

Calm down. The mere presence of an ADS doesn't mean that there is a problem. In fact, Microsoft uses ADS for a number of functions. I can almost guarantee that if you are reading this, you probably have some ADS on your computer. Let's take a look at a couple examples.

Internet Explorer: Ever download an executable file from the Internet and then get warned about it when you ran it? How does that work?

When the file is downloaded, IE slaps an ADS on it. The stream will store a tag that tells Windows what zone the file was downloaded from.


clip_image013

Look Familiar?

So using what I've learned so far, I can look at one of the files I've downloaded from the internet and see if there is an ADS on it.

```
PS C:\windows\system32> get-item -Path C:\test\testdownload.zip -Stream *


   FileName: C:\test\testdownload.zip

Stream                   Length
------                   ------
:$DATA                 55216795
Zone.Identifier              26
```

Yes, it is called 'Zone.Identifier'. And then we can query the contents of the 'Zone.Indentifier' ADS.

```
PS C:\windows\system32> get-content -Path C:\test\testdownload.zip -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
```

Now we know that the file was downloaded from zone 3. Using the zone chart we can see it came from the Internet zone.

> Value Setting
> ----------
> 0 My Computer
> 1 Local Intranet Zone
> 2 Trusted sites Zone

> 3 Internet Zone
> 4 Restricted Sites Zone

Notice that my test download file is in a test directory. This means I moved the file here from my download directory. This is the cool thing about ADS, since it is part of the file, it moves with the file. Even if I copied it, the ADS would be on the new copy as well.

Other Internet browsers use ADS in a similar fashion.

File Classification Infrastructure: FCI is very dependent on ADS. The way that the classification works is that it puts tags on your files that allows you to keep track of what the file was classified as, no matter what happens with the file. It could be edited, copied, moved to another server, and its classification tags remain intact.

Others: Office files and Outlook Express file use ADS. And it isn't limited to Microsoft programs. Numerous programs utilize the ADS functionality.

The point is that if you discover ADS on your system, it isn't necessarily a bad thing. And just blindly stripping these data streams out of files can actually do a great deal of harm.

And now that you have some tools to use for querying alternate data streams, they won't be so scary.

Thank you for your time and I hope this was educational.

Robert Mitchell
Senior Support Escalation Engineer
Microsoft Corp.

- **Anonymous**
  January 01, 2003
  ReFS is a different animal. It is meant to focus on reliability and as such only carries a subset of the functionality that NTFS provides. As such, there will be some scenarios that NTFS is a better fit and some where ReFS is the logical choice.
- **Anonymous**
  January 01, 2003
  Great article. . .Just to add that there are also some other PowerShell v3, cmdlets for Alternate data streams:Test-AlternateDataStream & Unblock-File.
  - **Anonymous**
    October 05, 2018
    Thanks for the addition of information. :)
- **Anonymous**
  January 01, 2003
  DIR of Win Vista/2008 or higher supports for a quick peak of ADSdir /r
- **Anonymous**
  January 01, 2003
  Correct. FAT file systems do not support more than one data stream.

- **Anonymous**
  March 25, 2013
  The comment has been removed
- **Anonymous**
  March 25, 2013
  @GkhalsaThe Stream only Works on NTFS, you will lose all the Stream Data if you copy it to The FAT32 FS.and even after you copy a file from NTFS --> FAT32 --> NTFS your Stream is Lost, as FAT32 doesntunderstand ADS.
- **Anonymous**
  March 27, 2013
  Alternate data streams are fun, but aren't they going away? I mean, ReFS does not support them, and the plan is to do away with a lot of non-mainstream (no pun intended :) features such as transactions and hard links, even though some are currently in use in the default OS installation, isn't it?
  - **Anonymous**
    August 10, 2018
    I know its been 5 years since this was posted, but I want to respond in case anyone has the same question.ReFS initially did NOT support alternate data streams. However, this became a problem for things like FCI and other legitimate applications that utilized ADS. So new functionality was added to ReFS. It now supports ADS. No changes to support hardlinks at this time.
- **Anonymous**
  July 02, 2013
  ...and that is why virtually no one wants to use ReFS right now, at least until it plays catch-up with NTFS compatibility-/feature-wise (EFS, streams, compression, etc.) and especially performance-wise. When we first heard of a new filesystem for Windows and then read all about the reliability enhancements, it was quite disheartening to learn that performance actually *decreased* with the new filesystem, and it doesn't even seem to be designed to address NTFS's shortcomings in this area. We've already seen both are possible (e.g., ZFS).We're left with a Sophie's Choice for Windows in this era of giant data: do you want data integrity, or do you want performance and compatibility?
- **Anonymous**
  August 26, 2013
  I received a zip file that was supposed to contain files with ADS, but there were no ADSs. Is there a tool out there that archives files like WinZip that handles ADS? Preferably supported on Windows Server 2008?
- **Anonymous**
  November 19, 2013
  Very well explained. Thank you, information is of great value for me.
- **Anonymous**
  December 04, 2013
  How does SMB/CIFS handle ADS?
- **Anonymous**
  December 16, 2013
  Hace unos días, visitando un cliente aquí en Colombia, me encontré con un problema muy interesante y

