Sun City Computer Club

Windows SIG

July 28, 2020

Questions, Comments, Suggestions welcomed at any time

Even Now

- Audio Recording of this session
- Use the link above to access MP4 audio recording

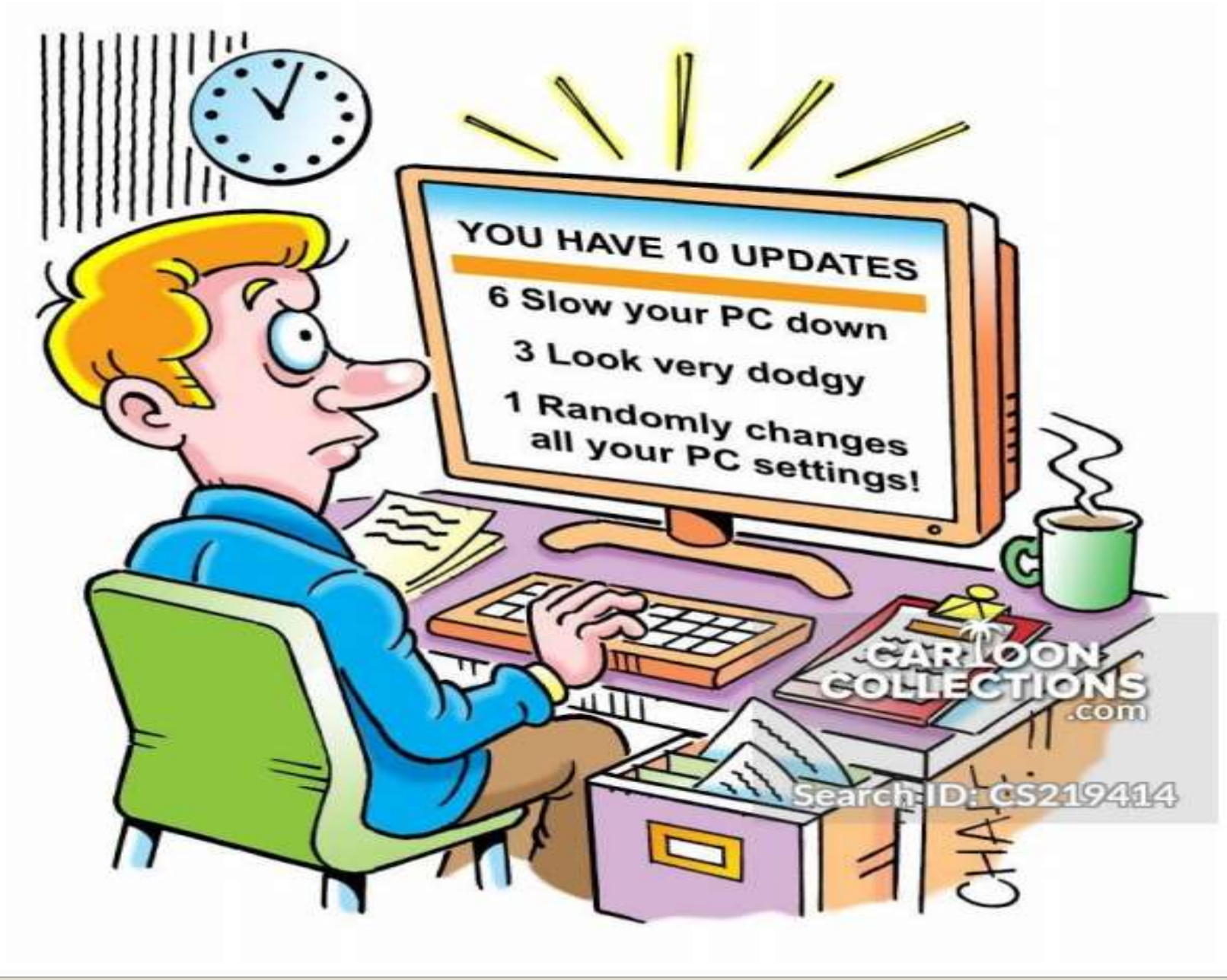
- Audio Recording in Progress

- SIG attendees are required to be members of the chartered club sponsoring that SIG.
- Sun City Community Association By-law

Windows SIG news

- Your input is desired, needed, requested,
- 2020 meeting schedule – Annex
  SIG leader?

- Windows SIG meeting/presentation frequency
  Once a month Second Tuesday


YOU HAVE 10 UPDATES
6 Slow your PC down
3 Look very dodgy
1 Randomly changes all your PC settings!
CARTOON COLLECTIONS .com
Search ID: CS219414

Windows News

- Slack EU suit Teams with Office 365
- Apple store vs. Microsoft store
- Microsoft store updates
- Updates & inventory
- My recent 2004 experience
  npcap driver
- A member's Enterprise license experience
- Folder vanish - rename
- Windows 10x

Microsoft store

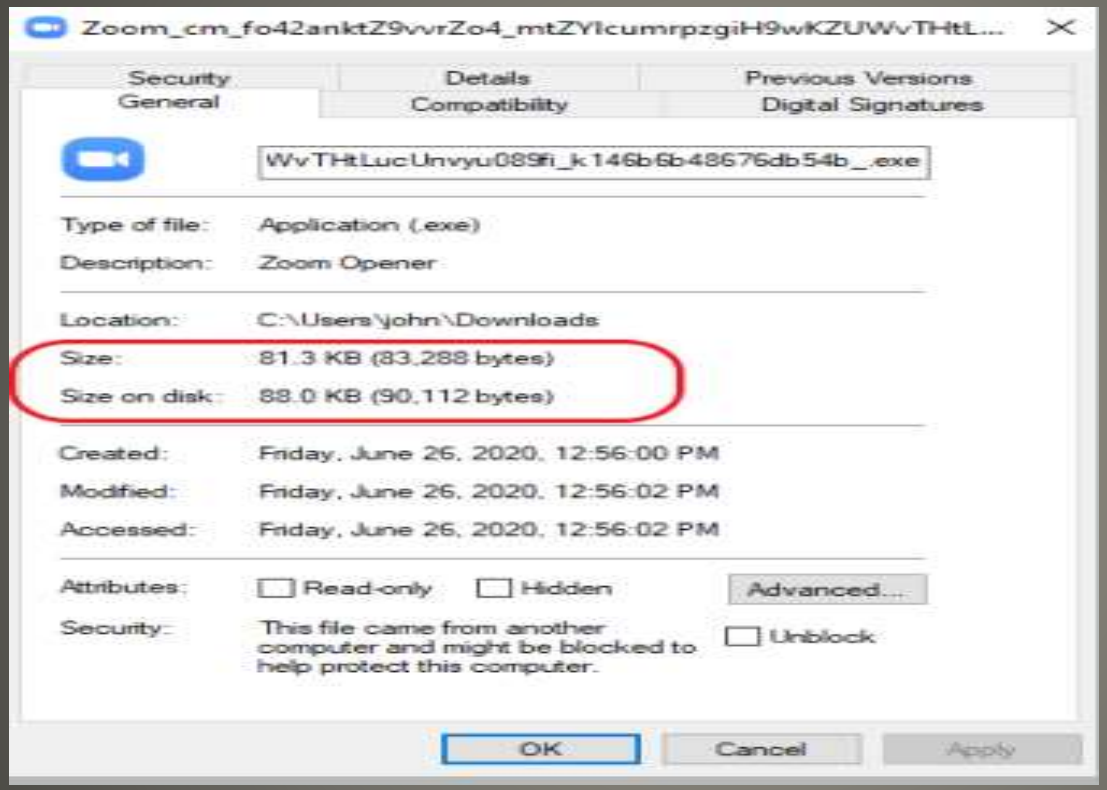
- Recent Updates
  - Your Phone
  - Microsoft Photos
  - Cortana
  - Office
  - Microsoft store
  - Mail & calendar
  - Surface

- Perhaps 1 feature update per year?
- Container model
- Perhaps no 32bit support
- Shed legacy support
- Cloud PC Thin Clients ?

