

Sun City Computer Club

Windows SIG

July 14, 2020

**Questions, Comments, Suggestions welcomed at
any time**

Even Now

- Audio Recording of this session
- Use the link above to access MP4 audio recording
- Audio Recording in Progress
- SIG attendees are required to be members of the chartered club sponsoring that SIG.
- Sun City Community Association By-law

- Your input is desired, needed, requested,
- 2020 meeting schedule – Annex
SIG leader?
- Then this happened
- Windows SIG meeting/presentation frequency
Once a month Second Tuesday

Windows SIG news

- Kernel Data Protection
iff hardware support
- Hardware Drivers Windows 10 2004 update
- Your settings aren't supported
- July 14 – Microsoft Patch Tuesday
Schedule B
123 vulnerabilities 17 critical 2 disclosed
KB4565483 1903 & 1901
KB4565503 2004

Windows News

What needs your attention

The following things need your attention to continue the installation and keep your Windows settings, personal files, and apps.

[Why am I seeing this?](#)

- ✖ This PC can't be upgraded to Windows 10.

Your PC settings aren't supported yet on this version of Windows 10. Microsoft is working to support your settings soon. No action is needed. Windows Update will offer this version of Windows 10 automatically when these settings are supported.

[Learn More](#)

- Panther folder
 - appraiser XML file
- OneDrive
Surface Pro 7

Reported block settings

Asset>

```
<PropertyList Type="Inventory">
```

```
  <Property Name="AssetType" Value="BlockingMatchingInfo" />
```

```
</PropertyList>
```

```
<PropertyList Type="DataSource">
```

```
  <Property Name="ApplicableTargetVersion" Value="20H1" Ordinal="1" />
```

```
  <Property Name="SdbAppGuid" Value="{afb67a42-a10a-48a0-9677-77b4d00efecc}" Ordinal="1" />
```

```
  <Property Name="SdbAppName" Value="OneDrive and Legacy filters" Ordinal="1" />
```

```
  <Property Name="SdbAppVendor" Value="Microsoft" Ordinal="1" />
```

```
  <Property Name="SdbBlockOverrideType" Value="SOB_UX_BLOCKTYPE_OVERRIDE_UPGRADE_BLOCK" Ordinal="1" />
```

```
  <Property Name="SdbBlockType" Value="BlockUpgrade" Ordinal="1" />
```

```
  <Property Name="SdbEntryGuid" Value="{b074d9ce-fc26-4e8b-9978-42e541e23388}" Ordinal="1" />
```

```
  <Property Name="SdbFileLink" Value="2113887" Ordinal="1" />
```

```
  <Property Name="SdbGenericMessageSummary" Value="Your PC settings aren't supported yet on this version of Windows 10. No action is needed. Windows Update will offer this version of Windows 10 automatically when these settings are supported." />
```

- Update/Upgrade drivers
 - Disable Core Isolation
 - Disconnect from Internet
 - Standalone update via USB
-
- Seeker vs avoider

Work (??) Arounds

Settings



General

Notifications

Security

Display

Allow List

Account

About

Limit who can change your Malwarebytes security settings



Beta updates

Get early access to the latest software and security features



Usage and threat statistics

Help fight Malware by providing usage and threat statistics



[View privacy policy](#)

Proxy server

Configure Malwarebytes to connect to the Internet using a proxy server



Review your update history

Check the Status column to ensure all important updates were successful. To remove an update, see [Installed Updates](#).

[Troubleshoot problems with installing updates](#)

