

Windows Alternate Data Streams (ADS)

November 13, 2025

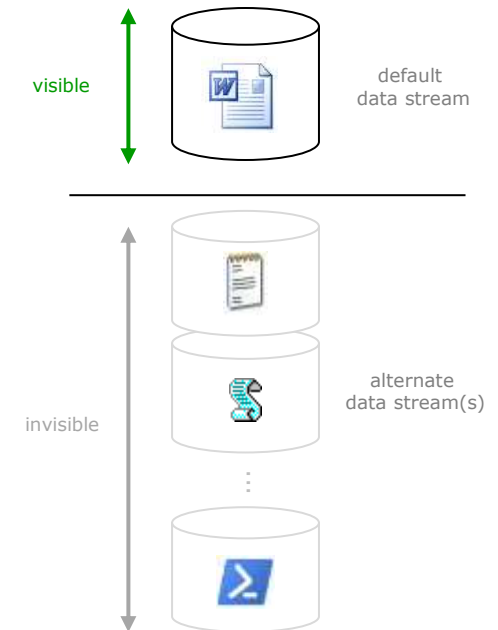
Marc Ochsenmeier

[@ochsenmeier](#)

www.winitor.com

Introduction

- A file is more than one file
- A file is a container
 - one visible file
 - none or several invisible files
 - ...with any kind of content and size
- A file is basically the first (default) file of a file

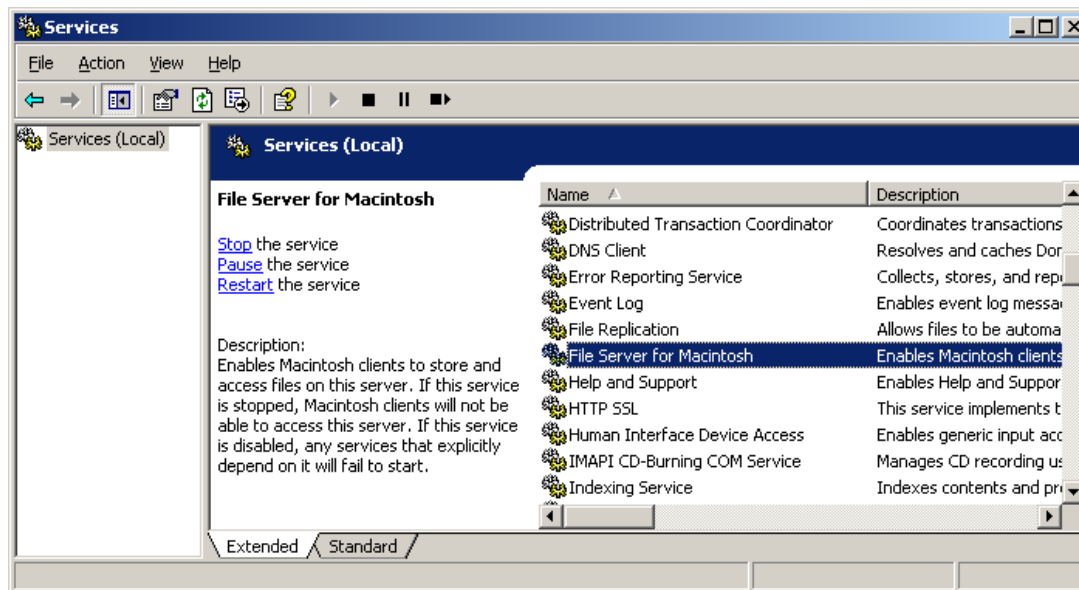


Importance

- ADS is inherent to NTFS infrastructure
 - cannot be disabled
 - is almost unknown
 - is stealth
- ADS can contain data
 - must be handled by backup
- ADS can contain code
 - must be handled by antivirus

History

- Since the inception of Windows NT 3.1
 - sharing file with Macintosh clients
 - separation data (content) and resource (management) forks
- Windows FSFM service



NTFS Basics - Streams

- A file is a **collection** of **attributes** stored as **separated** streams
 - some are mandatory (name, time stamps, ...)
 - some are optional (security descriptor, EFS, link, ...)
 - some may appear more than once (name, data)



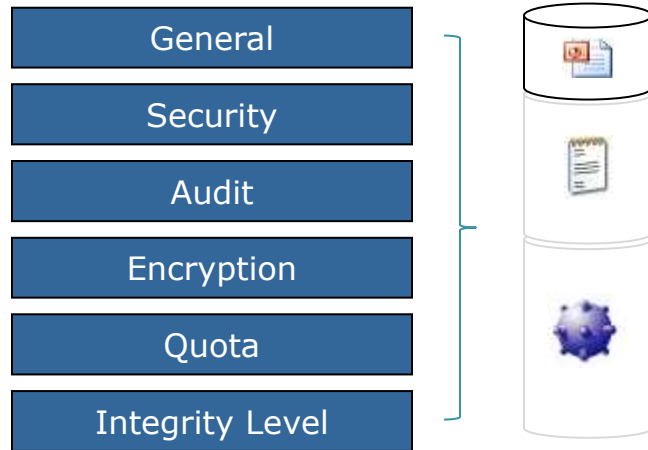
NTFS Basics – File Content

- The ***content*** of a file is one stream among others
- Windows doesn't manage files, it manages streams

\$STANDARD_INFORMATION	General (read-only, archive, time stamps, file creation, last modified, hardlink count....) attributes.
\$FILE_NAME	<u>one or more</u> filename (long file name, "8.3 name", hardlink name)
\$SECURITY_DESCRIPTOR	Discretionary Access Control List (DACL), Security Access Control List (SACL) and Integrity Level (IL).
\$DATA	<i>file</i> has <u>one</u> default (unnamed, primary) data stream. <i>directory</i> has <u>no</u> default (unnamed, primary) data stream.
\$EFS	version, list of authorized users, etc....

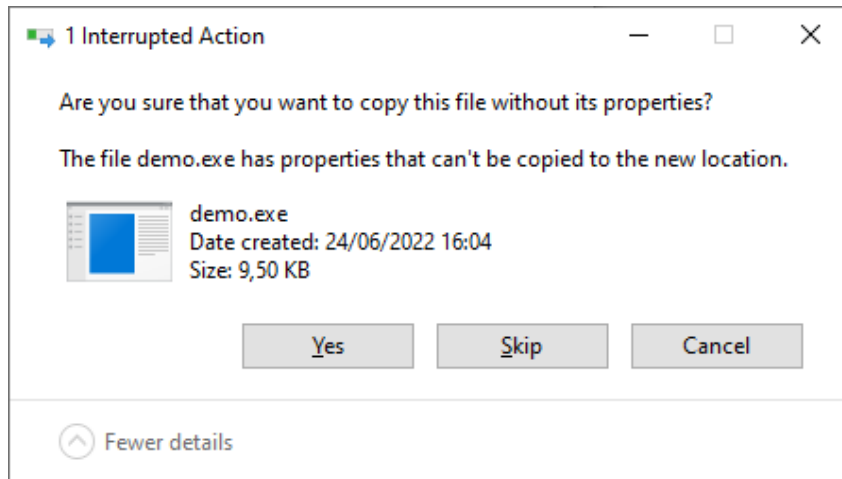
NTFS - Properties

- All streams of a file are ruled by common properties



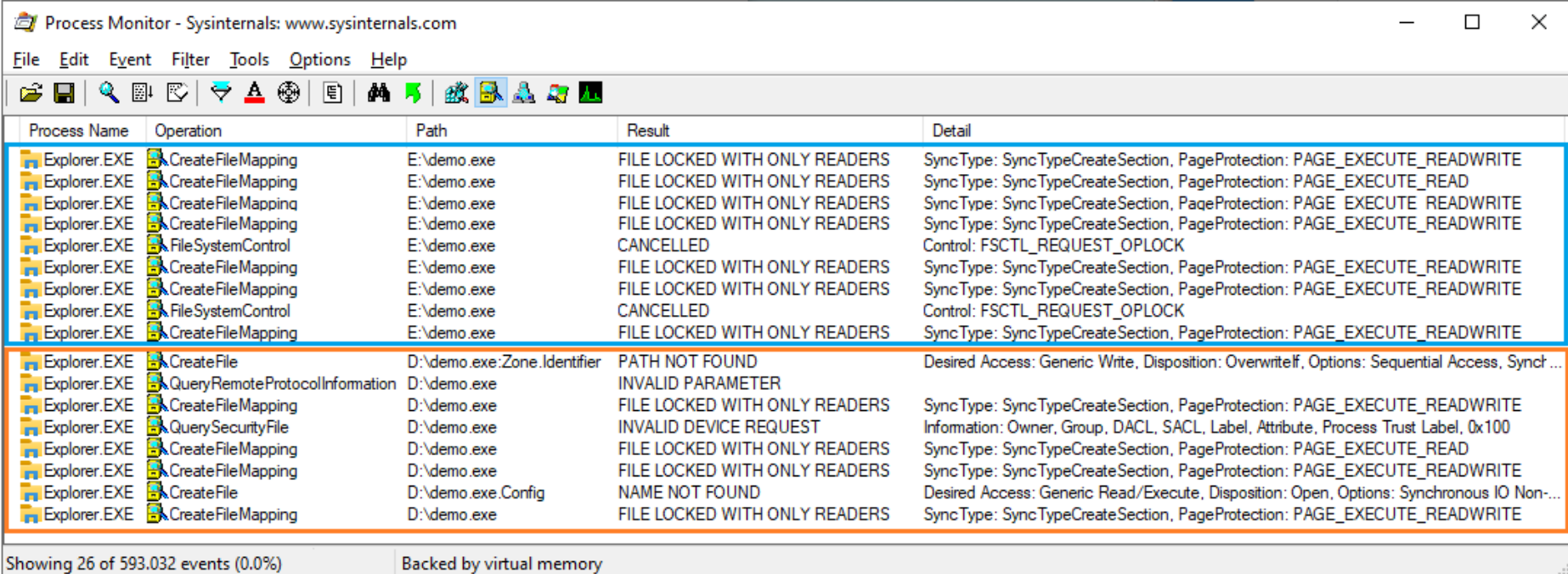
Support

- ADS is only supported on NTFS
 - ADS removed once a file leaves NTFS



Support

- ADS is only supported on NTFS
 - ADS removed once a file leaves NTFS



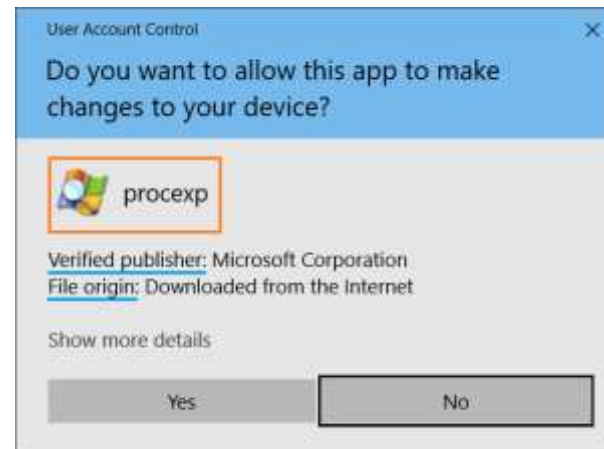
The screenshot shows the Process Monitor application window with a table of system events. The table has five columns: Process Name, Operation, Path, Result, and Detail. The events are grouped into two sections. The first section shows Explorer.EXE performing CreateFileMapping operations on E:\demo.exe, which result in 'FILE LOCKED WITH ONLY READERS' and 'CANCELLED' messages. The second section shows Explorer.EXE performing various operations on D:\demo.exe, including CreateFile, QueryRemoteProtocolInformation, CreateFileMapping, QuerySecurityFile, and CreateFile, which result in 'PATH NOT FOUND', 'INVALID PARAMETER', 'INVALID DEVICE REQUEST', and 'NAME NOT FOUND'.