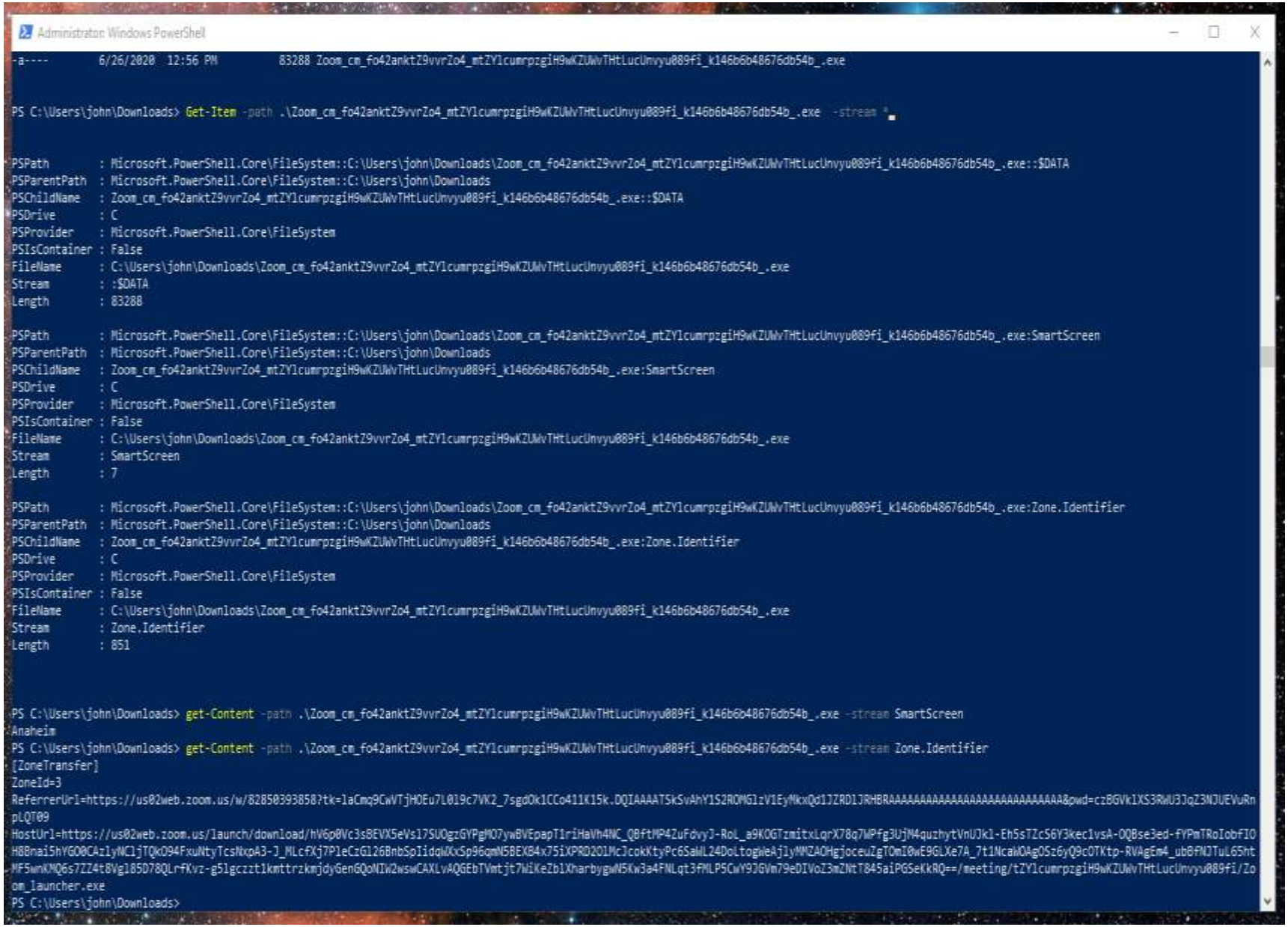
Microsoft Windows 10X

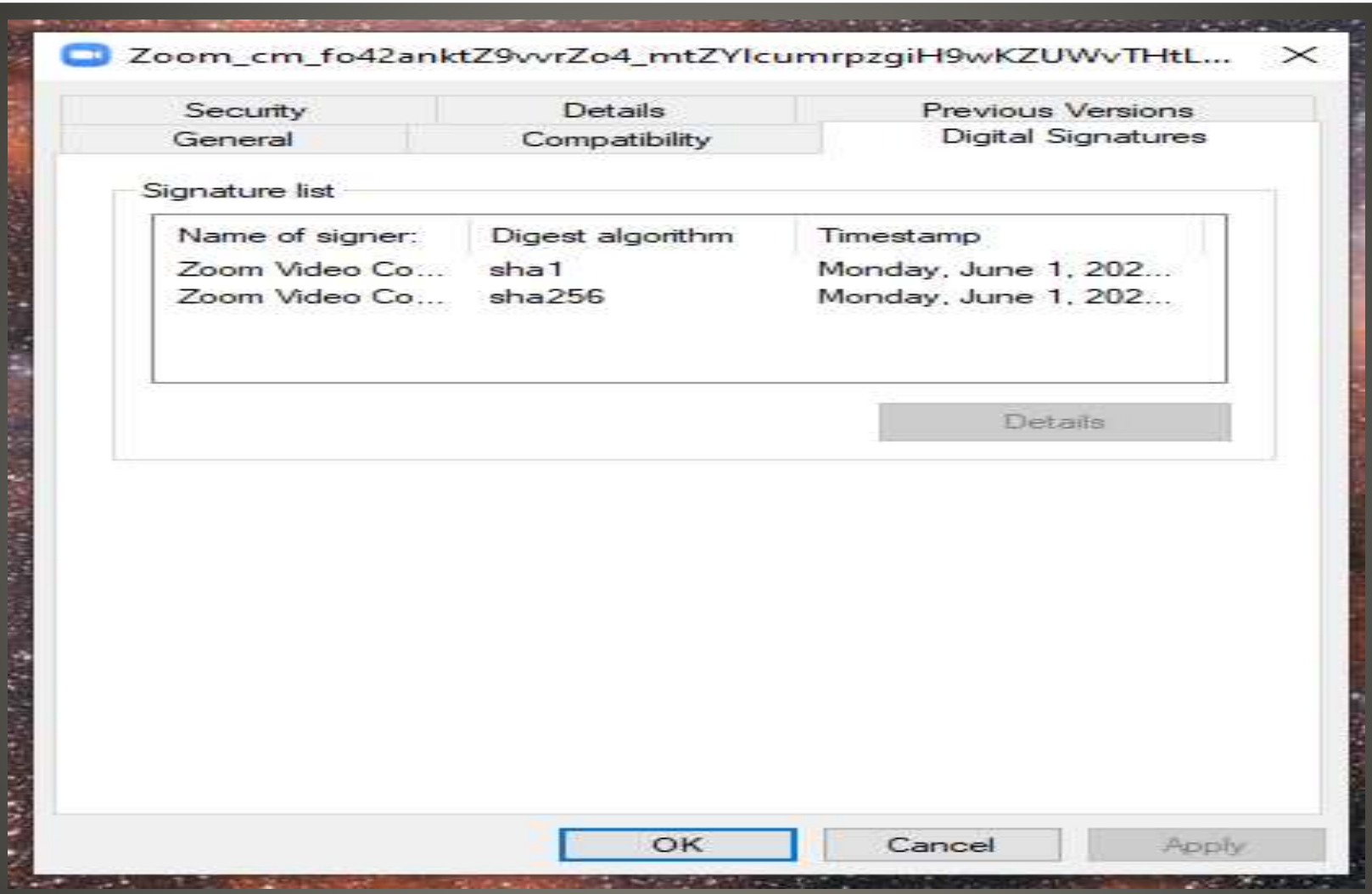
- Windows Home 1903, 1909, 2004
- More stable
- Windows Pro, Enterprise issues
  Windows Defender Application Guard
  Windows sandbox
- Windows 10 2004 seekers another phase
- Still no 2004 for Surface
- Securing Windows work in progress

