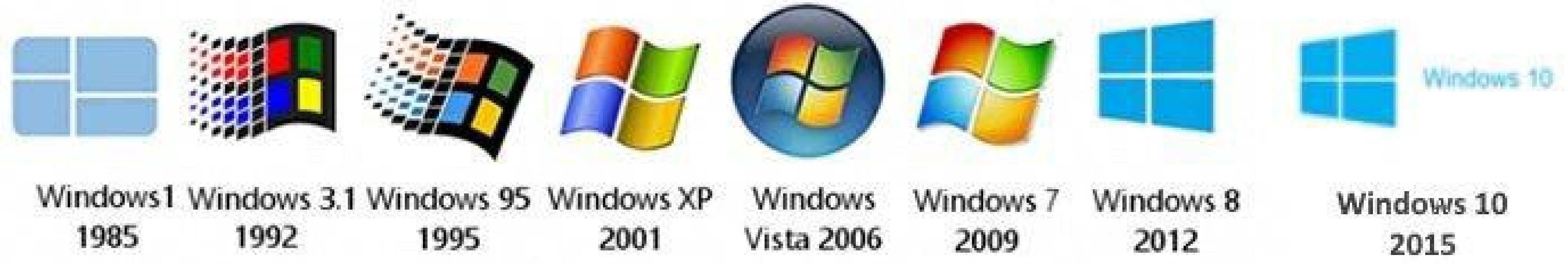
WINDOWS FUNDAMENTALS

Windows Operating Systems

What is an Operating System?

An operating system (OS) is a software program that manages and controls the hardware and software resources of a computer system.

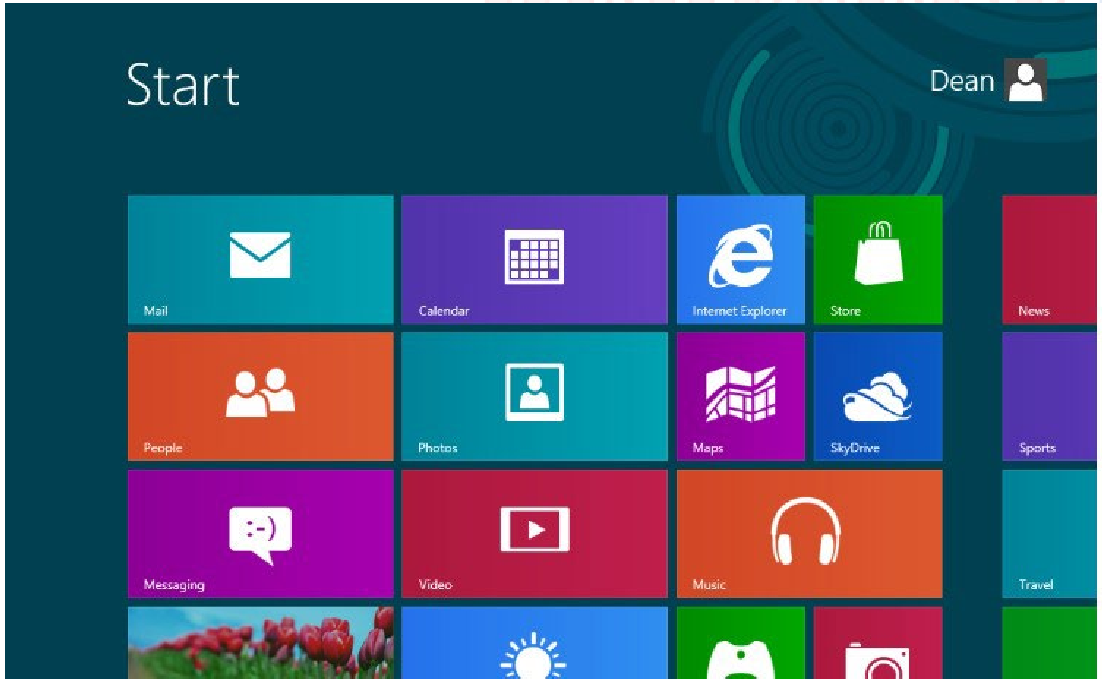


CHECK COMPUTER SPECIFICATION(SPECS)

