Logfile of random's system information tool 1.10 (written by random/random)

Run by Jakub at 2017-07-27 11:22:39

Microsoft Windows 10 Home

System drive C: has 68 GB (58%) free of 119 GB

Total RAM: 4061 MB (47% free)

Logfile of Trend Micro HijackThis v2.0.4

Scan saved at 11:22:51, on 27.7.2017

Platform: Unknown Windows (WinNT 6.02.1008)

MSIE: Internet Explorer v11.0 (11.00.15063.0000)

Boot mode: Normal

Running processes:

C:\Program Files\ASUS\Net4Switch\Net4Switch.exe

C:\Program Files (x86)\ASUS\Wireless Console 3\wcourier.exe

C:\Program Files (x86)\ASUS\SmartLogon\sensorsrv.exe

C:\Program Files (x86)\ASUS\ControlDeck\ControlDeckStartUp.exe

C:\Windows\AsScrPro.exe

C:\Program Files\AVAST Software\Avast\AvastUI.exe

C:\Users\Jakub\AppData\Local\Microsoft\OneDrive\OneDrive.exe

C:\Program Files (x86)\ASUS\ATK Media\DMedia.exe

C:\Program Files (x86)\ASUS\ATKOSD2\ATKOSD2.exe

C:\Users\Jakub\AppData\Roaming\Seznam.cz\bin\szndesktop.exe

C:\Program Files (x86)\ASUS\ATK Hotkey\HControlUser.exe

C:\Users\Jakub\AppData\Roaming\Seznam Browser\Seznam.cz.exe

C:\Users\Jakub\AppData\Roaming\Seznam Browser\Seznam.cz.exe

C:\Users\Jakub\AppData\Roaming\Seznam Browser\Seznam.cz.exe

C:\Users\Jakub\AppData\Roaming\Seznam Browser\Seznam.cz.exe

C:\Users\Jakub\AppData\Roaming\Seznam Browser\Seznam.cz.exe

C:\Program Files\trend micro\Jakub.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = https://www.seznam.cz/?clid=22668

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page = http://search.seznam.cz/?sourceid=quicksearch_22668&q={searchTerms}

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = https://www.seznam.cz/?clid=22668

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft.com/fwlink/p/?LinkId=255141

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/fwlink/?LinkId=54896

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896

R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/fwlink/p/?LinkId=255141

R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =

R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =

R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Local Page = C:\Windows\SysWOW64\blank.htm

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =

F2 - REG:system.ini: UserInit=

O2 - BHO: AcroIEHelperStub - {18DF081C-E8AD-4283-A596-FA578C2EBDC3} - C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll

O2 - BHO: Groove GFS Browser Helper - {72853161-30C5-4D22-B7F9-0BBC1D38A37E} - C:\Program Files (x86)\Microsoft Office\Office12\GrooveShellExtensions.dll

O4 - HKLM\..\Run: [ATKMEDIA] c:\program files (x86)\asus\atk media\dmedia.exe

O4 - HKLM\..\Run: [ATKOSD2] c:\program files (x86)\asus\atkosd2\atkosd2.exe

O4 - HKLM\..\Run: [HControlUser] c:\program files (x86)\asus\atk hotkey\hcontroluser.exe

O4 - HKLM\..\Run: [HDAudDeck] c:\program files (x86)\via\viaudioi\vdeck\vdeck.exe -r

O4 - HKLM\..\Run: [GrooveMonitor] "C:\Program Files (x86)\Microsoft Office\Office12\GrooveMonitor.exe"

O4 - HKLM\..\Run: [seznam-listicka-distribuce] "C:\Program Files (x86)\Seznam.cz\distribution\szninstall.exe" -s -d listicka 1 szn-software-listicka cz.seznam.software.autoupdate

O4 - HKCU\..\Run: [OneDrive] "C:\Users\Jakub\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

O4 - HKCU\..\Run: [CCleaner Monitoring] "C:\Program Files\CCleaner\CCleaner64.exe" /MONITOR

O4 - HKCU\..\Run: [cz.seznam.software.autoupdate] "C:\Users\Jakub\AppData\Roaming\Seznam.cz\szninstall.exe" -c

O4 - HKCU\..\Run: [cz.seznam.software.szndesktop] "C:\Users\Jakub\AppData\Roaming\Seznam.cz\bin\wszndesktop.exe" -q

O4 - HKUS\S-1-5-19\..\Run: [OneDriveSetup] C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup (User 'LOCAL SERVICE')

O4 - HKUS\S-1-5-20\..\Run: [OneDriveSetup] C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup (User 'NETWORK SERVICE')

O4 - Global Startup: SRS Premium Sound.lnk = ?

O8 - Extra context menu item: E&xport to Microsoft Excel - res://C:\Program Files (x86)\Microsoft Office\Office12\EXCEL.EXE/3000

O9 - Extra button: @C:\Program Files (x86)\Windows Live\Writer\WindowsLiveWriterShortcuts.dll,-1004 - {219C3416-8CB2-491a-A3C7-D9FCDDC9D600} - C:\Program Files (x86)\Windows Live\Writer\WriterBrowserExtension.dll

O9 - Extra 'Tools' menuitem: @C:\Program Files (x86)\Windows Live\Writer\WindowsLiveWriterShortcuts.dll,-1003 - {219C3416-8CB2-491a-A3C7-D9FCDDC9D600} - C:\Program Files (x86)\Windows Live\Writer\WriterBrowserExtension.dll

O9 - Extra button: Odeslat do aplikace OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\PROGRA~2\MICROS~1\Office12\ONBttnIE.dll

O9 - Extra 'Tools' menuitem: Od&eslat do aplikace OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\PROGRA~2\MICROS~1\Office12\ONBttnIE.dll

O9 - Extra button: Research - {92780B25-18CC-41C8-B9BE-3C9C571A8263} - C:\PROGRA~2\MICROS~1\Office12\REFIEBAR.DLL

O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics

O18 - Protocol: grooveLocalGWS - {88FED34C-F0CA-4636-A375-3CB6248B04CD} - C:\Program Files (x86)\Microsoft Office\Office12\GrooveSystemServices.dll

O18 - Protocol: tbauth - {14654CA6-5711-491D-B89A-58E571679951} - C:\Windows\SysWOW64\tbauth.dll

O18 - Protocol: windows.tbauth - {14654CA6-5711-491D-B89A-58E571679951} - C:\Windows\SysWOW64\tbauth.dll

O18 - Protocol: wlpg - {E43EF6CD-A37A-4A9B-9E6F-83F89B8E6324} - C:\Program Files (x86)\Windows Live\Photo Gallery\AlbumDownloadProtocolHandler.dll

O23 - Service: 602Updater (602XML Updater) - Software602 a.s. - C:\Program Files (x86)\Common Files\soft602\602updsvc\602updsvc.exe

O23 - Service: Adobe Flash Player Update Service (AdobeFlashPlayerUpdateSvc) - Adobe Systems Incorporated - C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe

O23 - Service: ADSM Service (ADSMService) - ASUSTek Computer Inc. - C:\Program Files (x86)\ASUS\ASUS Data Security Manager\ADSMSrv.exe

O23 - Service: AFBAgent - Unknown owner - C:\Windows\system32\FBAgent.exe (file missing)

O23 - Service: @%SystemRoot%\system32\Alg.exe,-112 (ALG) - Unknown owner - C:\WINDOWS\System32\alg.exe (file missing)

O23 - Service: ASLDR Service (ASLDRService) - ASUS - C:\Program Files (x86)\ASUS\ATK Hotkey\ASLDRSrv.exe

O23 - Service: aswbIDSAgent - AVAST Software s.r.o. - C:\Program Files\AVAST Software\Avast\x64\aswidsagenta.exe

O23 - Service: ATKGFNEX Service (ATKGFNEXSrv) - Unknown owner - C:\Program Files\ATKGFNEX\GFNEXSrv.exe

O23 - Service: Avast Antivirus (avast! Antivirus) - AVAST Software - C:\Program Files\AVAST Software\Avast\AvastSvc.exe

O23 - Service: @%SystemRoot%\system32\DiagSvcs\DiagnosticsHub.StandardCollector.ServiceRes.dll,-1000 (diagnosticshub.standardcollector.service) - Unknown owner - C:\WINDOWS\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe (file missing)

O23 - Service: @%SystemRoot%\system32\efssvc.dll,-100 (EFS) - Unknown owner - C:\WINDOWS\System32\lsass.exe (file missing)

O23 - Service: Elan Service (ETDService) - ELAN Microelectronics Corp. - C:\Program Files\Elantech\ETDService.exe

O23 - Service: @%systemroot%\system32\fxsresm.dll,-118 (Fax) - Unknown owner - C:\WINDOWS\system32\fxssvc.exe (file missing)

O23 - Service: Služba Google Update (gupdate) (gupdate) - Google Inc. - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe

O23 - Service: Služba Google Update (gupdatem) (gupdatem) - Google Inc. - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe

O23 - Service: InstallDriver Table Manager (IDriverT) - Macrovision Corporation - C:\Program Files (x86)\Common Files\InstallShield\Driver\1150\Intel 32\IDriverT.exe

O23 - Service: @keyiso.dll,-100 (KeyIso) - Unknown owner - C:\WINDOWS\system32\lsass.exe (file missing)

O23 - Service: @comres.dll,-2797 (MSDTC) - Unknown owner - C:\WINDOWS\System32\msdtc.exe (file missing)

O23 - Service: @mqutil.dll,-6102 (MSMQ) - Unknown owner - C:\WINDOWS\system32\mqsvc.exe (file missing)

O23 - Service: @%SystemRoot%\System32\netlogon.dll,-102 (Netlogon) - Unknown owner - C:\WINDOWS\system32\lsass.exe (file missing)

O23 - Service: @%systemroot%\system32\Locator.exe,-2 (RpcLocator) - Unknown owner - C:\WINDOWS\system32\locator.exe (file missing)

O23 - Service: @%SystemRoot%\system32\samsrv.dll,-1 (SamSs) - Unknown owner - C:\WINDOWS\system32\lsass.exe (file missing)

O23 - Service: @%systemroot%\system32\SecurityHealthAgent.dll,-1002 (SecurityHealthService) - Unknown owner - C:\WINDOWS\system32\SecurityHealthService.exe (file missing)

O23 - Service: @%SystemRoot%\system32\SensorDataService.exe,-101 (SensorDataService) - Unknown owner - C:\WINDOWS\System32\SensorDataService.exe (file missing)

O23 - Service: @%SystemRoot%\system32\snmptrap.exe,-3 (SNMPTRAP) - Unknown owner - C:\WINDOWS\System32\snmptrap.exe (file missing)

O23 - Service: @%systemroot%\system32\spectrum.exe,-101 (spectrum) - Unknown owner - C:\WINDOWS\system32\spectrum.exe (file missing)

O23 - Service: spmgr - Unknown owner - C:\Program Files\ASUS\NB Probe\SPM\spmgr.exe

O23 - Service: @%systemroot%\system32\spoolsv.exe,-1 (Spooler) - Unknown owner - C:\WINDOWS\System32\spoolsv.exe (file missing)

O23 - Service: @%SystemRoot%\system32\sppsvc.exe,-101 (sppsvc) - Unknown owner - C:\WINDOWS\system32\sppsvc.exe (file missing)

