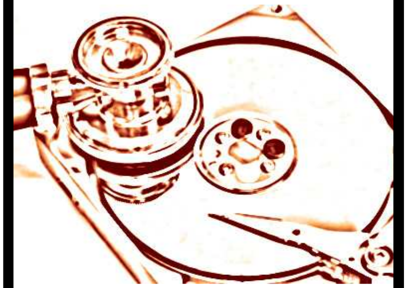

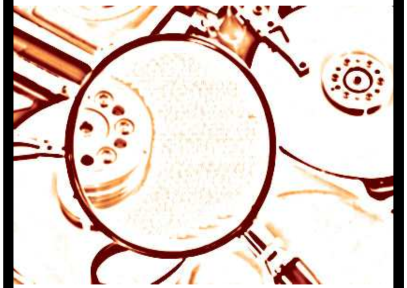

CONTACT US

Mail

PO Box: 724194
Atlanta, GA 31139

Telephone:

(404) 829-3057 (voice)

Online

WWW.ASDFED.COM

The American Society of
Digital Forensics & eDiscovery

Technical Bulletin

Domain Name	**09TB014-001**
Release Date:	**Sunday, October 04, 2009**
Title:	**NT Alternative Data Streams**
Chair (s):	**Danny Mares**
Level:	**Foundational**
Status:	**Ready for Release**

Outline

Purpose..**Error! Bookmark not defined.**
Copyright..3
Distribution..3
Disclaimer..3
Abstract:..3
Outline..2
Background..4
Explanation..4
Attributes..4
Example..5
Usages..5
Detection..6

Purpose

The American Society of Digital Forensics & eDiscovery (ASDFED) compiles and distributes technical bulletins submitted from its members. These bulletins cover a wide range of topics of interest across the digital forensics and electronic discovery disciplines. These bulletins are intended to assist members with their duties and are for informational purposes only.

Copyright

Distribution

Disclaimer

ASDFED makes every effort to insure this information is factually accurate, however all warranties are specifically disclaimed. The information is provided as is. The information expressed is the opinion(s) of the individual author(s) and does not reflect the official opinion of ASDFED.

Abstract:

An Alternate Data Stream is a file attribute that can point to more than one file. This article will explore their origins and explain how to use the items included with the Windows XP operating system to create one. Next it will focus how to use some tools from www.dmares.com to detect them and reveal their data. This is a foundational article, which provides the reader with critical information.

Background

Back in 1997 at an NT security conference, I was reminded about a little known part of the NTFS file system called "Alternate Data Streams". Most of us have never heard of Alternate Data Streams (referred below as ADS). In fact, the typical computer user will probably never have any need to use or deal with ADS.

Explanation

So what are Alternate Data Streams and why should we bother with them? The explanation that follows is not a technical one, and is therefore technically unsophisticated. It is intended to be useful when you need to provide an explanation to a non-technical person.

Let's start with what most people consider a normal data file. A normal file consists of an entry in the directory which typically contains the following: file name; date; time; size; an indication as to where the files resides on the physical disk (in DOS we call this the starting Cluster location; on NTFS it is information located in the Master File Table, or MFT); and the data of the file, which is contained in a series of bytes of data located in Clusters on the disk. That’s the simple explanation. Information about the NT Master File Table can be found in many places. One helpful reference is Executive Software International's site at: (http://www.execsoft.com/tech-support/articles/art-0004.htm, and http://www.execsoft.com/tech-support/articles/art-0004.htm/art-0020.htm).

Attributes

Now, comes NTFS. Disregarding for a moment that files of about 1500 bytes or less can reside entirely within the MFT, the MFT contains a significant amount more information about the file. This information is usually referred to as "attributes." Some authorities list more than 10 attributes of a file. An important point is that attributes can be resident (in the MFT) or nonresident, meaning located somewhere else on the disk.

One of the more significant attributes of a file is the **"DATA"** attribute. The data attribute points to the data, resident (located within the MFT) or not. This still sounds very simple. We have a file system, a way of tracking files (the directory entry), and attributes about the files. But things become more complex than this.