- Operating system (OS)
- RAM
- Storage
- CPU

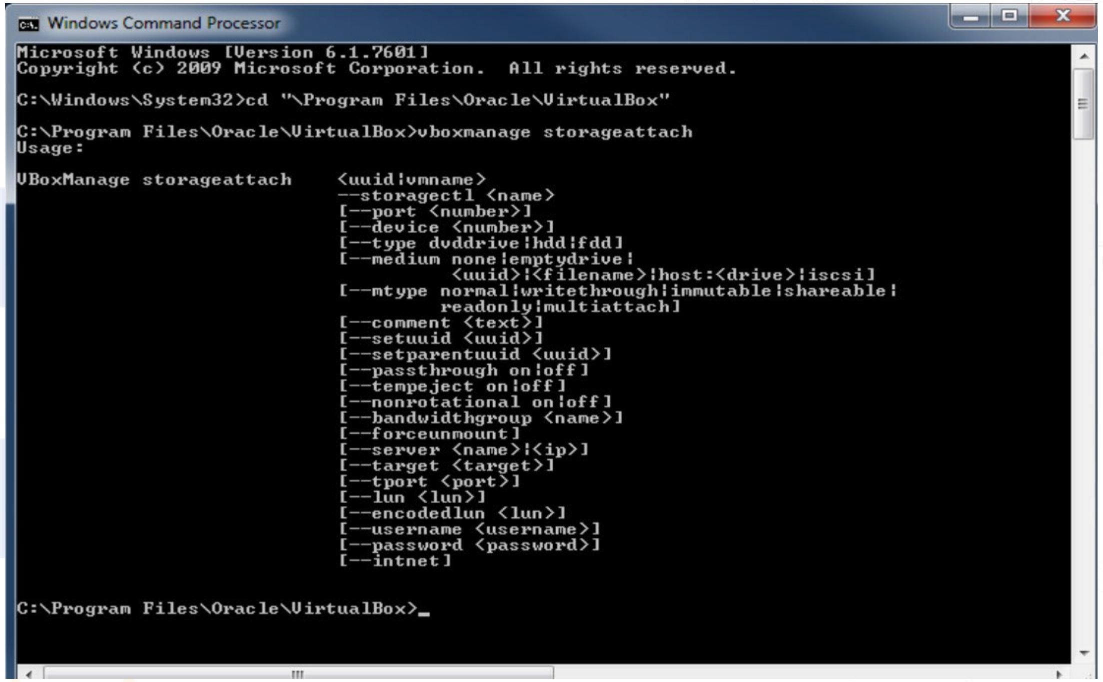
WINDOWS DESKTOP

Graphical User Interface – GUI



GUIs are designed to make computer systems more user-friendly and accessible to people who may not have a technical background.

Command Line Interface – CLI



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>cd "\Program Files\Oracle\VirtualBox"

C:\Program Files\Oracle\VirtualBox>vboxmanage storageattach
Usage:

VBoxManage storageattach    <uuid¦vmname>
                            --storagectl <name>
                            [--port <number>]
                            [--device <number>]
                            [--type dvddrive¦hdd¦fdd]
                            [--medium none¦emptydrive¦
                                      <uuid>¦<filename>¦host:<drive>¦iscsi]
                            [--mtype normal¦writethrough¦immutable¦shareable¦
                                     readonly¦multiattach]
                            [--comment <text>]
                            [--setuuid <uuid>]
                            [--setparentuuid <uuid>]
                            [--passthrough on¦off]
                            [--tempeject on¦off]
                            [--nonrotational on¦off]
                            [--bandwidthgroup <name>]
                            [--forceunmount]
                            [--server <name>¦<ip>]
                            [--target <target>]
                            [--tport <port>]
                            [--lun <lun>]
                            [--encodedlun <lun>]
                            [--username <username>]
                            [--password <password>]
                            [--intnet]