Name	Status	Importance	Date Installed
Microsoft Edge Update for Windows 7 for x64-based Systems (KB4567409)	Successful	Recommended	6/24/2020
Windows Malicious Software Removal Tool x64 - v5.82 (KB890830)	Successful	Important	6/24/2020
Security Intelligence Update for Microsoft Security Essentials - KB2310138 (Version 1.319.113.0)	Successful	Recommended	6/24/2020
Security Intelligence Update for Microsoft Security Essentials - KB2310138 (Version 1.307.2955.0)	Successful	Recommended	1/24/2020
Security Update for Windows 7 for x64-based Systems (KB3075226)	Successful	Important	1/22/2020
2020-01 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4534310)	Successful	Important	1/22/2020
Update for Windows 7 for x64-based Systems (KB2893519)	Successful	Recommended	1/22/2020
Update for Windows 7 for x64-based Systems (KB2923545)	Successful	Recommended	1/22/2020
Security Update for Windows 7 for x64-based Systems (KB3020388)	Successful	Important	1/22/2020
Security Intelligence Update for Microsoft Security Essentials - KB2310138 (Version 1.307.2821.0)	Successful	Recommended	1/22/2020
Update for Windows (KB2999226)	Successful	Important	1/22/2020
2019-10 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4524157)	Successful	Important	1/22/2020
2020-01 Servicing Stack Update for Windows 7 for x64-based Systems (KB4536952)	Successful	Important	1/22/2020
2019-09 Preview of Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4516048)	Successful	Optional	1/22/2020
2020-01 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4...	Successful	Important	1/22/2020
2019-10 Update for Windows 7 for x64-based Systems (KB4524752)	Successful	Recommended	1/22/2020
2019-09 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4516065)	Successful	Important	1/22/2020
2019-03 Servicing Stack Update for Windows 7 for x64-based Systems (KB4490628)	Successful	Important	1/22/2020
Intel Corporation - Graphics Adapter WDDM1.1. Graphics Adapter WDDM1.2. Graphics Adapter WDD...	Successful	Optional	1/21/2020

OK

Control Panel Home

Check for updates

Change settings

View update history

Restore hidden updates

Updates: frequently asked questions

Windows Update



Install updates for your computer

2 important updates are available

1 optional update is available

1 important update selected, 30.0 MB

Install updates

Most recent check for updates: Today at 9:26 AM


Updates were installed: Today at 9:27 AM. [View update history](#)

You receive updates: For Windows and other products from Microsoft Update

Find out more about free software from Microsoft Update. [Click here for details.](#)

See also

Installed Updates

 Windows Anytime Upgrade

Select the updates you want to install

<input checked="" type="checkbox"/>	Name	Size
	Windows 7 (1)	^
<input checked="" type="checkbox"/>	Microsoft Edge Update for Windows 7 for x64-based Systems (KB4567409)	80.6 MB

Microsoft Edge Update for Windows 7 for x64-based Systems (KB4567409)

Recommended Update

This update provides the latest feature and quality updates to Microsoft Edge.

Published: 6/17/2020



You may need to restart your computer after installing this update.