O23 - Service: @%SystemRoot%\system32\TieringEngineService.exe,-702 (TieringEngineService) - Unknown owner - C:\WINDOWS\system32\TieringEngineService.exe (file missing)

O23 - Service: @%SystemRoot%\system32\ui0detect.exe,-101 (UI0Detect) - Unknown owner - C:\WINDOWS\system32\UI0Detect.exe (file missing)

O23 - Service: @%SystemRoot%\system32\vaultsvc.dll,-1003 (VaultSvc) - Unknown owner - C:\WINDOWS\system32\lsass.exe (file missing)

O23 - Service: @%SystemRoot%\system32\vds.exe,-100 (vds) - Unknown owner - C:\WINDOWS\System32\vds.exe (file missing)

O23 - Service: @oem28.inf,%ViaKaraokeSrv.SvcDesc%;VIA Karaoke digital mixer Service (VIAKaraokeService) - Unknown owner - C:\WINDOWS\system32\viakaraokesrv.exe (file missing)

O23 - Service: @%systemroot%\system32\vssvc.exe,-102 (VSS) - Unknown owner - C:\WINDOWS\system32\vssvc.exe (file missing)

O23 - Service: @%systemroot%\system32\wbengine.exe,-104 (wbengine) - Unknown owner - C:\WINDOWS\system32\wbengine.exe (file missing)

O23 - Service: @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-320 (WdNisSvc) - Unknown owner - C:\Program Files (x86)\Windows Defender\NisSrv.exe (file missing)

O23 - Service: @%ProgramFiles%\Windows Defender\MpAsDesc.dll,-310 (WinDefend) - Unknown owner - C:\Program Files (x86)\Windows Defender\MsMpEng.exe (file missing)

O23 - Service: @%Systemroot%\system32\wbem\wmiapsrv.exe,-110 (wmiApSrv) - Unknown owner - C:\WINDOWS\system32\wbem\WmiApSrv.exe (file missing)

O23 - Service: @%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-101 (WMPNetworkSvc) - Unknown owner - C:\Program Files (x86)\Windows Media Player\wmpnetwk.exe (file missing)

--

End of file - 10910 bytes

======Listing Processes======

c:\windows\system32\svchost.exe -k dcomlaunch -s PlugPlay

"fontdrvhost.exe"

C:\WINDOWS\system32\svchost.exe -k DcomLaunch

c:\windows\system32\svchost.exe -k rpcss

c:\windows\system32\svchost.exe -k dcomlaunch -s LSM

C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetwork

c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -s NcbService

c:\windows\system32\svchost.exe -k netsvcs -s Schedule

c:\windows\system32\svchost.exe -k localservicenetworkrestricted -s TimeBrokerSvc

c:\windows\system32\svchost.exe -k netsvcs -s ProfSvc

c:\windows\system32\svchost.exe -k localservicenetworkrestricted -s EventLog

c:\windows\system32\svchost.exe -k localservice -s nsi

c:\windows\system32\svchost.exe -k netsvcs -s UserManager

c:\windows\system32\svchost.exe -k appmodel -s StateRepository

c:\windows\system32\svchost.exe -k localservicenetworkrestricted -s Dhcp

c:\windows\system32\svchost.exe -k networkservice -s NlaSvc

c:\windows\system32\svchost.exe -k localservice -s netprofm

c:\windows\system32\svchost.exe -k netsvcs -s Themes

c:\windows\system32\svchost.exe -k localservice -s EventSystem

c:\windows\system32\svchost.exe -k netsvcs -s SENS

c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -s AudioEndpointBuilder

c:\windows\system32\svchost.exe -k localservice -s FontCache

C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted

c:\windows\system32\svchost.exe -k localservicenetworkrestricted -s NgcCtnrSvc

c:\windows\system32\svchost.exe -k networkservice -s Dnscache

C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted

C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted

C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted

"C:\Windows\system32\FBAgent.exe"

"C:\Program Files (x86)\ASUS\ATK Hotkey\ASLDRSrv.exe"

"C:\Program Files\ATKGFNEX\GFNEXSrv.exe"

c:\windows\system32\svchost.exe -k netsvcs -s ShellHWDetection

C:\WINDOWS\System32\spoolsv.exe

c:\windows\system32\svchost.exe -k networkservice -s LanmanWorkstation

"C:\Program Files (x86)\Common Files\soft602\602updsvc\602updsvc.exe"

c:\windows\system32\svchost.exe -k apphost -s AppHostSvc

c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -s DeviceAssociationService

C:\WINDOWS\System32\svchost.exe -k utcsvc

c:\windows\system32\svchost.exe -k networkservice -s CryptSvc

"C:\Program Files\Elantech\ETDService.exe"

c:\windows\system32\svchost.exe -k localservicenonetwork -s DPS

c:\windows\system32\svchost.exe -k localservice -s WinHttpAutoProxySvc

c:\windows\system32\svchost.exe -k localserviceandnoimpersonation -s FDResPub

c:\windows\system32\svchost.exe -k iissvcs

C:\WINDOWS\system32\mqsvc.exe

c:\windows\system32\svchost.exe -k netsvcs -s LanmanServer

c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -s PcaSvc

c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -s SysMain

c:\windows\system32\svchost.exe -k appmodel -s tiledatamodelsvc

c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -s TrkWks

c:\windows\system32\viakaraokesrv.exe

c:\windows\system32\svchost.exe -k netsvcs -s Winmgmt

c:\windows\system32\svchost.exe -k netsvcs -s WpnService

dashost.exe {b0fb7f16-7731-4207-b530db7038efe04b}

c:\windows\system32\svchost.exe -k localservice -s WdiServiceHost

c:\windows\system32\svchost.exe -k netsvcs -s iphlpsvc

c:\windows\microsoft.net\framework64\v4.0.30319\smsvchost.exe

c:\windows\system32\svchost.exe -k localserviceandnoimpersonation -s SSDPSRV

"c:\windows\microsoft.net\framework64\v4.0.30319\smsvchost.exe" -netmsmqactivator

c:\windows\system32\svchost.exe -k netsvcs -s Appinfo

c:\windows\system32\svchost.exe -k netsvcs -s TokenBroker

C:\WINDOWS\system32\wbem\wmiprvse.exe

"C:\Program Files (x86)\ASUS\ASUS Data Security Manager\ADSMSrv.exe"

c:\windows\system32\svchost.exe -k localservice -s CDPSvc

"C:\Program Files\ASUS\NB Probe\SPM\spmgr.exe"

C:\WINDOWS\system32\SearchIndexer.exe /Embedding

c:\windows\system32\svchost.exe -k localservice -s LicenseManager

c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -s Netman

c:\windows\system32\svchost.exe -k localservicenetworkrestricted -s wscsvc

c:\windows\system32\svchost.exe -k localservicenetworkrestricted -s RmSvc

c:\windows\system32\svchost.exe -k localservice -s SstpSvc

c:\windows\system32\svchost.exe -k netsvcs -s RasMan

c:\windows\system32\svchost.exe -k netsvcs -s Browser

c:\windows\system32\svchost.exe -k networkservicenetworkrestricted -s PolicyAgent

c:\windows\system32\svchost.exe -k netsvcs

c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -s StorSvc

c:\windows\system32\svchost.exe -k netsvcs -s lfsvc

c:\windows\system32\svchost.exe -k localservicenetworkrestricted -s HomeGroupProvider

C:\WINDOWS\System32\svchost.exe -k LocalServiceNoNetwork -s NcdAutoSetup

C:\WINDOWS\system32\svchost.exe -k LocalService

C:\WINDOWS\System32\WinLogon.exe -SpecialSession

"fontdrvhost.exe"

"dwm.exe"

C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -s lmhosts

"C:\Program Files (x86)\ASUS\SmartLogon\smartlogon.exe" -switch-3be2f036c43042cdb03588591c9325c3

C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -s NgcSvc

"C:\Program Files (x86)\ASUS\ATK Hotkey\HControl.exe"

"C:\Program Files\Elantech\ETDCtrl.exe"

c:\windows\system32\svchost.exe -k unistacksvcgroup -s CDPUserSvc

sihost.exe

c:\windows\system32\svchost.exe -k unistacksvcgroup -s WpnUserService

"C:\Program Files (x86)\ASUS\ASUS CopyProtect\aspg.exe"

"C:\Program Files (x86)\ASUS\Splendid\ACMON.exe"

"C:\Program Files\ASUS\Net4Switch\Net4Switch.exe"

"C:\Program Files\P4G\BatteryLife.exe"

taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}

"C:\Program Files (x86)\ASUS\Wireless Console 3\wcourier.exe"

"C:\Program Files (x86)\ASUS\SmartLogon\sensorsrv.exe"

Atouch64.exe

"C:\Program Files (x86)\ASUS\ControlDeck\ControlDeckStartUp.exe"

C:\WINDOWS\Explorer.EXE

"C:\Windows\AsScrPro.exe"

"C:\Program Files\Elantech\ETDCtrlHelper.exe"

ATKOSD.exe

KBFiltr.exe

WDC.exe

"C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe" -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca

C:\Windows\System32\RuntimeBroker.exe -Embedding

"C:\Program Files\WindowsApps\Microsoft.SkypeApp_11.19.820.0_x64__kzf8qxf38zg5c\SkypeHost.exe" -ServerName:SkypeHost.ServerServer

"C:\Program Files\Windows Defender\MSASCuiL.exe"

"C:\Program Files (x86)\ASUS\ASUS WebStorage\SERVICE\AsusWSService.exe" mysyncfolder

AvastUI.exe /nogui

"C:\Users\Jakub\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

"C:\Program Files\SRS Labs\SRS Premium Sound Control Panel\SRSPremiumPanel_64.exe" /f=srs_premium_sound_nopreset.zip

"C:\Program Files (x86)\ASUS\ATK Media\DMedia.exe"

"C:\Program Files (x86)\ASUS\ATKOSD2\ATKOSD2.exe"

szndesktop.exe default start

"C:\Program Files (x86)\ASUS\ATK Hotkey\HControlUser.exe"

"C:\Users\Jakub\AppData\Roaming\Seznam.cz\bin\listicka-x64.exe"

\??\C:\WINDOWS\system32\conhost.exe 0x4

"C:\Program Files\CCleaner\CCleaner.exe" /MONITOR /uac

"C:\Windows\SysWOW64\ACEngSvr.exe" -Embedding

c:\windows\system32\svchost.exe -k unistacksvcgroup

"C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca

"C:\Users\Jakub\AppData\Roaming\Seznam Browser\Seznam.cz.exe"

"C:\Users\Jakub\AppData\Roaming\Seznam Browser\Seznam.cz.exe" --type=crashpad-handler /prefetch:7 "--database=C:\Users\Jakub\AppData\Local\Seznam.cz\User Data\Crashpad" "--metrics-dir=C:\Users\Jakub\AppData\Local\Seznam.cz\User Data" --annotation=channel= --annotation=plat=Win32 --annotation=prod=Seznam.cz --annotation=ver=4.0.0 --initial-client-data=0x274,0x278,0x27c,0x1cc,0x280,0x69366314,0x69366324,0x69366334