C:\Program Files\Oracle\VirtualBox>_
```

Users interact with the system or application by entering specific commands

WINDOWS CLI COMMANDS

☑ 1 systeminfo → Used for Displaying computer/system information

☑ 2. whoami → Used for Displaying user information

☑ 3. hostname → Used for Quickly finding your hostname/computer name

☑ 4. ping google.com → Used for Troubleshooting network connection issues

☑ 5. ipconfig → Used to check computer IP address

☑ 6. getmac → Used for Quickly finding your MAC address

☑ 7. dir → Used to list directories

☑ 8. NSLOOKUP google.com → Used for Troubleshooting connection issues

☑ 9. TRACERT google.com → Used for Troubleshooting NetBIOS issues (-n)

☑ 10. cd → check the current directory

☑ 11. help → Check all available windows commands

MORE COMMANDS

☑ 10. SHUTDOWN /s → Used to shutdown your computer

☑ 11. netstat –a → Used for Displaying network connections and ports

☑ 12. mkdir test → Used for creating a directory called test

☑ 13. CD test → Used for changing a directory

☑ 14. CD .. → Used for navigating to the previous directory

☑ 15. rmdir test → Used for deleting a directory

☑ 16. tasklist → Used for listing processes a machine.

☑ 17. taskkill /pid 3568 → Used for: Ending processes

☑ 18. route print → Used for displaying the route table

☑ 19. cls → Used for clearing the screen

☑ 20. echo hello > test.txt → Used for creating a file “test.txt” containing the word “hello”

☑ 21. type test.txt → Used for seeing the content of a file

☑ 22. > → Used to redirect output

☑ 23. >> → Used to append to the already existing content of a file

WINDOWS COMMANDS

https://activedirectorypro.com/windows-cmd-commands/#:~:text=50%20Basic%20Windows%20Commands%20with%20Examples%201%201.,8%208.%20dcdiag%20%28test%20domain%20controller%29%20More%20items