Process Name	Operation	Path	Result	Detail
Explorer.EXE	CreateFileMapping	E:\demo.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE
Explorer.EXE	CreateFileMapping	E:\demo.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READ
Explorer.EXE	CreateFileMapping	E:\demo.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE
Explorer.EXE	CreateFileMapping	E:\demo.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE
Explorer.EXE	FileSystemControl	E:\demo.exe	CANCELLED	Control: FSCTL_REQUEST_OPLOCK
Explorer.EXE	CreateFileMapping	E:\demo.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE
Explorer.EXE	CreateFileMapping	E:\demo.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE
Explorer.EXE	FileSystemControl	E:\demo.exe	CANCELLED	Control: FSCTL_REQUEST_OPLOCK
Explorer.EXE	CreateFileMapping	E:\demo.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE
Explorer.EXE	CreateFile	D:\demo.exe:Zone.Identifier	PATH NOT FOUND	Desired Access: Generic Write, Disposition: OverwriteIf, Options: Sequential Access, Syncf ...
Explorer.EXE	QueryRemoteProtocolInformation	D:\demo.exe	INVALID PARAMETER	
Explorer.EXE	CreateFileMapping	D:\demo.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE
Explorer.EXE	QuerySecurityFile	D:\demo.exe	INVALID DEVICE REQUEST	Information: Owner, Group, DACL, SACL, Label, Attribute, Process Trust Label, 0x100
Explorer.EXE	CreateFileMapping	D:\demo.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READ
Explorer.EXE	CreateFileMapping	D:\demo.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE
Explorer.EXE	CreateFile	D:\demo.exe:Config	NAME NOT FOUND	Desired Access: Generic Read/Execute, Disposition: Open, Options: Synchronous IO Non-...
Explorer.EXE	CreateFileMapping	D:\demo.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE

Showing 26 of 593.032 events (0.0%) Backed by virtual memory

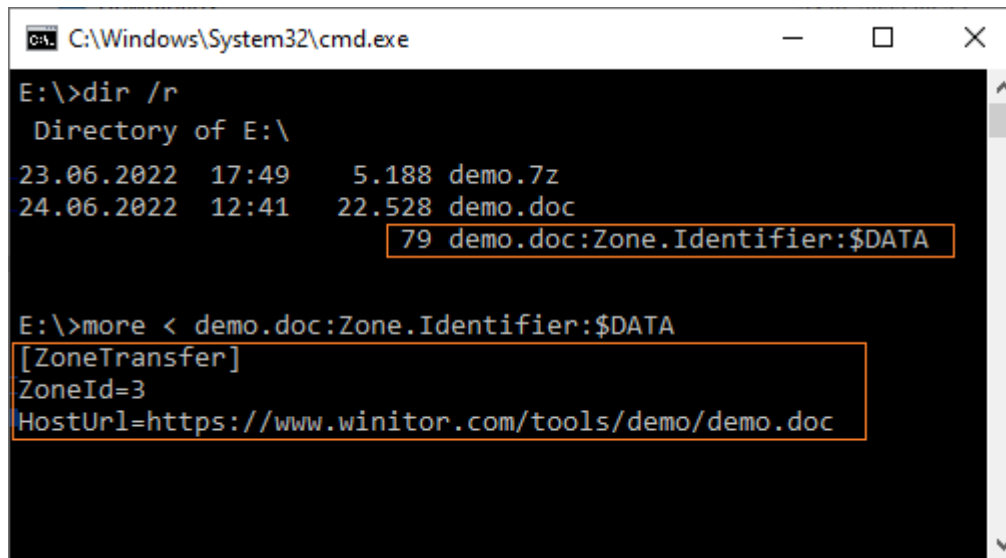
Usage > Zone Model

- A technique (aka. “Mark of the Web” - **MotW**) to document the origin of downloaded files
 - Execution triggers digital signature check and UAC consent



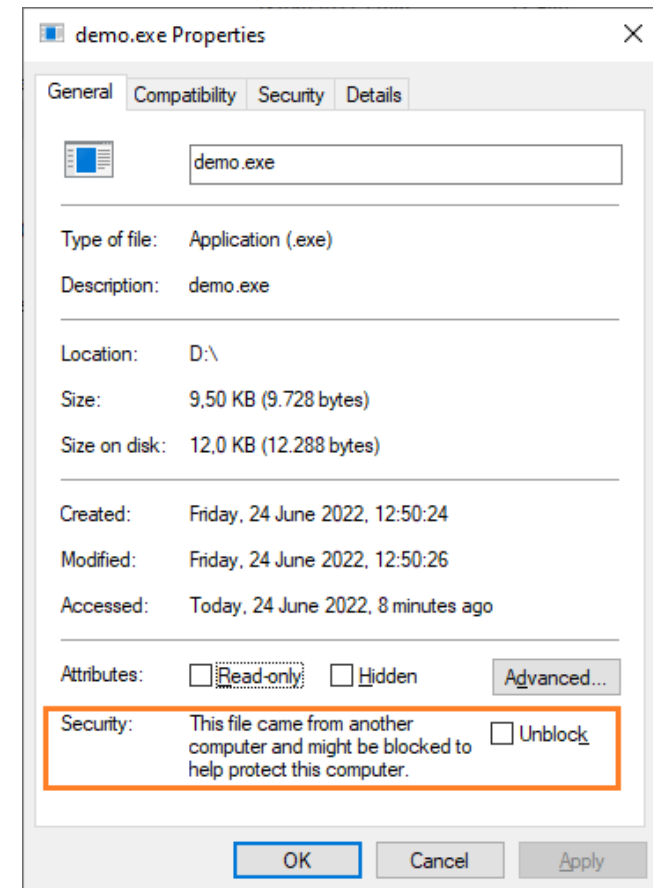
Usage > Internet Explorer

- The trust level of downloaded file stored as „Zone.Identifier“



```
C:\Windows\System32\cmd.exe
E:\>dir /r
Directory of E:\
23.06.2022 17:49    5.188 demo.7z
24.06.2022 12:41   22.528 demo.doc
79 demo.doc:Zone.Identifier:$DATA

E:\>more < demo.doc:Zone.Identifier:$DATA
[ZoneTransfer]
ZoneId=3
HostUrl=https://www.winator.com/tools/demo/demo.doc
```



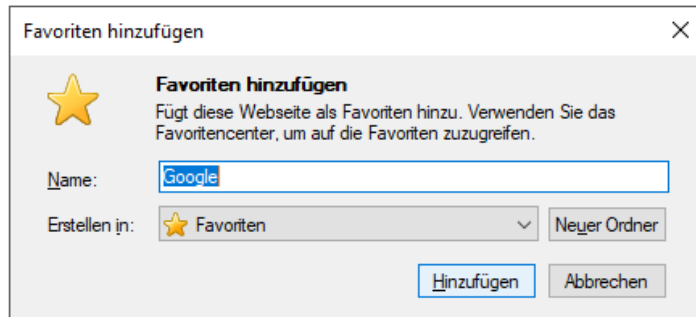
Usage > Office

- Office is MOTW aware and opens downloaded document in a “Protected View” mode to implement security boundary.



Usage > Internet Explorer

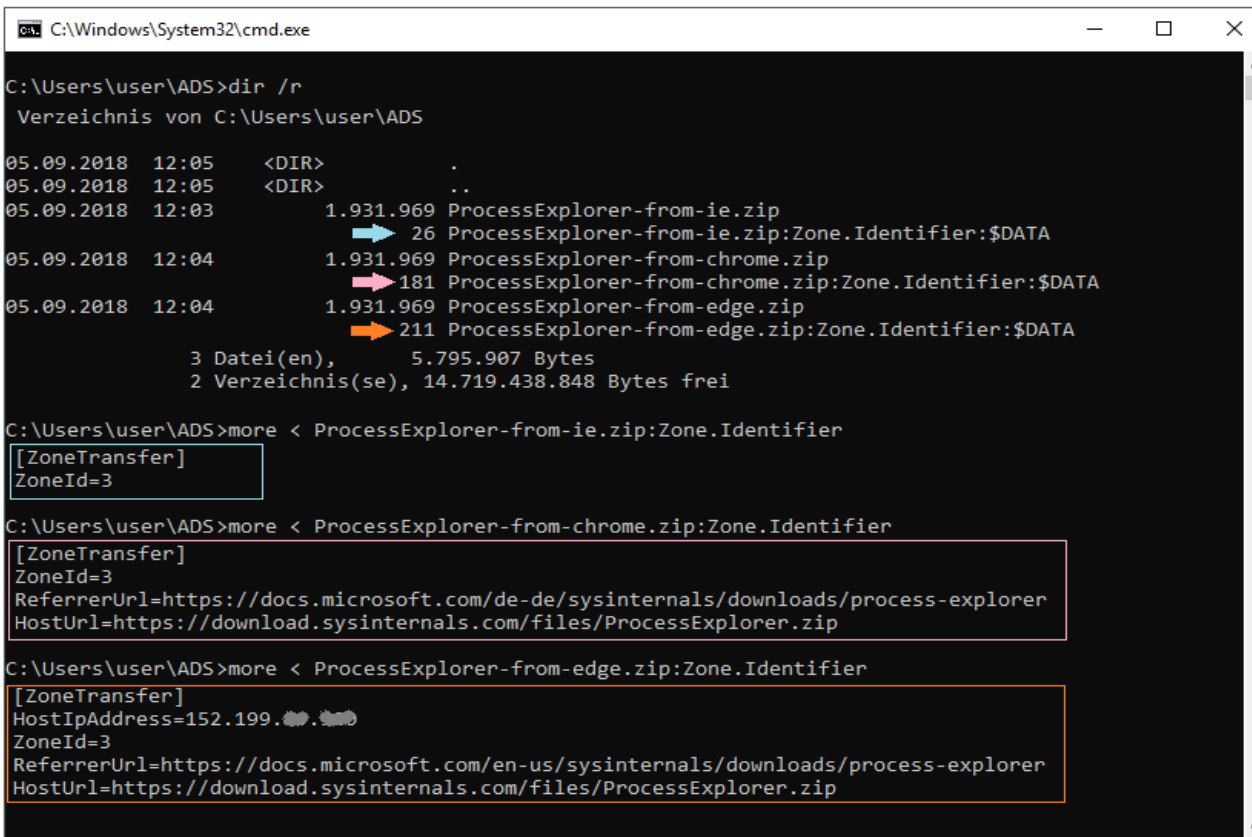
- Icons for Favorites are saved in the „favicon“ ADS of URL files



```
C:\Windows\System32\cmd.exe
C:\Users\user\Favorites>dir /r
05.09.2018  14:09    <DIR>      .
05.09.2018  14:09    <DIR>      ..
05.09.2018  14:05              270 Google.url
                5.430 Google.url:favicon:$DATA
                1 Datei(en),           270 Bytes
                3 Verzeichnis(se), 14.679.748.608 Bytes frei
```

Usage > Internet Browsers

- Recent browsers exhibit more metadata into ADS



```
C:\Windows\System32\cmd.exe
C:\Users\user\ADS>dir /r
Verzeichnis von C:\Users\user\ADS
05.09.2018 12:05 <DIR> .
05.09.2018 12:05 <DIR> ..
05.09.2018 12:03      1.931.969 ProcessExplorer-from-ie.zip
                26 ProcessExplorer-from-ie.zip:Zone.Identifier:$DATA
05.09.2018 12:04      1.931.969 ProcessExplorer-from-chrome.zip
                181 ProcessExplorer-from-chrome.zip:Zone.Identifier:$DATA
05.09.2018 12:04      1.931.969 ProcessExplorer-from-edge.zip
                211 ProcessExplorer-from-edge.zip:Zone.Identifier:$DATA
                3 Datei(en),      5.795.907 Bytes
                2 Verzeichnis(se), 14.719.438.848 Bytes frei

C:\Users\user\ADS>more < ProcessExplorer-from-ie.zip:Zone.Identifier
[ZoneTransfer]
ZoneId=3

C:\Users\user\ADS>more < ProcessExplorer-from-chrome.zip:Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://docs.microsoft.com/de-de/sysinternals/downloads/process-explorer
HostUrl=https://download.sysinternals.com/files/ProcessExplorer.zip

C:\Users\user\ADS>more < ProcessExplorer-from-edge.zip:Zone.Identifier
[ZoneTransfer]
HostIpAddress=152.199.
ZoneId=3
ReferrerUrl=https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer
HostUrl=https://download.sysinternals.com/files/ProcessExplorer.zip
```