Download is pending; please select this update to start downloading

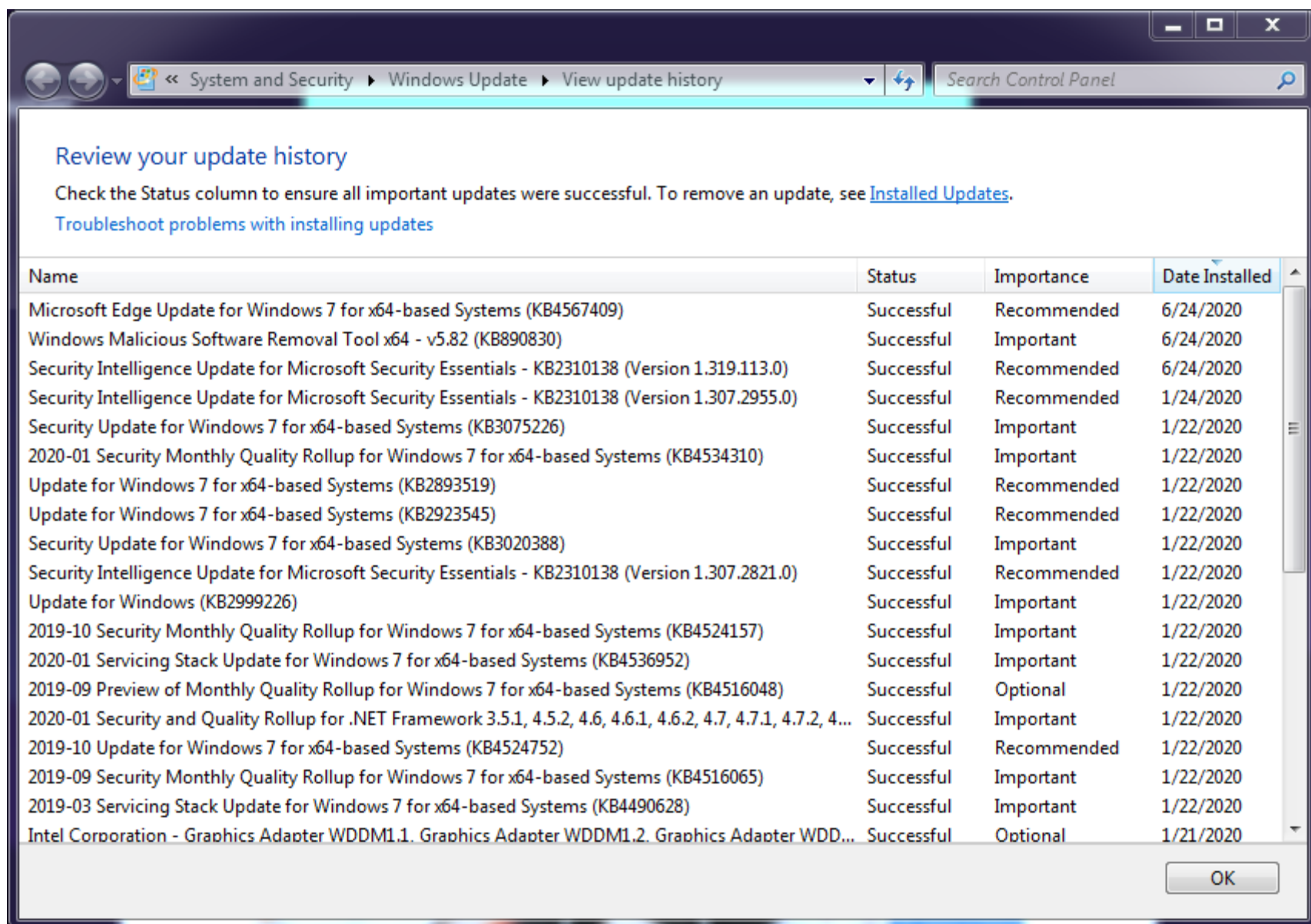
[More information](#)

[Support information](#)

Total selected: 1 important update

OK

Cancel



The screenshot shows a Windows 7 desktop with a blue background. On the left side, there are icons for Recycle Bin, Firefox, Google Chrome, Media Player Classic, Microsoft Edge, Microsoft Security..., and SupportAs... The taskbar at the bottom contains icons for Internet Explorer, File Explorer, Windows Media Center, Google Chrome, Microsoft Edge, and the Start button. The system tray in the bottom right corner shows the date and time as 9:50 AM on 6/24/2020.

The Windows Update history window is open, displaying a list of updates. The window title is "System and Security > Windows Update > View update history". The main heading is "Review your update history". Below the heading, there is a message: "Check the Status column to ensure all important updates were successful. To remove an update, see [Installed Updates](#)." and a link: "[Troubleshoot problems with installing updates](#)".

Name	Status	Importance	Date Installed
2020-01 Preview of Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4539601)	Successful	Optional	6/24/2020
Microsoft Edge Update for Windows 7 for x64-based Systems (KB4567409)	Successful	Recommended	6/24/2020
Windows Malicious Software Removal Tool x64 - v5.82 (KB890830)	Successful	Important	6/24/2020
Security Intelligence Update for Microsoft Security Essentials - KB2310138 (Version 1.319.113.0)	Successful	Recommended	6/24/2020
Security Intelligence Update for Microsoft Security Essentials - KB2310138 (Version 1.307.2955.0)	Successful	Recommended	1/24/2020
Security Update for Windows 7 for x64-based Systems (KB3075226)	Successful	Important	1/22/2020
2020-01 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4534310)	Successful	Important	1/22/2020
Update for Windows 7 for x64-based Systems (KB2893519)	Successful	Recommended	1/22/2020
Update for Windows 7 for x64-based Systems (KB2923545)	Successful	Recommended	1/22/2020
Security Update for Windows 7 for x64-based Systems (KB3020388)	Successful	Important	1/22/2020
Security Intelligence Update for Microsoft Security Essentials - KB2310138 (Version 1.307.2821.0)	Successful	Recommended	1/22/2020
Update for Windows (KB2999226)	Successful	Important	1/22/2020
2019-10 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4524157)	Successful	Important	1/22/2020
2020-01 Servicing Stack Update for Windows 7 for x64-based Systems (KB4536952)	Successful	Important	1/22/2020
2019-09 Preview of Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4516048)	Successful	Optional	1/22/2020
2020-01 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4...	Successful	Important	1/22/2020
2019-10 Update for Windows 7 for x64-based Systems (KB4524752)	Successful	Recommended	1/22/2020
2019-09 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4516065)	Successful	Important	1/22/2020
2019-03 Servicing Stack Update for Windows 7 for x64-based Systems (KB4490628)	Successful	Important	1/22/2020

