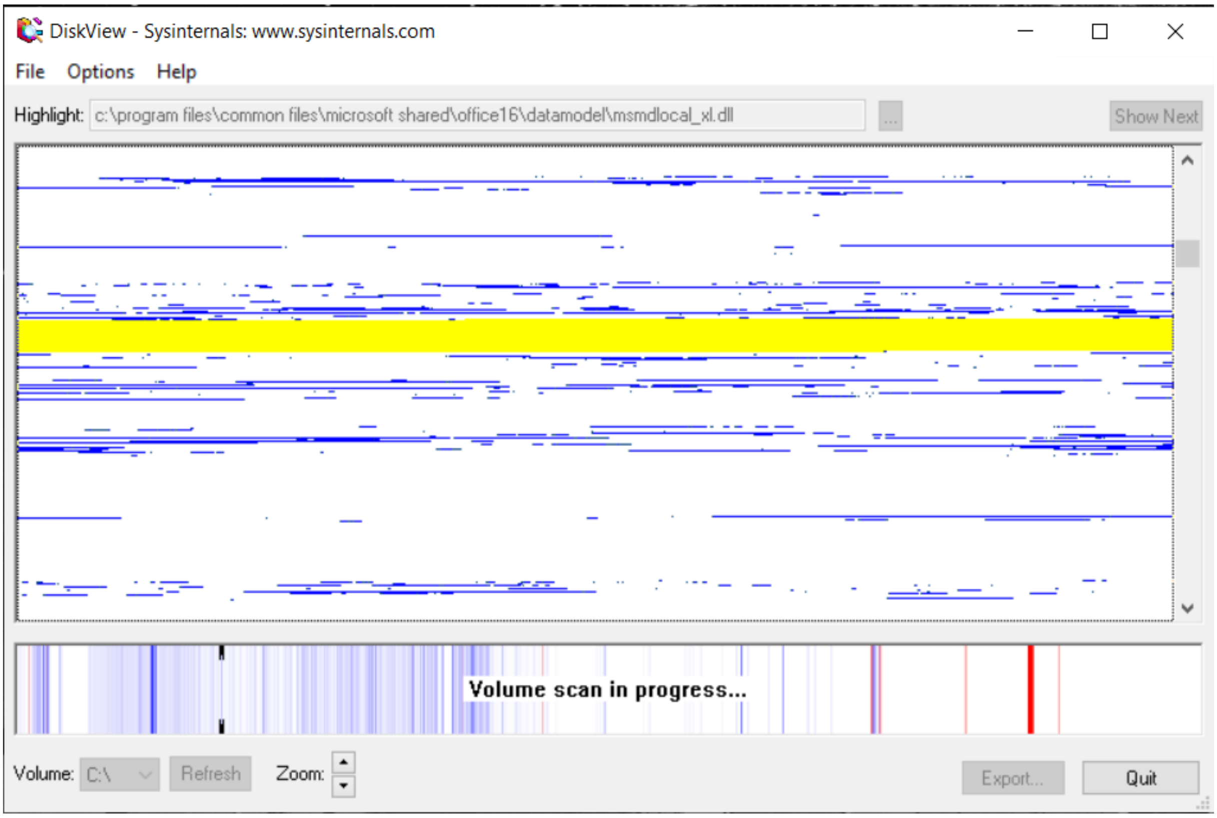
Windows Sysinternals

File and Disk Utilities:

DiskView



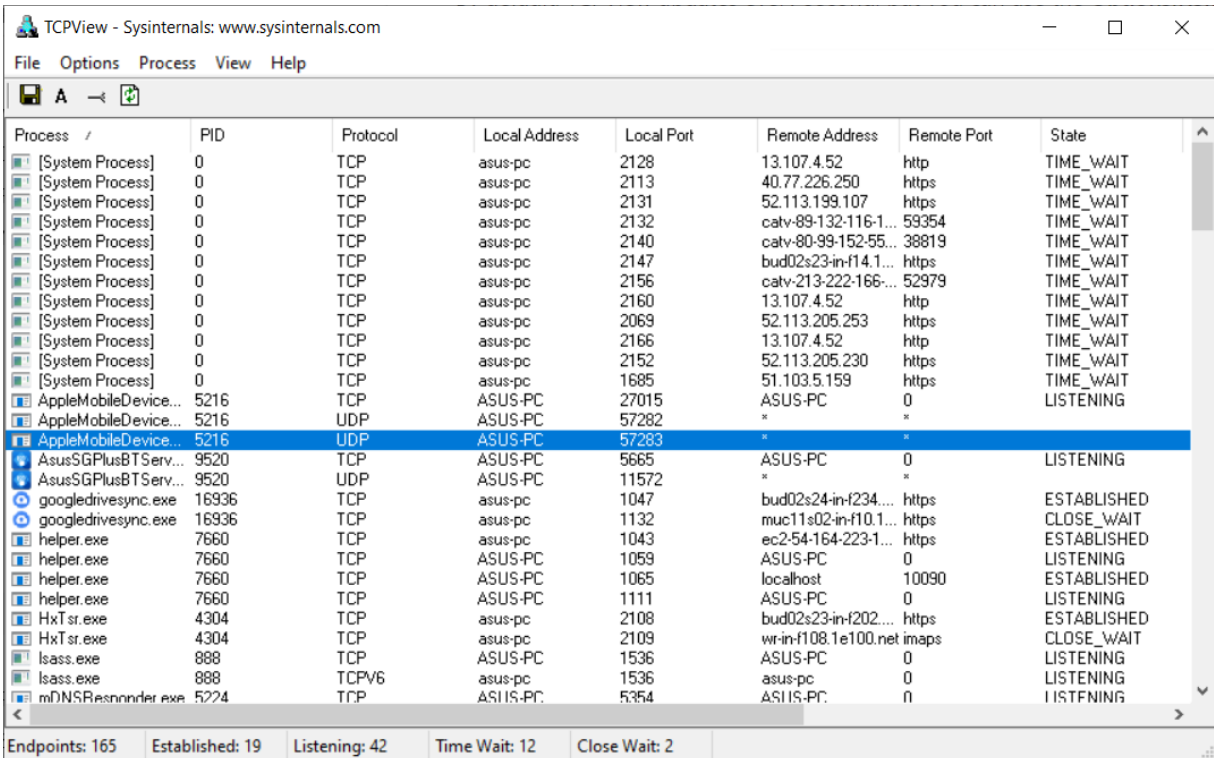
DiskView - Sysinternals: www.sysinternals.com
File Options Help
Show Next
Volume scan in progress...
Refresh
Zoom:
Export...
Quit

Highlight: c:\program files\common files\microsoft shared\office16\datamodel\msmdlocal_xl.dll

Volume: C:\

Networking Utilities:

