Defense Evasion: Alternate Data Streams

hackingarticles.in/defense-evasion-alternate-data-streams

Raj August 26, 2020

Alternate Data Stream is an artifact of New Technology File system (NTFS) which was introduced by Windows. It was traditionally introduced so that it could provide compatibility for file sharing with the older Hierarchical File system (HFS) of Macintosh systems where the data could be forked into different resources and to store additional data of a file which is called as metadata.

It was introduced for a legitimate purpose but the attackers have found a method to exploit this feature by hiding payloads, malware, keyloggers, etc in any type of file like text-file, audio -file, videos-video, images execute them without the knowledge of the users.

Many users still are unaware of this feature where there could be hidden files and could have malicious intent as these files are nearly impossible to be detected.

Table of Contents

- **NTFS**
- **Alternate Data Stream**
- **Key Notes on Alternate Data Stream**
- **Hiding a file**
- **ADS with PowerShell**
- **NTFS to FAT**
- **Hiding an image in a text file**
- **Hiding Audio in a text file**

New Technology File System (NTFS)

In the NTFS, all the allocated sectors in a volume are associated with a file. A file is composed of all the data within a file and that file's metadata. The metadata usually comprises of items like file name, attribute type, attribute name, file security information etc. The file metadata and file data are considered as a combined set. The Master File Table contains the base file record for every file and directory within an NTFS volume apart from the other file details.

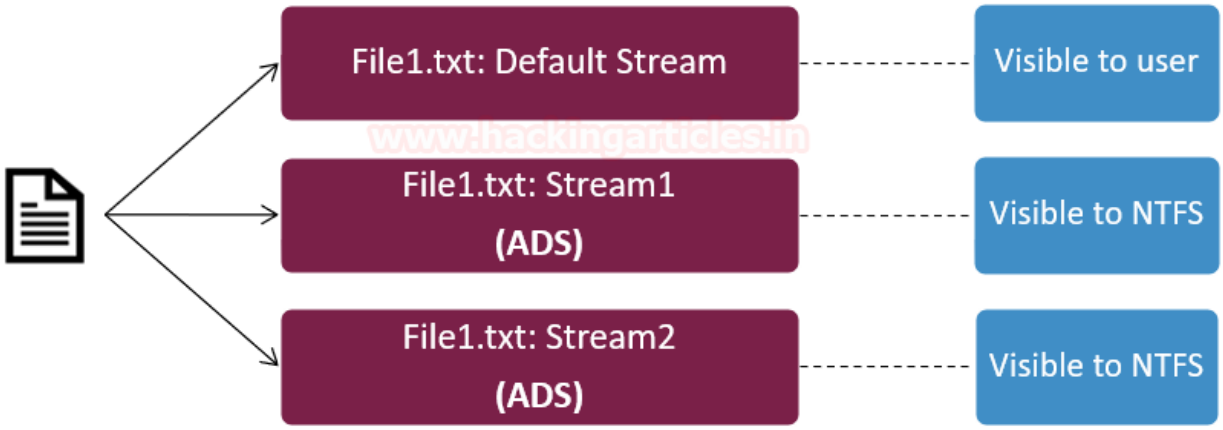
The name of the file and its timestamp is kept as resident attributes. If the attributes for a file cannot accommodate in the MFT file record, those file attributes are termed as a non-resident. These non-resident attributes are allocated to one or more clusters in the disk. These clusters hence become the alternate data streams within the NTFS volume.

The default stream is unnamed and the default stream type in NTFS is $DATA.

NTFS stores file in the following format.

Alternate Data Stream

Within NTFS, a file comprises of the various data stream. The primary data stream is an unnamed stream which actually contains the data of the file that is visible when we open this stream and hence it is called as the default stream. The second stream is usually the alternate data stream. A file can have more than one Alternate Data Streams for the various purpose which hold the metadata about the file. Any of the ADS files can have any malicious content within it which can be appended with the default stream. When you append an ADS file with a default stream file, there will be no change made to the size or the function of that file.