Usage > Windows Change Journal

- Windows Change Journal is an ADS

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

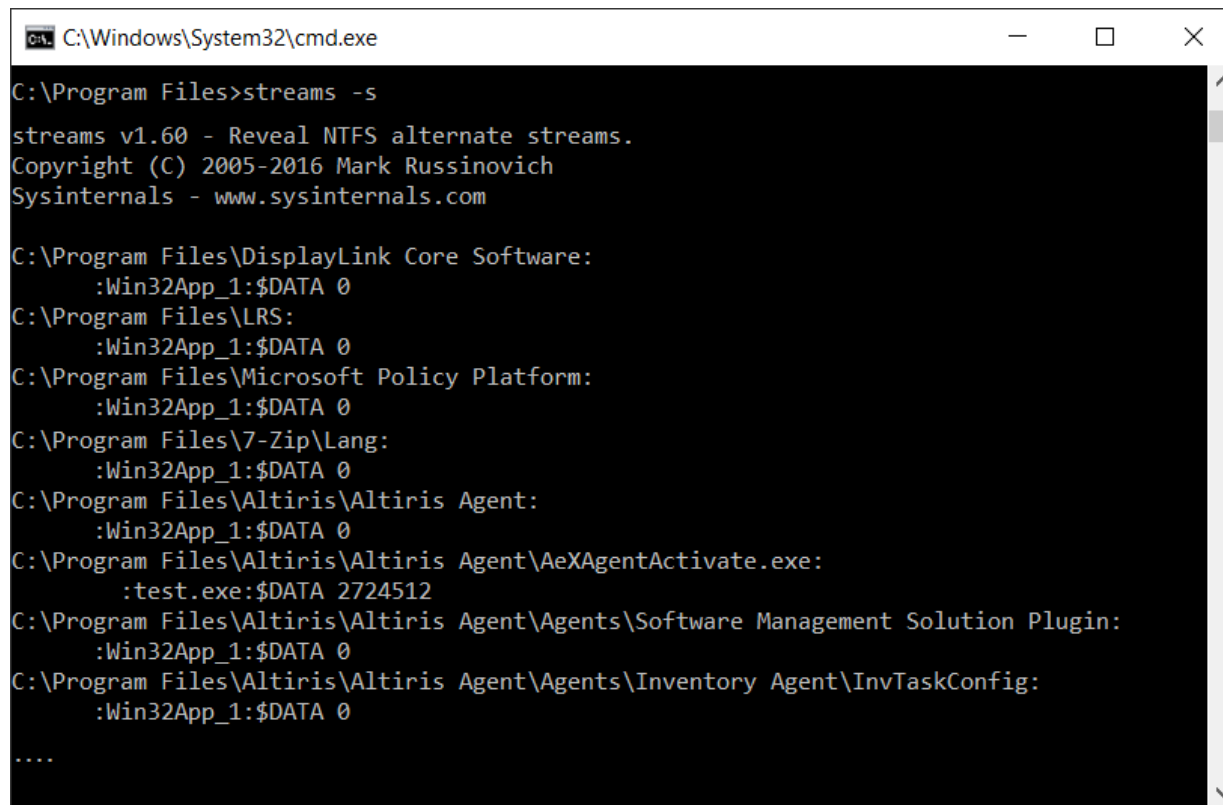
Process Name	Operation	Path	Result	Detail	Sequence
hh.exe	IRP_MJ_READ	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.291.200, Length: 96, I/O F...	475
taskhostw.exe	IRP_MJ_READ	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.295.296, Length: 96, I/O F...	476
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.979.328, Length: 4.096, I/...	497
System	IRP_MJ_READ	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.983.424, Length: 104, I/O ...	498
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.983.424, Length: 4.096, I/...	499
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.979.328, Length: 4.096, I/...	500
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.983.424, Length: 4.096, I/...	501
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.983.424, Length: 4.096, I/...	502
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.983.424, Length: 4.096, I/...	503
smartscreen.exe	IRP_MJ_READ	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.987.520, Length: 88, I/O F...	504
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.983.424, Length: 4.096, I/...	505
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.987.520, Length: 4.096, I/...	506
SystemSettings.exe	IRP_MJ_READ	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.991.616, Length: 112, I/O ...	507
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.991.616, Length: 4.096, I/...	508
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.987.520, Length: 4.096, I/...	509
svchost.exe	IRP_MJ_READ	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.995.712, Length: 112, I/O ...	510
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.991.616, Length: 8.192, I/...	511
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.995.712, Length: 4.096, I/...	512
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.995.712, Length: 4.096, I/...	513
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.995.712, Length: 4.096, I/...	514
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.995.712, Length: 4.096, I/...	515
System	IRP_MJ_READ	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.999.808, Length: 80, I/O F...	516
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.999.808, Length: 4.096, I/...	517
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.995.712, Length: 4.096, I/...	518
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.999.808, Length: 4.096, I/...	519
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.999.808, Length: 4.096, I/...	520
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.999.808, Length: 4.096, I/...	521
DllHost.exe	IRP_MJ_READ	C:\Extend\UsnJml:\$	SUCCESS	Offset: 43.003.904, Length: 88, I/O F...	522
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 43.003.904, Length: 4.096, I/...	523
System	IRP_MJ_WRITE	C:\Extend\UsnJml:\$	SUCCESS	Offset: 42.999.808, Length: 4.096, I/...	524

Showing 525 of 34.340.922 events (0.0%) Backed by virtual memory

File ADS

Usage > Storage Service

- „Win32App_1“ ADS (place holder?) in many directories



```
C:\Windows\System32\cmd.exe
C:\Program Files>streams -s
streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Program Files\DisplayLink Core Software:
:Win32App_1:$DATA 0
C:\Program Files\LRS:
:Win32App_1:$DATA 0
C:\Program Files\Microsoft Policy Platform:
:Win32App_1:$DATA 0
C:\Program Files\7-Zip\Lang:
:Win32App_1:$DATA 0
C:\Program Files\Altiris\Altiris Agent:
:Win32App_1:$DATA 0
C:\Program Files\Altiris\Altiris Agent\AeXAgentActivate.exe:
:test.exe:$DATA 2724512
C:\Program Files\Altiris\Altiris Agent\Agents\Software Management Solution Plugin:
:Win32App_1:$DATA 0
C:\Program Files\Altiris\Altiris Agent\Agents\Inventory Agent\InvTaskConfig:
:Win32App_1:$DATA 0
....
```

Usage > Symantec Endpoint Protection

- Symantec uses “Zone.Identifier” ...but not as MOTW

```
C:\Windows\System32\cmd.exe

C:\ProgramData\Symantec>streams -s

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

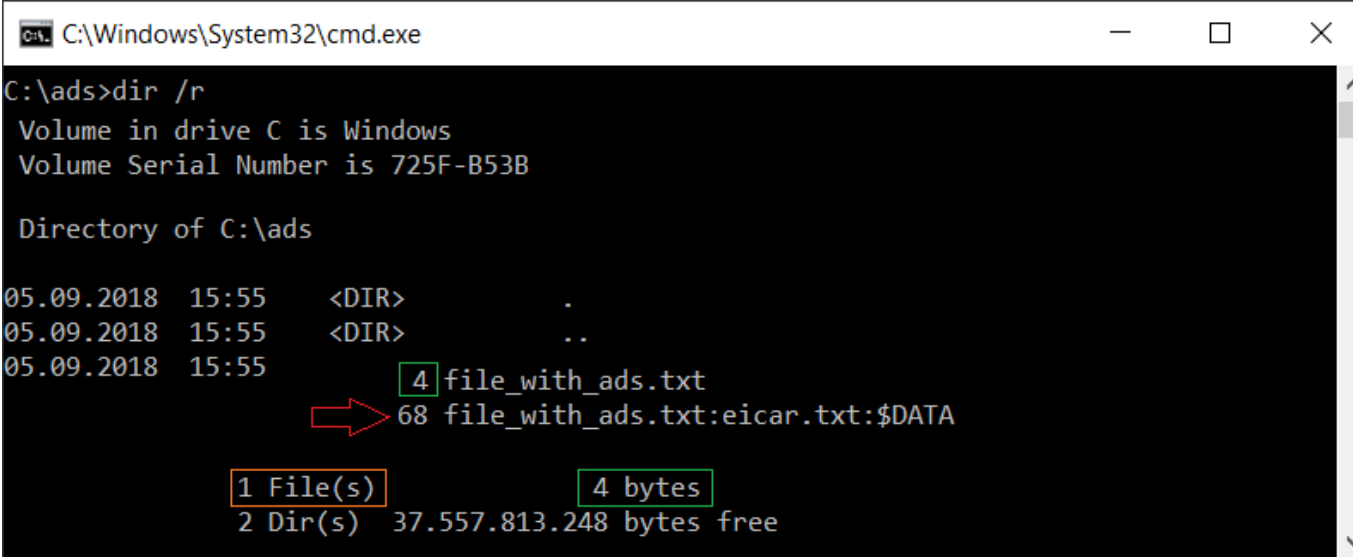
C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Quarantine\07700003\5FF53552.VBN:
:Zone.Identifier:$DATA          26
C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Quarantine\0770000A\5FF5355E.VBN:
:Zone.Identifier:$DATA          26
```

Symantec.zone.identifier.hex

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	01	0D	0A	35	34	3F	0E	28	3B	34	29	3C	3F	28	07	57	...54?.(;4)<?(.W
0010h:	50	0D	0A	35	34	3F	13	3E	67	69	57	50	0D	0A			P..54?.>giWP..

Visibility

- But size and count of ADS still ignored in the summary!



```
C:\Windows\System32\cmd.exe
C:\ads>dir /r
Volume in drive C is Windows
Volume Serial Number is 725F-B53B

Directory of C:\ads

05.09.2018  15:55    <DIR>          .
05.09.2018  15:55    <DIR>          ..
05.09.2018  15:55         4 file_with_ads.txt
                68 file_with_ads.txt:eicar.txt:$DATA

1 File(s)
2 Dir(s)  37.557.813.248 bytes free
```

Support > Windows built-in Binaries



LOLBAS ☆ Star 2,908

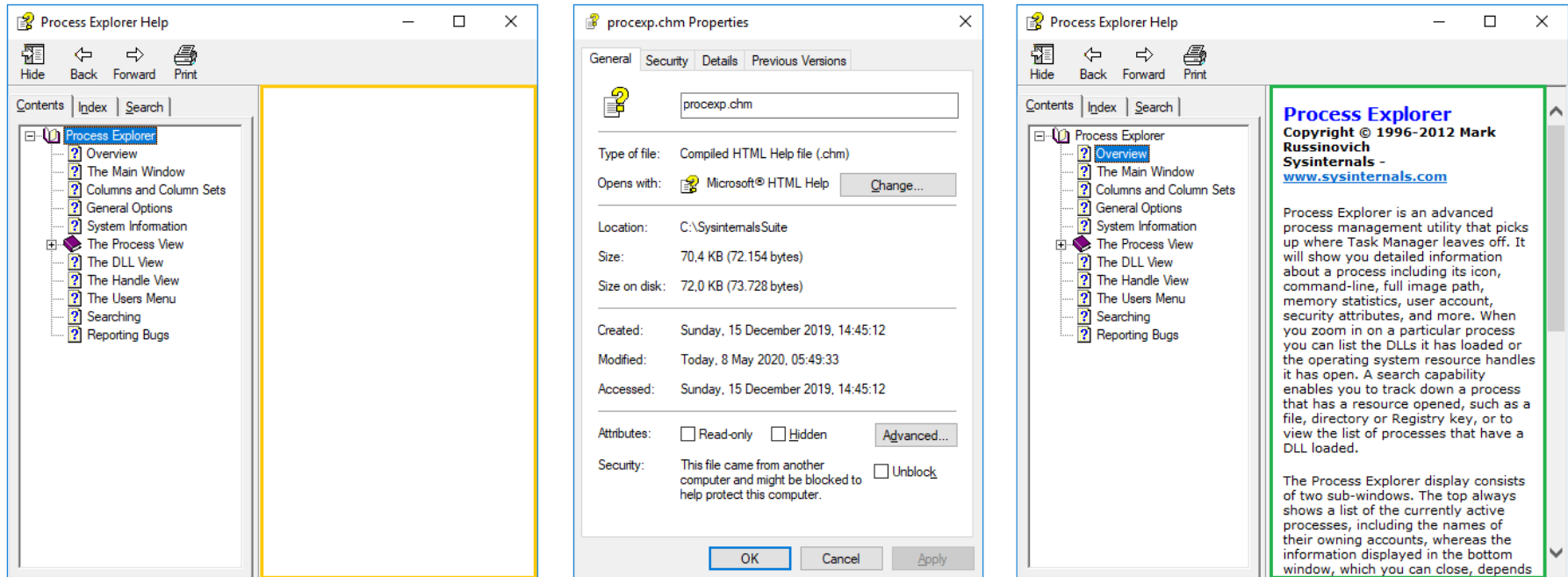
Living Off The Land Binaries and Scripts (and also Libraries)

Binary	Functions	Type
Bitsadmin.exe	Alternate data streams Download Copy Execute	Binaries
Certutil.exe	Download Alternate data streams Encode Decode	Binaries
Cmd.exe	Alternate data streams	Binaries
Control.exe	Alternate data streams	Binaries
Cscript.exe	Alternate data streams	Binaries
Diantz.exe	Alternate data streams Download	Binaries
Esentutil.exe	Copy Alternate data streams Download	Binaries
Expand.exe	Download Copy Alternate data streams	Binaries
Extrac32.exe	Alternate data streams Download Copy	Binaries
Findstr.exe	Alternate data streams Credentials Download	Binaries
Forfiles.exe	Execute Alternate data streams	Binaries
⋮		
Rundll32.exe	Execute Alternate data streams	Binaries
⋮		