An "OK" button is located at the bottom right of the window.

- Update Any/Everything



Update Windows Store



My library



All owned



Installed



Ready to install



Downloads



Included with device

Downloads and updates

[Get updates](#)**You're good to go**

All your trusted apps and games from Microsoft Store have the latest updates.

Recent activity

	Mail and Calendar	App	16005.12827.20508.0	Modified today
	Your Phone	App	1.20062.93.0	Modified today
	Windows Maps	App	10.2005.1.0	Modified today
	Windows Terminal	App	1.0.1811.0	Modified today
	Dropbox for S mode	App	22.4.4.0	Modified today
	HEVC Video Extens...	App	1.0.31823.0	Modified today
	Windows Voice Re...	App	10.2005.1672.0	Modified 6/27/2020
	Windows Alarms &...	App	10.2005.1675.0	Modified 6/27/2020

- Original delivery channel ?
- Speed <-> Security
- Want 1.0.31822.0 or 1.0.31823.0
or No Return from PowerShell

**High Efficiency Video Coding
CODEC**

```
PS C:\> Get-AppxPackage -Name Microsoft.HEVCVideoExtension
```

```
Name           : Microsoft.HEVCVideoExtension
Publisher      : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Architecture   : X64
ResourceId     :
Version        : 1.0.31823.0
PackageFullName : Microsoft.HEVCVideoExtension_1.0.31823.0_x64__8wekyb3d8bbwe
InstallLocation : C:\Program Files\WindowsApps\Microsoft.HEVCVideoExtension_1.0.31823.0_x64__8wekyb3d8bbwe
IsFramework    : False
PackageFamilyName : Microsoft.HEVCVideoExtension_8wekyb3d8bbwe
PublisherId    : 8wekyb3d8bbwe
IsResourcePackage : False
IsBundle       : False
IsDevelopmentMode : False
NonRemovable    : False
IsPartiallyStaged : False
SignatureKind   : Store
Status          : Ok
```