Alternate data streams usually deal with file integrity within the server. A user will never be able to recognise an ADS file by just looking at it and if it comprises of any extra executable or text element within it. Alternate data streams generally deal with maintaining the confidentiality of the file that is being sent or are at rest on the system.

ADS can be used by the attacker to evade any defences such as static indicator scanning tools and anti-virus software that are implemented by the victim. It is a quite popular method used by attackers to cover their tracks on Windows systems with the use of ADS.

Key Notes on Alternate Data Stream	
1	If the primary file is deleted, the related ADS files will also be deleted.
2	There is no in-built feature in Windows to detect ADS files.
3	Primary files could be word, text, image, video, audio, PDF, .exe files.
4	More than one hidden ADS file can be attached to the primary file.

Hiding a file

So, here we are going to learn to make use of Alternate Datastream to hide a file using 'command-prompt' in your windows PC. To get you started, let's start the windows system, and run command prompt as **administrator** so that these tasks can be performed.

Create a folder to locate your in-use files quickly. Here we have created a folder named **jeenali**.

Now make use of **cd** command to lead you to the path of your folder

Here, we are making use of .txt file as our primary stream to demonstrate ADS, you can use any file of your preference.

A .txt file is created and to add content in the file we can used the command;

```
echo Welcome to ignite Technologies > jeenali.txt
```

To display the contents of your .txt file, you can use;

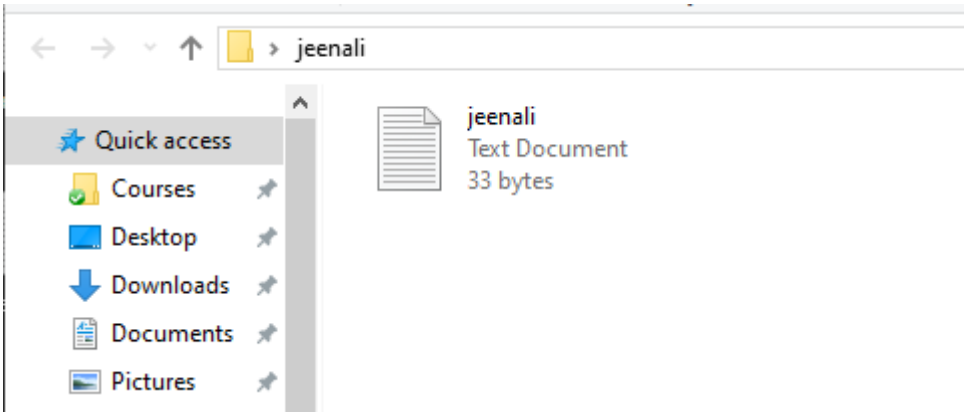
```
type jeenali.txt
```

To display the contents in the folder including Alternate Datastream, we use

```
dir /r
```

```
C:\Users\raj\Desktop\jeenali>echo Welcome to ignite Technologies > jeenali.txt

C:\Users\raj\Desktop\jeenali>type jeenali.txt
Welcome to ignite Technologies

C:\Users\raj\Desktop\jeenali>dir /r
 Volume in drive C has no label.
 Volume Serial Number is 8E59-6469

 Directory of C:\Users\raj\Desktop\jeenali

08/24/2020  09:42 PM    <DIR>          .
08/24/2020  09:42 PM    <DIR>          ..
08/24/2020  09:42 PM                33 jeenali.txt
               1 File(s)             33 bytes
               2 Dir(s)  652,358,492,160 bytes free

C:\Users\raj\Desktop\jeenali>
```

In the above image, you can see that there is no hidden file displayed. On directly visiting the GUI of the folder, you see that there is only one file. So now we will move to adding a hidden file in the folder.