<https://lolbas-project.github.io>

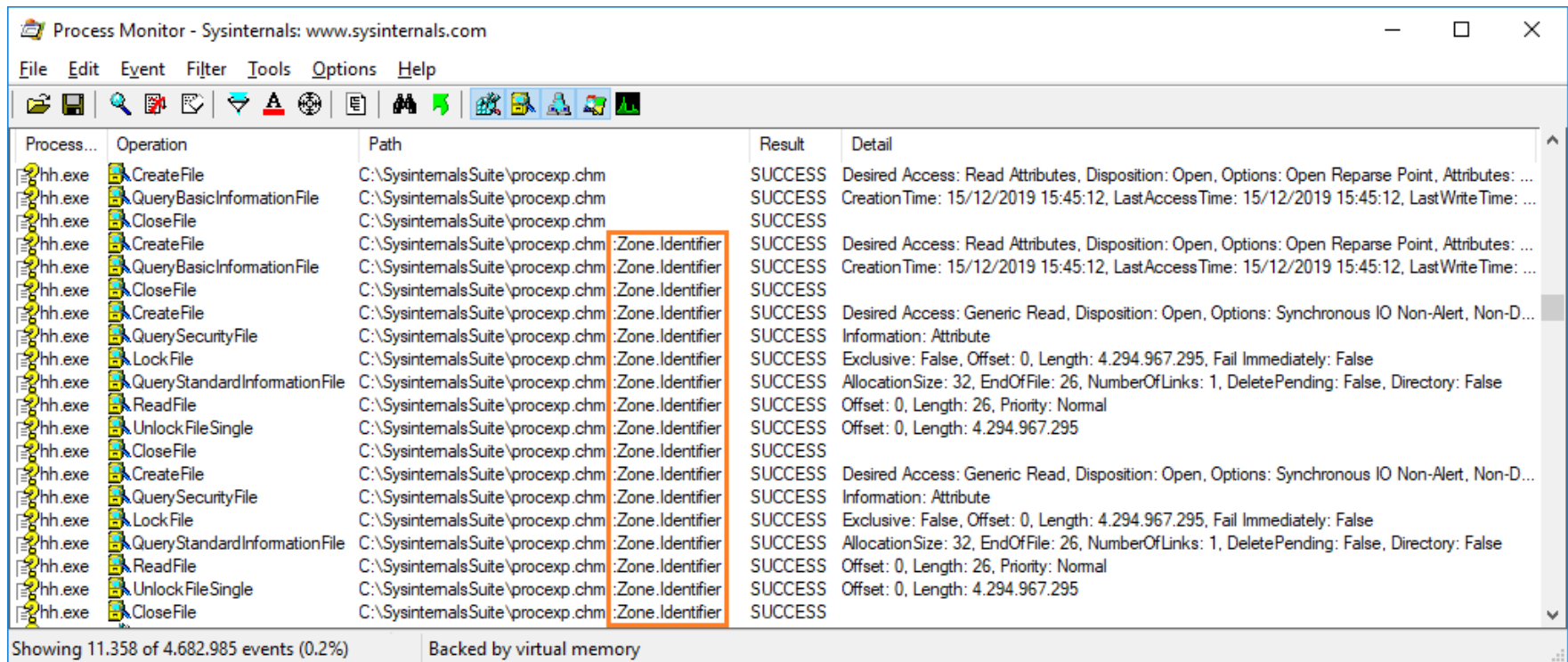
Impact

- Rendering a Compiled HTML Help (CHM) file



Impact

- Rendering a Compiled HTML Help (CHM) file



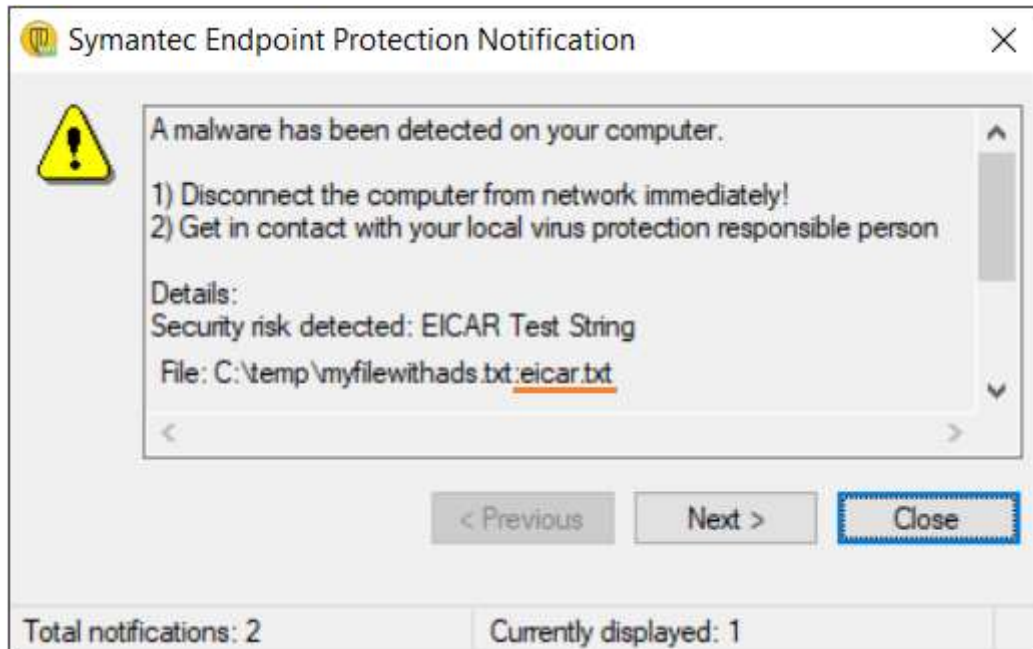
The screenshot shows the Process Monitor application window with a list of events. The 'Path' column for several events is highlighted in orange, showing the path to a CHM file with an alternate data stream named ':Zone.Identifier'.

Process...	Operation	Path	Result	Detail
hh.exe	CreateFile	C:\SysinternalsSuite\procexp.chm	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: ...
hh.exe	QueryBasicInformationFile	C:\SysinternalsSuite\procexp.chm	SUCCESS	CreationTime: 15/12/2019 15:45:12, LastAccessTime: 15/12/2019 15:45:12, LastWriteTime: ...
hh.exe	CloseFile	C:\SysinternalsSuite\procexp.chm	SUCCESS	
hh.exe	CreateFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: ...
hh.exe	QueryBasicInformationFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	CreationTime: 15/12/2019 15:45:12, LastAccessTime: 15/12/2019 15:45:12, LastWriteTime: ...
hh.exe	CloseFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	
hh.exe	CreateFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-D...
hh.exe	QuerySecurityFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	Information: Attribute
hh.exe	LockFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	Exclusive: False, Offset: 0, Length: 4.294.967.295, Fail Immediately: False
hh.exe	QueryStandardInformationFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	AllocationSize: 32, EndOfFile: 26, NumberOfLinks: 1, DeletePending: False, Directory: False
hh.exe	ReadFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	Offset: 0, Length: 26, Priority: Normal
hh.exe	UnlockFileSingle	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	Offset: 0, Length: 4.294.967.295
hh.exe	CloseFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	
hh.exe	CreateFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-D...
hh.exe	QuerySecurityFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	Information: Attribute
hh.exe	LockFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	Exclusive: False, Offset: 0, Length: 4.294.967.295, Fail Immediately: False
hh.exe	QueryStandardInformationFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	AllocationSize: 32, EndOfFile: 26, NumberOfLinks: 1, DeletePending: False, Directory: False
hh.exe	ReadFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	Offset: 0, Length: 26, Priority: Normal
hh.exe	UnlockFileSingle	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	Offset: 0, Length: 4.294.967.295
hh.exe	CloseFile	C:\SysinternalsSuite\procexp.chm :Zone.Identifier	SUCCESS	

Showing 11.358 of 4.682.985 events (0.2%) Backed by virtual memory

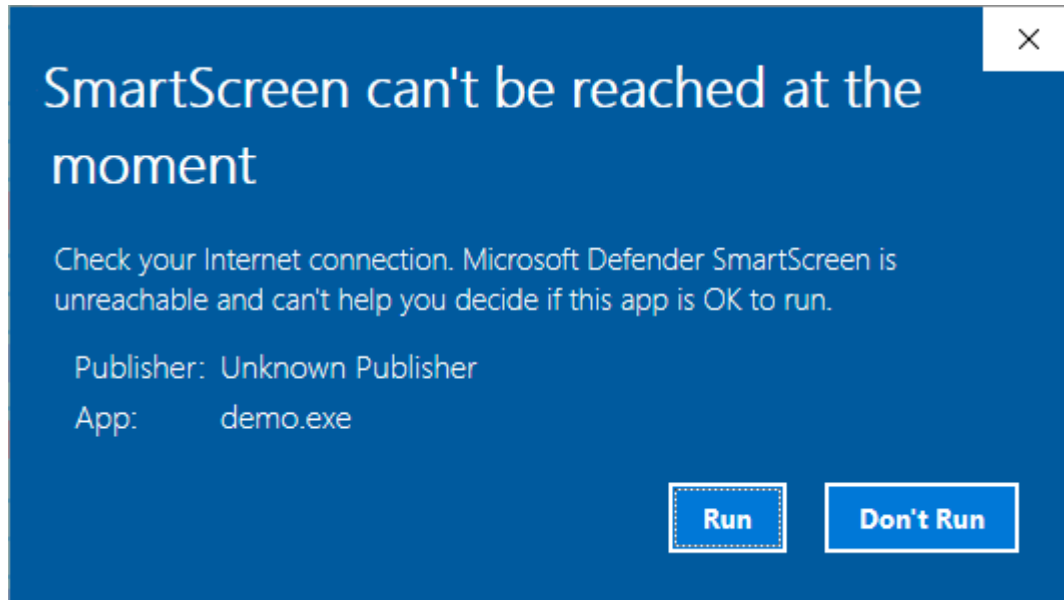
Detection

- Antivirus must handle ADS



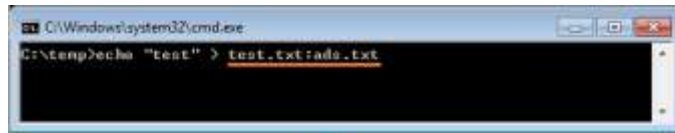
Detection

- Windows Defender SmartScreen is ADS aware

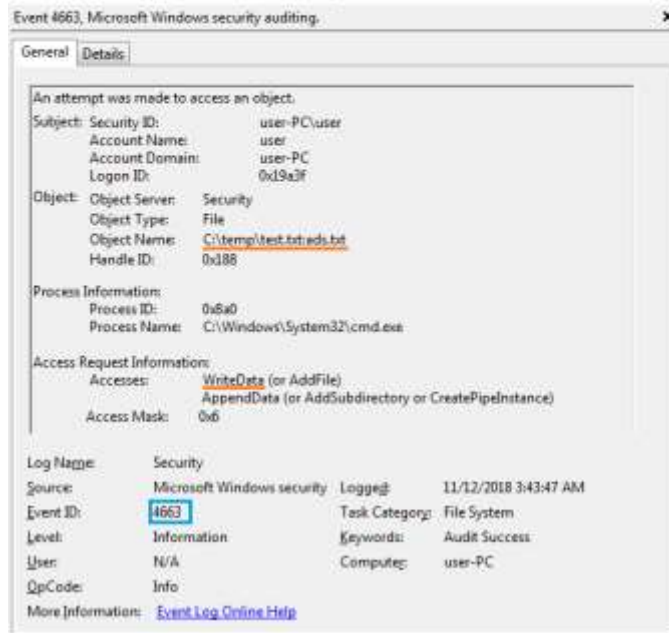


Detection

- When configured, the system audits access to ADS



```
C:\Windows\system32\cmd.exe
C:\temp>echo "test" > test.txt::ads.txt
```



Event 4663, Microsoft Windows security auditing.

General Details

An attempt was made to access an object.