Microsoft 365



Downloads and updates

Settings

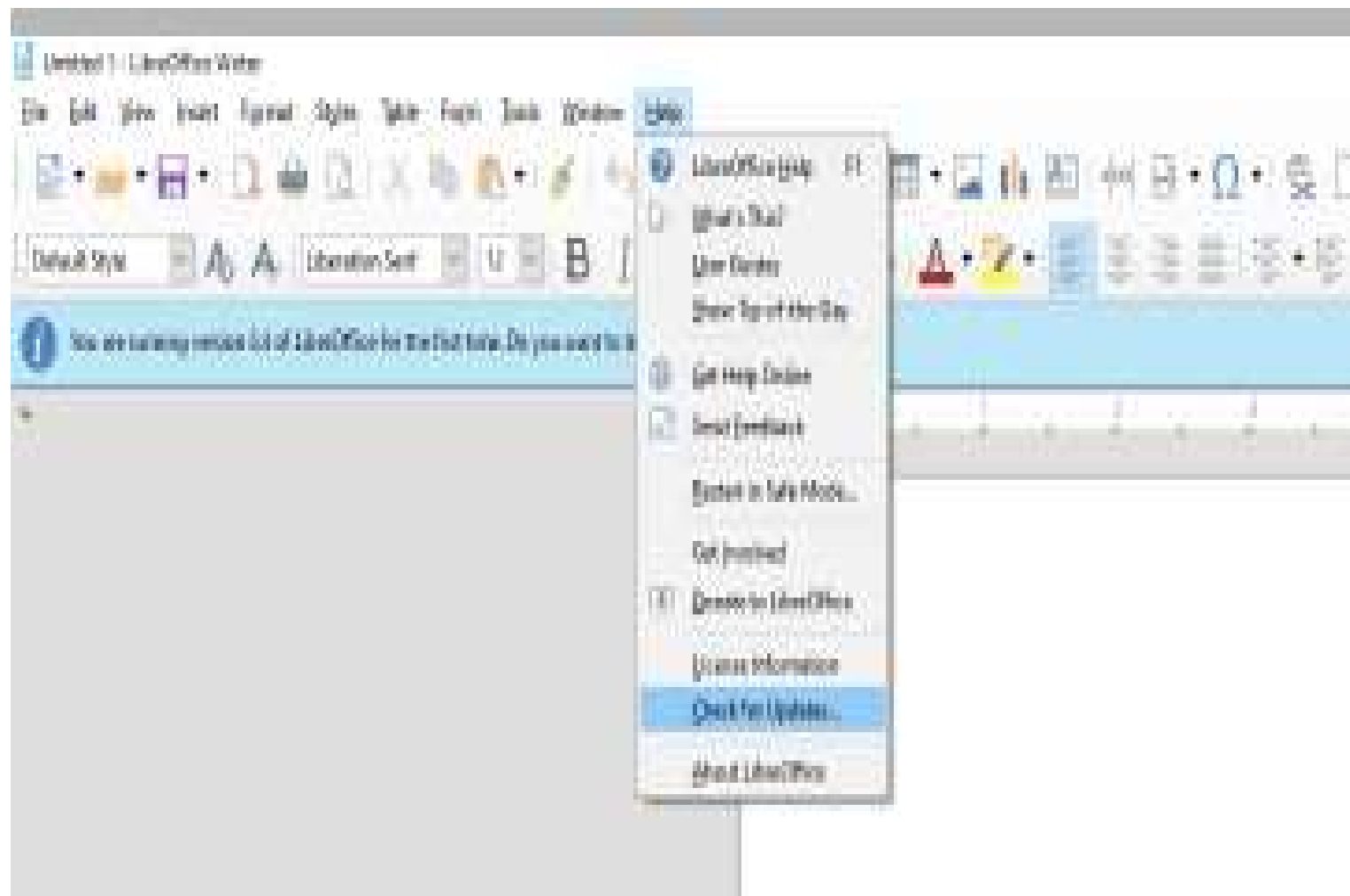
My Library

Send Feedback



Show all





Product Information

Office

Product Activated

Microsoft Office Home and Student 2016

This product contains



Change License



Office Updates

Updates are automatically downloaded and installed.

Microsoft Office Account

- Feature of NTFS
- Macintosh HFS resource fork
- Not well known
- Generally hidden
- Not easily found – security suites
- Many Windows uses:
Apple files, text files summary, tags for downloads,

Alternate Data Streams ADS

Administrator: Windows PowerShell

```
PS H:\A folder> Get-Item -path c:\Users\john\Documents\test.docx -stream *
```

```
PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\Users\john\Documents\test.docx::$DATA
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\john\Documents
PSChildName  : test.docx::$DATA
PSDrive      : C
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName     : C:\Users\john\Documents\test.docx
Stream       : :$DATA
Length       : 13792
```

```
PS H:\A folder>
```

PowerShell command Get-Item


```

Administrator: Windows PowerShell

PS H:\A Folder> dir

    Directory: H:\A Folder


Mode                LastWriteTime         Length Name
----                -
-a----            7/6/2020   3:46 PM             108 Output.txt
-a----            7/8/2020   1:41 PM          13765 Text test.docx

PS H:\A Folder> get-Item -path Output.txt -stream *

PSPath                : Microsoft.PowerShell.Core\FileSystem::H:\A Folder\Output.txt::$DATA
PSParentPath          : Microsoft.PowerShell.Core\FileSystem::H:\A Folder
PSChildName           : Output.txt::$DATA
PSDrive               : H
PSProvider            : Microsoft.PowerShell.Core\FileSystem
PSIsContainer         : False
FileName             : H:\A Folder\Output.txt
Stream               : :$DATA
Length               : 108

PSPath                : Microsoft.PowerShell.Core\FileSystem::H:\A Folder\Output.txt:HideMe
PSParentPath          : Microsoft.PowerShell.Core\FileSystem::H:\A Folder
PSChildName           : Output.txt:HideMe
PSDrive               : H
PSProvider            : Microsoft.PowerShell.Core\FileSystem
PSIsContainer         : False
FileName             : H:\A Folder\Output.txt
Stream               : HideMe
Length               : 27