"C:\Users\Jakub\AppData\Roaming\Seznam Browser\Seznam.cz.exe" --type=gpu-process --field-trial-handle=1376 --no-sandbox --user-data-dir="C:\Users\Jakub\AppData\Local\Seznam.cz\User Data" --nwapp-path="C:\Users\Jakub\AppData\Roaming\Seznam Browser" --disable-d3d11 --supports-dual-gpus=false --gpu-driver-bug-workarounds=7,10,16,19,23,41,61,74 --disable-gl-extensions="GL_KHR_blend_equation_advanced GL_KHR_blend_equation_advanced_coherent" --gpu-vendor-id=0x8086 --gpu-device-id=0x2a42 --gpu-driver-vendor="Intel Corporation" --gpu-driver-version=8.15.10.2702 --gpu-driver-date=3-11-2013 --gpu-secondary-vendor-ids=0x8086 --gpu-secondary-device-ids=0x2a43 --user-data-dir="C:\Users\Jakub\AppData\Local\Seznam.cz\User Data" --nwapp-path="C:\Users\Jakub\AppData\Roaming\Seznam Browser" --service-request-channel-token=900944373A6A8D46A95AE83271530756 --mojo-platform-channel-handle=1392 /prefetch:2

"C:\Users\Jakub\AppData\Roaming\Seznam Browser\Seznam.cz.exe" --type=renderer --no-sandbox --field-trial-handle=1376 --primordial-pipe-token=7A3A9DEF393AAA06E8234A4B3D64C116 --lang=cs --user-data-dir="C:\Users\Jakub\AppData\Local\Seznam.cz\User Data" --nwapp-path="C:\Users\Jakub\AppData\Roaming\Seznam Browser" --nwjs --extension-process --disable-client-side-phishing-detection --enable-offline-auto-reload-visible-only --blink-settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetchForDocWrittenScriptsInMainFrameOnSlowConnections=true,cssExternalScannerNoPreload=false,cssExternalScannerPreload=true --enable-pinch --device-scale-factor=1 --num-raster-threads=1 --content-image-texture-target=0,0,3553;0,1,3553;0,2,3553;0,3,3553;0,4,3553;0,5,3553;0,6,3553;0,7,3553;0,8,3553;0,9,3553;0,10,3553;0,11,3553;0,12,3553;0,13,3553;0,14,3553;0,15,3553;1,0,3553;1,1,3553;1,2,3553;1,3,3553;1,4,3553;1,5,3553;1,6,3553;1,7,3553;1,8,3553;1,9,3553;1,10,3553;1,11,3553;1,12,3553;1,13,3553;1,14,3553;1,15,3553;2,0,3553;2,1,3553;2,2,3553;2,3,3553;2,4,3553;2,5,3553;2,6,3553;2,7,3553;2,8,3553;2,9,3553;2,10,3553;2,11,3553;2,12,3553;2,13,3553;2,14,3553;2,15,3553;3,0,3553;3,1,3553;3,2,3553;3,3,3553;3,4,3553;3,5,3553;3,6,3553;3,7,3553;3,8,3553;3,9,3553;3,10,3553;3,11,3553;3,12,3553;3,13,3553;3,14,3553;3,15,3553;4,0,3553;4,1,3553;4,2,3553;4,3,3553;4,4,3553;4,5,3553;4,6,3553;4,7,3553;4,8,3553;4,9,3553;4,10,3553;4,11,3553;4,12,3553;4,13,3553;4,14,3553;4,15,3553 --disable-accelerated-video-decode --service-request-channel-token=7A3A9DEF393AAA06E8234A4B3D64C116 --renderer-client-id=3 --mojo-platform-channel-handle=2352 /prefetch:1

"C:\Users\Jakub\AppData\Roaming\Seznam Browser\Seznam.cz.exe" --type=renderer --no-sandbox --field-trial-handle=1376 --primordial-pipe-token=4FAEB9A361DF11BA166198D0EFCD165B --lang=cs --user-data-dir="C:\Users\Jakub\AppData\Local\Seznam.cz\User Data" --nwapp-path="C:\Users\Jakub\AppData\Roaming\Seznam Browser" --nwjs --disable-client-side-phishing-detection --enable-offline-auto-reload-visible-only --blink-settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetchForDocWrittenScriptsInMainFrameOnSlowConnections=true,cssExternalScannerNoPreload=false,cssExternalScannerPreload=true --enable-pinch --device-scale-factor=1 --num-raster-threads=1 --content-image-texture-target=0,0,3553;0,1,3553;0,2,3553;0,3,3553;0,4,3553;0,5,3553;0,6,3553;0,7,3553;0,8,3553;0,9,3553;0,10,3553;0,11,3553;0,12,3553;0,13,3553;0,14,3553;0,15,3553;1,0,3553;1,1,3553;1,2,3553;1,3,3553;

1,4,3553;1,5,3553;1,6,3553;1,7,3553;1,8,3553;1,9,3553;1,10,3553;1,11,3553;1,12,3553;1,13,3553;1,14,3553;1,15,3553;2,0,3553;2,1,3553;2,2,3553;2,3,3553;2,4,3553;2,5,3553;2,6,3553;2,7,3553;2,8,3553;2,9,3553;2,10,3553;2,11,3553;2,12,3553;2,13,3553;2,14,3553;2,15,3553;3,0,3553;3,1,3553;3,2,3553;3,3,3553;3,4,3553;3,5,3553;3,6,3553;3,7,3553;3,8,3553;3,9,3553;3,10,3553;3,11,3553;3,12,3553;3,13,3553;3,14,3553;3,15,3553;4,0,3553;4,1,3553;4,2,3553;4,3,3553;4,4,3553;4,5,3553;4,6,3553;4,7,3553;4,8,3553;4,9,3553;4,10,3553;4,11,3553;4,12,3553;4,13,3553;4,14,3553;4,15,3553 --disable-accelerated-video-decode --service-request-channel-token=4FAEB9A361DF11BA166198D0EFCD165B --renderer-client-id=5 --mojo-platform-channel-handle=2428 /prefetch:1

C:\WINDOWS\system32\SettingSyncHost.exe -Embedding

C:\WINDOWS\system32\ApplicationFrameHost.exe -Embedding

"C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.8241.41275.0_x64__8wekyb3d8bbwe\HxOutlook.exe" -ServerName:microsoft.windowslive.mail.AppXfbjsbkxvprcgqg6q4c9jfr0pn3kv9x5s.mca

"C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_17.8241.41275.0_x64__8wekyb3d8bbwe\HxTsr.exe" -ServerName:Hx.IPC.Server

"C:\WINDOWS\ImmersiveControlPanel\SystemSettings.exe" -ServerName:microsoft.windows.immersivecontrolpanel

"C:\Program Files\WindowsApps\Microsoft.WindowsStore_11706.1001.26.0_x64__8wekyb3d8bbwe\WinStore.App.exe" -ServerName:App.AppXc75wvwned5vhz4xyxxecvgdjhdkgsdza.mca

"C:\Program Files\WindowsApps\Microsoft.ZuneMusic_10.17062.14111.0_x64__8wekyb3d8bbwe\Music.UI.exe" -ServerName:Microsoft.ZuneMusic.AppX48dcrcgzqqdshm3kf61t0cm5e9pyd6h6.mca

c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -s DsSvc

C:\Windows\System32\SystemSettingsBroker.exe -Embedding

C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -s WdiSystemHost

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\Jakub\AppData\Local\Google\Chrome\User Data\Crashpad" "--metrics-dir=C:\Users\Jakub\AppData\Local\Google\Chrome\User Data" --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=59.0.3071.115 --initial-client-data=0x1e4,0x1e8,0x1ec,0x1e0,0x1f0,0x7ffa9aa319d0,0x7ffa9aa319b8,0x7ffa9aa319e8

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=watcher --main-thread-id=8724 --on-initialized-event-handle=680 --parent-handle=684 /prefetch:6

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=gpu-process --field-trial-handle=1556 --disable-d3d11 --supports-dual-gpus=false --gpu-driver-bug-workarounds=7,10,11,17,20,24,26,43,63,76 --disable-gl-extensions="GL_KHR_blend_equation_advanced GL_KHR_blend_equation_advanced_coherent" --gpu-vendor-id=0x8086 --gpu-device-id=0x2a42 --gpu-driver-vendor="Intel Corporation" --gpu-driver-version=8.15.10.2702 --gpu-driver-date=3-11-2013 --gpu-secondary-vendor-ids=0x8086 --gpu-secondary-device-ids=0x2a43 --service-request-channel-token=236A509F87BFED39514E1C667E06BF00 --mojo-platform-channel-handle=1592 --ignored=" --type=renderer " /prefetch:2

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1556 --primordial-pipe-token=67E0AE1DED9239B4AB4568AFB999834F --lang=cs --extension-process --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --blink-settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetchForDocWrittenScriptsInMainFrameOnSlowConnections=true --enable-pinch --device-scale-factor=1 --num-raster-threads=1 --content-image-texture-target=0,0,3553;0,1,3553;0,2,3553;0,3,3553;0,4,3553;0,5,3553;0,6,3553;0,7,3553;0,8,3553;0,9,3553;0,10,3553;0,11,3553;0,12,3553;0,13,3553;0,14,3553;0,15,3553;0,16,3553;1,0,3553;1,1,3553;1,2,3553;1,3,3553;1,4,3553;1,5,3553;1,6,3553;1,7,3553;1,8,3553;1,9,3553;1,10,3553;1,11,3553;1,12,3553;1,13,3553;1,14,3553;1,15,3553;1,16,3553;2,0,3553;2,1,3553;2,2,3553;2,3,3553;2,4,3553;2,5,3553;2,6,3553;2,7,3553;2,8,3553;2,9,3553;2,10,3553;2,11,3553;2,12,3553;2,13,3553;2,14,3553;2,15,3553;2,16,3553;3,0,3553;3,1,3553;3,2,3553;3,3,3553;3,4,3553;3,5,3553;3,6,3553;3,7,3553;3,8,3553;3,9,3553;3,10,3553;3,11,3553;3,12,3553;3,13,3553;3,14,3553;3,15,3553;3,16,3553;4,0,3553;4,1,3553;4,2,3553;4,3,3553;4,4,3553;4,5,3553;4,6,3553;4,7,3553;4,8,3553;4,9,3553;4,10,3553;4,11,3553;4,12,3553;4,13,3553;4,14,3553;4,15,3553;4,16,3553 --disable-accelerated-video-decode --service-request-channel-token=67E0AE1DED9239B4AB4568AFB999834F --renderer-client-id=4 --mojo-platform-channel-handle=2904 /prefetch:1