Subject: Security ID: user-PC\user
Account Name: user
Account Domain: user-PC
Logon ID: 0xd9a3f

Object: Object Server: Security
Object Type: File
Object Name: C:\temp\test.txt::ads.txt
Handle ID: 0xd88

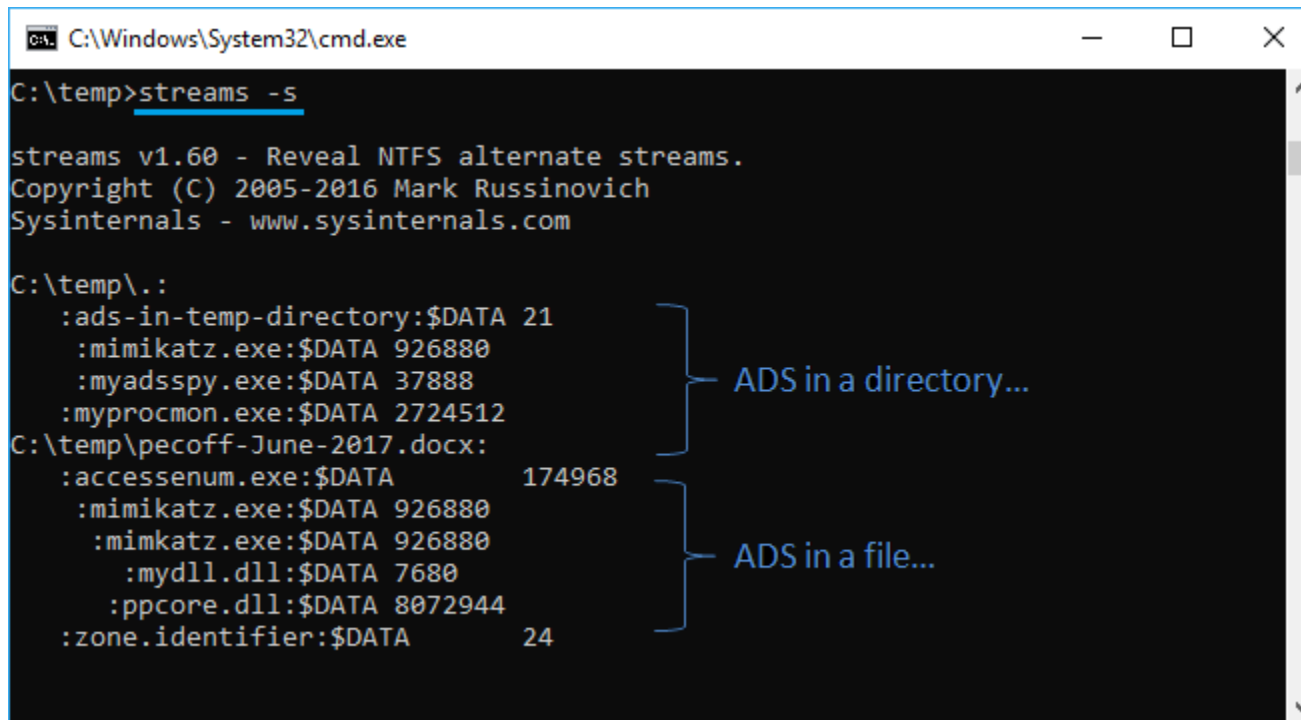
Process Information:
Process ID: 0x8a0
Process Name: C:\Windows\System32\cmd.exe

Access Request Information:
Accesses: WriteData (or AddFile)
AppendData (or AddSubdirectory or CreatePipeInstance)
Access Mask: 0xb

Log Name: Security
Source: Microsoft Windows security Logon@: 11/12/2018 3:43:47 AM
Event ID: 4663 Task Category: File System
Level: Information Keywords: Audit Success
User: N/A Computer: user-PC
OpCode: Info
More Information: [Event Log Online Help](#)

Detection

- streams.exe is your friend



```
C:\Windows\System32\cmd.exe
C:\temp>streams -s
streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\temp\.:
:ads-in-temp-directory:$DATA 21
:mimikatz.exe:$DATA 926880
:myadsspy.exe:$DATA 37888
:myprocmon.exe:$DATA 2724512
C:\temp\pecoff-June-2017.docx:
:accessenum.exe:$DATA 174968
:mimikatz.exe:$DATA 926880
:mimikatz.exe:$DATA 926880
:mydll.dll:$DATA 7680
:ppcore.dll:$DATA 8072944
:zone.identifier:$DATA 24
```

ADS in a directory...

ADS in a file...

Demo

- Following scenarios
 - Put ADS into an file
 - Put ADS into a directory
 - Execute a file located in ADS
 - Access ADS
 - Remove ADS

API

- Documented
 - CreateFile, ReadFile and WriteFile (kernel32.dll)
 - BackupRead, BackupSeek and BackupWrite (kernel32.dll)
 - FindFirstStream, FindNextStream (kernel32.dll)
 - IZoneIdentifier COM interface (urlmon.dll)
 - Powershell (get-item, get-content, remove-item...)
- Undocumented
 - NtQueryInformationFile (ntoskrnl.exe)

Issues

- Detection and removal
- Backup & restore
- Forensic
- File hash und checksum
- DOS Attack
- Code Execution
- Usage as persistency technique
- Misuse of valid ADS
- Unsupported outside NTFS

Summary

- ADS exist
- ADS cannot be disabled
- ADS are used
- ADS can be misused
- ADS must be watched

Tools

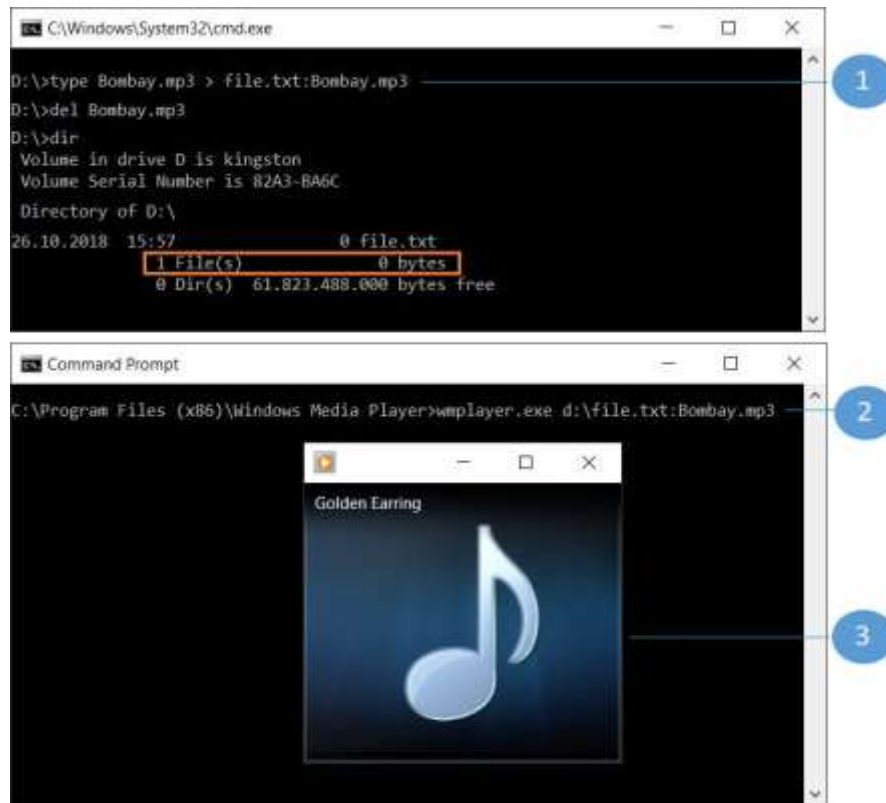
- Windows built-in tool “dir /r”
- Streams - www.sysinternals.com
- ADSSpy – www.bleepingcomputer.com

Backslide > demo > execute file located in ADS

- start
- mklink
- wmic
- csript
- wscript
- mshta
- powershell
- rundll32
- LoadLibrary
- WinExec

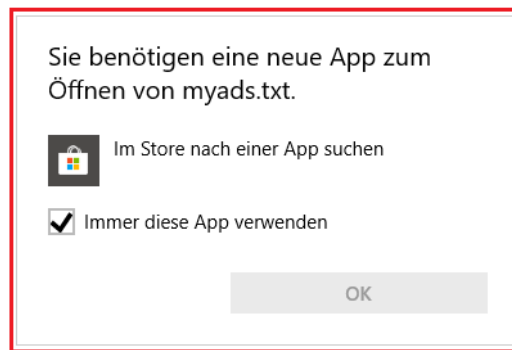
Backslide > demo

- Listening music located in an ADS

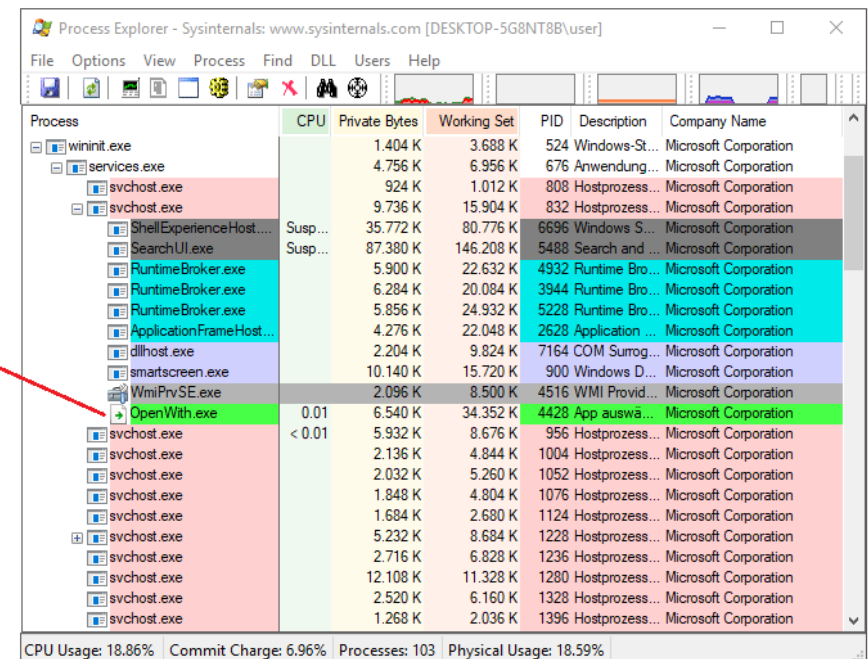


Backslide > demo

- start file:ads does not (fully) work anymore...



```
Eingabeaufforderung
Verzeichnis von C:\temp
27.08.2018 19:32 <DIR> .
27.08.2018 19:32 <DIR> ..
27.08.2018 19:32      0 myads.txt
                  461.680 myads.txt:Dbgview.exe:$DATA
                  1 Datei(en),      0 Bytes
                  2 Verzeichnis(se), 23.961.366.528 Bytes frei
C:\temp>start myads.txt:Dbgview.exe
```



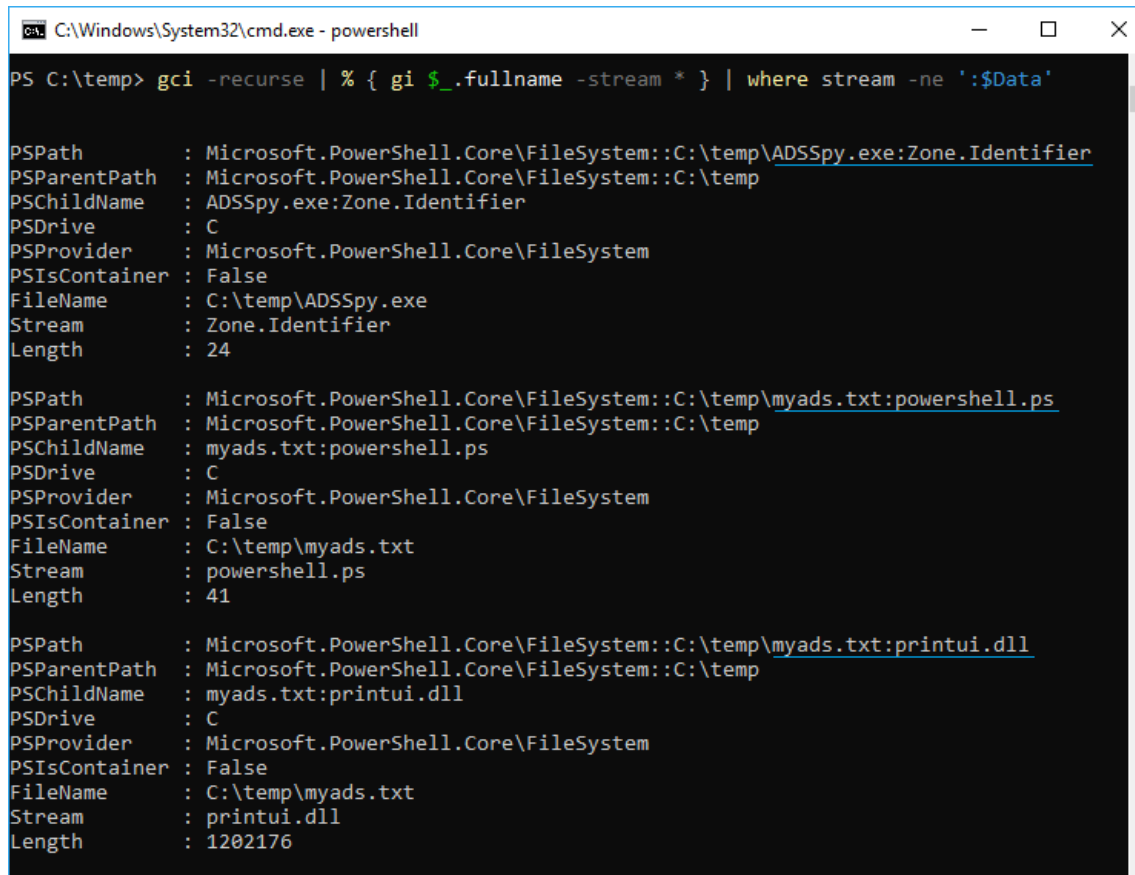
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-5G8NT8B\user]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
wininit.exe		1.404 K	3.688 K	524	Windows-St...	Microsoft Corporation
services.exe		4.756 K	6.956 K	676	Anwendung...	Microsoft Corporation
svchost.exe		924 K	1.012 K	808	Hostprozess...	Microsoft Corporation
svchost.exe		9.736 K	15.904 K	832	Hostprozess...	Microsoft Corporation
ShellExperienceHost...	Susp...	35.772 K	80.776 K	6696	Windows S...	Microsoft Corporation
SearchUI.exe	Susp...	87.380 K	146.208 K	5488	Search and...	Microsoft Corporation
RuntimeBroker.exe		5.900 K	22.632 K	4932	Runtime Bro...	Microsoft Corporation
RuntimeBroker.exe		6.284 K	20.084 K	3944	Runtime Bro...	Microsoft Corporation
RuntimeBroker.exe		5.856 K	24.932 K	5228	Runtime Bro...	Microsoft Corporation
ApplicationFrameHost...		4.276 K	22.048 K	2628	Application ...	Microsoft Corporation
dllhost.exe		2.204 K	9.824 K	7164	COM Surrog...	Microsoft Corporation
smartscreen.exe		10.140 K	15.720 K	900	Windows D...	Microsoft Corporation
WmiPrivSE.exe		2.096 K	8.500 K	4516	WMI Provid...	Microsoft Corporation
OpenWith.exe		6.540 K	34.352 K	4428	App auswä...	Microsoft Corporation
svchost.exe	0.01	5.932 K	8.676 K	956	Hostprozess...	Microsoft Corporation
svchost.exe	< 0.01	2.136 K	4.844 K	1004	Hostprozess...	Microsoft Corporation
svchost.exe		2.032 K	5.260 K	1052	Hostprozess...	Microsoft Corporation
svchost.exe		1.848 K	4.804 K	1076	Hostprozess...	Microsoft Corporation
svchost.exe		1.684 K	2.680 K	1124	Hostprozess...	Microsoft Corporation
svchost.exe		5.232 K	8.684 K	1228	Hostprozess...	Microsoft Corporation
svchost.exe		2.716 K	6.828 K	1236	Hostprozess...	Microsoft Corporation
svchost.exe		12.108 K	11.328 K	1280	Hostprozess...	Microsoft Corporation
svchost.exe		2.520 K	6.160 K	1328	Hostprozess...	Microsoft Corporation
svchost.exe		1.268 K	2.036 K	1396	Hostprozess...	Microsoft Corporation