- From July 14, 2020 Windows SIG



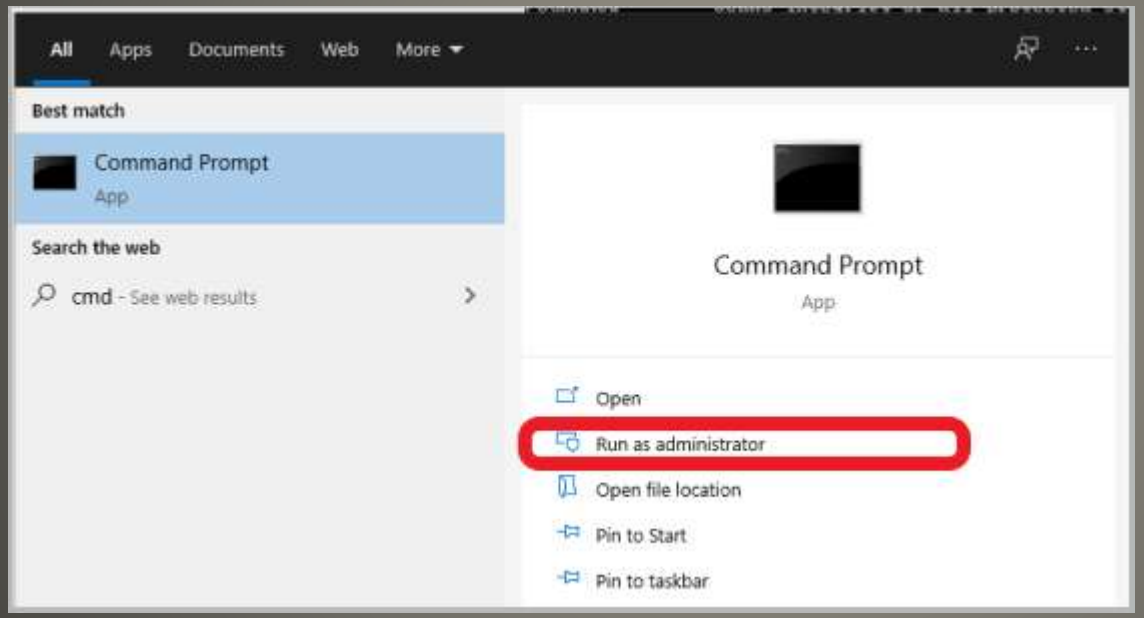
Alternate Data Stream


Administrator: Windows PowerShell
-a---- 6/26/2020 12:56 PM 83288 Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe
PS C:\Users\john\Downloads> Get-Item -path .\Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe -stream *
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\john\Downloads\Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe::$DATA
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\john\Downloads
PSChildName : Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe::$DATA
PSDrive : C
PSProvider : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName : C:\Users\john\Downloads\Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe
Stream : :$DATA
Length : 83288
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\john\Downloads\Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe:SmartScreen
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\john\Downloads
PSChildName : Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe:SmartScreen
PSDrive : C
PSProvider : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName : C:\Users\john\Downloads\Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe
Stream : SmartScreen
Length : 7
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\john\Downloads\Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe:Zone.Identifier
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\john\Downloads
PSChildName : Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe:Zone.Identifier
PSDrive : C
PSProvider : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName : C:\Users\john\Downloads\Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe
Stream : Zone.Identifier
Length : 851
PS C:\Users\john\Downloads> get-Content -path .\Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe -stream SmartScreen
Anaheim
PS C:\Users\john\Downloads> get-Content -path .\Zoom_cm_fo42anktZ9vvrZo4_mtZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi_k146b6b48676db54b_.exe -stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://us02web.zoom.us/w/82850393858?tk=laCmq9CwVTjHOEu7L019c7VK2_7sgdOk1CCo411K15k.DQIAAAATSkSvAhY1S2ROMGlzV1EyMkxQd1JZRD1JRHBRAAAAAAAAAAAAAAAAAAAAAAAAAAAA&pwd=czBGVk1XS3RWU3JqZ3NJUEVuRnpLQT09
HostUrl=https://us02web.zoom.us/launch/download/hV6p0Vc3sBEVX5eVs17SUQgzGYPgMO7ywBVEpapT1riHaVh4NC_QBftMP4ZuFdvyJ-RoL_a9KOGTzmitxLqrX78q7WPfg3UjN4quzhytVnUJk1-Eh5sTZcS6Y3kec1vsA-OQBse3ed-fYPmTRoIobfIOH8Bnai5hY6Q0CAz1yNCljTQkO94FxuNtyTcsNxpA3-J_MLcfXj7P1eCzG126BnbSpIidqWXxSp96qmN5BEXB4x75iXPRD2O1McJcokKtyPc6SaWL24DoLtogWeAjlyMMZAOHgjoceuIgTOmI0wE9GLXe7A_7t1NcaWOAgOSz6yQ9cOTKtp-RVAgEm4_ubBfNJTuL65htMF5wnKMQ6s7ZZ4t8Vg185D78QLrfKvz-g5lgczzt1kmttrzkmjdyGenGQoNIW2wswCAXLvAQGEbTVmtjt7WiKeZblXharbygwW5Kw3a4FNLqt3fMLP5CwY9JGVm79eDIVoZ3mZNtT845aiPGSeKkRQ==/meeting/tZYlcumrpzgiH9wKZUWvTHtLucUnvyu089fi/Zoom_launcher.exe
PS C:\Users\john\Downloads>

