Advanced NTFS Alternate Data Stream in windows 8

تقدیم به :

سازمان نظام صنفی رایانه ای استان کردستان

بررسی پیشرفته قابلیت ADS در فایل NTFS ویندوز های 8 و 10 و روشهای پنهان سازی اطلاعات توسط هکر

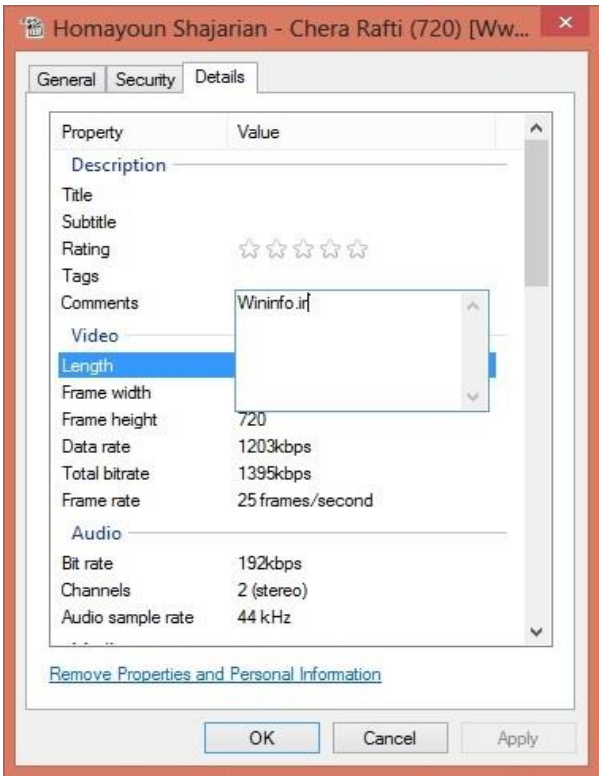
نویسنده : مسلم حقیقیان

wininfo.ir

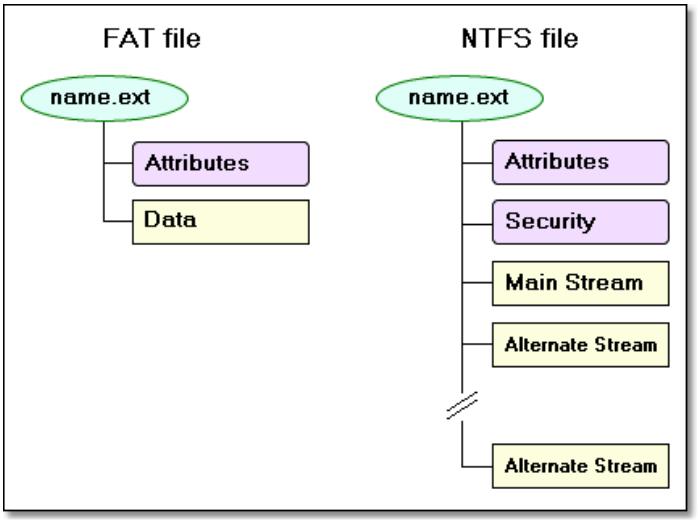
moslem.haghighian@yahoo.com

ویژگی ADS در سیستم فایل NTFS

یکی از ویژگی های بسیار مهم در سیستم فایل NTFS امکان اضافه کردن توضیحات به یک فایل می باشد به عنوان مثل اگر بر روی یک فایل صوتی کلیک راست و گزینه ی properties را ببزنید می توانید در قسمت Details یک سری جزئیات و مشخصات در مورد فایل می توان اضافه کرد .



و یا اینکه دیدید که یک فایل عکس به این فایل ها اضافه می کنند . از مهمترین ویژگی در سیستم فایل NTFS امکان اضافه کردن Stream به یک فایل است یعنی ما می توانید یک یا چند فایل را در یک فایل پنهان کنیم که این امکان در FAT وجود ندارد .