Here we will proceed with creating a hidden file. A .txt file is created with hidden ADS and to add content in the file we can used the command;

```
echo Join Our Training Programs > jeenali.txt:hidden
```

To display the contents of your newly created .txt file, you can use;

```
type jeenali.txt: hidden
```

Here you see that the filename is not recognised, therefore, to see hidden file content, you can type;

```
more < jeenali.txt:hidden
```

To display the contents in the folder including Alternate Datastream, we use;

```
dir /r
```

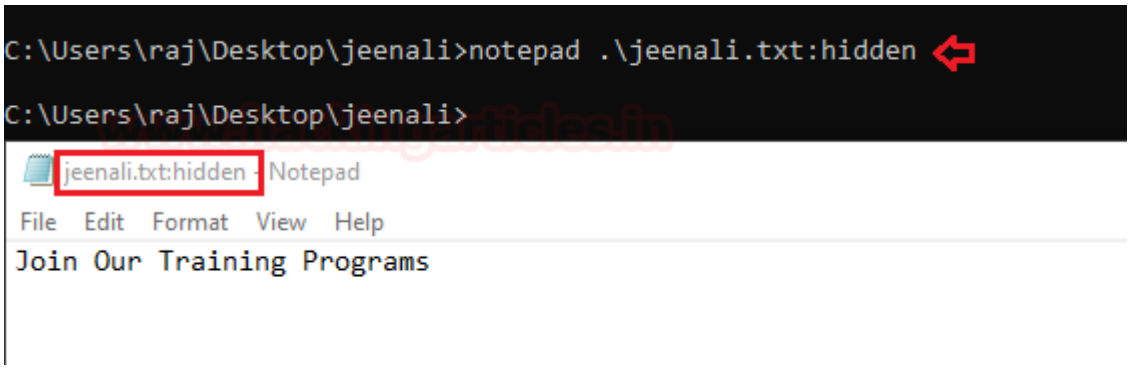
Here we see that the ads are seen is also displayed.

```
C:\Users\raj\Desktop\jeenali>echo Join Our Training Programs > jeenali.txt:hidden

C:\Users\raj\Desktop\jeenali>type jeenali.txt:hidden
The filename, directory name, or volume label syntax is incorrect.

C:\Users\raj\Desktop\jeenali>more < jeenali.txt:hidden
Join Our Training Programs

C:\Users\raj\Desktop\jeenali>dir /r
 Volume in drive C has no label.
 Volume Serial Number is 8E59-6469

 Directory of C:\Users\raj\Desktop\jeenali

08/24/2020  09:42 PM    <DIR>          .
08/24/2020  09:42 PM    <DIR>          ..
08/24/2020  09:44 PM                33 jeenali.txt
                                    29 jeenali.txt:hidden:$DATA
               1 File(s)             33 bytes
               2 Dir(s)  652,357,222,400 bytes free
```

To open the file and see the contents of the hidden file you can use

```
notepad .\jeenali.txt:hidden
```

here see can notice a notepad file prompts open and the contents are displayed.



ADS with PowerShell

Let's begin running PowerShell as an **administrator**

A .txt file is created with hidden ADS and to add content in the file we can used the command;

```
echo Welcome to Hacking Articles! > raj.txt
```

Now to create an ADS file, add content and hide it you can use;

```
Set-Content .\raj.txt -stream text
Hello World
```

We can see the hidden ADS content using

```
Get-Content .\raj.txt -stream text
```

But when you use the dir command, you cannot see your hidden file

```
dir
```

```
PS C:\Users\raj\Desktop\raaz> echo Welcome to Hacking Articles! > raj.txt
PS C:\Users\raj\Desktop\raaz> Set-Content .\raj.txt -stream text

cmdlet Set-Content at command pipeline position 1
Supply values for the following parameters:
Value[0]: Hello World
Value[1]:
PS C:\Users\raj\Desktop\raaz> Get-Content .\raj.txt -stream text
Hello World
PS C:\Users\raj\Desktop\raaz> dir


    Directory: C:\Users\raj\Desktop\raaz


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        8/24/2020  10:14 PM             68 raj.txt
```

To see all the files in the directory you can use

```
Get-Item -path .\raj.txt -stream *
```