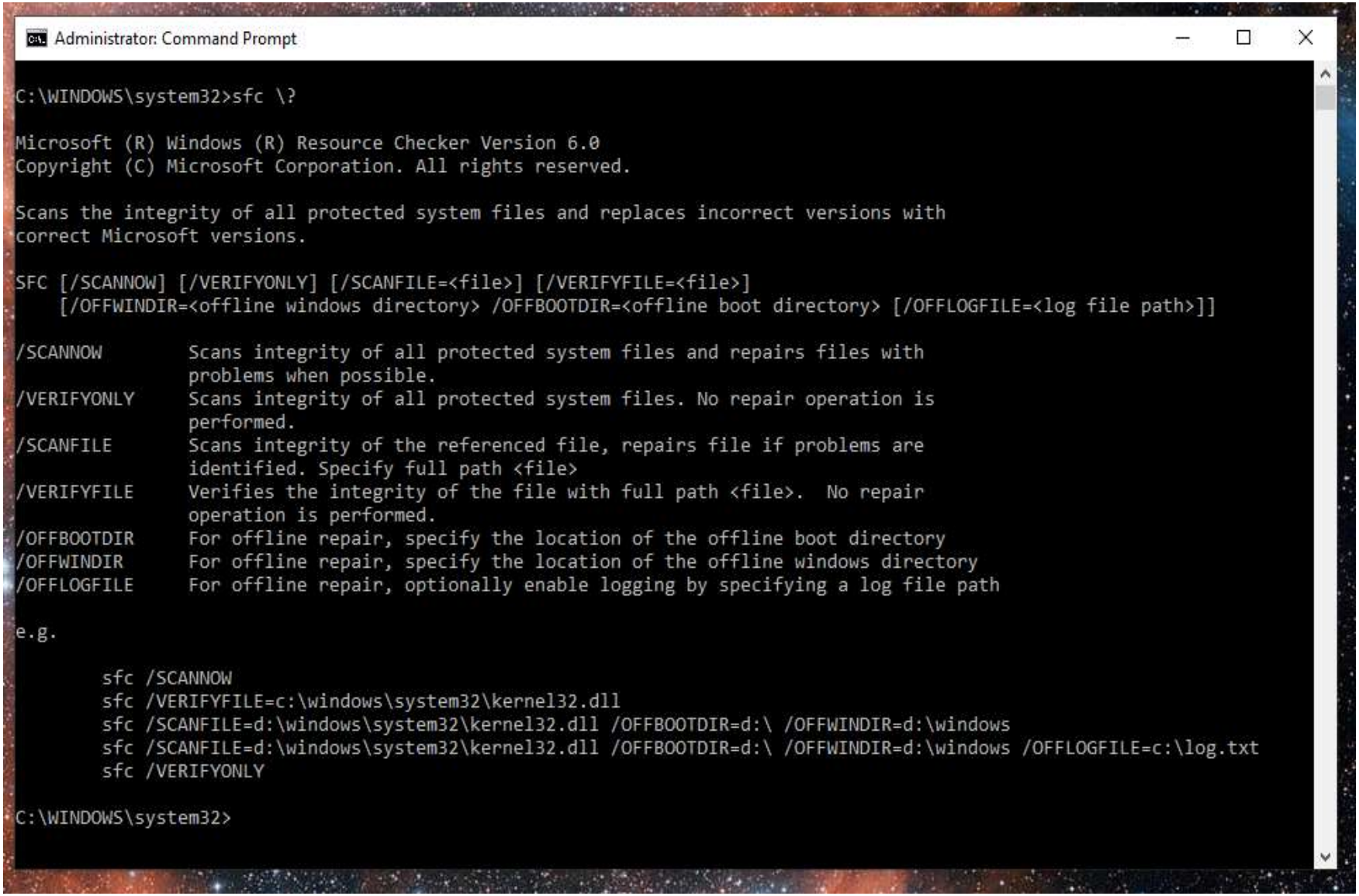


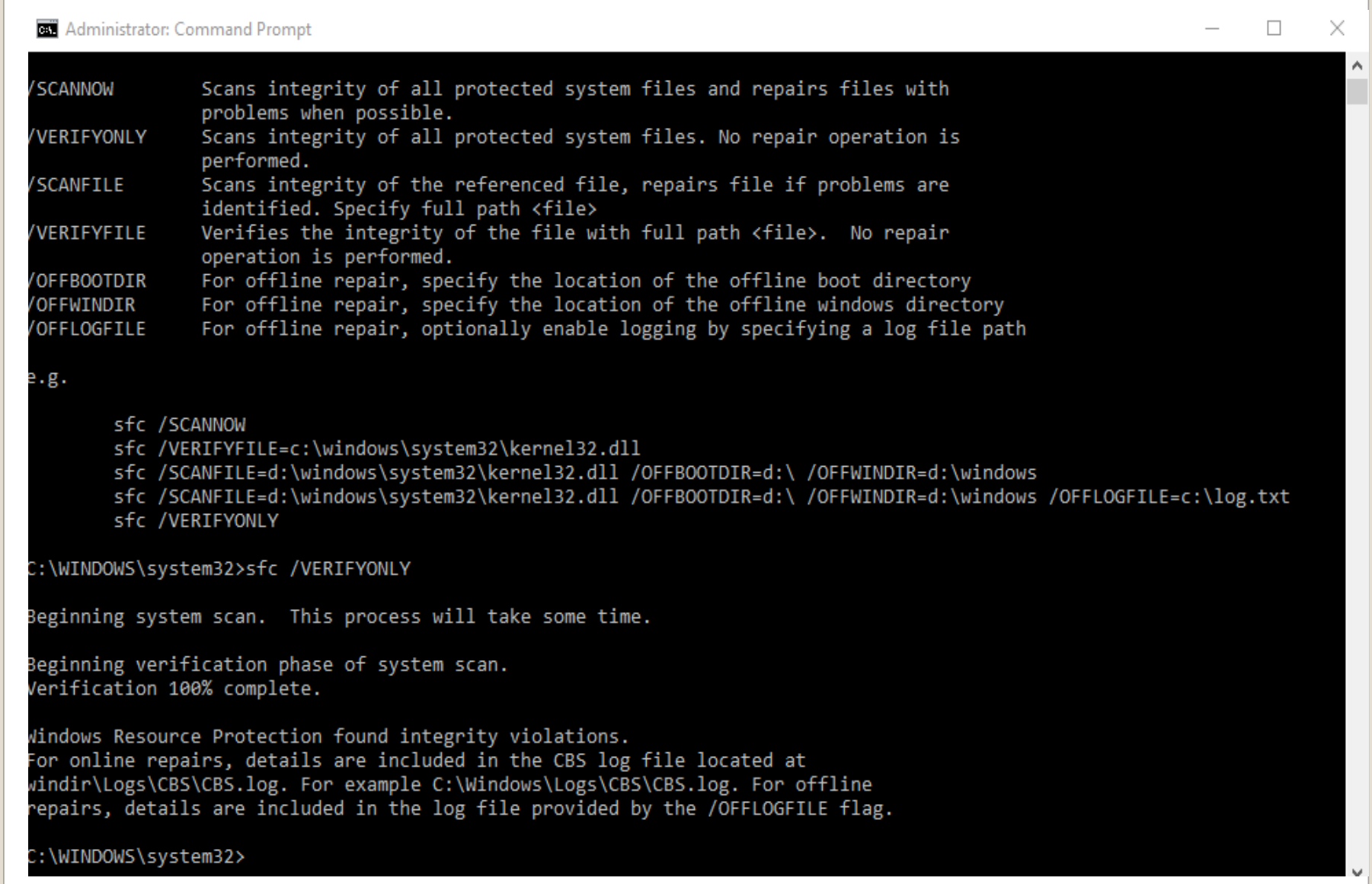
Check Digital Signature

- Scan, verify, fix operating system files
- Command line utility
- Start > Search > cmd



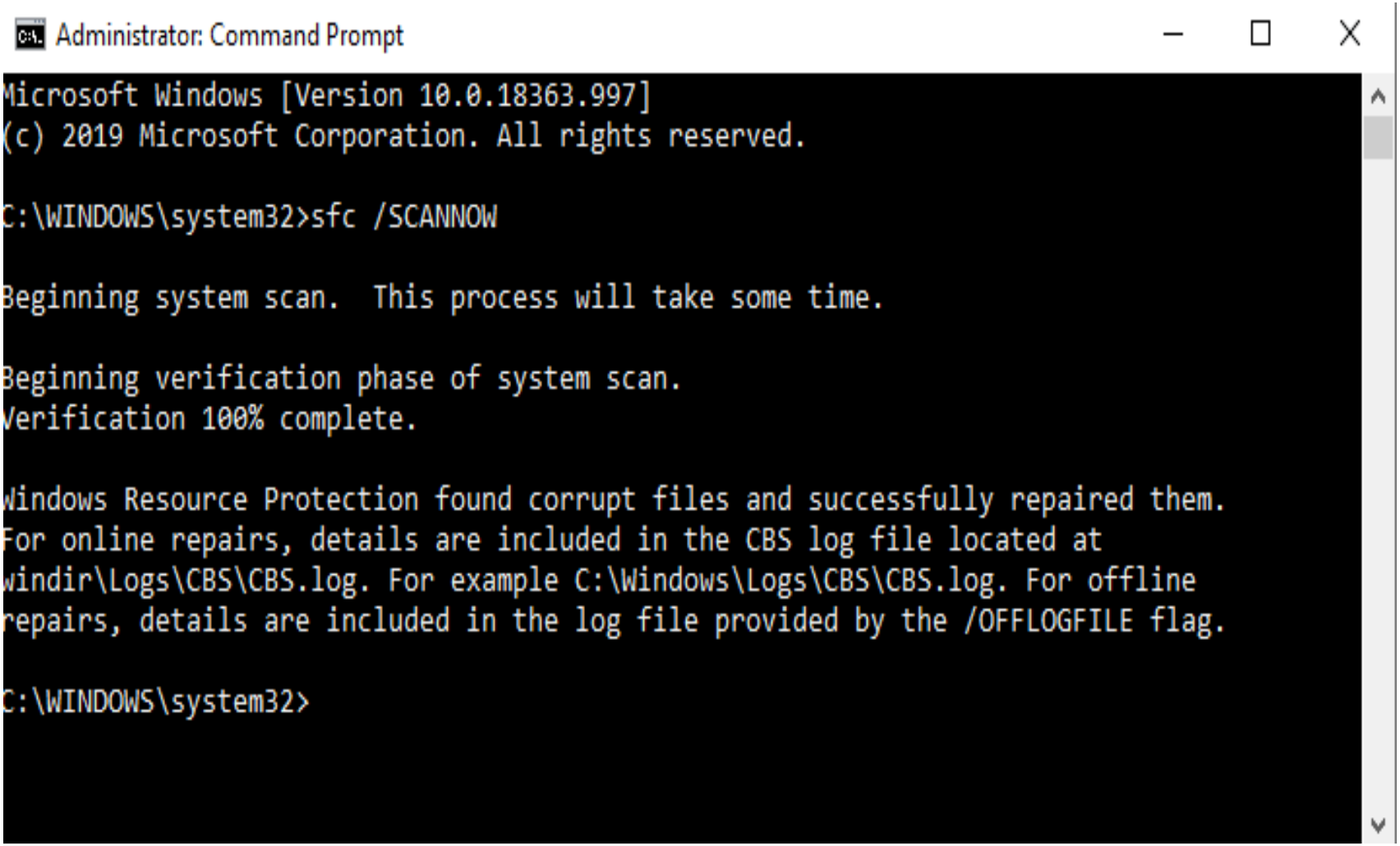
System File Check


Administrator: Command Prompt
C:\WINDOWS\system32>sfc \?
Microsoft (R) Windows (R) Resource Checker Version 6.0
Copyright (C) Microsoft Corporation. All rights reserved.
Scans the integrity of all protected system files and replaces incorrect versions with
correct Microsoft versions.
SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<file>] [/VERIFYFILE=<file>]
[/OFFWINDIR=<offline windows directory> /OFFBOOTDIR=<offline boot directory> [/OFFLOGFILE=<log file path>]]
/SCANNOW Scans integrity of all protected system files and repairs files with
problems when possible.
/VERIFYONLY Scans integrity of all protected system files. No repair operation is
performed.
/SCANFILE Scans integrity of the referenced file, repairs file if problems are
identified. Specify full path <file>
/VERIFYFILE Verifies the integrity of the file with full path <file>. No repair
operation is performed.
/OFFBOOTDIR For offline repair, specify the location of the offline boot directory
/OFFWINDIR For offline repair, specify the location of the offline windows directory
/OFFLOGFILE For offline repair, optionally enable logging by specifying a log file path
e.g.
sfc /SCANNOW
sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows /OFFLOGFILE=c:\log.txt
sfc /VERIFYONLY
C:\WINDOWS\system32>


Administrator: Command Prompt
/SCANNOW Scans integrity of all protected system files and repairs files with problems when possible.
/VERIFYONLY Scans integrity of all protected system files. No repair operation is performed.
/SCANFILE Scans integrity of the referenced file, repairs file if problems are identified. Specify full path <file>
/VERIFYFILE Verifies the integrity of the file with full path <file>. No repair operation is performed.
/OFFBOOTDIR For offline repair, specify the location of the offline boot directory
/OFFWINDIR For offline repair, specify the location of the offline windows directory
/OFFLOGFILE For offline repair, optionally enable logging by specifying a log file path
e.g.
sfc /SCANNOW
sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows /OFFLOGFILE=c:\log.txt
sfc /VERIFYONLY
C:\WINDOWS\system32>sfc /VERIFYONLY
Beginning system scan. This process will take some time.
Beginning verification phase of system scan.
Verification 100% complete.
Windows Resource Protection found integrity violations.
For online repairs, details are included in the CBS log file located at
windir\Logs\CBS\CBS.log. For example C:\Windows\Logs\CBS\CBS.log. For offline
repairs, details are included in the log file provided by the /OFFLOGFILE flag.
C:\WINDOWS\system32>

```
2020-07-28 13:08:06, Info                  CSI    00000094 CSIPERF - FilePI Queue 168ms
2020-07-28 13:08:06, Info                  CSI    00000095 CSIPERF - FilePI Queue 164ms
2020-07-28 13:08:07, Info                  CSI    00000096 CSIPERF - FilePI Queue 201ms
2020-07-28 13:08:07, Info                  CSI    00000097 CSIPERF - FilePI Queue 150ms
2020-07-28 13:08:07, Info                  CSI    00000098 CSIPERF - FilePI Queue 205ms
2020-07-28 13:08:08, Info                  CSI    00000099 CSIPERF - FilePI Queue 150ms
2020-07-28 13:08:08, Info                  CSI    0000009a CSIPERF - FilePI Queue 273ms
2020-07-28 13:08:08, Info                  CSI    0000009b Warning: Overlap: Directory \??\C:\WINDOWS\System32\drivers\en-US\ is owned twice or has its security set twice
  Original owner: Microsoft-Windows-Foundation-Default-Security.Resources, version 10.0.18362.1, arch amd64, culture [l:5]'en-US', nonSxS, pkt {l:8 b:31bf3856ad364e35}
  New owner: Microsoft-Windows-Foundation-Default-Security.Resources, version 10.0.18362.1, arch amd64, culture [l:5]'en-US', nonSxS, pkt {l:8 b:31bf3856ad364e35}
2020-07-28 13:08:08, Info                  CSI    0000009c Warning: Overlap: Directory \??\C:\WINDOWS\System32\wbem\en-US\ is owned twice or has its security set twice
  Original owner: Microsoft-Windows-Foundation-Default-Security.Resources, version 10.0.18362.1, arch amd64, culture [l:5]'en-US', nonSxS, pkt {l:8 b:31bf3856ad364e35}
  New owner: Microsoft-Windows-Foundation-Default-Security.Resources, version 10.0.18362.1, arch amd64, culture [l:5]'en-US', nonSxS, pkt {l:8 b:31bf3856ad364e35}
2020-07-28 13:08:08, Info                  CSI    0000009d Warning: Overlap: Directory \??\C:\WINDOWS\help\mui\0409\ is owned twice or has its security set twice
  Original owner: Microsoft-Windows-Foundation-Default-Security.Resources, version 10.0.18362.1, arch amd64, culture [l:5]'en-US', nonSxS, pkt {l:8 b:31bf3856ad364e35}
  New owner: Microsoft-Windows-Foundation-Default-Security.Resources, version 10.0.18362.1, arch amd64, culture [l:5]'en-US', nonSxS, pkt {l:8 b:31bf3856ad364e35}
2020-07-28 13:08:08, Info                  CSI    0000009e [SR] Verify complete
2020-07-28 13:08:08, Info                  CSI    0000009f [SR] Verifying 100 components
2020-07-28 13:08:08, Info                  CSI    000000a0 [SR] Beginning Verify and Repair transaction
```