شما می توانید یک فایل که نمی خواهید کسی آن را ببیند و یا اینکه یک پسورد خود را در داخل این فایل ها ذخیره کنید مثلا فرض اینکه شما یک هکر خراب کار هستید (black hat hacker) و می خواهید چیزی را مخفی کنید . **مسئله ی بسیار جالب اینجاست که ما هر فایلی با هر حجمی با استفاده از این متد مخفی کنیم حجم فایل اصلی در windows explorer تغییر نمی کند** (در اصل windows explorer آن را نمی تواند نشان دهد وگرنه در واقع تغییر می کند) . هرچند که استفاده از ابزار هایی مانند 7zip و winrar و دیگر ابزار هایی که با آن می توان یک فایل را پسورد گذاری و یا رمز نگاری کرد وجود دارد اما به هر حال این متد هم یکی از هزار روش مخفی سازی اطلاعات می باشد .

در این مقاله سعی داریم که روش مخفی سازی را شرح دهیم و سپس به طریقه ی مقابله و تشخیص فایل ها و کلمات مخفی شده بپردازیم .

روش مخفی سازی

ما اینجا یک فایل با نام wininfo.txt داریم و می خواهیم یک پسورد را در آن با استفاده از این متد ذخیره کنیم . خوب به شکل زیر عمل می کنیم .

اول از همه ما فایل wininfo.txt رو می سازیم و مقدار p4ssw0rd را به صورت مخفی در آن می گذاریم.

```
echo  p4ssw0rd > wininfo.txt:hidden
```

خوب حالا اگر فایل wininfo.txt را باز کنید می بینید که چیزی در داخل آن وجود ندارد و حتی اگر حجم آن را نیز ببینید همان 0 byte می باشد .

```
C:\test>dir wininfo.txt

 08:31  2014/24/04PM              0 wininfo.txt
```

حال شما وقتی فرمان زیر را به کار ببرید می توانید مقدار مخفی را ببینید . به شکل زیر

```
C:\test>more < test.txt:hidden
Hidden text
```

اگر بخواهیم به طور دقیق تر بررسی کنیم شکل کلی فرمان به صورت زیر است

```
filename:stream name:stream
```

که تنها نوع Stream که می توان با command prompt به آن دسترسی داشته باشیم $DATA می باشد .

```
C:\test>echo This is the file > wininfo.txt

C:\test>echo This is the stream > wininfo.txt:stream

C:\test>more < wininfo.txt::$DATA
This is the file

C:\test>more < wininfo.txt:stream:$DATA
This is the stream
```

لیستی از انواع Streamها را می توانید در اینجا ببینید .

http://msdn.microsoft.com/en-us/library/aa362667%28v=VS.85%29.aspx

که با استفاده از کد های WMI می توانید با آنها نیز کار کنید .

همچنین جهت کار با IDS ها در NTFS می توانید از زبان C++ کمک بگیرید
http://support.microsoft.com/kb/105763

حالت های دیگر کار با IDS

مخفی کردن یک فایل با نام hidden.txt که حاوی اطلاعات محرمانه ما می باشد با یک فایل متنی دیگر با نام wininfo.txt

اول از همه فایل های hidden.txt و wininfo.txtرا می سازیم .

```
Echo p4ssw0rd > hidden.txt
Echo nothing > wininfo.txt
```

خوب حالا فایل hidden را در فایل wininfo مخفی می سازیمو آن را اجرا کنیم .

```
echo Hidden text > wininfo.txt:hidden.txt
```

حالا اگر فایل wininfo را باز کیند همان مقدار nothing را در آن مشاهده می کنید . اما با فرمان زیر با استفاده از برنامه notepad می توانیم به فایل hidden.txt دسترسی پیدا کنیم .

```
notepad wininfo.txt:hidden.txt
```

مخفی کردن یک عکس پشت فایل و اجرای آن

یک عکس با نام secret.jpg را می خواهیم در فایل wininfo.txt مخفی کنیم .

```
type secret.jpg > wininfo.txt:secret.jpg
```

حال می خواهیم آن را بخوانیم باید با استفاده از برنامه mspaint این کار را انجام دهیم .

```
mspaint wininfo.txt:secret.jpg
```

مخفی کردن یک کد VBS در پشت یک فایل و اجرای آن

این کار می تواند بسیار خطرناک باشد چونکه می توان یک بد افزار که به زبان VBS و یا JS نوشته شده است را در پشت یک فایل ذخیره و آن را اجرا کرد .

```
type malware.vbs > wininfo.txt:malware.vbs
Wscript  wininfo.txt:malware.vbs
```