WINDOWS TOOLS FOR

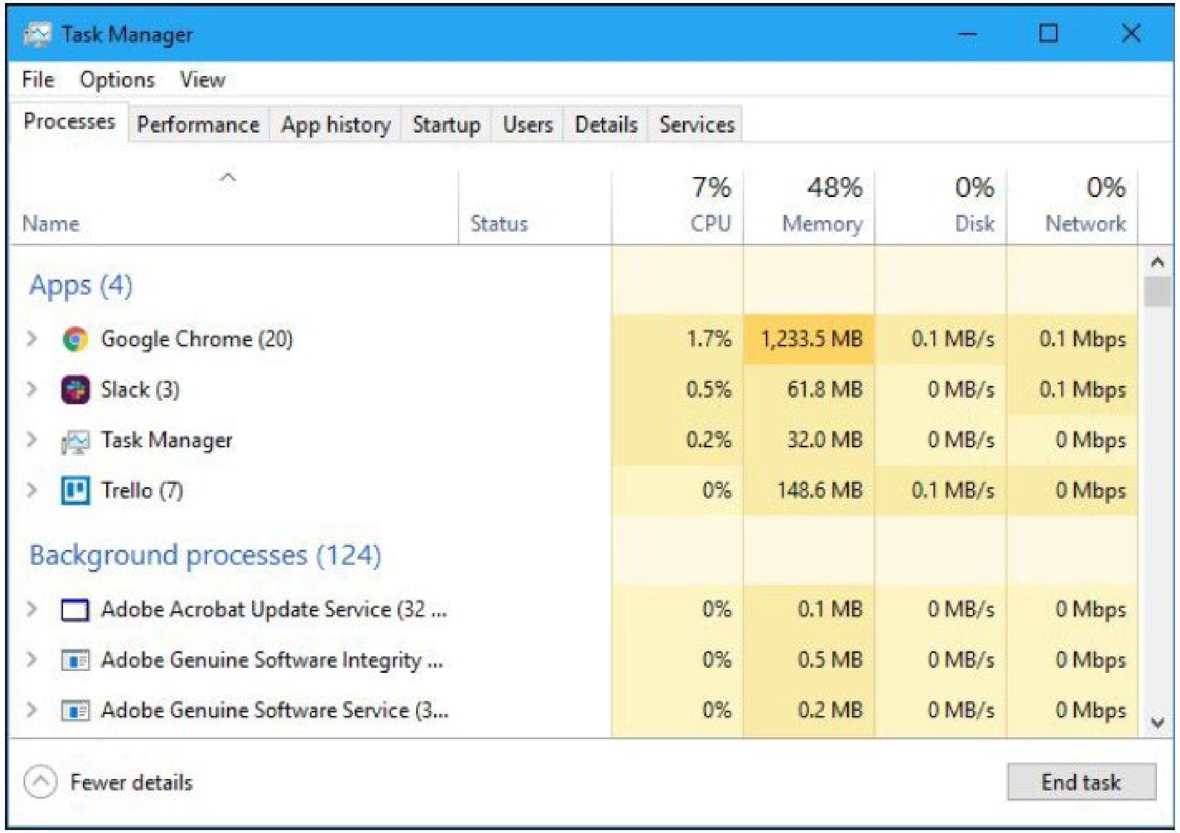
CYBER SECURITY ANALYST

TASK MANAGER

A task manager is a system monitor program used to provide information about the processes and applications running on a computer.

It can also be used to terminate processes and applications.

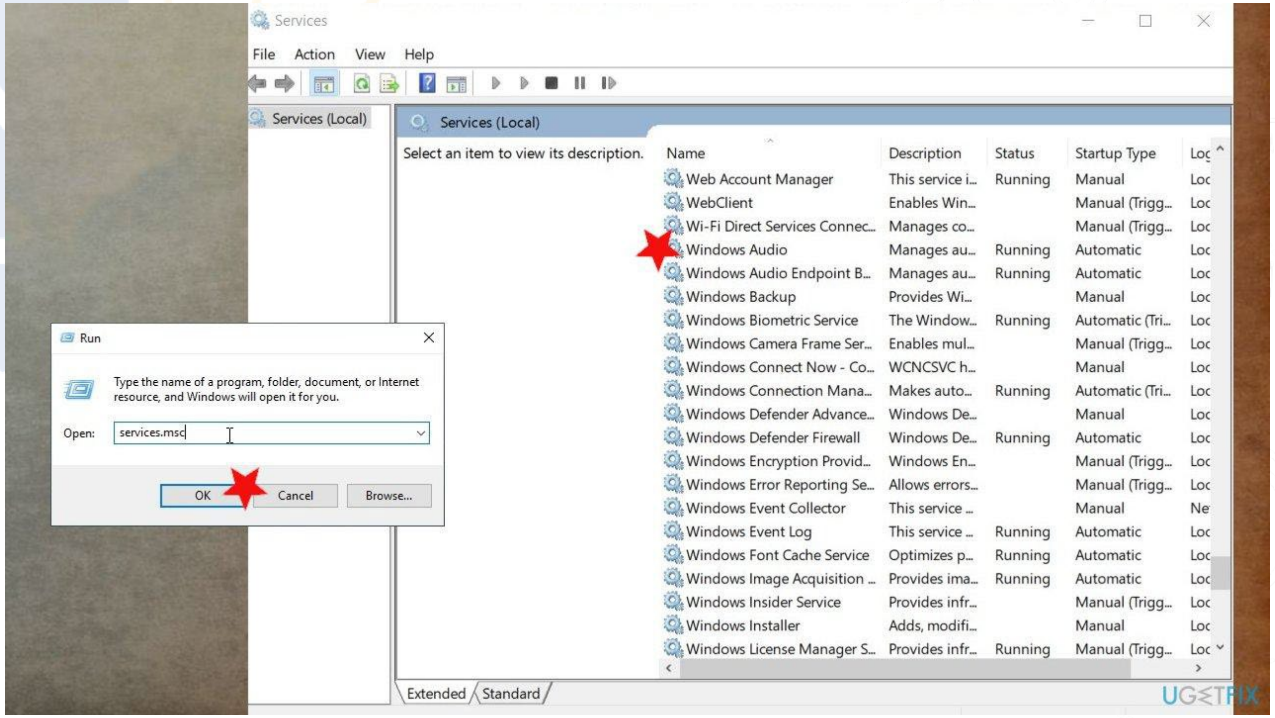
Ctr + Alt + Del



Name	Status	7% CPU	48% Memory	0% Disk	0% Network
Apps (4)					
Google Chrome (20)		1.7%	1,233.5 MB	0.1 MB/s	0.1 Mbps
Slack (3)		0.5%	61.8 MB	0 MB/s	0.1 Mbps
Task Manager		0.2%	32.0 MB	0 MB/s	0 Mbps
Trello (7)		0%	148.6 MB	0.1 MB/s	0 Mbps
Background processes (124)					
Adobe Acrobat Update Service (32 ...		0%	0.1 MB	0 MB/s	0 Mbps
Adobe Genuine Software Integrity ...		0%	0.5 MB	0 MB/s	0 Mbps
Adobe Genuine Software Service (3...		0%	0.2 MB	0 MB/s	0 Mbps

SERVICES

Microsoft Windows services, formerly known as NT services, enable you to create long-running executable applications that run in their own Windows sessions. These services can be automatically started when the computer boots, can be paused and restarted, and do not show any user interface.



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

OK Cancel Browse...

Select an item to view its description.

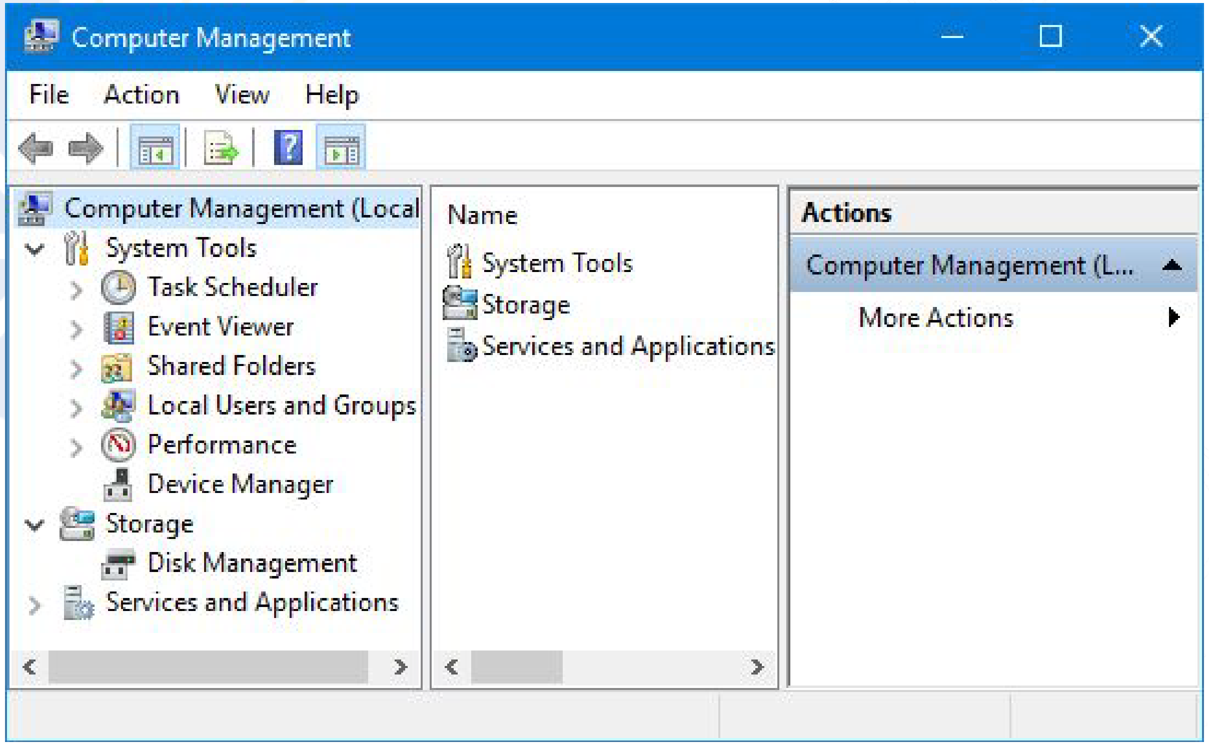
Name	Description	Status	Startup Type	Loc
Web Account Manager	This service i...	Running	Manual	Loc
WebClient	Enables Win...		Manual (Trigg...	Loc
Wi-Fi Direct Services Connec...	Manages co...		Manual (Trigg...	Loc
Windows Audio	Manages au...	Running	Automatic	Loc
Windows Audio Endpoint B...	Manages au...	Running	Automatic	Loc
Windows Backup	Provides Wi...		Manual	Loc