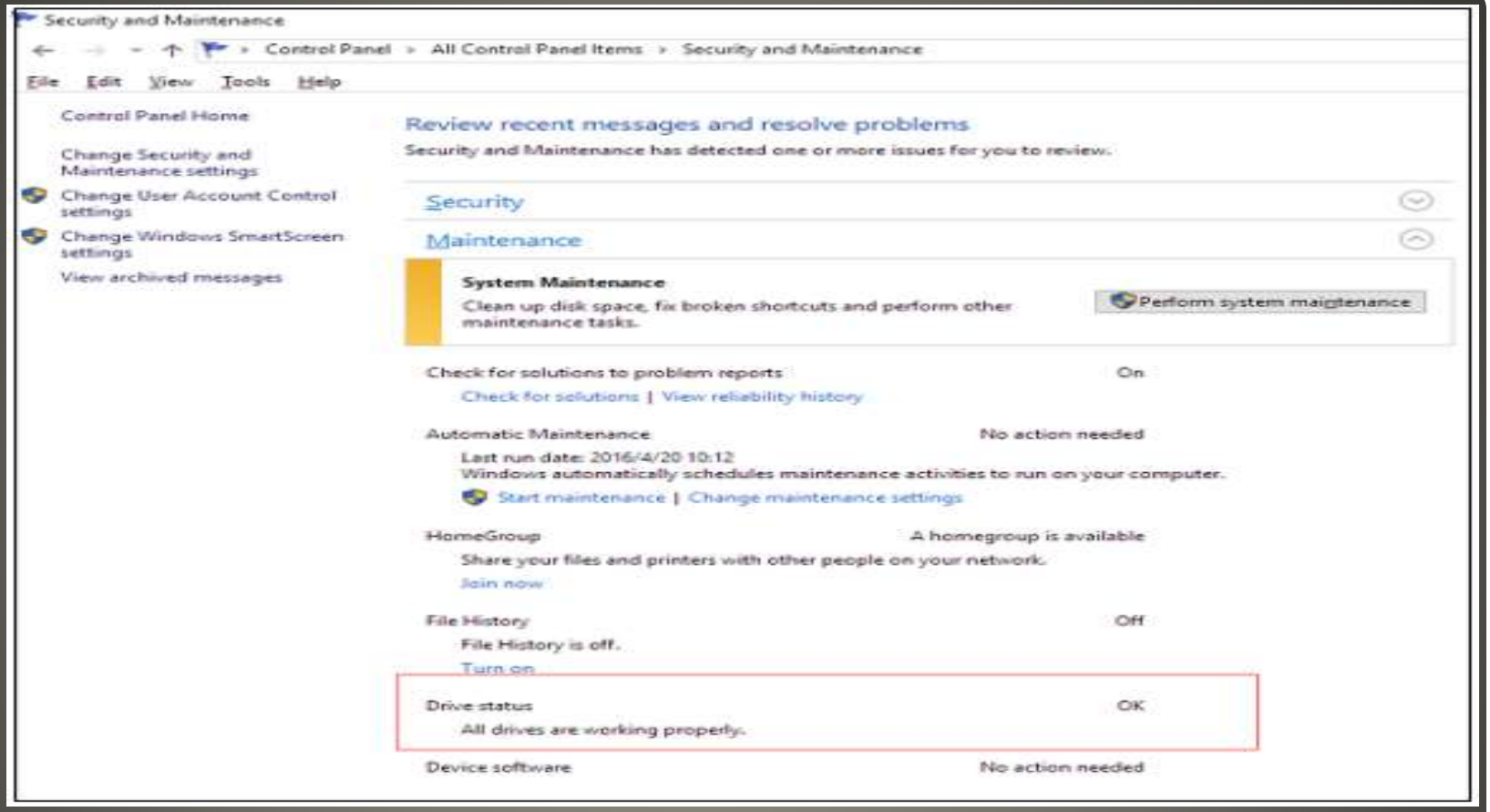
Component-Based Servicing


Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.997]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>sfc /SCANNOW
Beginning system scan. This process will take some time.
Beginning verification phase of system scan.
Verification 100% complete.
Windows Resource Protection found corrupt files and successfully repaired them.
For online repairs, details are included in the CBS log file located at
windir\Logs\CBS\CBS.log. For example C:\Windows\Logs\CBS\CBS.log. For offline
repairs, details are included in the log file provided by the /OFFLOGFILE flag.
C:\WINDOWS\system32>