مخفی کردن یک فایل EXE در پشت یک فایل دیگر و اجرای آن

خوب قسمت اصلی شاید همین مبحث در اینجا باشد که بتوان یک فایل exe را در پشت یک فایل دیگر مخفی و سپس آن را اجرا کرد حال می توینذ این فایل exe یک malware باشد و یا خیر .

```
type malware.exe > wininfo.txt: malware.exe
powershell  .\wininfo.txt:malware.exe
```

اضافه کردن یک مقدار دیگر Stream های فایل

همان طور که گفتیم شما می توانید چندین مقدار را در Stream های یک فایل اضافه کنید به عنوان مثال ما می خواهیم یک فایل دیگر که با نام malware2.exe هست را با نام KST در قسمت Stream ها اضافه کنیم .

```
type malware2.exe > wininfo.txt:KST
```

ایجاد IDS با استفاده از powershell ویندوز

همان طور که میدانید powershell دارای فرامین قدرتمند تر و بهتری نصبت به CMD ویندوز می باشد .

از فرامین زیر جهت ساختن و دیدن محتویات فایل متنی استفاده می کنیم .

```
$file = "wininfo.txt"
Set-Content -Path $file -Value 'Test'
Get-Content -Path $file
```

و از فرمان زیر جهت اضافه کردن مقادیر به Stream های فایل استفاده می شود .

```
Add-Content -Path $file -Value 'P4ssw0rd' -Stream 'secret'
```

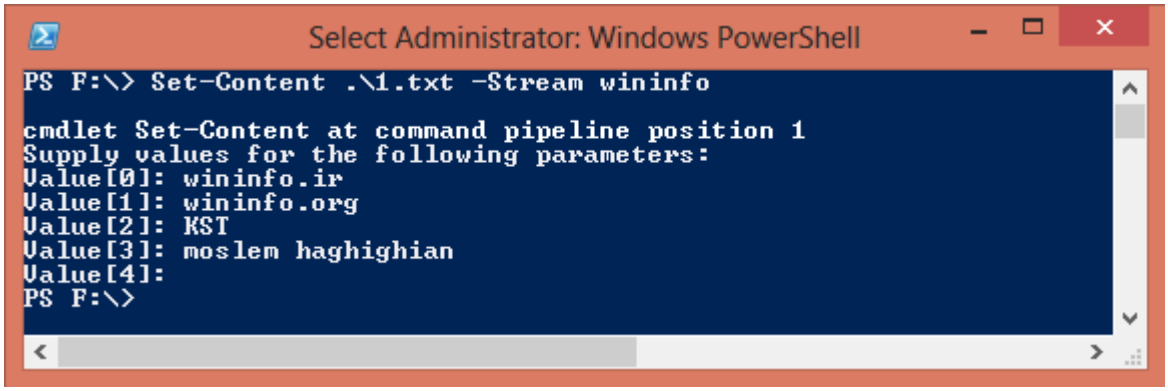
و می توانید جهت دیدن محتویات فایل در حالت عادی از فرمان زیر استفاده کنید .

```
Get-Content -Path $file
```

و جهت دیدن متن مخفی و دسترسی به Stream فایل از فرمان زیر می توانید استفاده کنید .

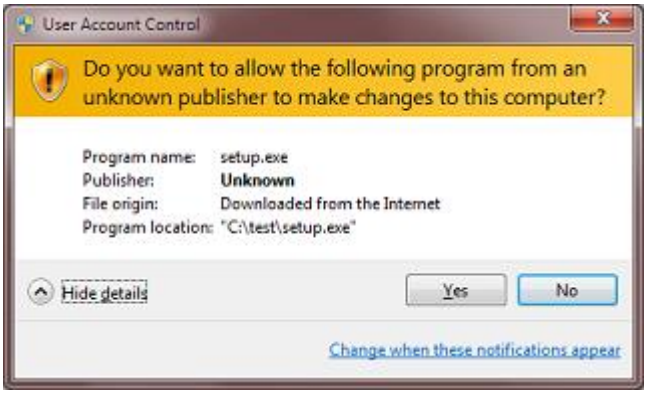
```
Get-Content -Path $file -Stream 'secret'
```