```

PowerShell get-Item

```
PS H:\A Folder> get-Content -path Output.txt -stream HideMe
```

Then he jumps back again

```
PS H:\A Folder> Type Output.txt
```

The

Quick

brown

fox

jumps

over

the

lazy

dog







```
PS H:\A Folder>
```

PowerShell Get-Content

- 0 - My Computer
- 1 - Local Internet Zone
- 2 - Trusted sites Zone
- 3 - Internet Zone
- 4 - Restricted Sites Zone

Zone IDentifiers

Operational Number of events: 46

Level	Date and Time	Source	Event ID	Task Category
 Information	6/29/2020 6:04:35 PM	Sysmon	15	File stream cre...
 Information	6/29/2020 6:04:35 PM	Sysmon	15	File stream cre...
 Information	6/29/2020 6:04:35 PM	Sysmon	15	File stream cre...
 Information	6/29/2020 6:04:35 PM	Sysmon	15	File stream cre...
 Information	6/29/2020 6:04:35 PM	Sysmon	15	File stream cre...
 Information	6/29/2020 6:04:35 PM	Sysmon	15	File stream cre...

Event 15, Sysmon

General Details

File stream created:
RuleName: -
UtcTime: 2020-06-29 16:04:35.163
ProcessGuid: {562ff2b1-1039-5efa-5e00-000000001d00}
ProcessId: 5580
Image: C:\WINDOWS\system32\browser_broker.exe
TargetFilename: C:\Users\testuser1\Downloads\oledump_V0_0_50.zip.zgh8j8w.partial:Zone.Identifier
CreationUtcTime: 2020-06-29 16:04:35.101
Hash: MD5=33148832C6B8BE3DD092A8C803688A12,SHA256=
8E829E6C918585D30DE45714AA4AB15BA0996E94A50A91C9659B7E35C3C383C4
Contents: [ZoneTransfer] Zoneld=3 ReferrerUrl=https://blog.didierstevens.com/programs/oledump-
bv/ HostUrl=http://didierstevens.com/files/software/oledump_V0_0_50.zip

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 15
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 6/29/2020 6:04:35 PM
Task Category: File stream created (rule: FileCreateStream
Keywords:
Computer: DESKTOP-Q4NDIRQ

- 3-2-1 backup
- File History
- Services & Applications
- LiFo
- App from Microsoft Store
- Windows 10 2004
- ADMINISTRATOR

Windows File Recovery

Windows File Recovery

Copyright (c) Microsoft Corporation. All rights reserved.

Version: 0.0.11761.0

=====

USAGE: winfr source-drive: destination-folder [/switches]

- /r - Segment mode (NTFS only, recovery using file record segments)
- /n <filter> - Filter search (default or segment mode, wildcards allowed, trailing \ for folder)
- /x - Signature mode (recovery using file headers)
- /y:<type(s)> - Recover specific extension groups (signature mode only, comma separated)
- /# - Displays signature mode extension groups and file types
- /? - Help text
- /! - Display advanced features