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1556 --primordial-pipe-token=A87D45919D731C22139557EB73BA3B26 --lang=cs --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --blink-settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetchForDocWrittenScriptsInMainFrameOnSlowConnections=true --enable-pinch --device-scale-factor=1 --num-raster-threads=1 --content-image-texture-target=0,0,3553;0,1,3553;0,2,3553;0,3,3553;0,4,3553;0,5,3553;0,6,3553;0,7,3553;0,8,3553;0,9,3553;0,10,3553;0,11,3553;0,12,3553;0,13,3553;0,14,3553;0,15,3553;0,16,3553;1,0,3553;1,1,3553;1,2,3553;1,3,3553;1,4,3553;1,5,3553;1,6,3553;1,7,3553;1,8,3553;1,9,3553;1,10,3553;1,11,3553;1,12,3553;1,13,3553;1,14,3553;1,15,3553;1,16,3553;2,0,3553;2,1,3553;2,2,3553;2,3,3553;2,4,3553;2,5,3553;2,6,3553;2,7,3553;2,8,3553;2,9,3553;2,10,3553;2,11,3553;2,12,3553;2,13,3553;2,14,3553;2,15,3553;2,16,3553;3,0,3553;3,1,3553;3,2,3553;3,3,3553;3,4,3553;3,5,3553;3,6,3553;3,7,3553;3,8,3553;3,9,3553;3,10,3553;3,11,3553;3,12,3553;3,13,3553;3,14,3553;3,15,3553;3,16,3553;4,0,3553;4,1,3553;4,2,3553;4,3,3553;4,4,3553;4,5,3553;4,6,3553;4,7,3553;4,8,3553;4,9,3553;4,10,3553;4,11,3553;4,12,3553;4,13,3553;4,14,3553;4,15,3553;4,16,3553 --disable-accelerated-video-decode --service-request-

channel-token=A87D45919D731C22139557EB73BA3B26 --renderer-client-id=10 --mojo-platform-channel-handle=5312 /prefetch:1

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1556 --primordial-pipe-token=A67F8F44E678FFD43E87DC7A42930C81 --lang=cs --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --blink-settings=disallowFetchForDocWrittenScriptsInMainFrame=false,disallowFetchForDocWrittenScriptsInMainFrameOnSlowConnections=true --enable-pinch --device-scale-factor=1 --num-raster-threads=1 --content-image-texture-target=0,0,3553;0,1,3553;0,2,3553;0,3,3553;0,4,3553;0,5,3553;0,6,3553;0,7,3553;0,8,3553;0,9,3553;0,10,3553;0,11,3553;0,12,3553;0,13,3553;0,14,3553;0,15,3553;0,16,3553;1,0,3553;1,1,3553;1,2,3553;1,3,3553;1,4,3553;1,5,3553;1,6,3553;1,7,3553;1,8,3553;1,9,3553;1,10,3553;1,11,3553;1,12,3553;1,13,3553;1,14,3553;1,15,3553;1,16,3553;2,0,3553;2,1,3553;2,2,3553;2,3,3553;2,4,3553;2,5,3553;2,6,3553;2,7,3553;2,8,3553;2,9,3553;2,10,3553;2,11,3553;2,12,3553;2,13,3553;2,14,3553;2,15,3553;2,16,3553;3,0,3553;3,1,3553;3,2,3553;3,3,3553;3,4,3553;3,5,3553;3,6,3553;3,7,3553;3,8,3553;3,9,3553;3,10,3553;3,11,3553;3,12,3553;3,13,3553;3,14,3553;3,15,3553;3,16,3553;4,0,3553;4,1,3553;4,2,3553;4,3,3553;4,4,3553;4,5,3553;4,6,3553;4,7,3553;4,8,3553;4,9,3553;4,10,3553;4,11,3553;4,12,3553;4,13,3553;4,14,3553;4,15,3553;4,16,3553 --disable-accelerated-video-decode --service-request-channel-token=A67F8F44E678FFD43E87DC7A42930C81 --renderer-client-id=13 --mojo-platform-channel-handle=5964 /prefetch:1

C:\WINDOWS\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-5A0F49CCDF3F}

c:\windows\system32\svchost.exe -k netsvcs -s BITS

C:\Windows\System32\smartscreen.exe -Embedding

C:\WINDOWS\system32\svchost.exe -k netsvcs -s gpsvc

C:\WINDOWS\system32\AUDIODG.EXE 0x424

C:\WINDOWS\system32\svchost.exe -k SDRSVC

"C:\Users\Jakub\Desktop\RSITx64.exe"

C:\WINDOWS\system32\wbem\wmiprvse.exe

======Registry dump======

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}]

Adobe PDF Link Helper - C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll [2013-05-08 77424]

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{72853161-30C5-4D22-B7F9-0BBC1D38A37E}]

Groove GFS Browser Helper - C:\Program Files (x86)\Microsoft Office\Office12\GrooveShellExtensions.dll [2009-02-26 2217832]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

"SecurityHealth"=C:\Program Files\Windows Defender\MSASCuiL.exe [2017-03-18 629152]

"ETDCtrl"=C:\Program Files\Elantech\ETDCtrl.exe [2015-11-01 3738336]

"ASUS WebStorage"=c:\program files (x86)\asus\asus webstorage\service\asuswsservice.exe [2009-12-24 1736704]

"ETDWare"=c:\program files\elantech\etdctrl.exe [2015-11-01 3738336]

"AvastUI.exe"=C:\Program Files\AVAST Software\Avast\AvLaunch.exe [2017-07-18 213832]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

"OneDrive"=C:\Users\Jakub\AppData\Local\Microsoft\OneDrive\OneDrive.exe [2017-07-18 1555664]

"CCleaner Monitoring"=C:\Program Files\CCleaner\CCleaner64.exe [2016-12-06 9288408]

"cz.seznam.software.autoupdate"=C:\Users\Jakub\AppData\Roaming\Seznam.cz\szninstall.exe [2013-05-16 1062472]

"cz.seznam.software.szndesktop"=C:\Users\Jakub\AppData\Roaming\Seznam.cz\bin\wszndesktop.exe [2015-05-26 103080]

[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupreg\ADSMTray]

C:\Program Files (x86)\ASUS\ASUS Data Security Manager\ADSMTray.exe [2009-06-24 272952]

[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupreg\ASUS Screen Saver Protector]

C:\Windows\AsScrPro.exe [2010-03-20 3058304]

[HKEY_LOCAL_MACHINE\Software\wow6432node\Microsoft\Windows\CurrentVersion\Run]

"ATKMEDIA"=c:\program files (x86)\asus\atk media\dmedia.exe [2009-08-20 170624]

"ATKOSD2"=c:\program files (x86)\asus\atkosd2\atkosd2.exe [2009-08-17 6859392]

"HControlUser"=c:\program files (x86)\asus\atk hotkey\hcontroluser.exe [2009-06-19 105016]

"HDAudDeck"=c:\program files (x86)\via\viaudioi\vdeck\vdeck.exe [2009-09-17 2245120]

"GrooveMonitor"=C:\Program Files (x86)\Microsoft Office\Office12\GrooveMonitor.exe [2009-02-26 30040]

"seznam-listicka-distribuce"=C:\Program Files (x86)\Seznam.cz\distribution\szninstall.exe [2013-05-16 1062472]

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

SRS Premium Sound.lnk - C:\Windows\Installer\{E5CF6B9C-3ABE-43C9-9413-AD5FFC98F049}\NewShortcut5_21C7B668029A47458B27645FE6E4A715.exe

[HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks]

"{B5A7F190-DDA6-4420-B3BA-52453494E6CD}"=C:\Program Files (x86)\Microsoft Office\Office12\GrooveShellExtensions.dll [2009-02-26 2217832]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Ahcache.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\CoreMessagingRegistrar]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\iai2c.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\SpbCx.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\StateRepository]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\TileDataModelSvc]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\uefi.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\UserManager]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{F2E7DD72-6468-4E36-B6F1-6488F42C1B52}]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\Ahcache.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\CoreMessagingRegistrar]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\NetSetupSvc]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\SpbCx.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\StateRepository]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\TileDataModelSvc]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\uefi.sys]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\UserManager]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\{F2E7DD72-6468-4E36-B6F1-6488F42C1B52}]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]

"DSCAutomationHostEnabled"=2

"SoftwareSASGeneration"=1

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy\standardprofile\authorizedapplications\list]

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy\domainprofile\authorizedapplications\list]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32]

"midimapper"=midimap.dll

"msacm.imaadpcm"=imaadp32.acm

"msacm.l3acm"=C:\Windows\System32\l3codeca.acm

"msacm.msadpcm"=msadp32.acm

"msacm.msg711"=msg711.acm

"msacm.msgsm610"=msgsm32.acm

"vidc.i420"=iyuv_32.dll

"vidc.iyuv"=iyuv_32.dll

"vidc.mrle"=msrle32.dll

"vidc.msvc"=msvidc32.dll

"vidc.uyvy"=msyuv.dll

"vidc.yuy2"=msyuv.dll

"vidc.yvu9"=tsbyuv.dll

"vidc.yvyu"=msyuv.dll

"wavemapper"=msacm32.drv

"MSVideo8"=VfWWDM32.dll

"wave"=wdmaud.drv

"midi"=wdmaud.drv

"mixer"=wdmaud.drv

"aux"=wdmaud.drv

======File associations======

.js - edit - C:\Windows\System32\Notepad.exe %1

.js - open - C:\Windows\System32\WScript.exe "%1" %*

======List of files/folders created in the last 1 month======

2017-07-27 11:22:39 ----D---- C:\rsit

2017-07-24 12:14:00 ----SD---- C:\WINDOWS\SYSWOW64\Microsoft

2017-07-19 22:00:31 ----D---- C:\ProgramData\SWCUTemp

2017-07-18 21:34:34 ----A---- C:\WINDOWS\system32\aswBoot.exe

2017-07-18 21:30:56 ----SHD---- C:\Recovery

2017-07-18 21:25:34 ----D---- C:\Windows.old

2017-07-18 21:21:47 ----A---- C:\WINDOWS\SYSWOW64\wmpmde.dll

2017-07-18 21:21:47 ----A---- C:\WINDOWS\system32\wmpmde.dll

2017-07-18 21:21:47 ----A---- C:\WINDOWS\system32\SecurityHealthService.exe

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\WindowsCodecsExt.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Xaml.Resources.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Xaml.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\Windows.System.Profile.RetailInfo.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\Windows.Payments.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.Bluetooth.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\Unistore.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\thumbcache.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\rasapi32.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\policymanager.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\MbaeApi.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\LicenseManager.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\iertutil.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\gdi32.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\dwmcore.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\d3d10warp.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\credprovhost.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\CloudExperienceHostUser.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\CloudExperienceHostCommon.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\ClipboardServer.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\AzureSettingSyncProvider.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\ActiveSyncProvider.dll

2017-07-18 21:21:46 ----A---- C:\WINDOWS\SYSWOW64\aadtb.dll

2017-07-18 21:21:45 ----A---- C:\WINDOWS\SYSWOW64\WWAHost.exe

2017-07-18 21:21:45 ----A---- C:\WINDOWS\SYSWOW64\WpcWebFilter.dll

2017-07-18 21:21:45 ----A---- C:\WINDOWS\SYSWOW64\wininet.dll

2017-07-18 21:21:45 ----A---- C:\WINDOWS\SYSWOW64\Windows.Internal.Management.dll

2017-07-18 21:21:45 ----A---- C:\WINDOWS\SYSWOW64\Windows.Data.Pdf.dll

2017-07-18 21:21:38 ----A---- C:\WINDOWS\SYSWOW64\urlmon.dll

2017-07-18 21:21:38 ----A---- C:\WINDOWS\SYSWOW64\rastls.dll

2017-07-18 21:21:38 ----A---- C:\WINDOWS\SYSWOW64\msftedit.dll

2017-07-18 21:21:38 ----A---- C:\WINDOWS\SYSWOW64\mos.dll

2017-07-18 21:21:38 ----A---- C:\WINDOWS\SYSWOW64\MapRouter.dll

2017-07-18 21:21:38 ----A---- C:\WINDOWS\SYSWOW64\InstallAgentUserBroker.exe

2017-07-18 21:21:38 ----A---- C:\WINDOWS\SYSWOW64\InstallAgent.exe

2017-07-18 21:21:38 ----A---- C:\WINDOWS\SYSWOW64\dmcmnutils.dll

2017-07-18 21:21:38 ----A---- C:\WINDOWS\SYSWOW64\dcomp.dll

2017-07-18 21:21:38 ----A---- C:\WINDOWS\SYSWOW64\D3DCompiler_47.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\winmde.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\WindowsCodecs.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Xaml.Maps.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\windows.storage.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\Windows.Internal.Bluetooth.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\ucrtbase.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\tquery.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\SndVolSSO.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\SearchProtocolHost.exe