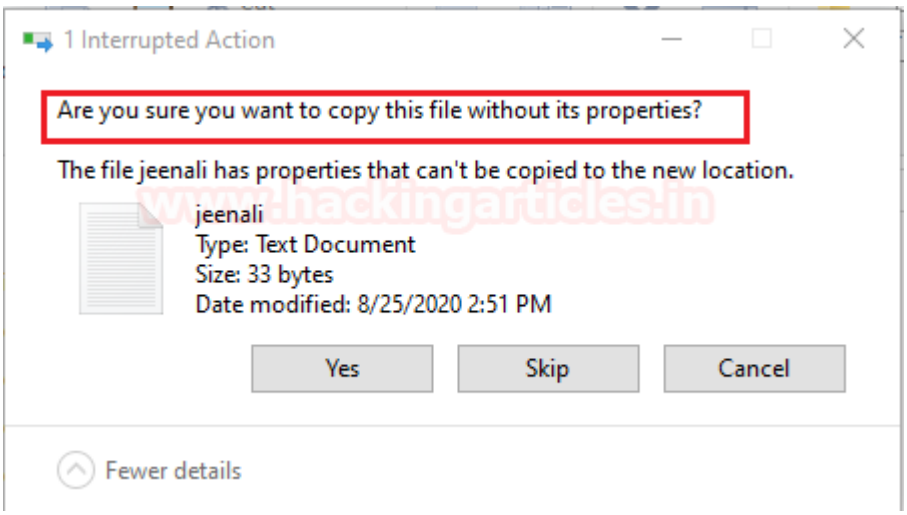
Here you can see the primary .txt as well as the newly created ADS .txt .

```
PS C:\Users\raj\Desktop\raaz> Get-Item -path .\raj.txt -stream *


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\raj\Desktop\raaz\raj.txt::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\raj\Desktop\raaz
PSChildName   : raj.txt::$DATA
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\raj\Desktop\raaz\raj.txt
Stream        : :$DATA
Length        : 68

PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\raj\Desktop\raaz\raj.txt:text
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\raj\Desktop\raaz
PSChildName   : raj.txt:text
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\raj\Desktop\raaz\raj.txt
Stream        : text
Length        : 13
```

NTFS to FAT

If you transfer an ADS file from NTFS to FAT32 you will be automatically destroying the Alternative Data Stream.

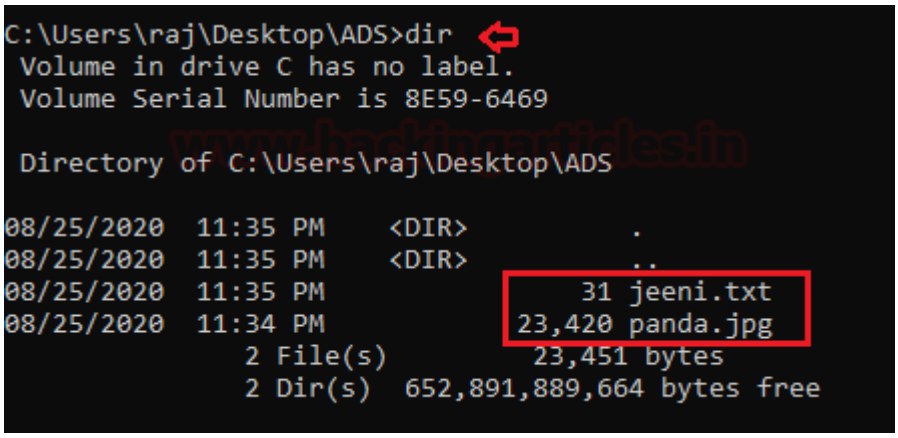
Here, an ADS file was created in an NTFS system but as soon as it is transferred to a FAT32 flash drive, you see the below prompt which won't allow you to copy the file with ADS. This is because the ADS feature was introduced in NTFS and FAT32 does not support it.