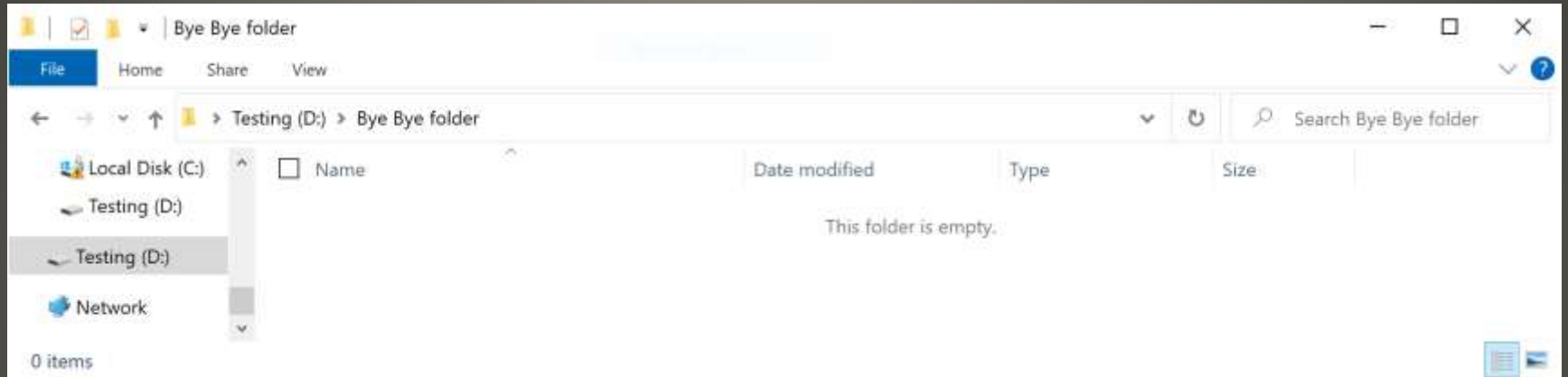
Example usage - winfr C: D:\RecoveryDestination /n Users\<username>\Downloads\
winfr C: D:\RecoveryDestination /x /y:PDF,JPEG
winfr C: D:\RecoveryDestination /r /n *.pdf /n *.jpg

Visit <https://aka.ms/winfrhelp> for user guide
For support, please email winfr@microsoft.com

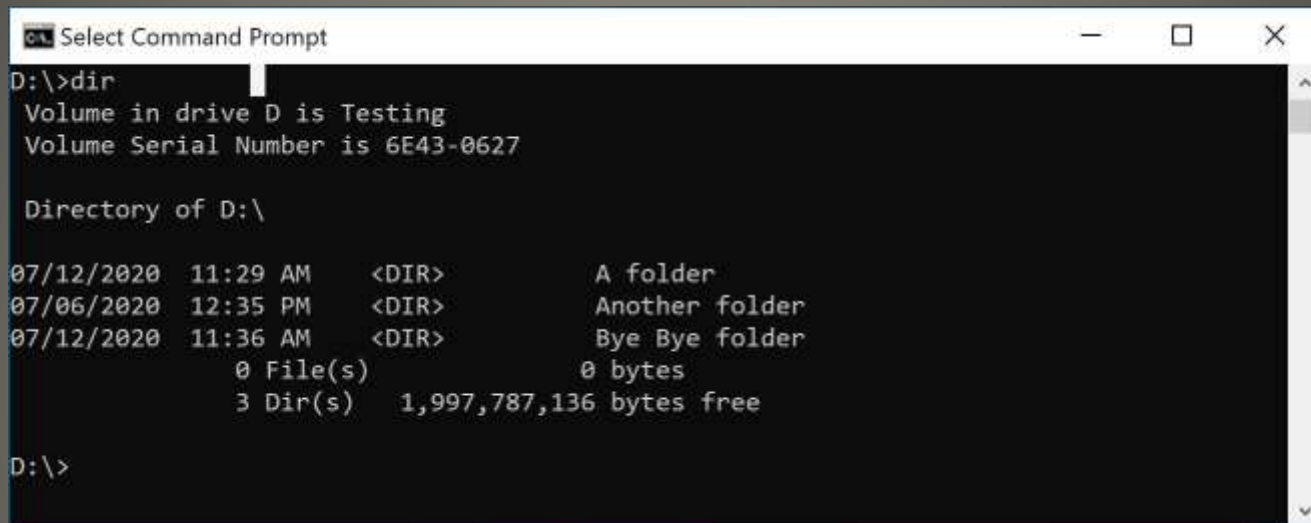
C:\WINDOWS\system32>

- Delete folder with file and stream data
- Move USB disk to Windows 10 2004 with Windows File Recovery installed
- Use Windows File Recovery to find and recover deleted folder
- Check to ensure stream contained original data