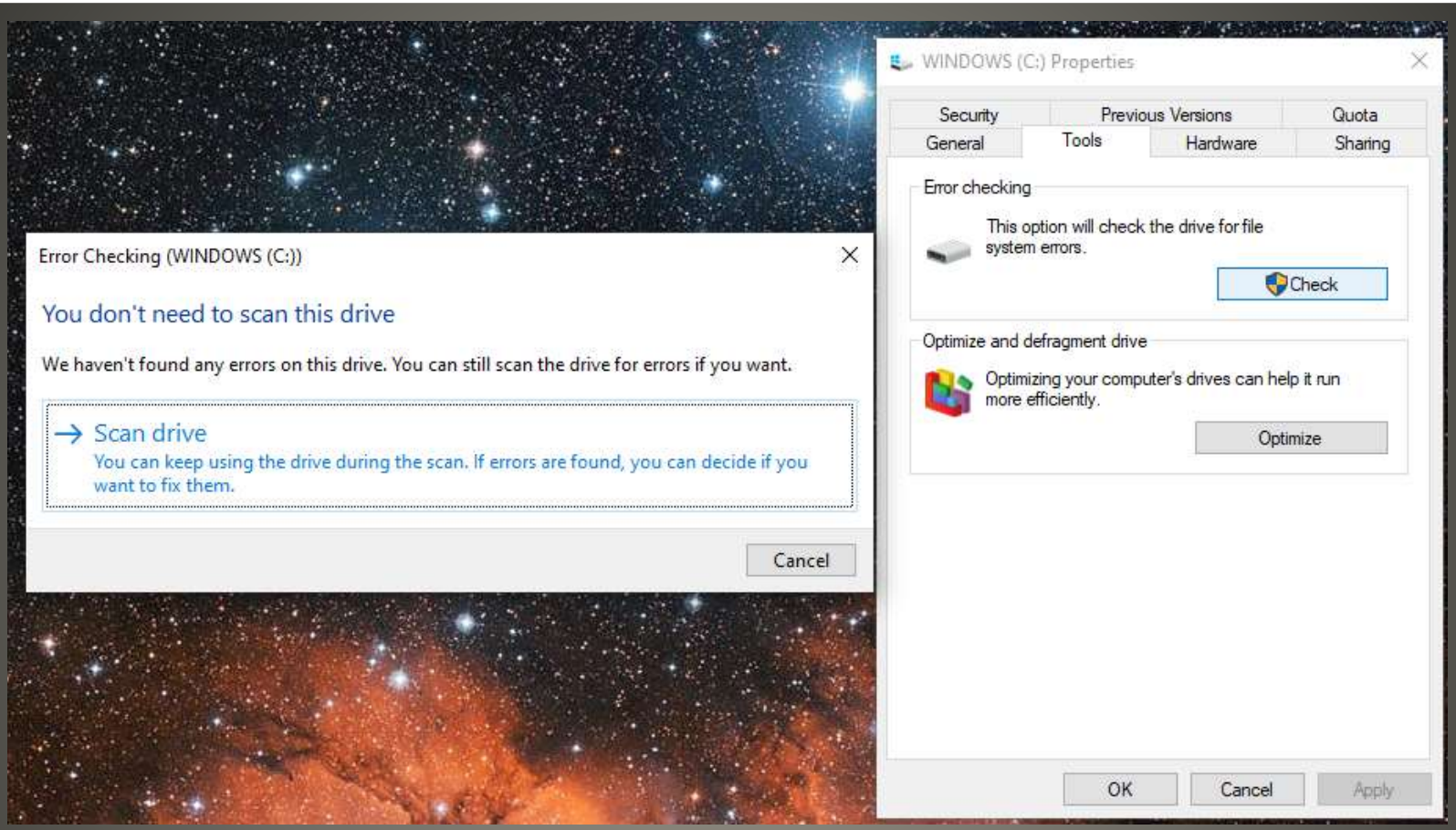
CBS.log - Notepad

File Edit Format View Help

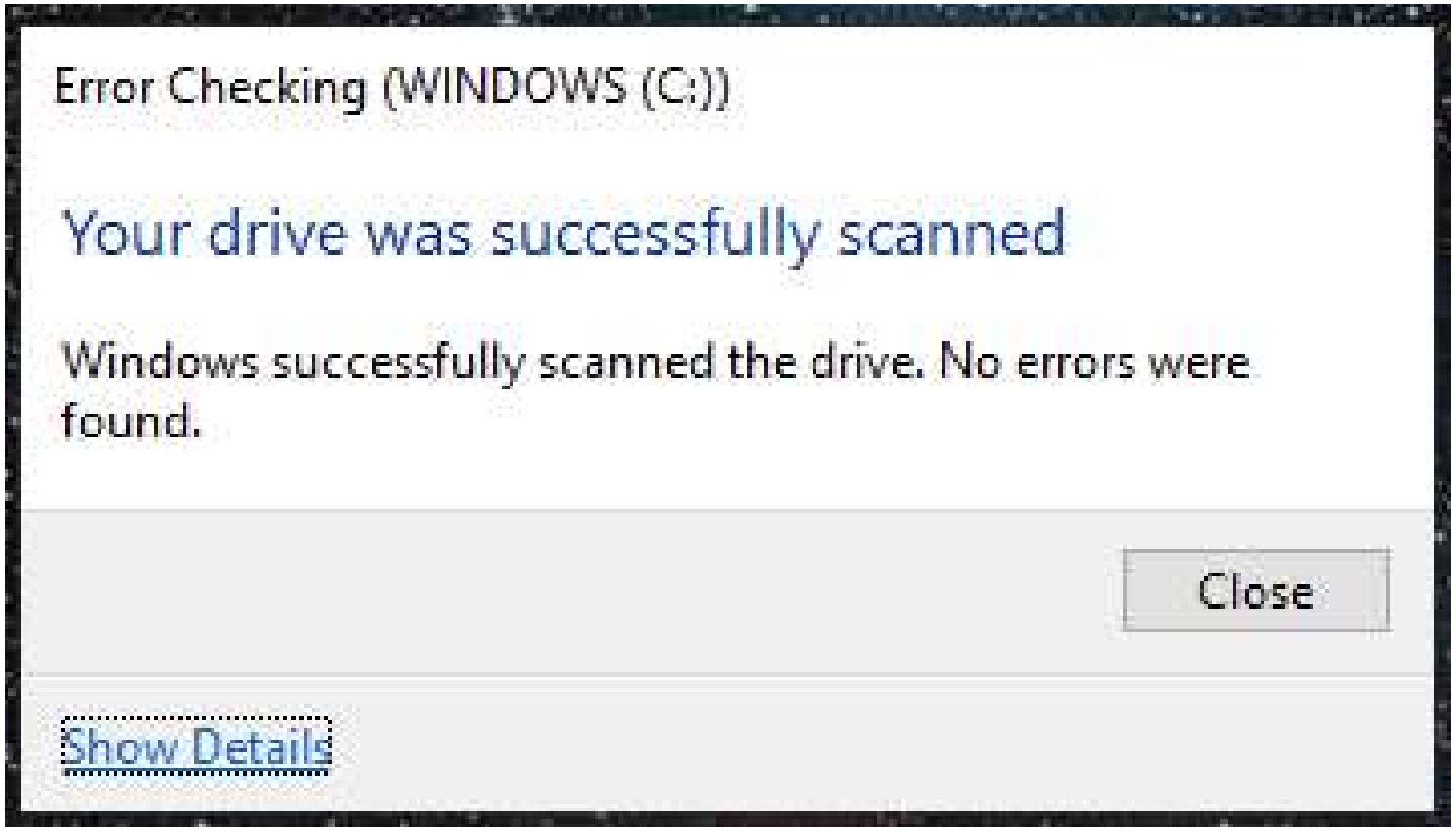
```
2020-07-28 14:00:34, Info                  CSI    0000025c [SR] Beginning Verify and Repair transaction
2020-07-28 14:00:36, Info                  CSI    0000025d [SR] Verify complete
2020-07-28 14:00:36, Info                  CSI    0000025e [SR] Verifying 100 components
2020-07-28 14:00:36, Info                  CSI    0000025f [SR] Beginning Verify and Repair transaction
2020-07-28 14:00:37, Info                  CSI    00000260 [SR] Verify complete
2020-07-28 14:00:38, Info                  CSI    00000261 [SR] Verifying 100 components
2020-07-28 14:00:38, Info                  CSI    00000262 [SR] Beginning Verify and Repair transaction
2020-07-28 14:00:39, Info                  CSI    00000263 CSIPERF - FilePI Queue 115ms
2020-07-28 14:00:39, Info                  CSI    00000264 CSIPERF - FilePI Queue 130ms
2020-07-28 14:00:39, Info                  CSI    00000265 [SR] Verify complete
2020-07-28 14:00:40, Info                  CSI    00000266 [SR] Verifying 100 components
2020-07-28 14:00:40, Info                  CSI    00000267 [SR] Beginning Verify and Repair transaction
2020-07-28 14:00:41, Info                  CSI    00000268 CSIPERF - FilePI Queue 104ms
2020-07-28 14:00:41, Info                  CSI    00000269 [SR] Verify complete
2020-07-28 14:00:42, Info                  CSI    0000026a [SR] Verifying 100 components
2020-07-28 14:00:42, Info                  CSI    0000026b [SR] Beginning Verify and Repair transaction
2020-07-28 14:00:43, Info                  CSI    0000026c CSIPERF - FilePI Queue 157ms
2020-07-28 14:00:44, Info                  CSI    0000026d [SR] Verify complete
2020-07-28 14:00:44, Info                  CSI    0000026e [SR] Verifying 100 components
2020-07-28 14:00:44, Info                  CSI    0000026f [SR] Beginning Verify and Repair transaction
2020-07-28 14:00:46, Info                  CSI    00000270 CSIPERF - FilePI Queue 414ms
2020-07-28 14:00:46, Info                  CSI    00000271 [SR] Verify complete
2020-07-28 14:00:46, Info                  CSI    00000272 [SR] Verifying 100 components
2020-07-28 14:00:46, Info                  CSI    00000273 [SR] Beginning Verify and Repair transaction
2020-07-28 14:00:48, Info                  CSI    00000274 CSIPERF - FilePI Queue 142ms
2020-07-28 14:00:48, Info                  CSI    00000275 [SR] Verify complete
2020-07-28 14:00:49, Info                  CSI    00000276 [SR] Verifying 100 components
2020-07-28 14:00:49, Info                  CSI    00000277 [SR] Beginning Verify and Repair transaction
2020-07-28 14:00:50, Info                  CSI    00000278 CSIPERF - FilePI Queue 109ms
2020-07-28 14:00:51, Info                  CSI    00000279 CSIPERF - FilePI Queue 123ms
2020-07-28 14:00:51, Info                  CSI    0000027a [SR] Verify complete
2020-07-28 14:00:51, Info                  CSI    0000027b [SR] Verifying 33 components
2020-07-28 14:00:51, Info                  CSI    0000027c [SR] Beginning Verify and Repair transaction
2020-07-28 14:00:52, Info                  CSI    0000027d [SR] Verify complete
2020-07-28 14:00:52, Info                  CSI    0000027e [SR] Repairing 0 components
2020-07-28 14:00:52, Info                  CSI    0000027f [SR] Beginning Verify and Repair transaction
2020-07-28 14:00:52, Info                  CSI    00000280 [SR] Repair complete
2020-07-28 14:02:55, Info                  CBS    Trusted Installer is shutting down because: SHUTDOWN_REASON_AUTOSTOP
```