On NTFS systems, (and only on NTFS), this "DATA" attribute can actually be multiple data attributes pointing to more than one piece of "data". In this case 'data' means the contents of a file, or other information such as security information. Thus the "DATA" attribute can point to more than one file. These additional files are called Alternate Data Streams. I think of them as additional files that are sitting--or more appropriately--hiding behind the visible file.

ADS are sort of like invisible attachments to a file. Their physical information is not included in the results of a DIR or Explorer window. DIR or Explorer will never tell you a file contains ADS. In most cases, if one existed, its size would be so insignificant to the overall size of a physical drive that you wouldn't even notice that unaccounted-for space was being taken up. So how do you look for them? Very carefully.

Example

Actually, before we start looking for Alternate Data Streams, I should first tell you how to create a simple ADS. The easiest way is to use Notepad. Assume we have an existing file called **test.txt**. It is a text file, sitting out there on the disk. Now let's create a simple ADS, named **alternate.txt**. Using Notepad, at the prompt, enter the command

```
C:>notepad test.txt:alternate.txt
```

Notice the format for creating an ADS. You use the filename of the main data file, then add a colon (**:**), followed by the name of the ADS you wish to create or access. There should be no spaces within this entire string of characters. (Unless you quote the string, which is another matter.)

Because the ADS doesn't currently exist, Notepad will probably say that **alternate.txt** does not exist and ask if you want to create it. Answer "**yes**." Notepad will open an empty file and you can enter any information, just as usual. When you finish, save the file and exit. Look at the size of the **test.txt** file that DIR shows. The filesize hasn't changed at all and you will not see any indication of alternate.txt anywhere. Interesting. Where did the data go? It went into one of those Alternate Data Streams that is now associated with the original file **test.txt**.

Now that you have created an ADS, you can go in and create a second, third, fourth, and so on. To access these ADS files later, all you need to do is use Notepad to edit the ADS just as you did when originally creating it.

```
C:>Notepad test.txt:alternate.txt
```

Usages

Does ADS simply seem like a toy? Well, this toy could be used to hide data "behind" any file within the NTFS file system. Under normal forensic processing you wouldn't even know it existed. If you did a string search on the entire physical drive you might find the text strings if they weren't encrypted or in a binary format. A suspect may very easily create an ADS containing passwords, contacts or other incriminating information and only he would know where it was and by what name it could be seen. An encrypted file could be sent on an NTFS formatted Jazz or Zip disk to someone, and the password might be sent right along with it in the form of an ADS. Binary images could be attached to simple text or document files for later retrieval. There might already be some sophisticated FTP programs that will transfer ADS files. It would certainly be an easy programming task to create one.

Once you've created a text ADS, it is easy to add a binary data file as an ADS. You simply use the command:

```
C:>type binary.file >> test.txt:binary.mds
```

Detection

This would add the **binary.file** to the **test.txt** as an ADS. Although I haven’t seen a published program to extract out the binary data from the ADS, creating one is a relatively simple programming task. In fact, Maresware's 32 bit versions of **Diskcat**, **Hash**, **MD5** and **Crckit** can detect and perform the appropriate analysis on these ADS. And Maresware's **Mdir** and **Diskcat** can identify the existence of ADS files.

Here is a sample output of **Mdir** when it finds a file with an ADS. Notice the ADS do not carry a different date, so I indicate their presence with the term Alternate Data or ADATA.

Filename size date time TZ attributes

```
junk_3               103 11/17/1998 12:41w EST A....
junk_3:altdata.txt:   40 ALTERNATE DATA    EST ADATA
junk_3:alternat.txt:  43 ALTERNATE DATA    EST ADATA
junk_3:alternate.txt: 16 ALTERNATE DATA    EST ADATA
```

For more information on Alternate Data Streams you can research the web using the keyword Alternate Data Streams, or try these sites:

http://merxsoft.com/mersoft-Free/Information/ntfsmds.htm or
http://premium.microsoft.com/msdn/library/winresource/dnwinnt/f1d/d1e/s838b.htm and look at the 4th page where ADS is discussed.

One other very important thing to remember: If you are copying a file with an ADS and you are going from NTFS to NTFS, the ADS will tag along. No special command is necessary to maintain ADS integrity. However, ADS are only valid when dealing with NTFS disks. So, if you copy a file having ADS to a non NFTS drive, the ADS are lost. This has its good and bad points.

For more information please visit www.dmares.com.