- **Anonymous**
  June 08, 2014
  In windows 8, Ads file cannot be called by start command.. same command works in xp.. Why? have you tried to call hidden file using start??
- **Anonymous**
  February 28, 2015
  Why when I have this problem?
  Looks like a bug
  http://www.reddit.com/r/microsoft/comments/2xa896/windows_bug_video_if_you_select_a_download_file/

  the report

  http://answers.microsoft.com/en-us/windows/forum/windows_7-performance/make-new-folder-and-a-malaware-runs-i-select-left/a3963cc4-1d8a-4d86-99e5-f1d7b49d1824

- **Anonymous**
  April 05, 2015
  I'm lost. Please point me to a better place.

  In file explorer (Win7) you can show extra columns for something I will call "characteristics" of a file (since I don't know what the accurate nomenclature is) like "album" or "tags" or "Assistant's phone" or even "SAP".

  I want to understand the architecture and ontology here. How do characteristics get defined? Where is it documented what characteristics are defined, by whom, for what programs, and with what intended meaning?

  What is stored, at what level? What's behind what is being shown in explorer, some kind of use of alternate data streams? Where are the maps and filters that determine what Explorer chooses to show? The file extension is playing a role here, not just the manual selection of columns to show in the explorer details pane.

  My ultimate goal is to be able to set some binary characteristic from Java code on html files I am creating, such that my program can mark out a smaller subset of files in a directory containing many files, and an interactive user of the file explorer can sort on a column showing these marks, and bring the marked files together for viewing.

  But I think somebody must have written up the general design somewhere and I'd like to read it.

  TIA/Jim

- **Anonymous**
  April 21, 2015
  JWG, check that page: http://blogs.technet.com/b/askcore/archive/2010/08/25/ntfs-file-attributes.aspx
- **Anonymous**
  July 02, 2015

I use ADS in my data files and I am curious if there is a limit to the number of streams or the maximum content that can be stored in the streams. My testing indicates a limit of around 3000 streams , but I have not been able determine the exact mechanism for calculating when the limit will be hit. Any help in this area would be appreciated.

  - **Anonymous**
    June 07, 2016
    I have worked with files that have 58,000 named streams. Mind you I didn't create these, there were created by a RSA security application. In my own testing, I can get up to about 7,000 streams. so not sure how to get higher; there must be another factor than just count of streams.

- **Anonymous**
  October 12, 2015
  Excellent article mate :) Thanks for taking the time in writing such an easy to understand explanation
- **Anonymous**
  October 16, 2015
  Great article and very useful. Thank for the details.
- **Anonymous**
  October 27, 2015
  Interesting. Comodo is actually using streams to detect origin of files in order to apply restrictions. I'm guessing people did not knew such feature would be useful in the security domain.
- **Anonymous**
  December 26, 2015
  Super post.
- **Anonymous**
  August 10, 2016
  How can set ZoneId = 3 for Zone.Identifier from Windows command promt?
  - **Anonymous**
    November 24, 2016
    Powershell> set-content file.name -stream zone.identifierValue[0]: [ZoneTransfer]Value[1]: ZoneId=3Value[2]:^^^ like that.
- **Anonymous**
  February 25, 2017
  The comment has been removed
- **Anonymous**
  March 28, 2017
  Sincere Thanks for the detailed explanation. Now that I understand how ADS works I have few questions WHY does NTFS have this feature what good does it bring? Is Microsoft going away with this feature in future?
- **Anonymous**
  November 10, 2017
  You can just open the data stream with notepad actually..c:\ notepad your file.txt:Zone.Identifier works fine..

- **Anonymous**
  December 13, 2017
  Thanks for this helpful post! Now if I can manage to hop on board your time machine (some of the comments below appear to have been made 48 years ago!), I'll have a huge payday and everything will be gravy. ;-)
  - **Anonymous**
    August 10, 2018
    Thanks Ron. Blogs that are meant as reference material tend to get used over a longer period of time. Mostly I wrote this information in a blog so I could refer customers to it that kept asking me the same questions. :)