Windows Biometric Service	The Window...	Running	Automatic (Tri...	Loc
Windows Camera Frame Ser...	Enables mul...		Manual (Trigg...	Loc
Windows Connect Now - Co...	WCNCSVC h...		Manual	Loc
Windows Connection Mana...	Makes auto...	Running	Automatic (Tri...	Loc
Windows Defender Advance...	Windows De...		Manual	Loc
Windows Defender Firewall	Windows De...	Running	Automatic	Loc
Windows Encryption Provid...	Windows En...		Manual (Trigg...	Loc
Windows Error Reporting Se...	Allows errors...		Manual (Trigg...	Loc
Windows Event Collector	This service ...		Manual	Ne
Windows Event Log	This service ...	Running	Automatic	Loc
Windows Font Cache Service	Optimizes p...	Running	Automatic	Loc
Windows Image Acquisition ...	Provides ima...	Running	Automatic	Loc
Windows Insider Service	Provides infr...		Manual (Trigg...	Loc
Windows Installer	Adds, modifi...		Manual	Loc
Windows License Manager S...	Provides infr...	Running	Manual (Trigg...	Loc

winKey + s then type services

COMPUTER MANAGEMENT

Computer Management is a handy console included in Windows that allows you to view event logs, partition your hard drive, manage the devices and services, etc.

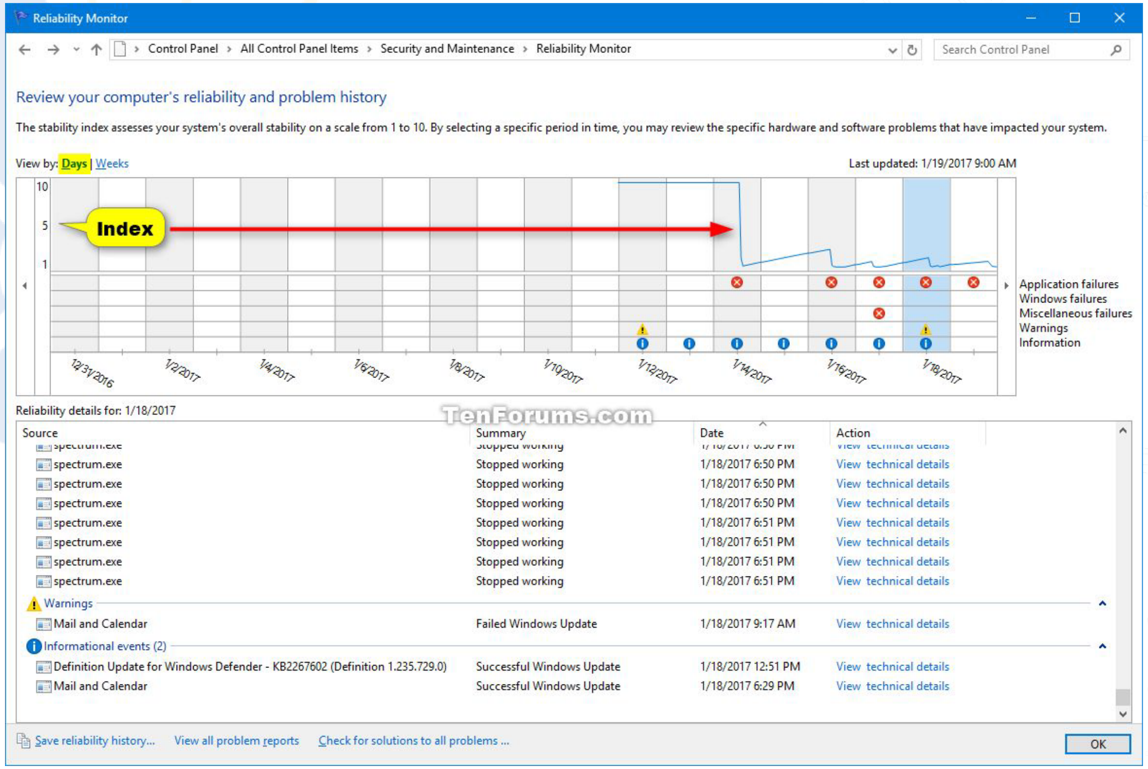
winKey + s then type computer management



RELIABILITY HISTORY

Windows 10 keeps track of errors and system failures, and thanks to this feature, you can easily learn more about specific errors that occurred in the past.

winKey + s then type Reliability



Review your computer's reliability and problem history

The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that have impacted your system.

View by: Days | Weeks

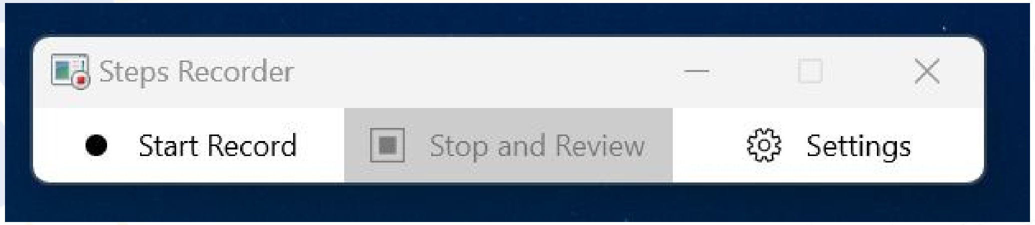
Last updated: 1/19/2017 9:00 AM

Reliability details for: 1/18/2017