TCPView

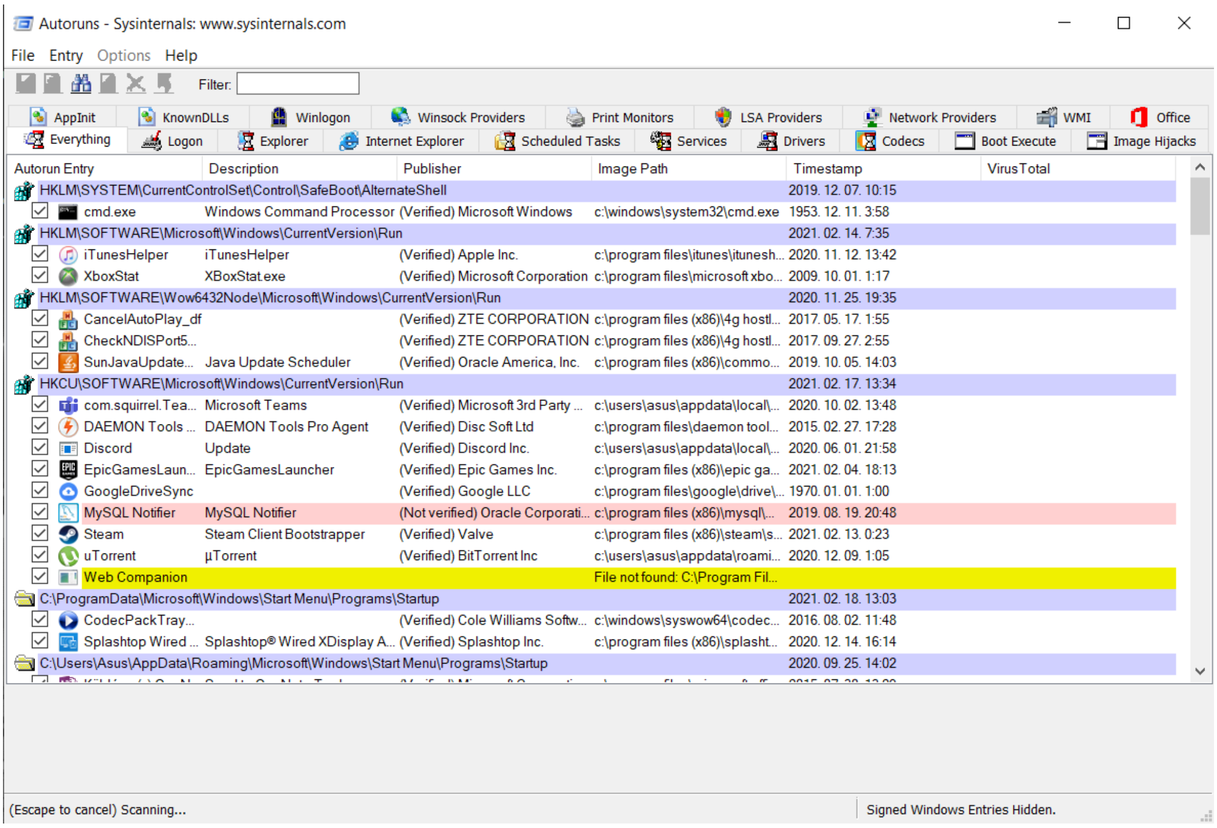


Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Process]	0	TCP	asus-pc	2128	13.107.4.52	http	TIME_WAIT
[System Process]	0	TCP	asus-pc	2113	40.77.226.250	https	TIME_WAIT
[System Process]	0	TCP	asus-pc	2131	52.113.199.107	https	TIME_WAIT
[System Process]	0	TCP	asus-pc	2132	catv-89-132-116-1...	59354	TIME_WAIT
[System Process]	0	TCP	asus-pc	2140	catv-80-99-152-55...	38819	TIME_WAIT
[System Process]	0	TCP	asus-pc	2147	bud02s23-in-f14.1...	https	TIME_WAIT
[System Process]	0	TCP	asus-pc	2156	catv-213-222-166-...	52979	TIME_WAIT
[System Process]	0	TCP	asus-pc	2160	13.107.4.52	http	TIME_WAIT
[System Process]	0	TCP	asus-pc	2069	52.113.205.253	https	TIME_WAIT
[System Process]	0	TCP	asus-pc	2166	13.107.4.52	http	TIME_WAIT
[System Process]	0	TCP	asus-pc	2152	52.113.205.230	https	TIME_WAIT
[System Process]	0	TCP	asus-pc	1685	51.103.5.159	https	TIME_WAIT
AppleMobileDevice...	5216	TCP	ASUS-PC	27015	ASUS-PC	0	LISTENING
AppleMobileDevice...	5216	UDP	ASUS-PC	57282	*	*	
AppleMobileDevice...	5216	UDP	ASUS-PC	57283	*	*	
AsusSGPlusBTServ...	9520	TCP	ASUS-PC	5665	ASUS-PC	0	LISTENING
AsusSGPlusBTServ...	9520	UDP	ASUS-PC	11572	*	*	
googledrivesync.exe	16936	TCP	asus-pc	1047	bud02s24-in-f234....	https	ESTABLISHED
googledrivesync.exe	16936	TCP	asus-pc	1132	muc11s02-in-f10.1...	https	CLOSE_WAIT
helper.exe	7660	TCP	asus-pc	1043	ec2-54-164-223-1...	https	ESTABLISHED
helper.exe	7660	TCP	ASUS-PC	1059	ASUS-PC	0	LISTENING
helper.exe	7660	TCP	ASUS-PC	1065	localhost	10090	ESTABLISHED
helper.exe	7660	TCP	ASUS-PC	1111	ASUS-PC	0	LISTENING
HxTsr.exe	4304	TCP	asus-pc	2108	bud02s23-in-f202....	https	ESTABLISHED
HxTsr.exe	4304	TCP	asus-pc	2109	wr-in-f108.1e100.net	imaps	CLOSE_WAIT
lsass.exe	888	TCP	ASUS-PC	1536	ASUS-PC	0	LISTENING
lsass.exe	888	TCPV6	asus-pc	1536	asus-pc	0	LISTENING
mDNSResponder.exe	5224	TCP	ASUS-PC	5354	ASUS-PC	0	LISTENING

