

Re: Alternate data Streams

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2007-05/msg06347.html>

- *From:* Mike Hoban <MikeHoban@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 24 May 2007 04:26:00 -0700
-

Fun indeed. Thanks. Your suggestion re copying to CD and back to the HD worked, and the folder I tested now has no ADS data (visibly) attached to the file name. It also took a fraction of the time to scan the folder. However on doing so, it claimed to have scanned 450 files, when in fact there are only 150 files in the folder, is this something else I should be worried about?. I am currently looking many thousands of affected files.

Many Thanks again.

--

Mike H

"Wesley Vogel" wrote:

Keep having fun, Mike. :-)

--

Hope this helps. Let us know.

Wes

MS-MVP Windows Shell/User

In <news:31D37451-0D8C-4A53-8A60-73AF2555D657@xxxxxxxxxxxxxxxxx>,

Mike Hoban <MikeHoban@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> hunted and pecked:

Extraordinarily helpfull and usefull response, thank you very much. I will read everything and take it all on board.

Best Wishes

Mike

--

Mike H

"Wesley Vogel" wrote:

Hi Mike,

Re: Alternate data Streams

Thank You. Very Helpfull, I will try that.
All of my external HDs are
NTFS formatted, and all retain the ADS
when files are copied between
them.

To get rid of Alternate Data Streams on any file, move to a
non NTFS
media, like a floppy, a CD or a memory stick and then move
the file back
to the hard drive.

If I
were to create new external HD's formatted
to FAT32, then copy the files
from the NTFS drives, would that remove
the ADS?.

Seems awful drastic.

Keep in mind that adding Comments to any file adds ADS.

<quote>

To add a comment to a file

1. Right click a file.
 2. Click Properties.
 3. On the Summary tab, type your comment in the
Comments area.
- or–

On the Summary tab, click Simple, and then type your
comment in the
Comments area.

Notes

To display the comments you add to files, double-click the
folder that
contains the files you want to view. On the View menu, click
Choose
Details, and select the Comment check box, and then click
OK. On the
View menu, click Details to see comments for several files at
once, or
select a file and click Details in the left pane to view the
comment for

Re: Alternate data Streams

the selected file. <quote>
from...

Add a comment to a file

<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/windows>

Not all Alternate Data Streams are evil. Although with SP2
Microsoft adds
zone info as ADS with the Attachment Manager.

You can use the HijackThis ADS Spy to remove ADS.

Both of these are copied and pasted from HijackThis.

HijackThis ADS Spy

Alternate Data Streams (ADSs) are pieces of info hidden as
metadata on
files. They are not visible in Explorer and the size they take
up is not
reported by Windows. Recent browser hijackers started
hiding their files
inside ADSs, and very few anti-malware scanners detect this
(yet). Use ADS
Spy to find and remove these streams. Note: this app also
displays
legitimate ADS streams. Do not delete streams if you are not
completely
sure they are malicious!

OK

HijackThis

Using ADS Spy is very easy: just click 'Scan', wait until the
scan
completes, then select the ADS streams you want to remove
and click
'Remove selected'. If you are unsure which streams to
remove, ask
someone for help. Don't delete streams if you don't know
what they
are! The three checkboxes are: Quick Scan: only scans the
Windows folder.
So far all known malware that uses ADS to hide itself, hides
in the
Windows folder. Unchecking this will make ADS Spy scan
the entire system
(i.e. all drives). Ignore safe system info streams: Windows,
Internet
Explorer and a few antivirus programs use ADS to store
metadata for

Re: Alternate data Streams

certain folders and files. These streams can safely be ignored, they are harmless. Calculate MD5 checksums of streams: For antispysware program development or antivirus analysis only. Note: the default settings of above three checkboxes should be fine for most people. There's no need to change any of them unless you are a developer or anti-malware expert.

OK

HijackThis (More for the advanced user)

<http://www.spywareinfo.com/~merijn/downloads.html>

HijackThis log tutorial

<http://www.spywareinfo.com/~merijn/htlogtutorial.html>

HijackThis Log Tutorial

<http://www.aumha.org/a/hjttutor.htm>

See 9. How to use ADS Spy

How to use HijackThis to remove Browser Hijackers & Spyware

<http://www.bleepingcomputer.com/tutorials/tutorial42.html>

NTFS Alternate (Multiple) Data Streams articles

The first four are short and to the point.

