Secret Message
Alternate Data Stream

What is ADS

Although created to make the system compatible with the Mac HFS, alternate data streams are used for other purposes. In Windows 2000 and XP, applications can create additional named streams and access the streams by referring to their names. This feature permits related data to be managed as a single unit. Here are some examples of alternate data streams:

- Multiple multi-media components (such as thumbnails)
- Anti-virus checksums to watch for data change
- File summary information (also called metadata)

For example, a graphics program can store a thumbnail image of a bitmap in a named data stream within the NTFS file containing the image, and another alternate data stream can contain summary information about the file.

Why – NTFS File System Only

- **Every file has an "Unnamed Data Stream"**
  - **Main File Data**
  - **Forks gone by**
- **Files may have "Alternate Data Streams"**
  - **Summary Information**
  - **Thumbnail Graphic Information**
  - **"Hidden" additional stream information**
- **"Alternate Data Streams" can be added to:**
  - **Folders**
  - **Text files**
  - **Graphic files**
  - **Almost any files !**

How

Only for NTFS systems, MFT Entry---- multiple data attributes!!!

Alternate data streams can be created by applications or by users. Applications create data streams for information like thumbnails or file information. Alternate data streams are specific to NTFS. If files with alternate data streams are copied to another file system such as FAT, a message appears indicating that the alternate data streams might be lost.

In addition to the alternate data streams created by applications, users can easily add alternate data streams to any file.

To create an alternate data stream associated with the Testfile.txt file:

1. At the command prompt, type **notepad testfile.txt:secret1.txt**.
2. When Windows states that it cannot find the file and asks if you want to create it, click **Yes**.
3. Inside the data stream, testfile.txt:secret1.txt, add a sentence of text.
4. From the File menu, click **Save** > **Exit** to save the file and close it.

How to Detect

Although Microsoft provides a means for creating specific alternate data streams, the tools and functionality for detecting the presence of alternate data streams are not included in the Windows operating systems. None of the Windows DIR commands or Windows Explorer can detect the presence of alternate data streams.

Moreover, you cannot detect the alternate data streams by checking the file size. If your original file is 10 bytes, and you add an alternate data stream that is 5 bytes, the file size does not change; however, the modification date does change.

Note: Windows does track available disk space if the alternate data stream becomes non-resident from the Master File Table.

Forensic Toolkit® (FTK™) allows you to view alternate data streams in the Explore tab; however, FTK does not currently classify alternate data streams in any container. You must specifically locate a document with alternate data streams to view them in the Explore tab.

Process ADS

FTK lists alternate data streams by the name of the file they are originally associated with. Alternate data streams are shown as items under the file. In the file tree view, the file is displayed with its respective metadata and the alternate data stream items below it.

In addition to being listed in FTK, alternate data streams are indexed by FTK. Therefore, FTK returns hits for any text in an alternate data stream. The results show that the alternate data stream is within another file.

ADS Lab – Create and Process ADS

- You need a clean thumb drive to complete this lab
- You do not need thumb drive to complete the second part of the lab