Hiding an image in a text file

So, let us start a command prompt as an administrator and change our directory to the folder in which we have our files. To check the contents of the file, type

```
C:\Users\raj\Desktop\ads> dir
```



You see that there are two files (one is a text-primary stream and other is an image file). So Now we will append the image file to the text file using;

```
type panda.jpg > jeeni.txt:panda.jpg
```

After we are done with appending the primary stream file, we will delete the image file from the folder.

```
del panda.jpg
```

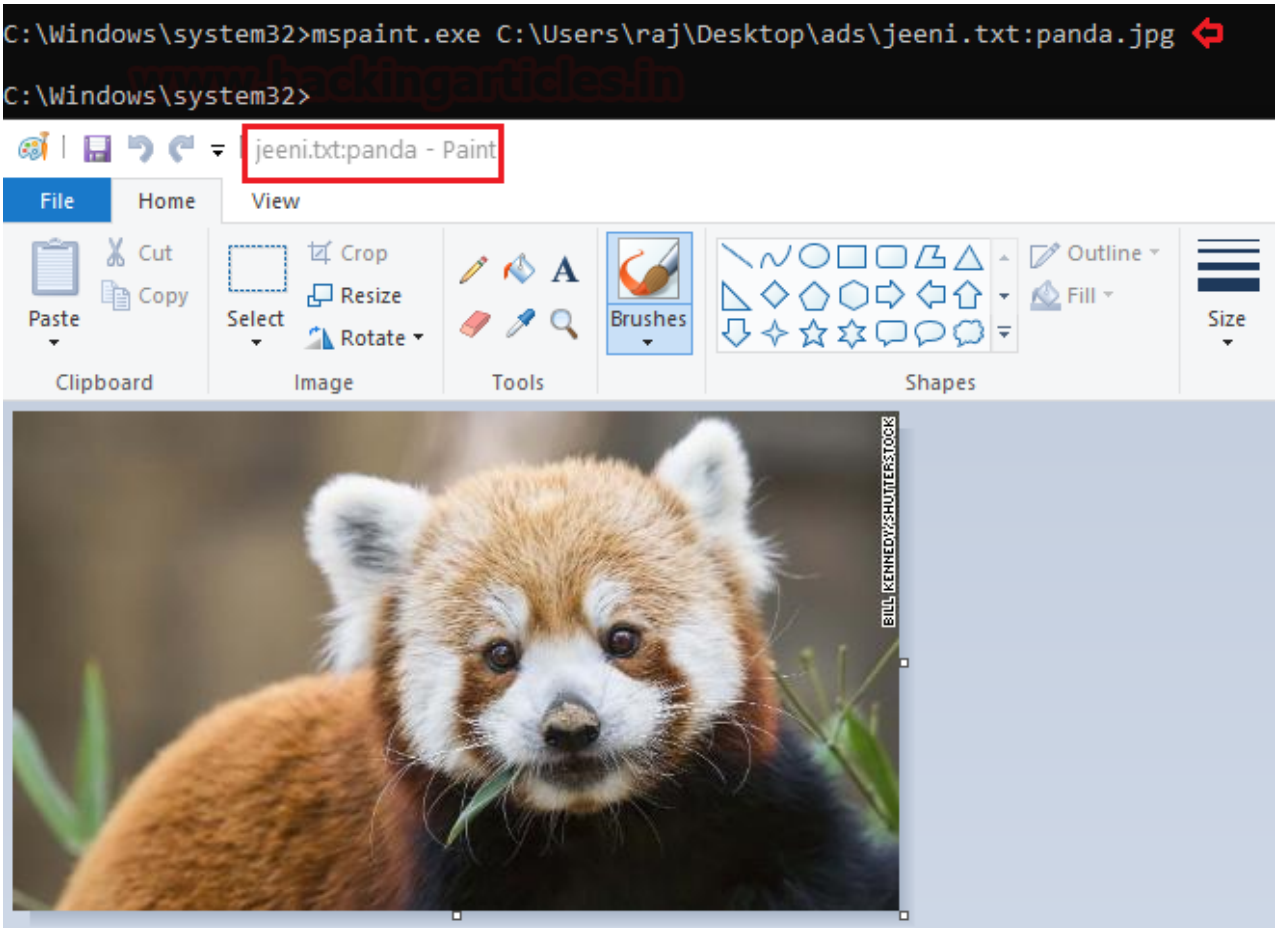
Now, you will see that the image file is gone but a new ADS is created and you can check it using

```
dir /r
```

```
C:\Users\raj\Desktop\ADS>type panda.jpg > jeeni.txt:panda.jpg

C:\Users\raj\Desktop\ADS>del panda.jpg

C:\Users\raj\Desktop\ADS>dir /r
 Volume in drive C has no label.
 Volume Serial Number is 8E59-6469

 Directory of C:\Users\raj\Desktop\ADS

08/25/2020  11:36 PM    <DIR>          .
08/25/2020  11:36 PM    <DIR>          ..
08/25/2020  11:36 PM                31 jeeni.txt
                            23,420 jeeni.txt:panda.jpg:$DATA
               1 File(s)             31 bytes
               2 Dir(s)  652,891,762,688 bytes free

C:\Users\raj\Desktop\ADS>
```