NTFS Data Streams – Windows Alternate Data Stream, NP.EXE

<http://www.auditmypc.com/freescan/readingroom/ntfsstreams.asp>

Windows Alternate Data Streams

<http://www.bleepingcomputer.com/forums/tutorial25.html>

Windows NTFS Alternate Data Streams

<http://www.securityfocus.com/infocus/1822>

NTFS Streams

<http://www.alcpres.com/articles/ads.html>

Alternate Data Streams Threat or Menace Why Alternate Data Streams

<http://www.informit.com/articles/article.asp?p=413685&rl=1>

Re: Alternate data Streams

FAQ Alternate Data Streams in NTFS

<http://www.heysoft.de/nt/ntfs-ads.htm>

Fork (filesystem)

http://en.wikipedia.org/wiki/Alternate_data_stream

Hidden NTFS Alternate Data Streams (ADS) Explained – Are You At Risk?

<http://www.diamondcs.com.au/web/streams/streams.htm>

Hidden Threat Alternate Data Streams

http://www.windowsecurity.com/articles/Alternate_Data_Streams.html

NTFS Alternate Data Streams Â» Girl Geekette dotNet

<http://www.girlgeekette.net/2005/09/16/ntfs-alternate-data-streams/>

NTFS Data Streams

<http://www.relsoft.net/datastreams.html>

NTFS Streams – Everything you need to know (demos and tests included)

<http://www.diamondcs.com.au/index.php?page=archive&id=ntfs-streams>

Practical Guide to Alternative Data Streams in NTFS

<http://www.irongeek.com/i.php?page=security/altds>

Is there any advantage to the NTFS format over FAT32?, . Finally, can I reformat the existing NTFS drives to FAT32 (obviously losing the data in the process?.

You cannot reformat an NTFS drive to FAT32 without some 3rd party utility.

You can do whatever you like, but NTFS is the way to go, not FAT32.

What Is NTFS?

<http://technet2.microsoft.com/WindowsServer/en/Library/59a9462a-cbdd-45e7-828b-12c6c>

FAT & NTFS File Systems in Windows XP

<http://www.aumha.org/win5/a/ntfs.htm>

Limitations of the FAT32 File System in Windows XP

<http://support.microsoft.com/kb/314463>

Re: Alternate data Streams

NTFS vs. FAT: Which Is Right for You?

<http://www.microsoft.com/windowsxp/expertzone/columns/russel/october01.asp>

Overview of FAT, HPFS, and NTFS File Systems

<http://support.microsoft.com/kb/100108>

--

Hope this helps. Let us know.

Wes

MS-MVP Windows Shell/User

In

<news:F869C836-D6CC-4D0B-83D6-15589BB5F4DF@xxxxxxxxxxxxxx>,

Mike Hoban <MikeHoban@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

hunted and pecked:

Thank You. Very Helpfull, I will try that.
All of my external HDs are
NTFS formatted, and all retain the ADS
when files are copied between
them. If I were to create new external HD's
formatted to FAT32, then
copy the files from the NTFS drives, would
that remove the ADS?.

Is there any advantage to the NTFS format
over FAT32?, . Finally, can I
reformat the existing NTFS drives to FAT32
(obviously losing the data
in the process?.

Many Many Thanks
Mike

--

Mike H

"Wesley Vogel" wrote:

ADS probably does not
slow down your system.

To get rid of Alternate Data
Streams on any file, move to
a non NTFS
media, like a floppy, a CD
or a memory stick and then

Re: Alternate data Streams

move the file
back to the hard drive. ADS
can only exist on NTFS
formatted drives,
moving or copying files
strips the files of the ADS
crap.

You get Confirm Stream
Loss messages when
copying files with ADS to
non-NTFS formatted
media...

Confirm Stream Loss

The file
'xxxxxxxxxxxxx.zzz' has
extra information
attached to it that might be
lost if you continue copying.
The
contents of the file will not
be affected. Information that
might be
lost includes:
Summary Info
Document Summary Info

Do you want to proceed
anyway?

Click YES because there is
nothing you can do about it.

--
Hope this helps. Let us
know.

Wes
MS-MVP Windows
Shell/User

In
news:790E5795-6EFE-40EE-93C2-150D3DD87F10@xxxxxxxxxxxxxx,
Mike Hoban
<MikeHoban@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
hunted and pecked:

Re: Alternate data Streams

Hello, I am
looking for
advice on
how to
locate and
remove
Alternate
data
Streams
from jpeg
files. They
during in
my virus
scan, but no
where else.
I fear they
are causing
my system
to slow
down
considerably.
thanks

--

Mike H