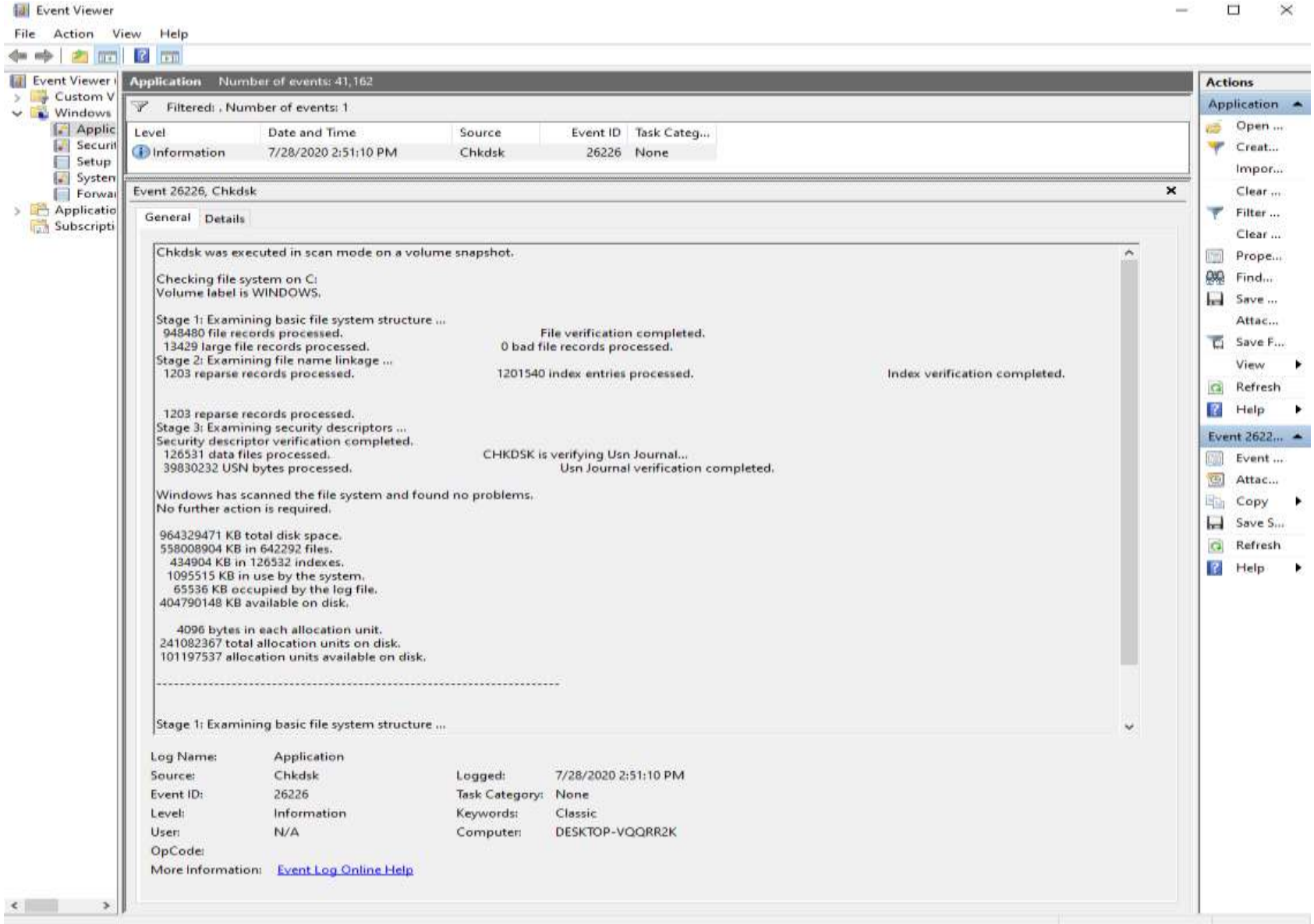


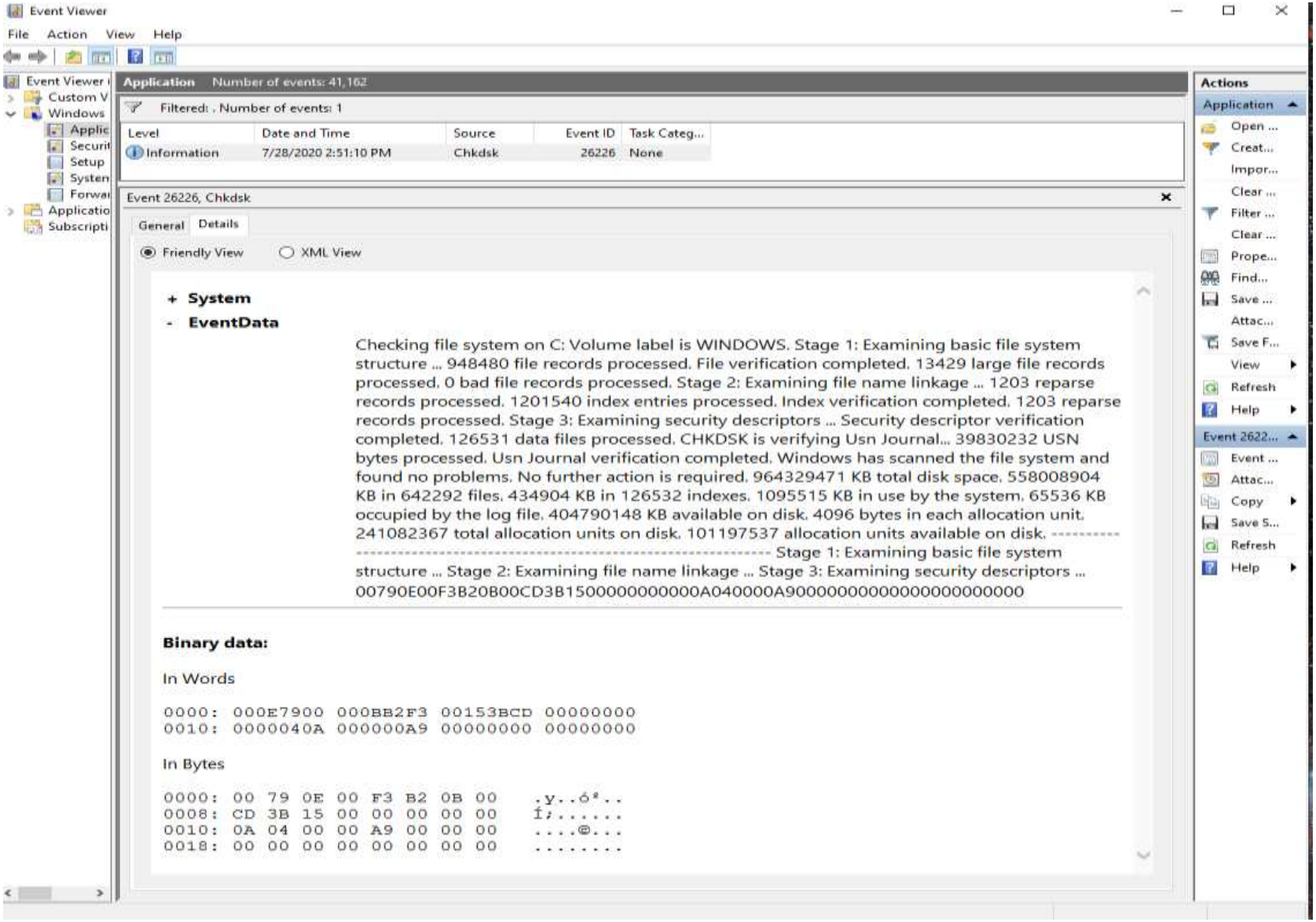
Control Panel > Security & Maintenance

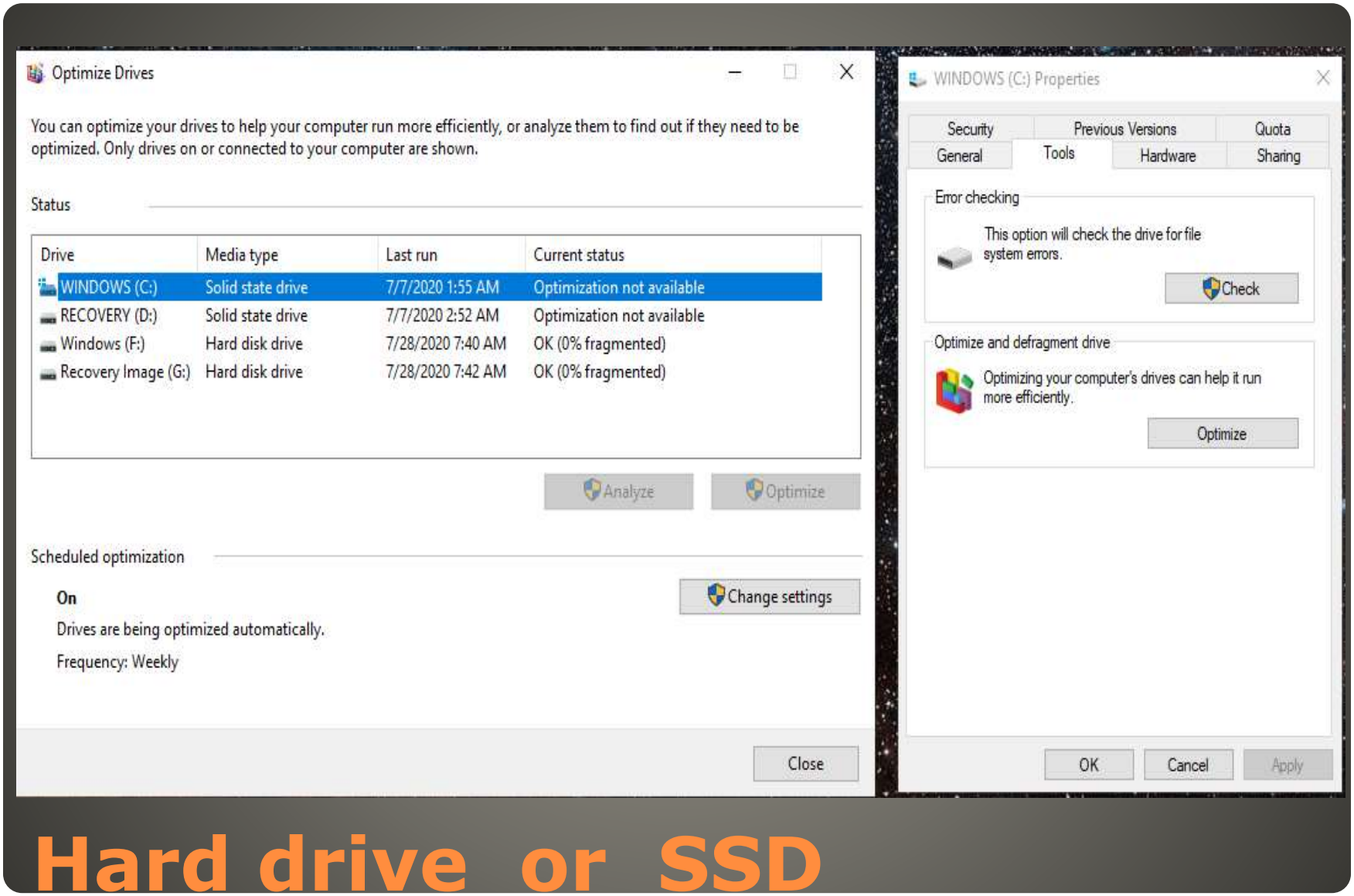


Disk Properties


Error Checking (WINDOWS (C:))
Your drive was successfully scanned
Windows successfully scanned the drive. No errors were found.
Close
Show Details

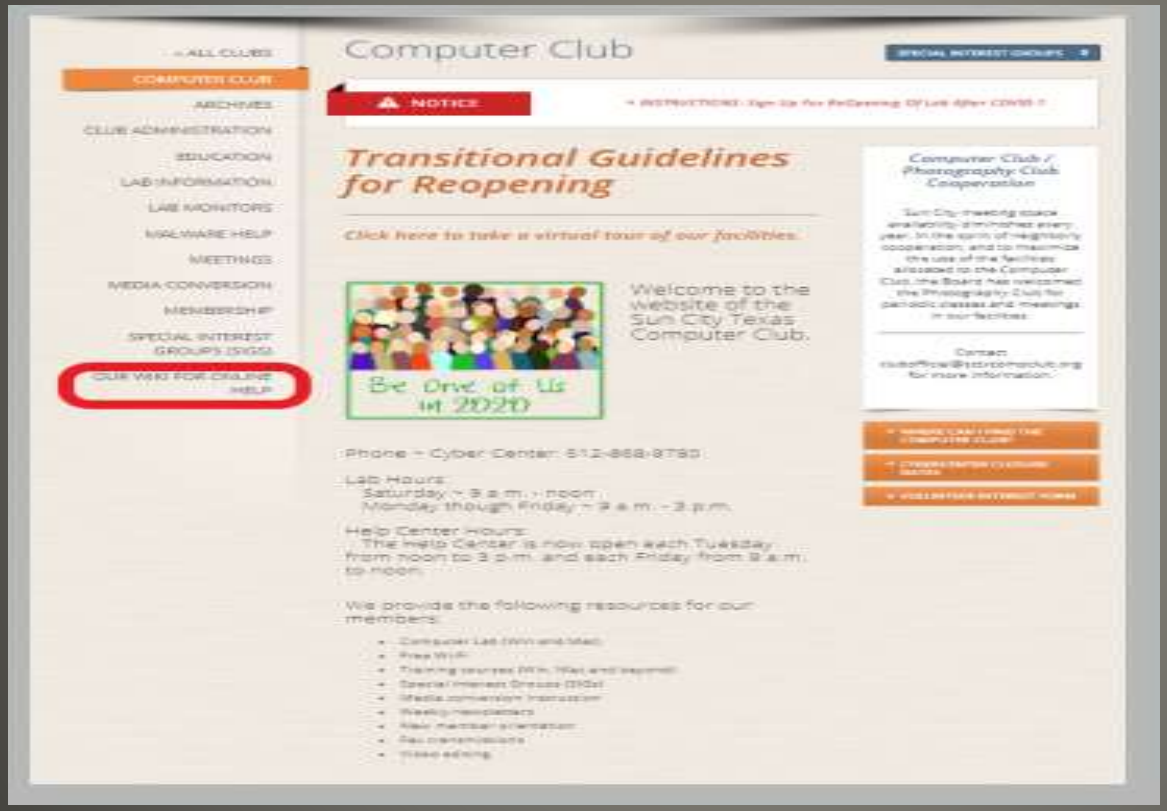

Event Viewer
File Action View Help
Application Number of events: 41,162
Filtered: , Number of events: 1
Level Date and Time Source Event ID Task Categ...
Information 7/28/2020 2:51:10 PM Chkdsk 26226 None
Event 26226, Chkdsk
General Details
Chkdsk was executed in scan mode on a volume snapshot.
Checking file system on C:
Volume label is WINDOWS.
Stage 1: Examining basic file system structure ...
948480 file records processed. File verification completed.
13429 large file records processed. 0 bad file records processed.
Stage 2: Examining file name linkage ...
1203 reparse records processed. 1201540 index entries processed. Index verification completed.
1203 reparse records processed.
Stage 3: Examining security descriptors ...
Security descriptor verification completed.
126531 data files processed. CHKDSK is verifying Usn Journal...
39830232 USN bytes processed. Usn Journal verification completed.
Windows has scanned the file system and found no problems.
No further action is required.
964329471 KB total disk space.
558008904 KB in 642292 files.
434904 KB in 126532 indexes.
1095515 KB in use by the system.
65536 KB occupied by the log file.
404790148 KB available on disk.
4096 bytes in each allocation unit.
241082367 total allocation units on disk.
101197537 allocation units available on disk.
Stage 1: Examining basic file system structure ...
Log Name: Application
Source: Chkdsk Logged: 7/28/2020 2:51:10 PM
Event ID: 26226 Task Category: None
Level: Information Keywords: Classic
User: N/A Computer: DESKTOP-VQQRR2K
OpCode:
More Information: Event Log Online Help
Actions
Application
Open ...
Creat...
Impor...
Clear ...
Filter ...
Clear ...
Prope...
Find...
Save ...
Attac...
Save F...
View
Refresh
Help
Event 2622...
Event ...
Attac...
Copy