Source	Summary	Date	Action
spectrum.exe	Stopped working	1/18/2017 6:50 PM	View technical details
spectrum.exe	Stopped working	1/18/2017 6:50 PM	View technical details
spectrum.exe	Stopped working	1/18/2017 6:50 PM	View technical details
spectrum.exe	Stopped working	1/18/2017 6:50 PM	View technical details
spectrum.exe	Stopped working	1/18/2017 6:51 PM	View technical details
spectrum.exe	Stopped working	1/18/2017 6:51 PM	View technical details
spectrum.exe	Stopped working	1/18/2017 6:51 PM	View technical details
spectrum.exe	Stopped working	1/18/2017 6:51 PM	View technical details
⚠ Warnings			
Mail and Calendar	Failed Windows Update	1/18/2017 9:17 AM	View technical details
ℹ Informational events (2)			
Definition Update for Windows Defender - KB2267602 (Definition 1.235.729.0)	Successful Windows Update	1/18/2017 12:51 PM	View technical details
Mail and Calendar	Successful Windows Update	1/18/2017 6:29 PM	View technical details

STEPS RECORDER

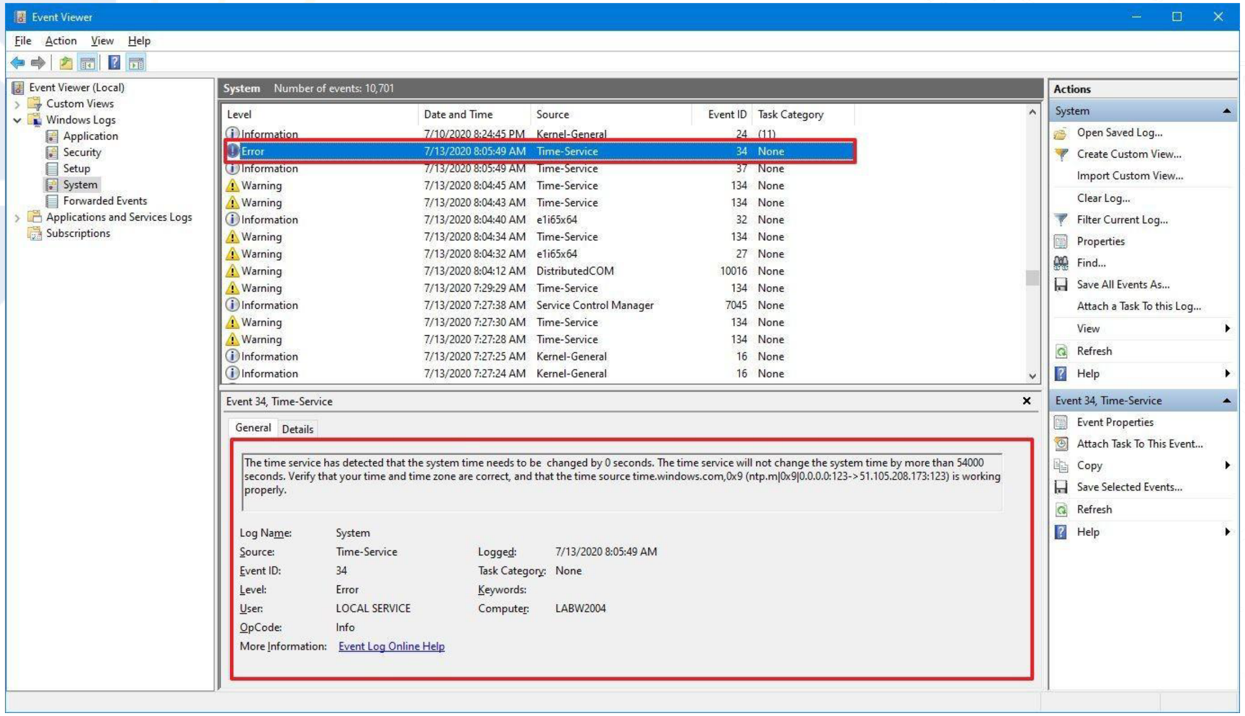
Problem Steps Recorder (PSR) to automatically capture steps on a computer. Steps Recorder is a combination keylogger, screen capture, and annotation tool for Windows. It's used to quickly and easily document actions made on a computer for troubleshooting purposes.



winKey + s then type Steps Recorder

EVENT VIEWER

On Windows 10, the Event Viewer is a handy legacy tool designed to aggregate event logs from apps and system components into an easily digestible structure, which you can then analyze to troubleshoot and fix software or hardware problems with your computer.



System Number of events: 10,701

Level	Date and Time	Source	Event ID	Task Category
Information	7/10/2020 8:24:45 PM	Kernel-General	24	(11)
Error	7/13/2020 8:05:49 AM	Time-Service	34	None