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\raschap.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\ntdll.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\mssrch.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\MSAudDecMFT.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\mfsvr.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\MFMediaEngine.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\MFCaptureEngine.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\edputil.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\eapprovp.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\d2d1.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\BingMaps.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\bcastdvr.exe

2017-07-18 21:21:37 ----A---- C:\WINDOWS\SYSWOW64\ActivationManager.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\system32\MSAudDecMFT.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\system32\mfsvr.dll

2017-07-18 21:21:37 ----A---- C:\WINDOWS\system32\MFMediaEngine.dll

2017-07-18 21:21:36 ----A---- C:\WINDOWS\system32\Windows.Media.dll

2017-07-18 21:21:36 ----A---- C:\WINDOWS\system32\mfps.dll

2017-07-18 21:21:36 ----A---- C:\WINDOWS\system32\MFCaptureEngine.dll

2017-07-18 21:21:36 ----A---- C:\WINDOWS\system32\fveapi.dll

2017-07-18 21:21:36 ----A---- C:\WINDOWS\system32\drivers\mrxsmb10.sys

2017-07-18 21:21:34 ----A---- C:\WINDOWS\SYSWOW64\WindowsCodecsRaw.dll

2017-07-18 21:21:33 ----A---- C:\WINDOWS\SYSWOW64\PhotoScreensaver.scr

2017-07-18 21:21:33 ----A---- C:\WINDOWS\system32\WindowsCodecsRaw.dll

2017-07-18 21:21:33 ----A---- C:\WINDOWS\system32\PhotoScreensaver.scr

2017-07-18 21:21:28 ----A---- C:\WINDOWS\SYSWOW64\SensorsApi.dll

2017-07-18 21:21:28 ----A---- C:\WINDOWS\system32\sensrsvc.dll

2017-07-18 21:21:28 ----A---- C:\WINDOWS\system32\SensorsApi.dll

2017-07-18 21:21:27 ----A---- C:\WINDOWS\SYSWOW64\vbscript.dll

2017-07-18 21:21:27 ----A---- C:\WINDOWS\SYSWOW64\mshtml.dll

2017-07-18 21:21:27 ----A---- C:\WINDOWS\SYSWOW64\iepeers.dll

2017-07-18 21:21:27 ----A---- C:\WINDOWS\system32\iepeers.dll

2017-07-18 21:21:26 ----A---- C:\WINDOWS\SYSWOW64\MshtmlDac.dll

2017-07-18 21:21:26 ----A---- C:\WINDOWS\SYSWOW64\Chakra.dll

2017-07-18 21:21:26 ----A---- C:\WINDOWS\system32\MshtmlDac.dll

2017-07-18 21:21:26 ----A---- C:\WINDOWS\system32\mshtml.dll

2017-07-18 21:21:26 ----A---- C:\WINDOWS\system32\Chakradiag.dll

2017-07-18 21:21:26 ----A---- C:\WINDOWS\system32\Chakra.dll

2017-07-18 21:21:25 ----A---- C:\WINDOWS\SYSWOW64\webplatstorageserver.dll

2017-07-18 21:21:25 ----A---- C:\WINDOWS\SYSWOW64\mshtmled.dll

2017-07-18 21:21:25 ----A---- C:\WINDOWS\SYSWOW64\jscript9.dll

2017-07-18 21:21:25 ----A---- C:\WINDOWS\SYSWOW64\edgehtml.dll

2017-07-18 21:21:25 ----A---- C:\WINDOWS\SYSWOW64\dxtrans.dll

2017-07-18 21:21:25 ----A---- C:\WINDOWS\system32\mshtmled.dll

2017-07-18 21:21:25 ----A---- C:\WINDOWS\system32\jscript9diag.dll

2017-07-18 21:21:25 ----A---- C:\WINDOWS\system32\jscript9.dll

2017-07-18 21:21:25 ----A---- C:\WINDOWS\system32\dxtrans.dll

2017-07-18 21:21:24 ----A---- C:\WINDOWS\SYSWOW64\msfeeds.dll

2017-07-18 21:21:24 ----A---- C:\WINDOWS\system32\msfeeds.dll

2017-07-18 21:21:24 ----A---- C:\WINDOWS\system32\edgehtml.dll

2017-07-18 21:21:23 ----A---- C:\WINDOWS\SYSWOW64\ieframe.dll

2017-07-18 21:21:22 ----A---- C:\WINDOWS\SYSWOW64\iedkcs32.dll

2017-07-18 21:21:22 ----A---- C:\WINDOWS\system32\ieframe.dll

2017-07-18 21:21:22 ----A---- C:\WINDOWS\system32\iedkcs32.dll

2017-07-18 21:21:20 ----A---- C:\WINDOWS\system32\ieui.dll

2017-07-18 21:21:20 ----A---- C:\WINDOWS\system32\HoloSI.PCShell.dll

2017-07-18 21:21:19 ----A---- C:\WINDOWS\SYSWOW64\twinui.dll

2017-07-18 21:21:19 ----A---- C:\WINDOWS\SYSWOW64\themeui.dll

2017-07-18 21:21:19 ----A---- C:\WINDOWS\SYSWOW64\shell32.dll

2017-07-18 21:21:19 ----A---- C:\WINDOWS\SYSWOW64\sendmail.dll

2017-07-18 21:21:19 ----A---- C:\WINDOWS\SYSWOW64\ExplorerFrame.dll

2017-07-18 21:21:19 ----A---- C:\WINDOWS\SYSWOW64\DevicePairing.dll

2017-07-18 21:21:19 ----A---- C:\WINDOWS\SYSWOW64\dataclen.dll

2017-07-18 21:21:19 ----A---- C:\WINDOWS\SYSWOW64\comdlg32.dll

2017-07-18 21:21:19 ----A---- C:\WINDOWS\SYSWOW64\AboveLockAppHost.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\wininitext.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\wdc.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\VAN.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\SmartcardCredentialProvider.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\scksp.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\rpchttp.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\rpcrt4.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\olepro32.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\ole32.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\msinfo32.exe

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\daxexec.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\certutil.exe

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\basecsp.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\SYSWOW64\apphelp.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\system32\uDWM.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\system32\oleacc.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\system32\msctfuimanager.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\system32\GdiPlus.dll

2017-07-18 21:21:12 ----A---- C:\WINDOWS\system32\fontdrvhost.exe

2017-07-18 21:21:12 ----A---- C:\WINDOWS\system32\ConhostV2.dll

2017-07-18 21:21:11 ----A---- C:\WINDOWS\system32\Windows.UI.dll

2017-07-18 21:21:11 ----A---- C:\WINDOWS\system32\TSWorkspace.dll

2017-07-18 21:21:11 ----A---- C:\WINDOWS\system32\mstscax.dll

2017-07-18 21:21:11 ----A---- C:\WINDOWS\system32\duser.dll

2017-07-18 21:21:10 ----A---- C:\WINDOWS\system32\Windows.Shell.BlueLightReduction.dll

2017-07-18 21:21:09 ----A---- C:\WINDOWS\system32\SettingsHandlers_Notifications.dll

2017-07-18 21:21:09 ----A---- C:\WINDOWS\system32\NetworkMobileSettings.dll

2017-07-18 21:21:09 ----A---- C:\WINDOWS\system32\CloudDomainJoinDataModelServer.dll

2017-07-18 21:21:09 ----A---- C:\WINDOWS\system32\CloudDomainJoinAUG.dll

2017-07-18 21:21:08 ----A---- C:\WINDOWS\system32\shell32.dll

2017-07-18 21:21:08 ----A---- C:\WINDOWS\system32\InputSwitch.dll

2017-07-18 21:21:08 ----A---- C:\WINDOWS\system32\DevicePairing.dll

2017-07-18 21:21:08 ----A---- C:\WINDOWS\system32\CloudExperienceHost.dll

2017-07-18 21:21:08 ----A---- C:\WINDOWS\system32\AboveLockAppHost.dll

2017-07-18 21:21:07 ----A---- C:\WINDOWS\system32\themeui.dll

2017-07-18 21:21:07 ----A---- C:\WINDOWS\system32\sendmail.dll

2017-07-18 21:21:07 ----A---- C:\WINDOWS\system32\ExplorerFrame.dll

2017-07-18 21:21:07 ----A---- C:\WINDOWS\system32\dataclen.dll

2017-07-18 21:21:07 ----A---- C:\WINDOWS\system32\CloudExperienceHostBroker.dll

2017-07-18 21:21:06 ----A---- C:\WINDOWS\system32\twinui.dll

2017-07-18 21:21:06 ----A---- C:\WINDOWS\system32\SettingsHandlers_nt.dll

2017-07-18 21:21:06 ----A---- C:\WINDOWS\system32\prntvpt.dll

2017-07-18 21:21:06 ----A---- C:\WINDOWS\system32\localspl.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\wpncore.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\wininet.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\Windows.System.Profile.RetailInfo.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\Windows.Internal.Management.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\wincredui.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\vbscript.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\urlmon.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\twinui.pcshell.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\SystemSettingsThresholdAdminFlowUI.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\SettingsEnvironment.Desktop.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\RDXTaskFactory.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\rasmans.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\raschap.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\officecsp.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\LogonController.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\LockHostingFramework.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\eapprovp.dll

2017-07-18 21:21:05 ----A---- C:\WINDOWS\system32\CredentialUIBroker.exe

2017-07-18 21:21:05 ----A---- C:\WINDOWS\explorer.exe

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\wwansvc.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\wwanprotdim.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\WpcWebFilter.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\WFDSConMgrSvc.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\WFDSConMgr.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\wcmsvc.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\rastls.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\rasapi32.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\provengine.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\policymanager.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\omadmclient.exe

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\iertutil.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\edputil.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\dwmcore.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\drivers\WdiWiFi.sys

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\drivers\mskssrv.sys

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\DMPushRouterCore.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\dmcmnutils.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\dcomp.dll

2017-07-18 21:21:04 ----A---- C:\WINDOWS\system32\ActiveSyncProvider.dll

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\wuuhext.dll

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\winsrv.dll

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\usocore.dll

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\updatehandlers.dll

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\TokenBrokerUI.dll

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\SRH.dll

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\SIHClient.exe

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\rascustom.dll

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\PsmServiceExtHost.dll

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\PerceptionSimulationExtensions.dll

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\drivers\mrxsmb20.sys

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\cldapi.dll

2017-07-18 21:21:03 ----A---- C:\WINDOWS\system32\ActiveSyncCsp.dll

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\SndVolSSO.dll

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\OpcServices.dll

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\GamePanel.exe

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\drivers\pdc.sys

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\drivers\ntfs.sys

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\drivers\bridge.sys

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\dosvc.dll

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\domgmt.dll

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\csrsrv.dll

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\bcastdvr.exe

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\AppXDeploymentServer.dll

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\AppXDeploymentExtensions.onecore.dll