Change the directory to system 32, and you can see that your image file is executed when you open the text file which has ADS appended.

```
C:\Windows\system32>
mspaint.exe C:\Users\raj\Desktop\ads\jeeni.txt:panda.jpg
```

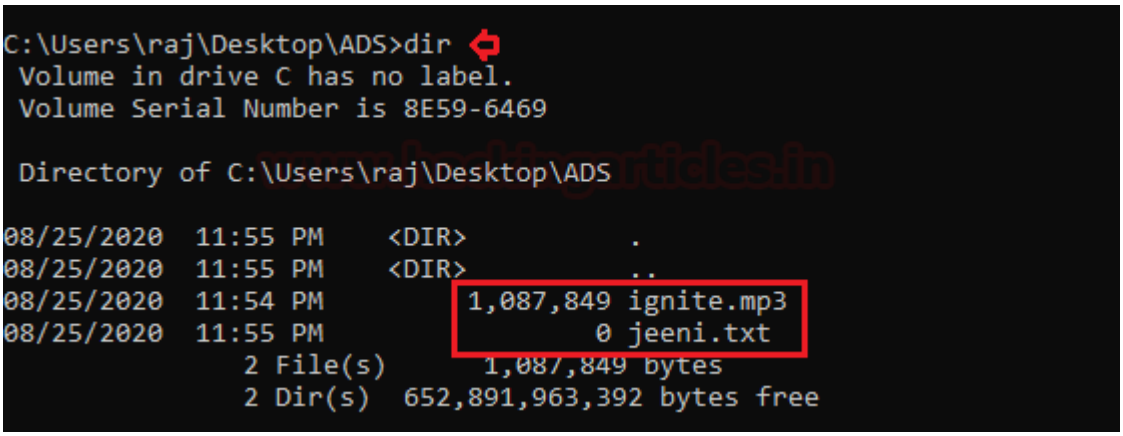


Hiding Audio in a text file

Now, we can start a command prompt as an administrator and change our directory to the folder in which we have our files. To check the contents of the file, type

```
C:\Users\raj\Desktop\ads> dir
```

You see that there only a text file and an audio file.



So Now we will append the audio file to the text file using;

```
type ignite.mp3 > jeeni.txt:ignite.mp3
```

After we are done with appending the primary stream file, we will delete the audio file from the folder.

```
del ignite.mp3
```

Now, you will see that the audio file is gone but a new ADS is created and you can check it using

```
dir /r
```


```
C:\Program Files (x86)\Windows Media Player
wmplayer.exe C:\Users\raj\Desktop\ads\jeeni.txt:ignite.mp3
```

Conclusion: We hope this article has given you a better understanding of alternate data streams. There are many more methods with which Alternate Data Streams can be performed.

Author: Jeenali Kothari is a Digital Forensics enthusiast and enjoys technical content writing. You can reach her on **Here**