Information	7/13/2020 8:05:49 AM	Time-Service	37	None
Warning	7/13/2020 8:04:45 AM	Time-Service	134	None
Warning	7/13/2020 8:04:43 AM	Time-Service	134	None
Information	7/13/2020 8:04:40 AM	e1i65x64	32	None
Warning	7/13/2020 8:04:34 AM	Time-Service	134	None
Warning	7/13/2020 8:04:32 AM	e1i65x64	27	None
Warning	7/13/2020 8:04:12 AM	DistributedCOM	10016	None
Warning	7/13/2020 7:29:29 AM	Time-Service	134	None
Information	7/13/2020 7:27:38 AM	Service Control Manager	7045	None
Warning	7/13/2020 7:27:30 AM	Time-Service	134	None
Warning	7/13/2020 7:27:28 AM	Time-Service	134	None
Information	7/13/2020 7:27:25 AM	Kernel-General	16	None
Information	7/13/2020 7:27:24 AM	Kernel-General	16	None

Event 34, Time-Service

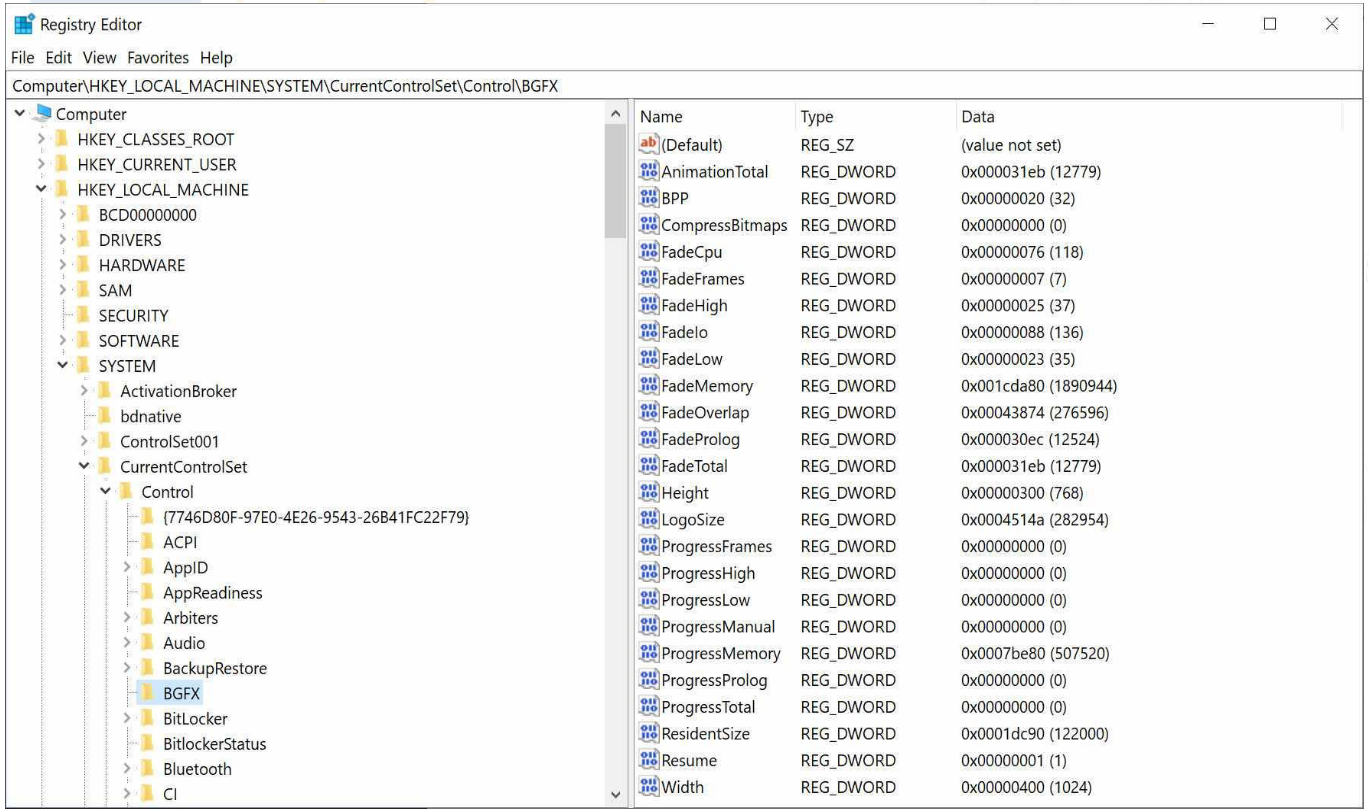
The time service has detected that the system time needs to be changed by 0 seconds. The time service will not change the system time by more than 54000 seconds. Verify that your time and time zone are correct, and that the time source time.windows.com,0x9 (ntp.m|0x9|0.0.0.0:123->51.105.208.173:123) is working properly.

Log Name: System
Source: Time-Service
Logged: 7/13/2020 8:05:49 AM
Event ID: 34
Task Category: None
Level: Error
Keywords:
User: LOCAL SERVICE
Computer: LABW2004
OpCode: Info
More Information: Event Log Online Help

winKey + s then type event viewer

WINDOWS REGISTRY

Windows Registry is one of the key components of the Windows operating system. This hierarchical database contains windows settings, application settings, device driver info and user passwords. When an application is installed, some part of the software is stored in the Registry file, i.e. RegEdit.exe.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BGFX