CPU Usage: 18.86% | Commit Charge: 6.96% | Processes: 103 | Physical Usage: 18.59%

Backslide > demo

- Powershell > flexible programmatic access to handle ADS



```
C:\Windows\System32\cmd.exe - powershell
PS C:\temp> gci -recurse | % { gi $_.fullname -stream * } | where stream -ne ':$Data'

PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\temp\ADSSpy.exe:Zone.Identifier
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\temp
PSChildName  : ADSSpy.exe:Zone.Identifier
PSDrive      : C
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName     : C:\temp\ADSSpy.exe
Stream       : Zone.Identifier
Length       : 24

PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\temp\myads.txt:powershell.ps
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\temp
PSChildName  : myads.txt:powershell.ps
PSDrive      : C
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName     : C:\temp\myads.txt
Stream       : powershell.ps
Length       : 41

PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\temp\myads.txt:printui.dll
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\temp
PSChildName  : myads.txt:printui.dll
PSDrive      : C
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName     : C:\temp\myads.txt
Stream       : printui.dll
Length       : 1202176
```

Backslide > demo

- Powershell > flexible programmatic access to handle ADS

```
C:\Windows\System32\cmd.exe - powershell
PS C:\temp> get-item -path .\myads.txt -stream *
PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\temp\myads.txt:Dbgview.exe
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\temp
PSChildName  : myads.txt:Dbgview.exe
PSDrive     : C
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName    : C:\temp\myads.txt
Stream      : Dbgview.exe
Length      : 461680

PS C:\temp> get-item -path .\myads.txt -stream Dbgview.exe
PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\temp\myads.txt:Dbgview.exe
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\temp
PSChildName  : myads.txt:Dbgview.exe
PSDrive     : C
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName    : C:\temp\myads.txt
Stream      : Dbgview.exe
Length      : 461680

PS C:\temp> get-content -path .\myads.txt -stream DbgView.exe
MZ
!..LI!This program cannot be run in DOS mode.

$
  qxµ5hæ5hæ5hæ+äiæhæ+äýæ#hæpæ4hæ5hæiæhæpæ&hæ+äëæ|hæ+äüæ4hæ+äüæ4hæRich5hæ
o7äh   à
|² È   P   .   ø p   E   "   @   @   >>s   €   .t
ext   Å#   $   .rdata   j   @   Ž   (   @   @.data   -x   @   @   @   Å.r
src   .   P   @   @

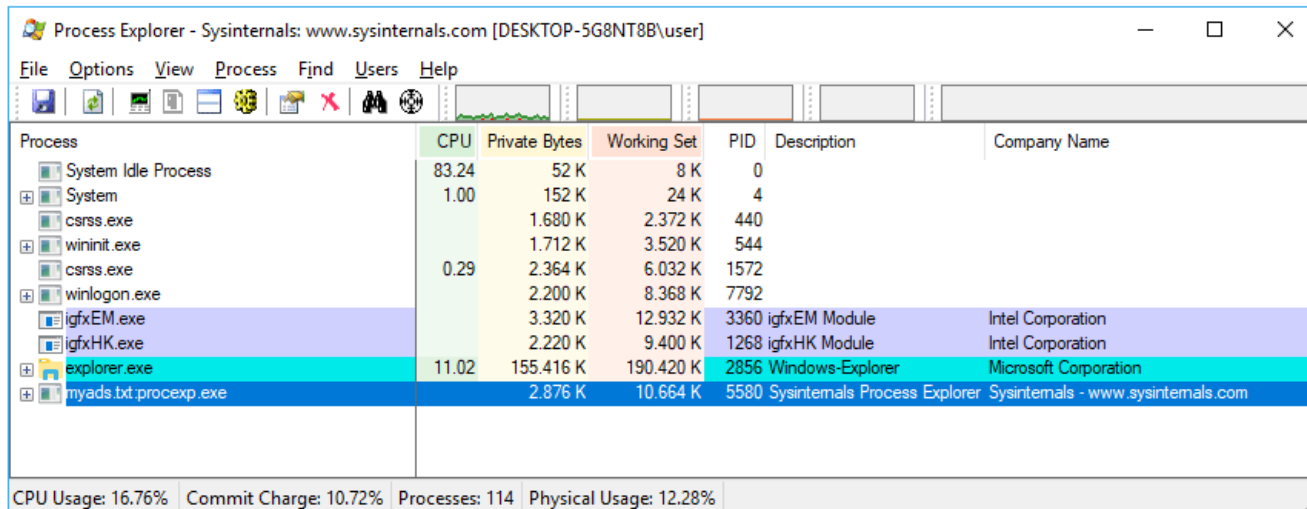
PS C:\temp> remove-item -path .\myads.txt -stream DbgView.exe
```

Backslide > demo

- WMI command-line utility

```
C:\Windows\System32\cmd.exe

C:\temp>wmic process call create c:\temp\test.txt:procexp.exe
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ProcessId = 11208;
    ReturnValue = 0;
};
```

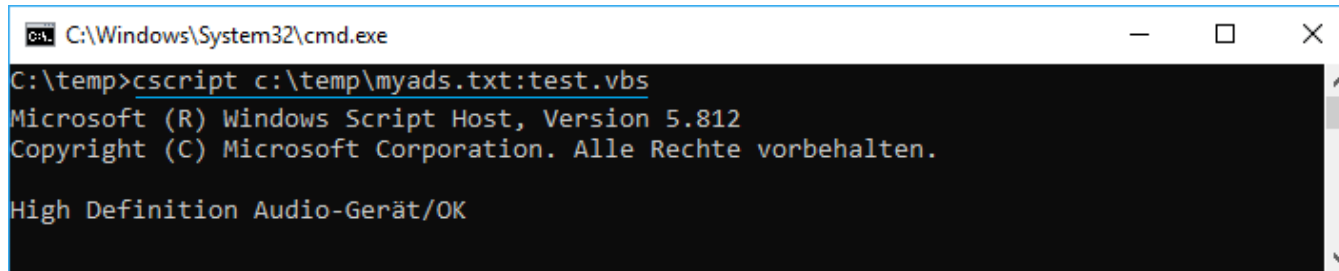


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	83.24	52 K	8 K	0		
System	1.00	152 K	24 K	4		
csrss.exe		1.680 K	2.372 K	440		
wininit.exe		1.712 K	3.520 K	544		
csrss.exe	0.29	2.364 K	6.032 K	1572		
winlogon.exe		2.200 K	8.368 K	7792		
igfxEM.exe		3.320 K	12.932 K	3360	igfxEM Module	Intel Corporation
igfxHK.exe		2.220 K	9.400 K	1268	igfxHK Module	Intel Corporation
explorer.exe	11.02	155.416 K	190.420 K	2856	Windows-Explorer	Microsoft Corporation
myads.txt:procexp.exe		2.876 K	10.664 K	5580	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com

CPU Usage: 16.76% Commit Charge: 10.72% Processes: 114 Physical Usage: 12.28%

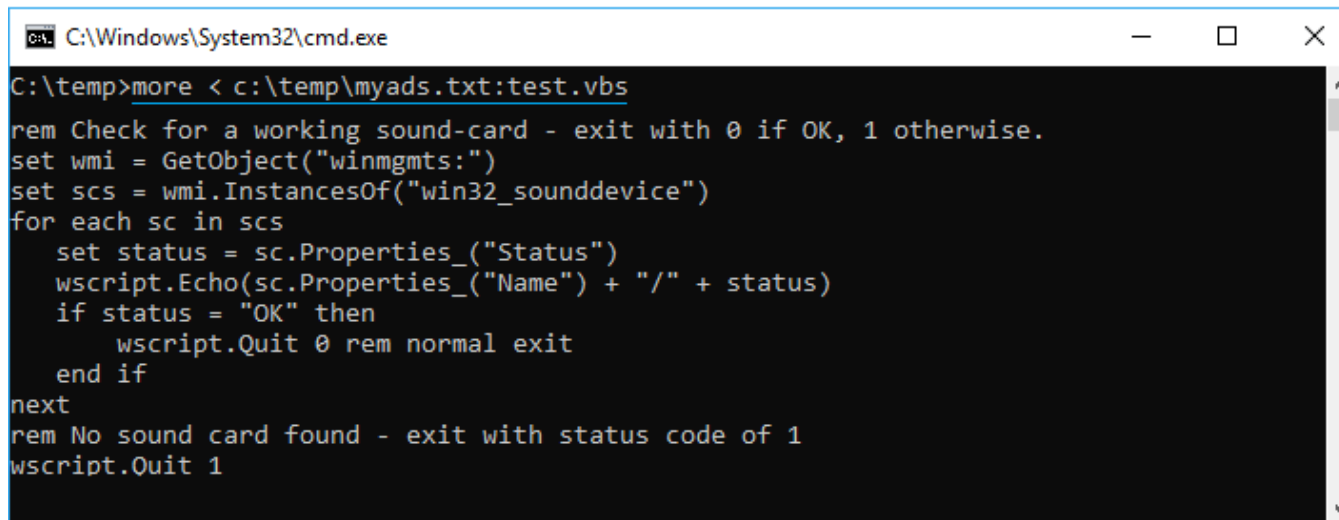
Backslide > demo

- Console based Script Host



```
C:\Windows\System32\cmd.exe
C:\temp>cscript c:\temp\myads.txt:test.vbs
Microsoft (R) Windows Script Host, Version 5.812
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

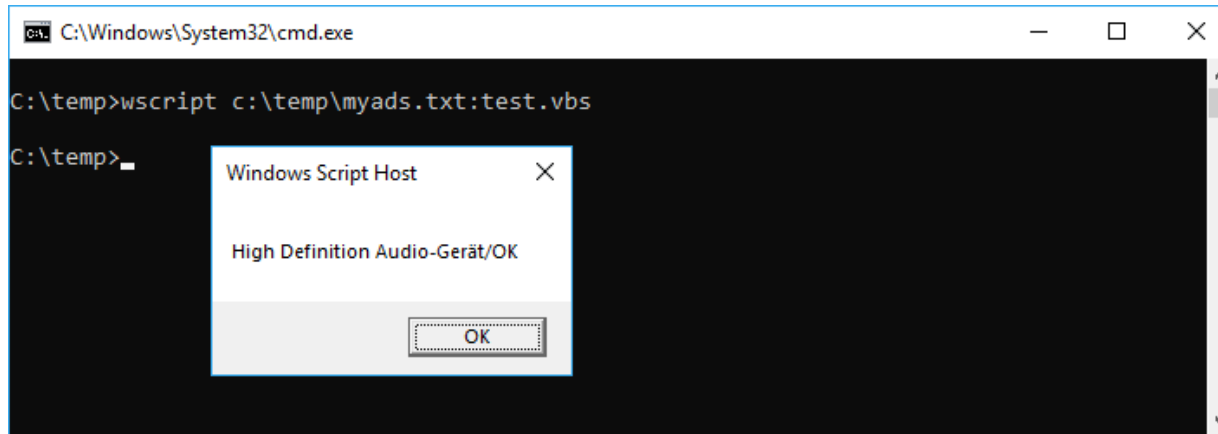
High Definition Audio-Gerät/OK
```