A test



Folder is empty



```
D:\>dir
Volume in drive D is Testing
Volume Serial Number is 6E43-0627

Directory of D:\

07/12/2020  11:29 AM    <DIR>          A folder
07/06/2020  12:35 PM    <DIR>          Another folder
07/12/2020  11:36 AM    <DIR>          Bye Bye folder
               0 File(s)                0 bytes
               3 Dir(s)  1,997,787,136 bytes free

D:\>
```

```
Administrator: C:\Windows\System32\cmd.exe
Visit https://aka.ms/winfrhelp for user guide
For support, please email winfr@microsoft.com

C:\WINDOWS\system32>winfr d: c:\Recovery /r

Windows File Recovery
Copyright (c) Microsoft Corporation. All rights reserved
Version: 0.0.11761.0
-----

Source drive:      d:
Destination folder: c:\Recovery\Recovery_20200712_134941
Filter:            *.*
Extension filter:  *

Sector count:      0x00000000003c07ff
Cluster size:      0x00001000
Sector size:       0x00000200
Overwrite:         Prompt
Mode:              Segment

Continue? (y/n)
Pass 1: Scanning and processing disk
Scanning disk: 100%

Pass 2: Recovering files
Files recovered: 1, total files: 3, current filename: c:\Recovery\Recovery_20200712_134941\Documents\txt\Output.txt
Files recovered: 2, total files: 3, current filename: c:\Recovery\Recovery_20200712_134941\Misc\tmp\~WRL1871.tmp
Files recovered: 3, total files: 3, current filename: c:\Recovery\Recovery_20200712_134941\Documents\docx\Text test.docx

Progress: 100%

View recovered files? (y/n)
```

Windows File Recovery

Windows PowerShell

```
PS C:\Recovery\Recovery_20200712_134941\Documents\txt> Get-Content -path c:\Recovery\Recovery_20200712_134941\Documents\txt\Output.txt -stream HideMe
Then he jumps back again
PS C:\Recovery\Recovery_20200712_134941\Documents\txt> Get-Item -path c:\Recovery\Recovery_20200712_134941\Documents\txt\Output.txt -stream *

PSPath           : Microsoft.PowerShell.Core\FileSystem::C:\Recovery\Recovery_20200712_134941\Documents\txt\Output.txt::$DATA
PSParentPath     : Microsoft.PowerShell.Core\FileSystem::C:\Recovery\Recovery_20200712_134941\Documents\txt
PSChildName      : Output.txt::$DATA
PSDrive          : C
PSProvider       : Microsoft.PowerShell.Core\FileSystem
PSIsContainer    : False
FileName        : C:\Recovery\Recovery_20200712_134941\Documents\txt\Output.txt
Stream          :::$DATA
Length          : 108

PSPath           : Microsoft.PowerShell.Core\FileSystem::C:\Recovery\Recovery_20200712_134941\Documents\txt\Output.txt:HideMe
PSParentPath     : Microsoft.PowerShell.Core\FileSystem::C:\Recovery\Recovery_20200712_134941\Documents\txt
PSChildName      : Output.txt:HideMe
PSDrive          : C
PSProvider       : Microsoft.PowerShell.Core\FileSystem
PSIsContainer    : False
FileName        : C:\Recovery\Recovery_20200712_134941\Documents\txt\Output.txt
Stream          : HideMe
Length          : 27

PS C:\Recovery\Recovery_20200712_134941\Documents\txt> Get-Content -path c:\Recovery\Recovery_20200712_134941\Documents\txt\Output.txt -stream HideMe
Then he jumps back again
PS C:\Recovery\Recovery_20200712_134941\Documents\txt>
```

Success

- <https://support.microsoft.com/en-us/help/4538642/windows-10-restore-lost-files>
- NTFS, ReFS, FAT, exFAT
- USB, SD, Camera, etc.
- Reformatted ??
- Scan will take time

Windows File Recovery

- None of us are as experienced as all of us
- Awareness, Preparedness, Understanding
- Participate
- Topic Suggestions
- Questions: scccwindows@gmail.com