Endpoints: 165 | Established: 19 | Listening: 42 | Time Wait: 12 | Close Wait: 2

Process Utilities:

Autoruns



Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2019. 12. 07. 10:15	
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	1953. 12. 11. 3:58	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 02. 14. 7:35	
☑ iTunesHelper	iTunesHelper	(Verified) Apple Inc.	c:\program files\itunes\itunesh...	2020. 11. 12. 13:42	
☑ XboxStat	XBoxStat.exe	(Verified) Microsoft Corporation	c:\program files\microsoft xbo...	2009. 10. 01. 1:17	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				2020. 11. 25. 19:35	
☑ CancelAutoPlay_df		(Verified) ZTE CORPORATION	c:\program files (x86)\4g hostl...	2017. 05. 17. 1:55	
☑ CheckNDISPort5...		(Verified) ZTE CORPORATION	c:\program files (x86)\4g hostl...	2017. 09. 27. 2:55	
☑ SunJavaUpdate...	Java Update Scheduler	(Verified) Oracle America, Inc.	c:\program files (x86)\commo...	2019. 10. 05. 14:03	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2021. 02. 17. 13:34	
☑ com.squirrel.Tea...	Microsoft Teams	(Verified) Microsoft 3rd Party ...	c:\users\asus\appdata\local\...	2020. 10. 02. 13:48	
☑ DAEMON Tools ...	DAEMON Tools Pro Agent	(Verified) Disc Soft Ltd	c:\program files\daemon tool...	2015. 02. 27. 17:28	
☑ Discord	Update	(Verified) Discord Inc.	c:\users\asus\appdata\local\...	2020. 06. 01. 21:58	
☑ EpicGamesLaun...	EpicGamesLauncher	(Verified) Epic Games Inc.	c:\program files (x86)\epic ga...	2021. 02. 04. 18:13	
☑ GoogleDriveSync		(Verified) Google LLC	c:\program files\google\drive\...	1970. 01. 01. 1:00	
☑ MySQL Notifier	MySQL Notifier	(Not verified) Oracle Corporati...	c:\program files (x86)\mysql\...	2019. 08. 19. 20:48	
☑ Steam	Steam Client Bootstrapper	(Verified) Valve	c:\program files (x86)\steam\s...	2021. 02. 13. 0:23	
☑ uTorrent	µTorrent	(Verified) BitTorrent Inc	c:\users\asus\appdata\roami...	2020. 12. 09. 1:05	
☑ Web Companion			File not found: C:\Program Fil...		
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				2021. 02. 18. 13:03	
☑ CodecPackTray...		(Verified) Cole Williams Softw...	c:\windows\syswow64\codec...	2016. 08. 02. 11:48	
☑ Splashtop Wired ...	Splashtop® Wired XDisplay A...	(Verified) Splashtop Inc.	c:\program files (x86)\splasht...	2020. 12. 14. 16:14	
C:\Users\Asus\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				2020. 09. 25. 14:02	

(Escape to cancel) Scanning...

Signed Windows Entries Hidden.