و یا می توان فرمان را اینگونه به کار برد



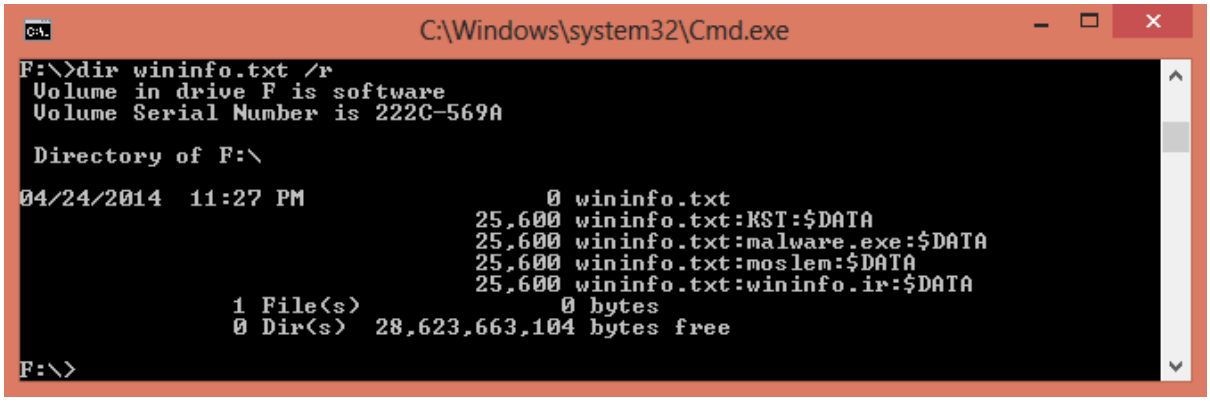
طریقه ی شناسایی فایل ها با قابلیت IDS

در صورتی که یک فایل که دارای IDS می باشد از اینترنت دانلود نمایید فورا مرور گر پیغامی به شما می دهد که فایل دارای IDS (Zone.Identifier) می باشد به مانند زیر که هنگام دانلود فایل setup.exe که دارای IDS بود مرورگر IE فورا پیغامی را بالا آورد . علاوه بر آن انواع آنتی ویروس ها به سیستم تشخیص IDS مجهز هستند .



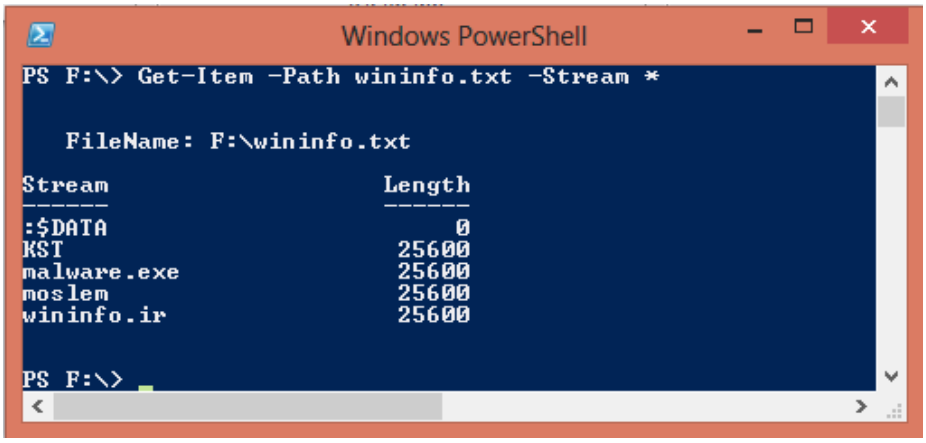
جهت تشخیص و شناسایی این فایل ها روش های مختلفی وجود دارد روش اول که ساده ترین روش است استفاده از خود برنامه CMD ویندوز و فرمان DIR هست

در صورتی که فرمان DIR با استفاده از سویچ /R استفاده شود می تواند مقادیر Stream موجود در یک فایل را با آن ببینید . با این فرمان لیست تمامی Stream ها را می توانید مشاهده کنید که در اینجا با نام های Wininfo.ir و Moslem و Malware.exe و KST می باشد .



روش دیگر و قوی تر استفاده از powershell ویندوز می باشد .که می توانید با فرمان زیر آن ها را بررسی کنید .