```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    DRIVERS
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
      ActivationBroker
      bdnative
      ControlSet001
      CurrentControlSet
        Control
          {7746D80F-97E0-4E26-9543-26B41FC22F79}
          ACPI
          AppID
          AppReadiness
          Arbiters
          Audio
          BackupRestore
          BGFX
          BitLocker
          BitlockerStatus
          Bluetooth
          CI
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
AnimationTotal	REG_DWORD	0x000031eb (12779)
BPP	REG_DWORD	0x00000020 (32)
CompressBitmaps	REG_DWORD	0x00000000 (0)
FadeCpu	REG_DWORD	0x00000076 (118)
FadeFrames	REG_DWORD	0x00000007 (7)
FadeHigh	REG_DWORD	0x00000025 (37)
FadeIo	REG_DWORD	0x00000088 (136)
FadeLow	REG_DWORD	0x00000023 (35)
FadeMemory	REG_DWORD	0x001cda80 (1890944)
FadeOverlap	REG_DWORD	0x00043874 (276596)
FadeProlog	REG_DWORD	0x000030ec (12524)
FadeTotal	REG_DWORD	0x000031eb (12779)
Height	REG_DWORD	0x00000300 (768)
LogoSize	REG_DWORD	0x0004514a (282954)
ProgressFrames	REG_DWORD	0x00000000 (0)
ProgressHigh	REG_DWORD	0x00000000 (0)
ProgressLow	REG_DWORD	0x00000000 (0)
ProgressManual	REG_DWORD	0x00000000 (0)
ProgressMemory	REG_DWORD	0x0007be80 (507520)
ProgressProlog	REG_DWORD	0x00000000 (0)
ProgressTotal	REG_DWORD	0x00000000 (0)
ResidentSize	REG_DWORD	0x0001dc90 (122000)
Resume	REG_DWORD	0x00000001 (1)
Width	REG_DWORD	0x00000400 (1024)

winKey + r then type regedit

CYBER ANALYSIS TOOLS

Process Hacker → https://processhacker.sourceforge.io/

Process Monitor → https://learn.microsoft.com/en-us/sysinternals/downloads/procmon

Autorun → https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns

TcpView → https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview

ASSIGNMENT

Watch the video and email 5 new commands you learnt to jtata@beriteck.com

https://www.youtube.com/watch?v=Jfvg3CS1X3A