FAQ: Alternate Data Streams in NTFS

What is NTFS?

It is the abbreviation of *New Technology File System* - Windows NT's preferred file system.

What is an alternate data stream (ADS)?

In NTFS, a file consits of different data streams. One stream holds the security information (access rights and such things), another one holds the "real data" you expect to be in a file. There may be another stream with link information instead of the real data stream, if the file actually is a link. And there may be alternate data streams, holding data the same way the standard data stream does.

What is wrong with alternate data streams?

I could say: Nothing, they work as expected and as documented (yes, Microsoft did document this feature).
But stop - there is something wrong: They are totally hidden. You can have a file with 1 byte in the official main data stream and some hundred MB in one or more alternate data streams. What do you expect the dir command, file manager or explorer to show as the size of this file? It is 1 byte!

That means a user can hide quite a lot of data in alternate data streams and nobody will know?

So it is.

But a user does need certain special priviledges to use alternate data streams?

No. Even guest can create such streams in every file where he has write access for.

How does somebody create an ADS?

You can do it on the command prompt, like `notepad visible.txt:hidden.txt`. This will create an hidden stream `hidden.txt` in the file `visible.txt.` It doesn't matter if the file exists or not.

How does somebody copy data into an ADS?

`type atextfile > visible.txt:hidden2.txt`.
This will create another hidden stream `hidden2.txt` in the file `visible.txt.`

How does somebody copy text data from an ADS into a "normal" file?

`more < visible.txt:hidden2.txt > newfile.txt`.
This will create a file `newfile.txt` from the hidden stream `hidden2.txt` in the file `visible.txt.`

How does somebody copy binary data from an ADS into a "normal" file?

`cat visible.txt:hidden.exe > hack.exe`.
This will create a file `hack.exe` from the hidden stream `hidden.exe` in the file `visible.txt`.
(Cat is a tool from the Ressource Kit.)

How does somebody delete an ADS?

Let us assume you know there is a file `important.exe` with an ADS attached to it. The file is very important and the ADS very dangerous. You need to hold the main stream and delete the ADS. Let us assume there is no FAT drive on your network, otherwise you could move the file to this drive and than move it back again. All you need to do is:

```
ren important.exe temp.exe
cat temp.exe > important.exe
del temp.exe
```

The method above does not work when the ADS is attached to a directory. If you need to remove, for instance c:\Windows:harmful.exe without reinstalling Windows, you could use this trick. (If you use NT 5.x, you need a copy of Notepad.exe from NT 4!)

1. Open the ADS with Notepad:
   C:\NT4Tools\Notepad.exe c:\Windows:harmful.exe
2. Delete the entire content of the ADS
3. Close notepad. It will ask whether you want to save your changes
4. Answer YES
5. Notpad will tell you that the file is empty and that it will delete it

Now you are done, the ADS is gone.

Can somebody add an ADS to a directory entry instead of a file?

Yes, it works the same way.

What possibilities does Microsoft provide to check if there are alternate data streams on my NTFS disks?

Do you expect they care?

But if the sum of available and used storage on a hard disk is much less than it's size, I want to know a way to check if there are alternate data streams on my NTFS disks!

You can move all files onto a FAT drive and back to the NTFS drive. This way all alternate data streams will be deleted, because FAT does not know how to save this kind of data.

OK, but this is not quite handy. And I might be interested in viewing the data, before I will delete it!

I have developed a command line tool called ***LADS*** (List Alternate Data Streams), which scans the entire drive or a given directory. It lists the names and size of all alternate data streams it finds. You can download the current Freeware version of LADS. This software is provided "as is", without warranty of any kind! Use it on your own risk!

Which permissions do I need to run LADS?

The program is a tool for Administrators. As Administrator you normally have all necessary

permissions. The error message "Acess is denied" never should occur. If it does, make sure that your account has Backup priviledges!

Is LADS broken?

If I use the commands
```
C:\TEMP\t>echo Hallo > t
C:\TEMP\t>echo My Secret > t:secret
```
it does not find the ADS `C:\TEMP\t\t:secret`!
Nothing is broken **here** ;-)
With the second command, you did not create an ADS, but you did create a file `secret` on drive `t:\` instead.
Use a longer file name and try again.

LADS version 2.10 and above calculates another sum of the file sizes of a directory than version 2.0 did. How this?

Version 2.10 has been optimized for fast execution. When possible, not every file will be scanned. The only disadvantage is the missing possibility to find out the size of every file header, which is now neglected when calculating the sum of used space.

Can I run LADS from a bootable DOS floppy?

The program uses some API functions of Windows NT, therefore it needs to run under some kind of Windows NT (as NT4, W2K or WXP).

How does LADS detect an ADS?

In NTFS, every stream of a file has a header. LADS reads all these headers and shows only those which belong to an ADS.

When I doubleclick on LADS.exe to install it, I see a black DOS-window during only 10 microseconds and can't find it thereafter.

LADS is a command line program, there is nothing to install.

How do I use LADS properly?

1. Open a command window
2. Go into the directory where LADS sits
3. Enter "LADS" and press the ENTER button of the keyboard
4. Read the Readme file for more information

LADS is a security related software, why can I get no source code for free? As long as I can only get the exe file, I will not use it.

According to this logic you probably do not need LADS at all. If you only run software with freely available source code, you do not run any version of Windows NT. So why should you use LADS at all? I do not force anybody to use LADS. Besides, the program changes nothing in the file system. It only reads the available information with the help of the apropriate API functions.

Where can I find more information regarding ADS?

See **The Dark Side of NTFS** by H. Carvey

Welcome page