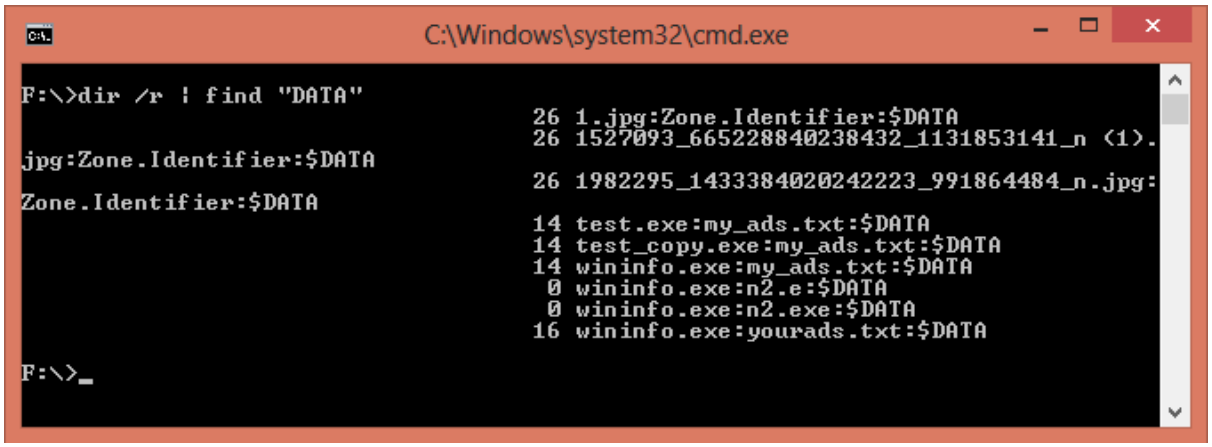
```
Get-Item -Path wininfo.txt -Stream*
```



که در اینجا می توان به جای ستاره فقط نام stream مورد نظر را بنویسید .

لیست کردن تمام فایل هایی که دارای IDS می باشند .

با استفاده از فرمان Find در CMD امکان این کار برای شما وجود دارد .