Save S...
Refresh
Help


Event Viewer
File Action View Help
Application Number of events: 41,162
Filtered: . Number of events: 1
Level Date and Time Source Event ID Task Categ...
Information 7/28/2020 2:51:10 PM Chkdsk 26226 None
Event 26226, Chkdsk
General Details
Friendly View XML View
+ System
- EventData
Checking file system on C: Volume label is WINDOWS. Stage 1: Examining basic file system structure ... 948480 file records processed. File verification completed. 13429 large file records processed. 0 bad file records processed. Stage 2: Examining file name linkage ... 1203 reparse records processed. 1201540 index entries processed. Index verification completed. 1203 reparse records processed. Stage 3: Examining security descriptors ... Security descriptor verification completed. 126531 data files processed. CHKDSK is verifying Usn Journal... 39830232 USN bytes processed. Usn Journal verification completed. Windows has scanned the file system and found no problems. No further action is required. 964329471 KB total disk space. 558008904 KB in 642292 files. 434904 KB in 126532 indexes. 1095515 KB in use by the system. 65536 KB occupied by the log file. 404790148 KB available on disk. 4096 bytes in each allocation unit. 241082367 total allocation units on disk. 101197537 allocation units available on disk. ---------- Stage 1: Examining basic file system structure ... Stage 2: Examining file name linkage ... Stage 3: Examining security descriptors ...
00790E00F3B20B00CD3B1500000000000A040000A900000000000000000000000000
Binary data:
In Words
0000: 000E7900 000BB2F3 00153BCD 00000000
0010: 0000040A 000000A9 00000000 00000000
In Bytes
0000: 00 79 0E 00 F3 B2 0B 00 .y..ó²..
0008: CD 3B 15 00 00 00 00 00 Í;......
0010: 0A 04 00 00 A9 00 00 00 ....©...
0018: 00 00 00 00 00 00 00 00 ....
Actions
Application
Open ...
Creat...
Impor...
Clear ...
Filter ...
Clear ...
Prope...
Find...
Save ...
Attac...
Save F...
View
Refresh
Help
Event 2622...
Event ...
Attac...
Copy
Save S...
Refresh
Help



Hard drive or SSD

- More information
- Computer Club Wiki



chkdsk

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