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\AppXDeploymentExtensions.desktop.dll

2017-07-18 21:21:02 ----A---- C:\WINDOWS\system32\AppxAllUserStore.dll

2017-07-18 21:21:01 ----A---- C:\WINDOWS\system32\winresume.exe

2017-07-18 21:21:01 ----A---- C:\WINDOWS\system32\ntoskrnl.exe

2017-07-18 21:21:01 ----A---- C:\WINDOWS\system32\ntdll.dll

2017-07-18 21:21:01 ----A---- C:\WINDOWS\system32\drivers\clfs.sys

2017-07-18 21:21:00 ----A---- C:\WINDOWS\system32\winload.exe

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\wudriver.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\winlogon.exe

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\wininitext.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\SmartcardCredentialProvider.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\scksp.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\ScDeviceEnum.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\SCardSvr.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\ole32.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\Narrator.exe

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\msxml3.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\msinfo32.exe

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\lsass.exe

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\KernelBase.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\invagent.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\generaltel.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\EditionUpgradeManagerObj.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\EditionUpgradeHelper.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\drivers\tcpip.sys

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\drivers\netio.sys

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\drivers\ndis.sys

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\drivers\http.sys

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\devinv.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\CoreMessaging.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\CompatTelRunner.exe

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\certutil.exe

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\certprop.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\basecsp.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\appraiser.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\aeinv.dll

2017-07-18 21:20:54 ----A---- C:\WINDOWS\system32\acmigration.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\WMPhoto.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\wdc.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\PlayToDevice.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\MMDevAPI.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\FrameServer.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\DolbyMATEnc.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\daxexec.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\audiosrv.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\AudioSes.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\AudioEng.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\AudioEndpointBuilder.dll

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\audiodg.exe

2017-07-18 21:20:53 ----A---- C:\WINDOWS\system32\aitstatic.exe

2017-07-18 21:20:52 ----A---- C:\WINDOWS\system32\Windows.Media.Protection.PlayReady.dll

2017-07-18 21:20:52 ----A---- C:\WINDOWS\system32\WinBioDataModelOOBE.exe

2017-07-18 21:20:52 ----A---- C:\WINDOWS\system32\WinBioDataModel.dll

2017-07-18 21:20:52 ----A---- C:\WINDOWS\system32\psmsrv.dll

2017-07-18 21:20:52 ----A---- C:\WINDOWS\system32\DolbyHrtfEnc.dll

2017-07-18 21:20:52 ----A---- C:\WINDOWS\system32\DmApiSetExtImplDesktop.dll

2017-07-18 21:20:52 ----A---- C:\WINDOWS\system32\bisrv.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\WWAHost.exe

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\wuuhosdeployment.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\wuaueng.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\wuapi.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\Wldap32.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\winmde.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\wininit.exe

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\WindowsCodecsExt.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\WindowsCodecs.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\Windows.Payments.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\win32kfull.sys

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\win32kbase.sys

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\Unistore.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\tquery.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\tileobjserver.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\TDLMigration.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\storewuauth.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\SensorService.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\SearchProtocolHost.exe

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\PlayToReceiver.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\MusUpdateHandlers.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\MusNotification.exe

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\msv1_0.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\mssrch.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\mos.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\MbaeApi.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\MapRouter.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\LicenseManager.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\kerberos.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\InstallAgentUserBroker.exe

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\InstallAgent.exe

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\InputService.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\hvloader.exe

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\hvix64.exe

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\hvax64.exe

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\FntCache.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\DWrite.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\drivers\wcifs.sys

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\drivers\dxgkrnl.sys

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\DeviceCensus.exe

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\dcntel.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\dbgeng.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\D3DCompiler_47.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\d2d1.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\CoreUIComponents.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\BluetoothApis.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\BingMaps.dll

2017-07-18 21:20:50 ----A---- C:\WINDOWS\system32\aepic.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\Windows.UI.Xaml.Maps.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\windows.storage.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\Windows.Internal.Bluetooth.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\Windows.Devices.Bluetooth.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\Windows.Data.Pdf.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\wbiosrvc.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\twinui.appcore.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\msftedit.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\MrmCoreR.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\Microsoft.Bluetooth.Profiles.Gatt.Interface.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\Microsoft.Bluetooth.Profiles.Gatt.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\CloudExperienceHostUser.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\CloudExperienceHostCommon.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\aadtb.dll

2017-07-18 21:20:49 ----A---- C:\WINDOWS\system32\aadcloudap.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\wudriver.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\wuapi.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\WMPhoto.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\Wldap32.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Protection.PlayReady.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\Windows.ApplicationModel.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\wincredui.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\win32kfull.sys

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\webservices.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\UIAutomationCore.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\TokenBrokerUI.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\SRH.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\PlayToDevice.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\OpcServices.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\oleacc.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\msxml3.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\msv1_0.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\mstscax.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\msctfuimanager.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\msasn1.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\MMDevAPI.dll

2017-07-18 21:20:48 ----A----
C:\WINDOWS\SYSWOW64\Microsoft.Bluetooth.Profiles.Gatt.Interface.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\KernelBase.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\kerberos.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\InputService.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\GdiPlus.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\fontdrvhost.exe

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\explorer.exe

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\dwmapi.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\dbghelp.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\dbgeng.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\CoreUIComponents.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\CoreMessaging.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\combase.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\Clipc.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\cldapi.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\CertEnroll.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\certcli.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\certca.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\BluetoothApis.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\AudioSes.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\AudioEng.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\AppxPackaging.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\AppxAllUserStore.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\SYSWOW64\aepic.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\WpAXHolder.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\Windows.UI.Xaml.Resources.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\Windows.UI.Xaml.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\Windows.ApplicationModel.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\UIAutomationCore.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\rdpudd.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\OneCoreUAPCommonProxyStub.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\drivers\usbvideo.sys

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\drivers\USBHUB3.SYS

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\drivers\msiscsi.sys

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\drivers\hdaudbus.sys

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\ClipSVC.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\Clipc.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\ClipboardServer.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\CertEnroll.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\certcli.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\certca.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\AzureSettingSyncProvider.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\AppReadiness.dll

2017-07-18 21:20:48 ----A---- C:\WINDOWS\system32\ActivationManager.dll

2017-07-18 21:20:33 ----D---- C:\ProgramData\Microsoft OneDrive

2017-07-18 21:09:07 ----A---- C:\WINDOWS\system32\wmpps.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\XpsDocumentTargetPrint.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\xboxgipsynthetic.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\wpnapps.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\Windows.Web.Diagnostics.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\Windows.System.Launcher.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\Windows.ApplicationModel.Store.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\WiFiDisplay.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\VEEventDispatcher.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\UserDataTimeUtil.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\twinui.appcore.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\twinapi.appcore.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\StoreAgent.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\smartscreenps.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\ShareHost.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\SettingSyncHost.exe

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\SettingSyncCore.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\SearchIndexer.exe

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\quartz.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\PackageStateRoaming.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\OneDriveSettingSyncProvider.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\msIso.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\MessagingDataModel2.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\MapGeocoder.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\DWrite.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\DictationManager.dll

2017-07-18 21:09:02 ----A---- C:\WINDOWS\SYSWOW64\CloudBackupSettings.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\SYSWOW64\XpsPrint.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\SYSWOW64\MSVPXENC.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\SYSWOW64\mfplat.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\SYSWOW64\mfmp4srcsnk.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\SYSWOW64\mfmjpegdec.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\SYSWOW64\mfcore.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\SYSWOW64\DeviceFlows.DataModel.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\system32\MSVPXENC.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\system32\MSVideoDSP.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\system32\mfplat.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\system32\mfmp4srcsnk.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\system32\mfmjpegdec.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\system32\mfcore.dll

2017-07-18 21:09:01 ----A---- C:\WINDOWS\system32\drivers\srv.sys

2017-07-18 21:08:48 ----A---- C:\WINDOWS\SYSWOW64\ieapfltr.dll

2017-07-18 21:08:48 ----A---- C:\WINDOWS\system32\ieapfltr.dll

2017-07-18 21:08:47 ----A---- C:\WINDOWS\SYSWOW64\ieproxy.dll

2017-07-18 21:08:47 ----A---- C:\WINDOWS\system32\webplatstorageserver.dll

2017-07-18 21:08:47 ----A---- C:\WINDOWS\system32\ieproxy.dll

2017-07-18 21:08:43 ----A---- C:\WINDOWS\system32\ie4uinit.exe

2017-07-18 21:08:42 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Immersive.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\SYSWOW64\webcheck.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\SYSWOW64\UIRibbonRes.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\SYSWOW64\RstrtMgr.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\SYSWOW64\offreg.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\SYSWOW64\NPSMDesktopProvider.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\SYSWOW64\mspaint.exe

2017-07-18 21:08:42 ----A---- C:\WINDOWS\SYSWOW64\kernel32.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\SYSWOW64\InputSwitch.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\SYSWOW64\comctl32.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\SYSWOW64\asycfilt.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\winsrvext.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\Windows.UI.AppDefaults.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\Windows.SharedPC.AccountManager.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\webcheck.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\UIRibbonRes.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\StartTileData.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\SettingsHandlers_Display.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\RDXService.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\NotificationController.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\msctf.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\gdi32full.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\dwmredir.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\DeviceFlows.DataModel.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\atmlib.dll

2017-07-18 21:08:42 ----A---- C:\WINDOWS\system32\atmfd.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\XpsPrint.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\wpnprv.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\wpnapps.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\Windows.UI.Logon.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\Windows.UI.Immersive.dll

2017-07-18 21:08:41 ----A----
C:\WINDOWS\system32\Windows.Shell.UnifiedTile.CuratedTileCollections.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\Windows.Internal.Shell.Broker.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\win32spl.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\SystemSettingsAdminFlows.exe

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\SystemSettings.Handlers.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\SharedStartModel.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\NPSMDesktopProvider.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\mspaint.exe

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\LockAppBroker.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\drivers\ksthunk.sys

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\comdlg32.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\comctl32.dll

2017-07-18 21:08:41 ----A---- C:\WINDOWS\system32\AppResolver.dll

2017-07-18 21:08:33 ----A---- C:\WINDOWS\system32\XpsDocumentTargetPrint.dll

2017-07-18 21:08:33 ----A---- C:\WINDOWS\system32\XboxNetApiSvc.dll

2017-07-18 21:08:33 ----A---- C:\WINDOWS\system32\WiFiDisplay.dll

2017-07-18 21:08:33 ----A---- C:\WINDOWS\system32\wcmcsp.dll

2017-07-18 21:08:33 ----A---- C:\WINDOWS\system32\msIso.dll

2017-07-18 21:08:33 ----A---- C:\WINDOWS\system32\EnterpriseModernAppMgmtCSP.dll

2017-07-18 21:08:33 ----A---- C:\WINDOWS\system32\enterprisecsps.dll

2017-07-18 21:08:33 ----A---- C:\WINDOWS\system32\EnterpriseAppMgmtSvc.dll

2017-07-18 21:08:33 ----A---- C:\WINDOWS\system32\efscore.dll

2017-07-18 21:08:33 ----A---- C:\WINDOWS\system32\DictationManager.dll

2017-07-18 21:08:33 ----A---- C:\WINDOWS\system32\CloudBackupSettings.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\SYSWOW64\imagehlp.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\xboxgipsynthetic.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\XblGameSaveExt.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\wpx.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\Windows.Web.Diagnostics.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\Windows.UI.Core.TextInput.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\Windows.System.Launcher.dll