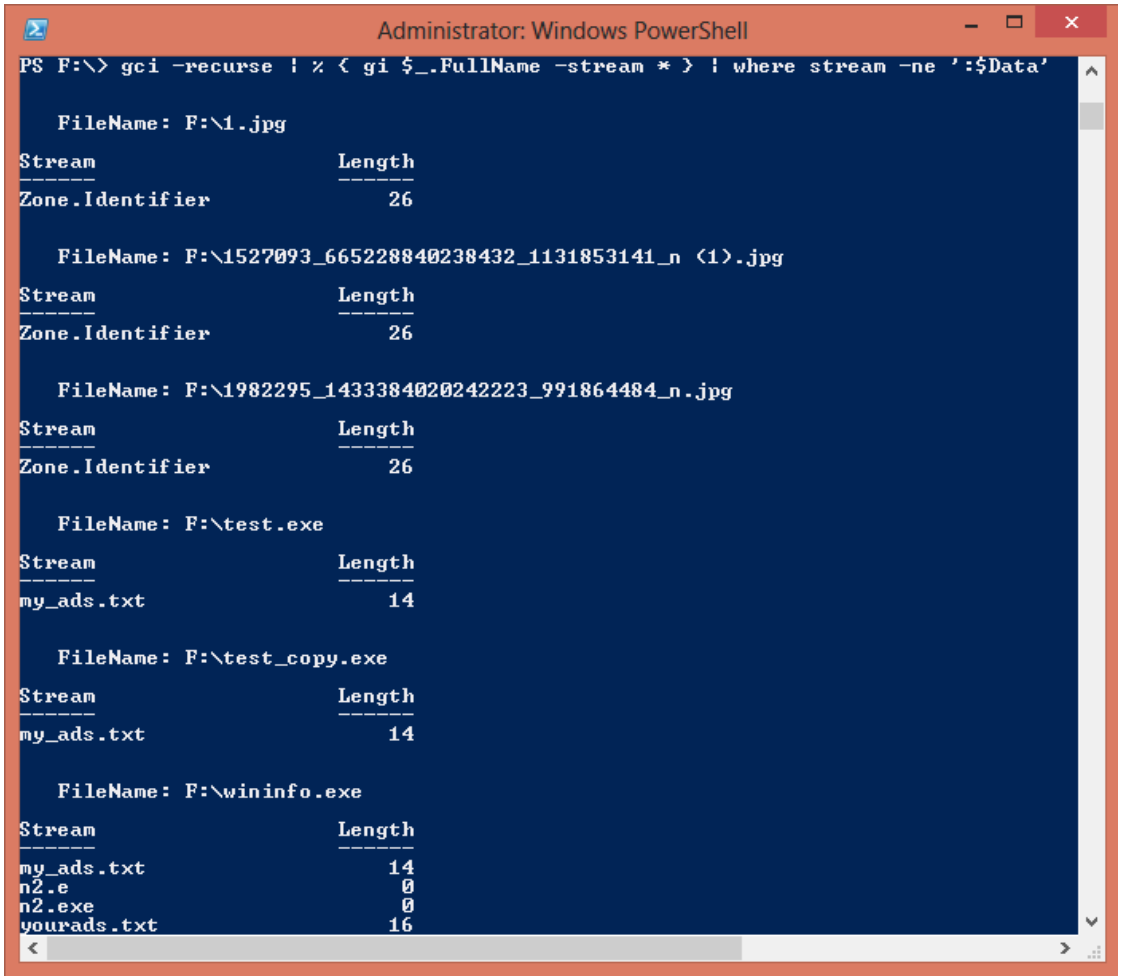


همچنین با استفاده از کد زیر در powershell شما می توانید لیستی از تمام فایل هایی که در stream $DATA هستند را در داخل یم فولدر بینید .

```
Get-Item * -stream *
```

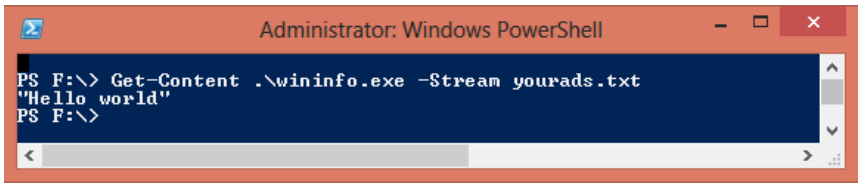
و همچنین می توان از فرمان زیر نیز استفاده کرد

```
gci -recurse | % { gi $_.FullName -stream * } | where stream -ne ':$Data'
```



و می توان جهت دیدن محتویات STReam مورد نظر با استفاده از فرامین powershell از فرمان زیر استفاده کرد

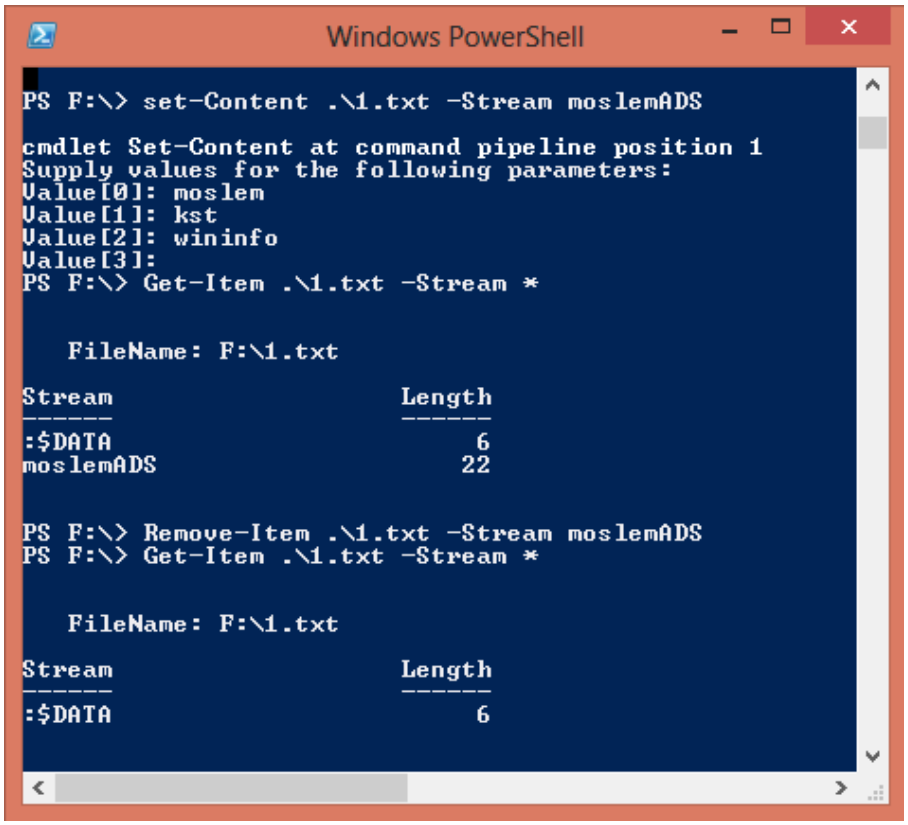
```
Get-Content .\wininfo.exe -Stream yourads.txt
```