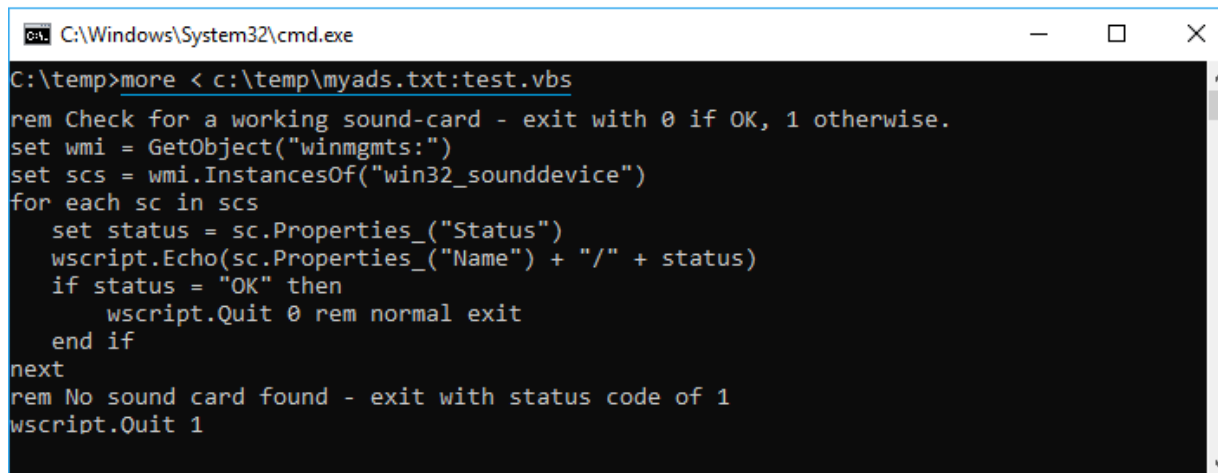
```
C:\Windows\System32\cmd.exe
C:\temp>more < c:\temp\myads.txt:test.vbs
rem Check for a working sound-card - exit with 0 if OK, 1 otherwise.
set wmi = GetObject("winmgmts:")
set scs = wmi.InstancesOf("win32_sounddevice")
for each sc in scs
    set status = sc.Properties_("Status")
    wscript.Echo(sc.Properties_("Name") + "/" + status)
    if status = "OK" then
        wscript.Quit 0 rem normal exit
    end if
next
rem No sound card found - exit with status code of 1
wscript.Quit 1
```

Backslide > demo

- Windows based Script Host



```
C:\Windows\System32\cmd.exe
C:\temp>wscript c:\temp\myads.txt:test.vbs
C:\temp>
```



```
C:\Windows\System32\cmd.exe
C:\temp>more < c:\temp\myads.txt:test.vbs
rem Check for a working sound-card - exit with 0 if OK, 1 otherwise.
set wmi = GetObject("winmgmts:")
set scs = wmi.InstancesOf("win32_sounddevice")
for each sc in scs
    set status = sc.Properties_("Status")
    wscript.Echo(sc.Properties_("Name") + "/" + status)
    if status = "OK" then
        wscript.Quit 0 rem normal exit
    end if
next
rem No sound card found - exit with status code of 1
wscript.Quit 1
```

Backslide > demo

- Powershell

```
C:\Windows\System32\cmd.exe

C:\temp>powershell -ep bypass - < c:\temp\myads.txt:powershell.ps

PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\temp\myads.txt::$DATA
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\temp
PSChildName  : myads.txt::$DATA
PSDrive     : C
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName    : C:\temp\myads.txt
Stream      :::$DATA
Length      : 0

PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\temp\myads.txt:powershell.ps
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\temp
PSChildName  : myads.txt:powershell.ps
PSDrive     : C
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName    : C:\temp\myads.txt
Stream      : powershell.ps
Length      : 44
```

```
C:\Windows\System32\cmd.exe

C:\temp>more < myads.txt:powershell.ps
get-item -path c:\temp\myads.txt -stream *
```

Backslide > demo

- Symbolic link

```
C:\> Administrator: Command Prompt
C:\temp>mklink test.exe c:\temp\test.txt:procexp64.exe
symbolic link created for test.exe <==> c:\temp\test.txt:procexp64.exe
C:\temp>test.exe
```

Process Explorer - Sysinternals: www.sysinternals.com

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Integrity	ASLR
System Idle Process	97.31	52 K	8 K	0				n/a
System	0.15	140 K	28 K	4			System	n/a
csrss.exe	< 0.01	1.808 K	2.300 K	624	Client Server Runtime Pr...	Microsoft Corporation	System	ASLR
wininit.exe		1.496 K	1.884 K	728	Windows Start-Up Applic...	Microsoft Corporation	System	ASLR
csrss.exe	0.02	2.396 K	6.084 K	5828	Client Server Runtime Pr...	Microsoft Corporation	System	ASLR
winlogon.exe		2.772 K	11.124 K	2476	Windows Logon Applicati...	Microsoft Corporation	System	ASLR
SynTPHelper.exe		1.360 K	5.956 K	180	Synaptics Pointing Devic...	Synaptics Incorporated	High	ASLR
explorer.exe	0.03	35.564 K	87.468 K	11612	Windows Explorer	Microsoft Corporation	Medium	ASLR
test.txt:procexp64.exe	0.43	27.872 K	49.488 K	10480	Sysinternals Process Ex...	Sysinternals - www.sysinter...	High	ASLR

CPU Usage: 4.40% Commit Charge: 9.46% Processes: 165 Physical Usage: 10.86%

Backslide > demo

- rundll32 invokes an exported function of a DLL located in an ADS

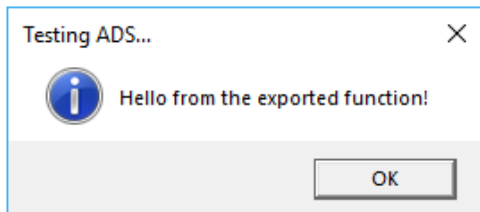
```
#include "stdafx.h"
// This is an example of an exported function.
extern "C" __declspec(dllexport) void doit (void)
{
    ::MessageBox (
        NULL,
        L"Hello from the exported function!",
        L"Testing ADS...",
        MB_ICONINFORMATION );
}
```

1

```
C:\Windows\System32\cmd.exe
C:\temp>type mydll.dll > pecoff-June-2017.docx:mydll.dll
C:\temp>rundll32 pecoff-June-2017.docx:mydll.dll,doit
```

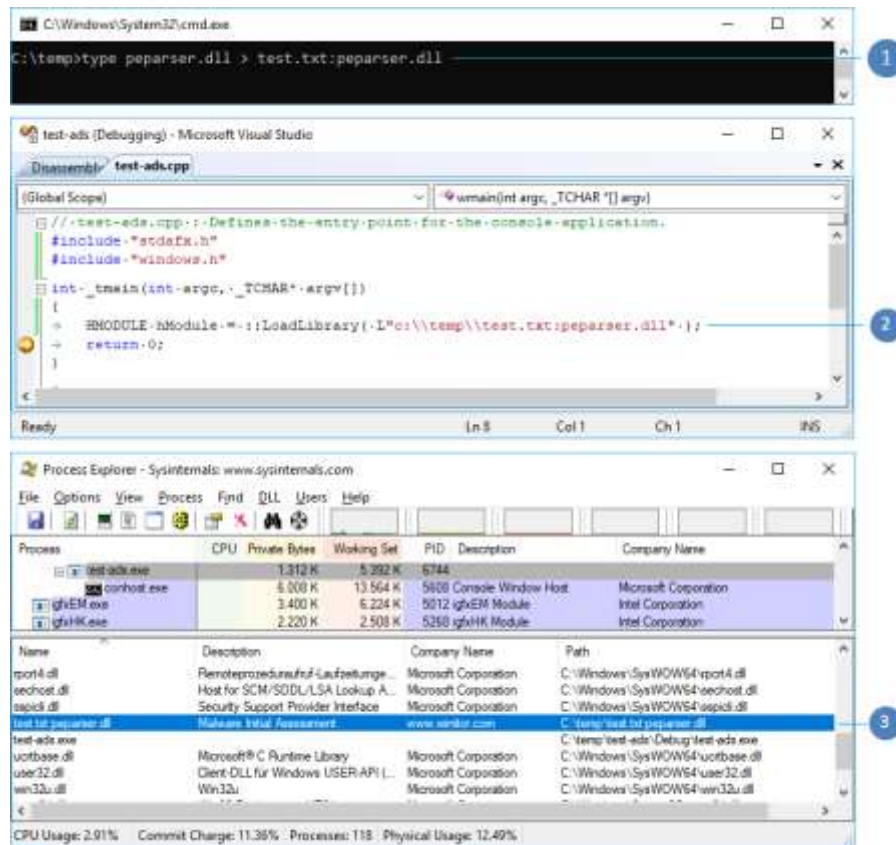
2

3



Backslide > demo

- Load an executable file located in ADS using LoadLibrary



Backslide > demo

- start mimikatz located in an ADS using WinExec

1

```
C:\Windows\System32\cmd.exe
C:\temp>type mimikatz.exe > pecoff-June-2017.docx:mimikatz.exe
```

2

```
(Global Scope)
// test-ads.cpp : Defines the entry point for the console application.
#include "stdafx.h"
#include "windows.h"

int _tmain(int argc, _TCHAR* argv[])
{
    WinExec("c:\\temp\\pecoff-June-2017.docx\\mimikatz.exe", SW_SHOW );
}
```

3

```
#####  mimikatz 2.1.1 (x86) built on Sep 25 2018 15:07:03
## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ## /**** Benjamin DELPY "gentilkiwi" ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
** v **' Vincent LE TOUX ( vincent.letoux@gmail.com )
##### > http://pingcastle.com / http://mysmartlogon.com ****/
mimikatz #
```

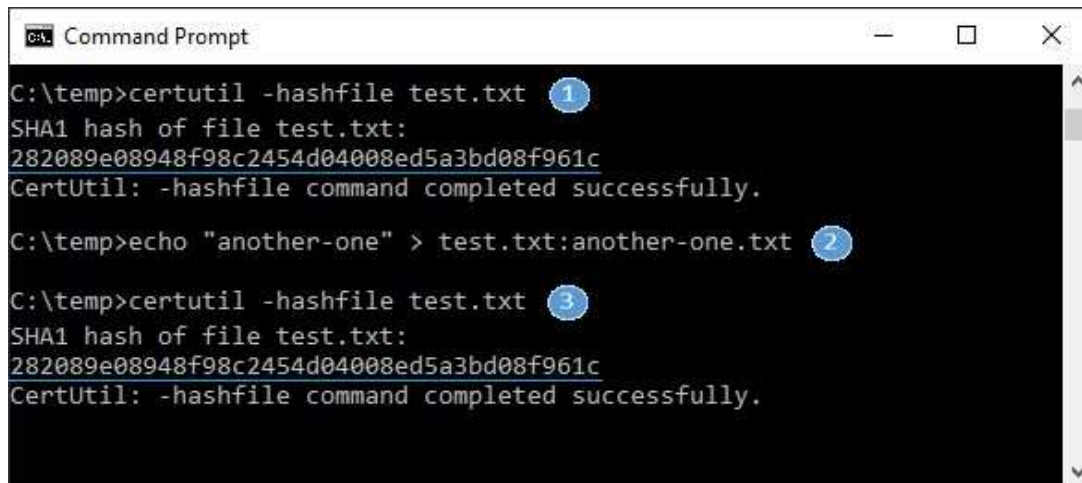
4

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	39.09	52 K	8 K	0		
System	0.02	152 K	24 K	4		
csrss.exe		1.676 K	2.040 K	436	Client-Server-Laufzeitprozess	Microsoft Corporation
wininit.exe		1.416 K	1.076 K	540	Windows-Startanwendung	Microsoft Corporation
csrss.exe	0.02	2.388 K	3.388 K	1756	Client-Server-Laufzeitprozess	Microsoft Corporation
winlogon.exe		2.196 K	3.420 K	6704	Windows-Anmeldeanwendung	Microsoft Corporation
winexplorer.exe	0.08	67.864 K	112.724 K	4516	Windows-Explorer	Microsoft Corporation
pecoff-June-2017.docx:mimikatz.exe		1.060 K	0.116 K	3052	mimikatz for Windows	gentilkiwi (Benjamin DELPY)