2017-07-18 21:08:32 ----A----
C:\WINDOWS\system32\Windows.Security.Authentication.Identity.Provider.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\Windows.Media.Streaming.ps.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\Windows.Gaming.Preview.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\Windows.Devices.Midi.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\Windows.ApplicationModel.Store.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\WindowManagement.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\wc_storage.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\vss_ps.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\VEStoreEventHandlers.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\utcutil.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\UserDataTimeUtil.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\UpdateAgent.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\umpo.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\ucrtbase.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\tzres.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\twinapi.appcore.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\TpmCoreProvisioning.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\TileDataRepository.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\sysmain.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\StorSvc.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\StoreAgent.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\snmptrap.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\smartscreenps.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\smartscreen.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\ShareHost.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\SettingSyncHost.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\SettingSyncCore.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\SecurityHealthSSO.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\securekernel.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\SearchIndexer.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\RstrtMgr.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\rpcss.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\ResetEngine.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\rdbui.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\quartz.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\PackageStateRoaming.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\OneDriveSettingSyncProvider.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\oleaut32.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\odbcconf.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\NPSM.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\NotificationObjFactory.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\ngcsvc.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\MusNotifyIcon.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\MusNotificationUx.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\musdialoghandlers.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\mssprxy.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\modernexecserver.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\mmgaserver.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\MBR2GPT.EXE

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\MapsStore.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\MapGeocoder.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\kernel32.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\ISM.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\imagehlp.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\embeddedmodesvc.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\drivers\tm.sys

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\drivers\tdx.sys

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\drivers\srv2.sys

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\drivers\rootmdm.sys

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\drivers\fastfat.sys

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\drivers\dxgmms2.sys

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\drivers\dxgmms1.sys

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\drivers\dam.sys

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\diagtrack.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\devicengccredprov.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\DeviceCredentialDeployment.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\dbghelp.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\crypt32.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\comsvcs.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\combase.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\ci.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\cdpsvc.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\catsrvps.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\browserbroker.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\browser_broker.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\bcdedit.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\bcdboot.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\autochk.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\asycfilt.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\system32\AppXDeploymentClient.dll

2017-07-18 21:08:32 ----A---- C:\WINDOWS\HelpPane.exe

2017-07-18 21:08:32 ----A---- C:\WINDOWS\bfsvc.exe

2017-07-18 21:08:31 ----A---- C:\WINDOWS\system32\TokenBroker.dll

2017-07-18 21:08:31 ----A---- C:\WINDOWS\system32\capauthz.dll

2017-07-18 21:08:29 ----A----
C:\WINDOWS\SYSWOW64\Windows.Security.Authentication.Identity.Provider.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.Midi.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\PlayToManager.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\NPSM.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\msctf.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\gdi32full.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\capauthz.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\bcryptprimitives.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\autochk.exe

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\atmlib.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\atmfd.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\AppXDeploymentClient.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\SYSWOW64\AppResolver.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\system32\SpeechPal.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\system32\offreg.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\system32\MessagingDataModel2.dll

2017-07-18 21:08:29 ----A---- C:\WINDOWS\system32\drivers\storport.sys

2017-07-18 21:08:28 ----A---- C:\WINDOWS\SYSWOW64\tzres.dll

2017-07-18 21:08:28 ----A---- C:\WINDOWS\SYSWOW64\TpmCoreProvisioning.dll

2017-07-18 21:08:28 ----A---- C:\WINDOWS\SYSWOW64\TokenBroker.dll

2017-07-18 21:08:28 ----A---- C:\WINDOWS\SYSWOW64\oleaut32.dll

2017-07-18 21:08:28 ----A---- C:\WINDOWS\SYSWOW64\odbcconf.dll

2017-07-18 21:08:28 ----A---- C:\WINDOWS\SYSWOW64\mmgaserver.exe

2017-07-18 21:08:28 ----A---- C:\WINDOWS\SYSWOW64\devicengccredprov.dll

2017-07-18 21:08:28 ----A---- C:\WINDOWS\SYSWOW64\crypt32.dll

2017-07-18 21:08:28 ----A---- C:\WINDOWS\system32\drivers\xboxgip.sys

2017-07-18 21:08:28 ----A---- C:\WINDOWS\system32\drivers\vhdmp.sys

2017-07-18 21:08:28 ----A---- C:\WINDOWS\system32\drivers\USBXHCI.SYS

2017-07-18 21:08:28 ----A---- C:\WINDOWS\system32\drivers\tpm.sys

2017-07-18 21:08:28 ----A---- C:\WINDOWS\system32\drivers\storahci.sys

2017-07-18 21:08:28 ----A---- C:\WINDOWS\system32\drivers\sdbus.sys

2017-07-18 21:08:28 ----A---- C:\WINDOWS\system32\drivers\netvsc.sys

2017-07-18 21:08:28 ----A---- C:\WINDOWS\system32\drivers\dumpsd.sys

2017-07-18 21:08:28 ----A---- C:\WINDOWS\system32\drivers\BasicRender.sys

2017-07-18 21:02:19 ----A---- C:\WINDOWS\SYSWOW64\NlsLexicons0009.dll

2017-07-18 21:02:19 ----A---- C:\WINDOWS\SYSWOW64\NlsData0009.dll

2017-07-18 21:02:19 ----A---- C:\WINDOWS\system32\prm0009.dll

2017-07-18 21:02:19 ----A---- C:\WINDOWS\system32\NlsLexicons0009.dll

2017-07-18 21:02:18 ----A---- C:\WINDOWS\system32\NlsData0009.dll

2017-07-18 21:01:18 ----D---- C:\WINDOWS\system32\Microsoft

2017-07-18 21:01:18 ----D---- C:\WINDOWS\ServiceProfiles

2017-07-18 20:58:18 ----D---- C:\WINDOWS\SYSWOW64\XPSViewer

2017-07-18 20:58:18 ----D---- C:\WINDOWS\SYSWOW64\BestPractices

2017-07-18 20:58:18 ----D---- C:\WINDOWS\system32\msmq

2017-07-18 20:58:18 ----D---- C:\WINDOWS\system32\BestPractices

2017-07-18 20:58:16 ----D---- C:\Program Files\Reference Assemblies

2017-07-18 20:58:16 ----D---- C:\Program Files\MSBuild

2017-07-18 20:58:16 ----D---- C:\Program Files (x86)\Reference Assemblies

2017-07-18 20:58:16 ----D---- C:\inetpub

2017-07-18 20:58:16 ----AD---- C:\Program Files (x86)\MSBuild

2017-07-18 20:57:17 ----A---- C:\WINDOWS\SYSWOW64\TsWpfWrp.exe

2017-07-18 20:57:17 ----A---- C:\WINDOWS\SYSWOW64\PresentationNative_v0300.dll

2017-07-18 20:57:17 ----A---- C:\WINDOWS\SYSWOW64\PresentationCFFRasterizerNative_v0300.dll

2017-07-18 20:57:09 ----A---- C:\WINDOWS\system32\TsWpfWrp.exe

2017-07-18 20:57:09 ----A---- C:\WINDOWS\system32\PresentationNative_v0300.dll

2017-07-18 20:57:08 ----A---- C:\WINDOWS\system32\PresentationCFFRasterizerNative_v0300.dll