روش حذف Stream های فایل

می توان جهت حذف کردن Stream های یک فایل با استفاده از فرامین powershell به صورت زیر عمل کرد

```
Remove-Item .\1.txt -Stream moslemADS
```



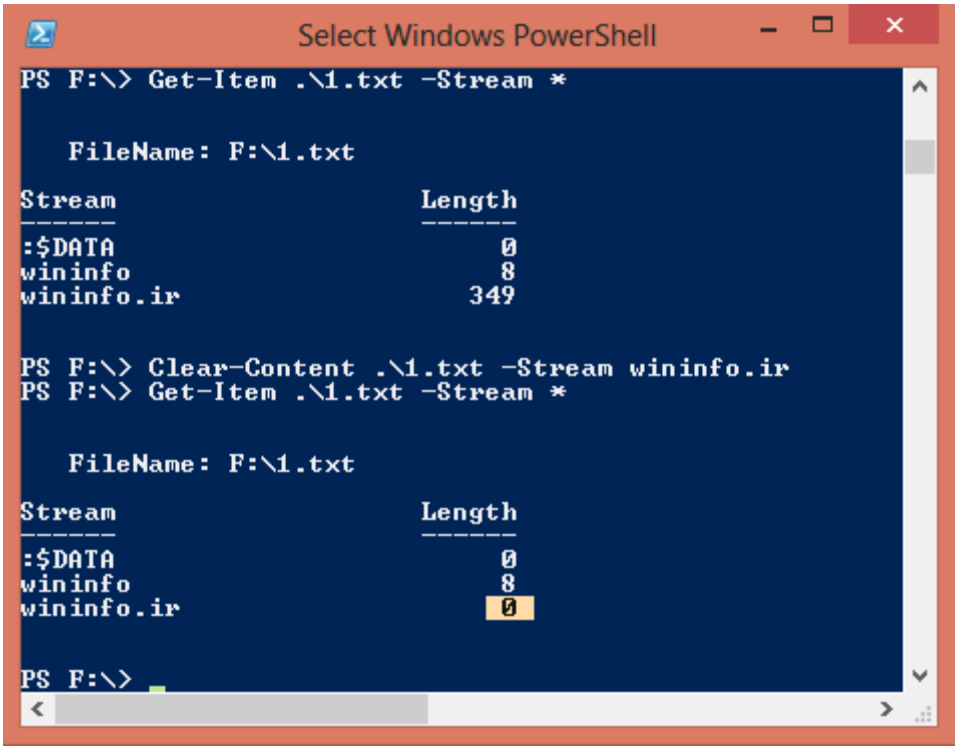
همانطور که در شکل بالا می بینید Stream با نام moslemADS ساخته شد و مقدار moslem mKST,wininfo را به آن دادیم سپس لیست تمامی Stream های موجود در فایل را بررسی کردیم و Stream ساخته شده را با فرمان Remove-item حذف کردیم .

جهت حذف تمامی مقادیر Steam می توان در powershell از فرمان زیر استفاده کرد

پاک کردن محتویات داخل Streamموجود در فایل

بسیاری از جاها ما نمی خواهیم نام Stream از بین رود بلکه می خواهیم محتویات آن را از بین ببریم در این صورت می توانیم از فرمان زیر استفاده کنیم .

```
Clear-Content .\1.txt -Stream wininfo.ir
```