CPU Usage: 0.91% | Commit Charge: 9.30% | Processes: 118 | Physical Usage: 9.96% | Own Physical Usage: 3.33%

Backslide > demo

- Adding an ADS to a file does not change the hash of the file



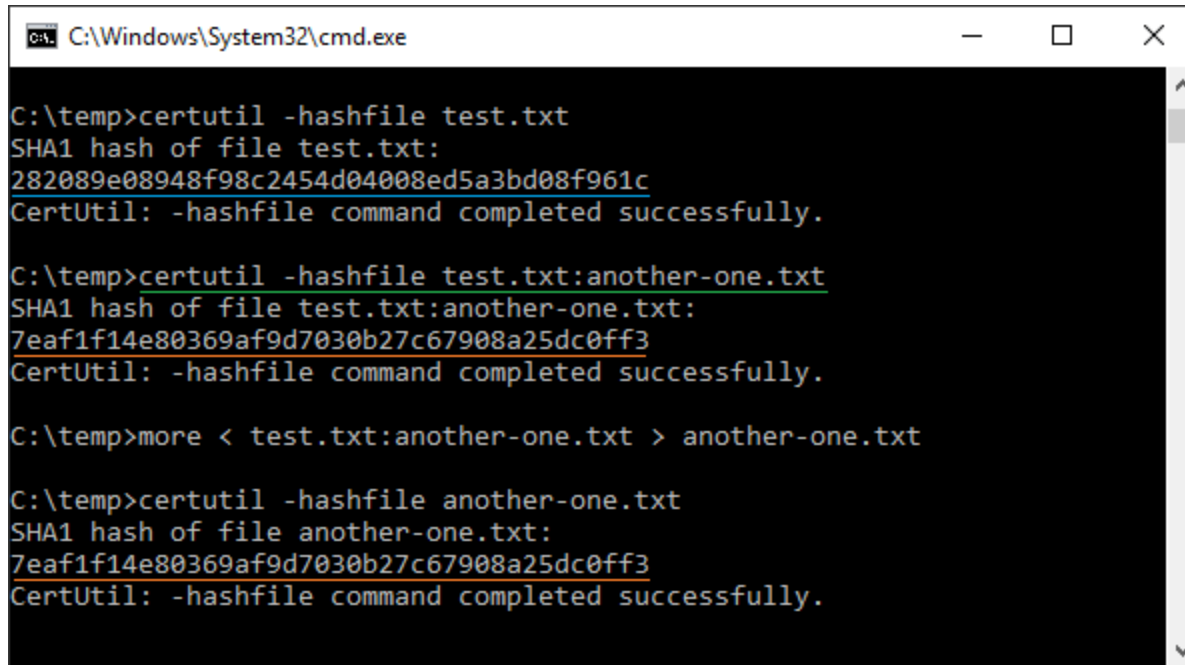
```
ca. Command Prompt
C:\temp>certutil -hashfile test.txt 1
SHA1 hash of file test.txt:
282089e08948f98c2454d04008ed5a3bd08f961c
CertUtil: -hashfile command completed successfully.

C:\temp>echo "another-one" > test.txt:another-one.txt 2

C:\temp>certutil -hashfile test.txt 3
SHA1 hash of file test.txt:
282089e08948f98c2454d04008ed5a3bd08f961c
CertUtil: -hashfile command completed successfully.
```

Backslide > demo

- Retrieve the hash of an ADS hidden in a file



```
C:\Windows\System32\cmd.exe

C:\temp>certutil -hashfile test.txt
SHA1 hash of file test.txt:
282089e08948f98c2454d04008ed5a3bd08f961c
CertUtil: -hashfile command completed successfully.

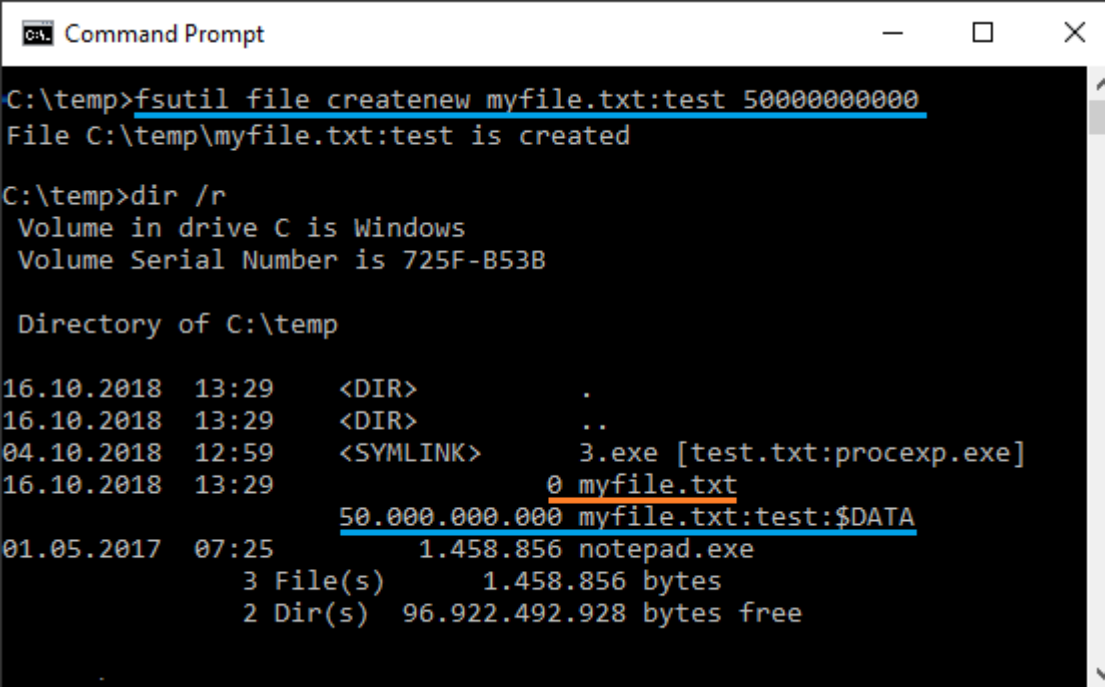
C:\temp>certutil -hashfile test.txt:another-one.txt
SHA1 hash of file test.txt:another-one.txt:
7eaf1f14e80369af9d7030b27c67908a25dc0ff3
CertUtil: -hashfile command completed successfully.

C:\temp>more < test.txt:another-one.txt > another-one.txt

C:\temp>certutil -hashfile another-one.txt
SHA1 hash of file another-one.txt:
7eaf1f14e80369af9d7030b27c67908a25dc0ff3
CertUtil: -hashfile command completed successfully.
```

Backslide > demo

- How to prepare a DOS with an ADS



```
Command Prompt
C:\temp>fsutil file createnew myfile.txt:test 5000000000
File C:\temp\myfile.txt:test is created

C:\temp>dir /r
Volume in drive C is Windows
Volume Serial Number is 725F-B53B

Directory of C:\temp

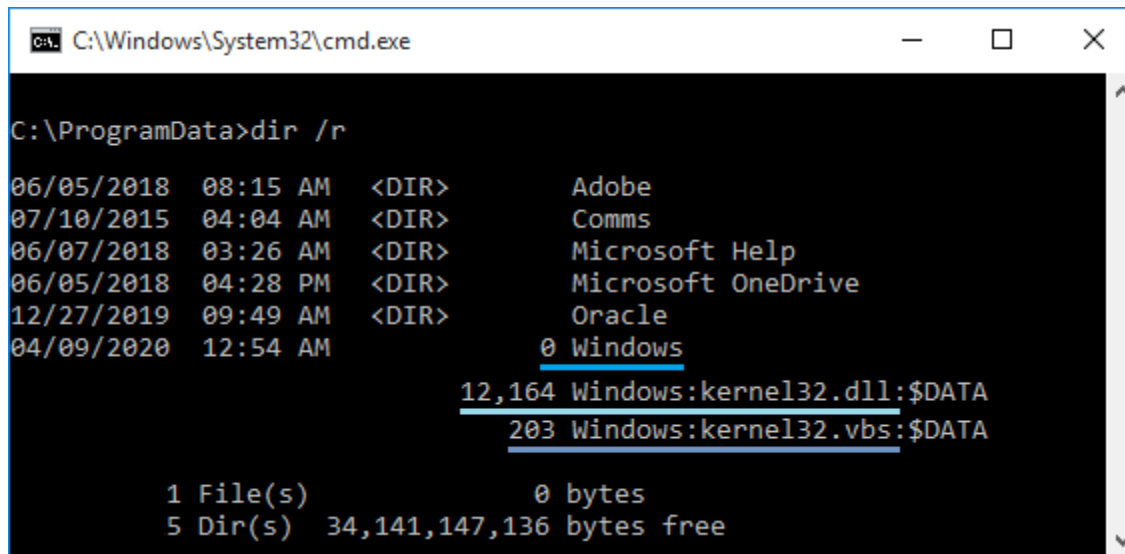
16.10.2018  13:29    <DIR>          .
16.10.2018  13:29    <DIR>          ..
04.10.2018  12:59    <SYMLINK>     3.exe [test.txt:procexp.exe]
16.10.2018  13:29                0 myfile.txt
                50.000.000.000 myfile.txt:test:$DATA
01.05.2017  07:25                1.458.856 notepad.exe
                3 File(s)      1.458.856 bytes
                2 Dir(s)    96.922.492.928 bytes free
```

Backslide > demo

- Malware uses Alternate Data Streams > [MITRE - T1096](#)

“The Tale of DNS Messenger”

<https://blog.talosintelligence.com/2017/03/dnsmessenger.html>



```
C:\Windows\System32\cmd.exe

C:\ProgramData>dir /r

06/05/2018  08:15 AM  <DIR>      Adobe
07/10/2015  04:04 AM  <DIR>      Comms
06/07/2018  03:26 AM  <DIR>      Microsoft Help
06/05/2018  04:28 PM  <DIR>      Microsoft OneDrive
12/27/2019  09:49 AM  <DIR>      Oracle
04/09/2020  12:54 AM           0 Windows
                12,164 Windows:kernel32.dll:$DATA
                203 Windows:kernel32.vbs:$DATA

1 File(s)                0 bytes
5 Dir(s) 34,141,147,136 bytes free
```

Backslide > demo

- Windows executable hidden on a Linux system via ADS

```

C:\Windows\System32\cmd.exe
F:\>type 7FB0F1BE30137334E481CC702389084D > test.txt:7FB0F1BE30137334E481CC702389084D

user@computer: /media/user/kingston
user@computer: /media/user/kingston$ ll test.txt
-rwxrwxrwx 1 user user 41 okt 17 16:35 test.txt*
user@computer: /media/user/kingston$ cat test.txt
this is the content of the text file ...
user@computer: /media/user/kingston$ xattr -l test.txt|less
user.7FB0F1BE30137334E481CC702389084D:
0000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ.....
0010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  .....!.!.!Th
0050  69 73 20 70 72 0F 67 72 61 6D 20 63 61 6E 6E 6F  ..is program canno
0060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  ..t be run in DOS
0070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  ..mode...$.
0080  50 45 00 00 64 86 00 00 E9 32 CD 59 00 00 00 00  ..PE..d...2.Y...
0090  00 00 00 00 F0 00 2E 22 0B 02 02 1C 00 8E 00 00  .....
00A0  00 D8 00 00 00 16 00 00 00 13 00 00 00 10 00 00  .....
00B0  00 00 8C 68 00 00 00 00 00 00 10 00 00 00 02 00  ..h.....
00C0  04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00  .....
00D0  00 60 01 00 00 04 00 00 2D 5F 01 00 02 00 00 00  .._.....
00E0  00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00  .....
00F0  00 00 10 00 00 00 00 00 10 00 00 00 00 00 00 00  .....
0100  00 00 00 00 10 00 00 00 10 01 00 7E 00 00 00 00  .....
0110  00 20 01 00 18 00 00 00 00 00 00 00 00 00 00 00  .....
0120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0130  00 50 01 00 70 00 00 00 00 00 00 00 00 00 00 00  ..P..p.....
0140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0160  00 00 00 00 00 00 00 00 00 00 00 D4 22 01 00 70  ..".p...
0170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0180  00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00  .....text...
```