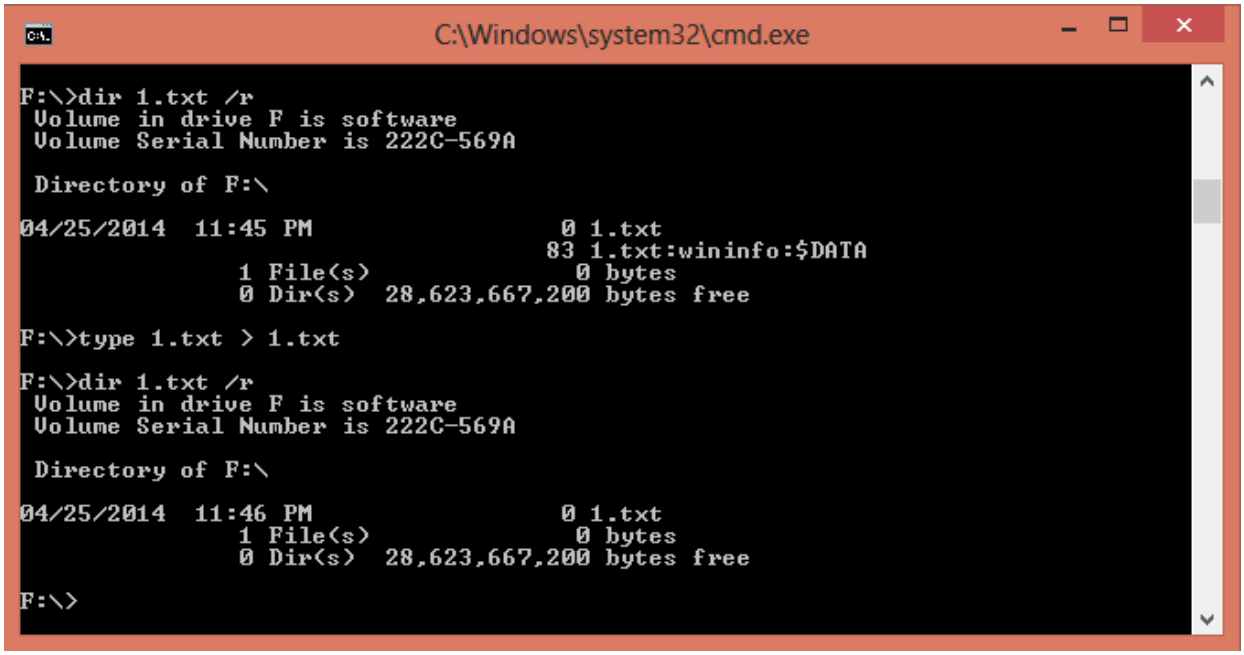


در این شکل مقدار wininfo.ir بعد از اجرای دستور 0 شده است اما نام آن پاک نشده است .

حذف کلیه ی Stream ها در CMD ویندوز

به کمک فرامین CMD هم امکان حذف Stream ها وجود دارد کافیست فرمان زیر را بنویسید

```
Type filename > filename
```

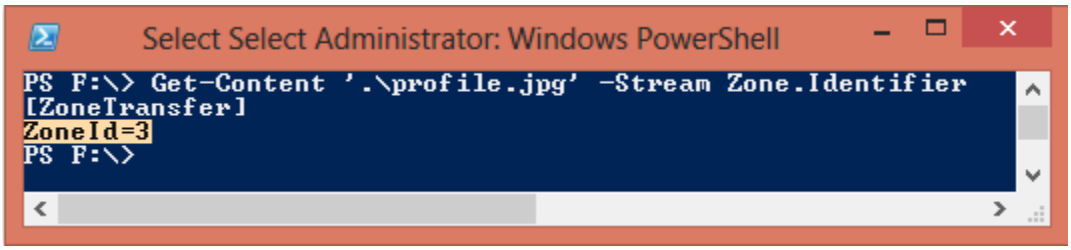


همانطور که در بالا می بینید txt:wininfo:$DATA.1 را برایمان نشان داده است در اولین گزارش گیری اما بعد از اجرای دستور type 1.txt > 1.txt دیگر Stream ها کامل پاک شده اند .

بررسی Zone.Identifier های stream

فایلی که در کامپیوتر شما وجود دارد همیشه یا از طریق اینترنت و و یا اینکه از طریق فلاش و یک کامپیوتر شبکه وارد سیستم شده است

در صورتی که شما از طریق internet explorer یک فایل را از اینترنت بگیرید همیشه به صورت اتوماتیک یک Stream در قسمت $DATA به فایل اضافه می شود که از 0 تا 5 شماره گذاری می شود .



هر کدام از این شماره ها نشان می دهند که فایل چگونه وارد سیستم شما شده است .

0 My Computer

1 Local Intranet Zone

2 Trusted sites Zone

3 Internet Zone

4 Restricted Sites Zone

که این همان لیست موجود در internet option می باشد .

Author : Moslem Haghighian
Nike name : l4tr0d3ctism
Website : www.wininfo.ir
Email : l4tr0d3ctism@gmail.com , moslem.haghighian@yahoo.com
Date of birth : 1989
Abute me : Microsoft security researcher and developer