2017-07-18 20:56:42 ----A---- C:\WINDOWS\system32\reseteng.dll

2017-07-18 20:53:11 ----ASH---- C:\hiberfil.sys

2017-07-18 20:43:00 ----D---- C:\ProgramData\USOShared

2017-07-18 20:42:00 ----D---- C:\Program Files\Common Files\SpeechEngines

2017-07-18 20:37:28 ----SD---- C:\Users\Jakub\AppData\Roaming\Microsoft

2017-07-18 20:36:14 ----A---- C:\WINDOWS\system32\PerfStringBackup.INI

2017-07-18 20:35:59 ----A---- C:\WINDOWS\SYSWOW64\PerfStringBackup.INI

2017-07-18 20:35:22 ----D---- C:\Program Files\VIA

2017-07-18 20:35:21 ----D---- C:\WINDOWS\system32\SRSLabs

2017-07-18 20:35:05 ----A---- C:\WINDOWS\SYSWOW64\PrintConfig.dll

2017-07-18 20:34:47 ----D---- C:\Program Files\Elantech

2017-07-18 20:33:34 ----AS---- C:\WINDOWS\bootstat.dat

2017-07-18 20:33:00 ----D---- C:\WINDOWS\Prefetch

2017-07-18 20:31:54 ----D---- C:\WINDOWS\system32\SleepStudy

2017-07-18 20:31:48 ----A---- C:\WINDOWS\system32\FNTCACHE.DAT

2017-07-14 19:11:28 ----DC---- C:\WINDOWS\Panther

2017-07-13 18:13:47 ----D---- C:\Users\Jakub\AppData\Roaming\Seznam Browser

2017-07-07 15:17:31 ----D---- C:\WINDOWS\system32\UNP

2017-07-07 15:17:31 ----AD---- C:\Program Files\UNP

======List of files/folders modified in the last 1 month======

2017-07-27 11:22:41 ----D---- C:\Program Files\Trend Micro

2017-07-27 11:18:42 ----D---- C:\WINDOWS\Temp

2017-07-27 10:59:49 ----D---- C:\WINDOWS\INF

2017-07-27 10:59:47 ----D---- C:\WINDOWS\debug

2017-07-27 10:59:47 ----D---- C:\Windows

2017-07-27 10:50:32 ----D---- C:\WINDOWS\system32\config

2017-07-27 10:36:18 ----D---- C:\WINDOWS\system32\DriverStore

2017-07-27 10:34:00 ----D---- C:\WINDOWS\system32\sru

2017-07-27 10:04:27 ----RD---- C:\WINDOWS\Microsoft.NET

2017-07-27 09:39:25 ----D---- C:\Users\Jakub\AppData\Roaming\Seznam.cz

2017-07-27 09:37:33 ----D---- C:\WINDOWS\AppReadiness

2017-07-27 09:37:32 ----HD---- C:\Program Files\WindowsApps

2017-07-27 09:35:14 ----D---- C:\WINDOWS\system32\WDI

2017-07-27 09:34:40 ----D---- C:\WINDOWS\system32\Tasks

2017-07-26 21:40:08 ----A---- C:\WINDOWS\system32\acovcnt.exe

2017-07-26 20:06:42 ----D---- C:\WINDOWS\System32

2017-07-26 19:59:25 ----D---- C:\WINDOWS\system32\catroot2

2017-07-26 19:40:06 ----D---- C:\WINDOWS\system32\NDF

2017-07-26 19:23:11 ----D---- C:\WINDOWS\system32\drivers

2017-07-24 14:05:19 ----D---- C:\WINDOWS\Logs

2017-07-24 14:01:04 ----D---- C:\WINDOWS\rescache

2017-07-24 12:14:00 ----AD---- C:\WINDOWS\SysWOW64

2017-07-21 11:13:02 ----RD---- C:\WINDOWS\assembly

2017-07-19 22:10:49 ----D---- C:\WINDOWS\WinSxS

2017-07-19 22:00:31 ----HD---- C:\ProgramData

2017-07-19 22:00:22 ----D---- C:\WINDOWS\system32\LogFiles

2017-07-19 18:42:47 ----D---- C:\WINDOWS\CbsTemp

2017-07-19 18:21:26 ----D---- C:\WINDOWS\appcompat

2017-07-19 18:19:05 ----D---- C:\WINDOWS\system32\Macromed

2017-07-19 18:18:49 ----D---- C:\WINDOWS\SYSWOW64\Macromed

2017-07-18 21:25:50 ----D---- C:\WINDOWS\Setup

2017-07-18 21:24:07 ----SD---- C:\WINDOWS\SYSWOW64\F12

2017-07-18 21:24:07 ----D---- C:\WINDOWS\system32\migwiz

2017-07-18 21:24:06 ----SD---- C:\WINDOWS\system32\F12

2017-07-18 21:24:06 ----D---- C:\WINDOWS\system32\drivers\UMDF

2017-07-18 21:24:06 ----D---- C:\WINDOWS\system32\Boot

2017-07-18 21:24:06 ----D---- C:\WINDOWS\system32\appraiser

2017-07-18 21:24:06 ----D---- C:\WINDOWS\ShellExperiences

2017-07-18 21:24:05 ----RD---- C:\Program Files\Windows Defender

2017-07-18 21:24:05 ----D---- C:\WINDOWS\AppPatch

2017-07-18 21:24:05 ----D---- C:\Program Files\Windows Photo Viewer

2017-07-18 21:24:05 ----D---- C:\Program Files (x86)\Windows Photo Viewer

2017-07-18 21:24:05 ----D---- C:\Program Files (x86)\Windows Defender

2017-07-18 21:18:05 ----RD---- C:\WINDOWS\ImmersiveControlPanel

2017-07-18 21:15:52 ----D---- C:\Program Files\Windows NT

2017-07-18 21:15:11 ----D---- C:\WINDOWS\system32\WinBioDatabase

2017-07-18 21:14:54 ----D---- C:\WINDOWS\SoftwareDistribution

2017-07-18 21:11:03 ----D---- C:\WINDOWS\SYSWOW64\Dism

2017-07-18 21:10:59 ----D---- C:\WINDOWS\system32\WinBioPlugIns

2017-07-18 21:10:59 ----D---- C:\WINDOWS\system32\Dism

2017-07-18 21:10:58 ----D---- C:\WINDOWS\Provisioning

2017-07-18 21:10:58 ----D---- C:\Program Files (x86)\Internet Explorer

2017-07-18 21:10:18 ----RSD---- C:\WINDOWS\Fonts

2017-07-18 21:10:18 ----D---- C:\WINDOWS\system32\Tasks_Migrated

2017-07-18 21:06:08 ----D---- C:\WINDOWS\Registration

2017-07-18 21:06:01 ----D---- C:\WINDOWS\HoloShell

2017-07-18 21:05:32 ----D---- C:\WINDOWS\Tasks

2017-07-18 21:05:14 ----SD---- C:\ProgramData\Microsoft

2017-07-18 21:04:12 ----RSD---- C:\WINDOWS\Media

2017-07-18 21:04:05 ----D---- C:\WINDOWS\system32\wbem

2017-07-18 21:04:03 ----D---- C:\WINDOWS\system32\drivers\etc

2017-07-18 21:02:30 ----D---- C:\WINDOWS\OCR

2017-07-18 20:58:18 ----D---- C:\WINDOWS\SYSWOW64\MUI

2017-07-18 20:58:18 ----D---- C:\WINDOWS\system32\MUI

2017-07-18 20:58:18 ----D---- C:\WINDOWS\system32\inetsrv

2017-07-18 20:58:09 ----A---- C:\WINDOWS\SYSWOW64\mqsnap.dll

2017-07-18 20:58:09 ----A---- C:\WINDOWS\SYSWOW64\mqcertui.dll

2017-07-18 20:58:08 ----A---- C:\WINDOWS\system32\wamregps.dll

2017-07-18 20:58:08 ----A---- C:\WINDOWS\system32\iisRtl.dll

2017-07-18 20:58:08 ----A---- C:\WINDOWS\system32\iisrstap.dll

2017-07-18 20:58:08 ----A---- C:\WINDOWS\system32\iisreset.exe

2017-07-18 20:58:08 ----A---- C:\WINDOWS\system32\cngkeyhelper.dll

2017-07-18 20:58:08 ----A---- C:\WINDOWS\system32\ahadmin.dll

2017-07-18 20:58:08 ----A---- C:\WINDOWS\system32\admwprox.dll

2017-07-18 20:58:07 ----A---- C:\WINDOWS\SYSWOW64\wamregps.dll

2017-07-18 20:58:07 ----A---- C:\WINDOWS\SYSWOW64\iisRtl.dll

2017-07-18 20:58:07 ----A---- C:\WINDOWS\SYSWOW64\iisrstap.dll

2017-07-18 20:58:07 ----A---- C:\WINDOWS\SYSWOW64\iisreset.exe

2017-07-18 20:58:07 ----A---- C:\WINDOWS\SYSWOW64\ahadmin.dll

2017-07-18 20:58:07 ----A---- C:\WINDOWS\SYSWOW64\admwprox.dll

2017-07-18 20:58:06 ----A---- C:\WINDOWS\SYSWOW64\mqoa.dll

2017-07-18 20:58:06 ----A---- C:\WINDOWS\SYSWOW64\cngkeyhelper.dll

2017-07-18 20:58:06 ----A---- C:\WINDOWS\system32\mqrt.dll

2017-07-18 20:58:05 ----A---- C:\WINDOWS\system32\mqlogmgr.dll

2017-07-18 20:58:04 ----A---- C:\WINDOWS\system32\mqutil.dll

2017-07-18 20:58:02 ----A---- C:\WINDOWS\system32\mqsnap.dll

2017-07-18 20:58:02 ----A---- C:\WINDOWS\system32\mqcertui.dll

2017-07-18 20:58:01 ----A---- C:\WINDOWS\SYSWOW64\mqrt.dll

2017-07-18 20:58:01 ----A---- C:\WINDOWS\system32\mqoa.dll

2017-07-18 20:58:00 ----A---- C:\WINDOWS\system32\mqqm.dll

2017-07-18 20:57:59 ----A---- C:\WINDOWS\SYSWOW64\mqutil.dll

2017-07-18 20:57:58 ----A---- C:\WINDOWS\system32\mqsvc.exe

2017-07-18 20:57:58 ----A---- C:\WINDOWS\system32\mqbkup.exe

2017-07-18 20:52:28 ----D---- C:\WINDOWS\SYSWOW64\drivers

2017-07-18 20:52:28 ----D---- C:\WINDOWS\SYSWOW64\ASUS_Screensaver dir

2017-07-18 20:52:28 ----D---- C:\WINDOWS\system32\wfp

2017-07-18 20:52:26 ----D---- C:\WINDOWS\system32\Service

2017-07-18 20:52:26 ----D---- C:\WINDOWS\system32\OEM

2017-07-18 20:52:23 ----D---- C:\WINDOWS\ShellNew

2017-07-18 20:52:22 ----HD---- C:\WINDOWS\Installer

2017-07-18 20:52:20 ----D---- C:\WINDOWS\cs

2017-07-18 20:52:20 ----D---- C:\Program Files (x86)\Common Files

2017-07-18 20:44:09 ----D---- C:\WINDOWS\SYSWOW64\migration

2017-07-18 20:44:08 ----D---- C:\WINDOWS\SYSWOW64\IME

2017-07-18 20:44:08 ----D---- C:\WINDOWS\SYSWOW64\en-US

2017-07-18 20:44:08 ----D---- C:\WINDOWS\SYSWOW64\drivers\UMDF

2017-07-18 20:44:07 ----D---- C:\WINDOWS\SYSWOW64\cs-CZ

2017-07-18 20:44:01 ----D---- C:\WINDOWS\system32\zh-HK

2017-07-18 20:43:58 ----D---- C:\WINDOWS\system32\SPReview

2017-07-18 20:43:58 ----D---- C:\WINDOWS\system32\spool

2017-07-18 20:43:54 ----D---- C:\WINDOWS\system32\oobe

2017-07-18 20:43:53 ----D---- C:\WINDOWS\system32\MRT

2017-07-18 20:43:53 ----D---- C:\WINDOWS\system32\migration

2017-07-18 20:43:52 ----D---- C:\WINDOWS\system32\IME

2017-07-18 20:43:52 ----D---- C:\WINDOWS\system32\EventProviders

2017-07-18 20:43:51 ----D---- C:\WINDOWS\system32\en-US

2017-07-18 20:43:51 ----D---- C:\WINDOWS\system32\drivers\cs-CZ

2017-07-18 20:43:49 ----D---- C:\WINDOWS\system32\cs-CZ

2017-07-18 20:43:05 ----D---- C:\ProgramData\regid.1991-06.com.microsoft

2017-07-18 20:43:01 ----D---- C:\ProgramData\USOPrivate

2017-07-18 20:42:34 ----D---- C:\WINDOWS\schemas

2017-07-18 20:42:33 ----D---- C:\WINDOWS\PolicyDefinitions

2017-07-18 20:42:32 ----D---- C:\WINDOWS\LiveKernelReports

2017-07-18 20:42:17 ----D---- C:\WINDOWS\ehome

2017-07-18 20:42:15 ----RD---- C:\Users

2017-07-18 20:42:14 ----D---- C:\WINDOWS\system32\CodeIntegrity

2017-07-18 20:42:07 ----RD---- C:\Program Files (x86)

2017-07-18 20:42:06 ----SHD---- C:\Program Files (x86)\Windows Sidebar

2017-07-18 20:42:05 ----D---- C:\Program Files (x86)\Windows Mail

2017-07-18 20:42:05 ----AD---- C:\Program Files (x86)\Windows Live

2017-07-18 20:42:04 ----D---- C:\Program Files (x86)\Microsoft.NET

2017-07-18 20:42:01 ----SHD---- C:\Program Files\Windows Sidebar

2017-07-18 20:42:00 ----RD---- C:\Program Files

2017-07-18 20:42:00 ----D---- C:\Program Files\Windows Mail

2017-07-18 20:42:00 ----D---- C:\Program Files\Windows Live

2017-07-18 20:42:00 ----D---- C:\Program Files\Microsoft Games

2017-07-18 20:42:00 ----D---- C:\Program Files\Internet Explorer

2017-07-18 20:42:00 ----D---- C:\Program Files\Common Files

2017-07-18 20:42:00 ----AD---- C:\Program Files\Common Files\microsoft shared

2017-07-18 20:41:04 ----D---- C:\WINDOWS\SYSWOW64\inetsrv

2017-07-18 20:40:59 ----D---- C:\WINDOWS\system32\Recovery

2017-07-18 20:35:30 ----D---- C:\WINDOWS\system32\Sysprep

2017-07-18 19:41:26 ----RASH---- C:\BOOTSECT.BAK

2017-07-18 19:41:22 ----SHD---- C:\Boot

2017-07-18 19:30:39 ----HD---- C:\$WINDOWS.~BT

2017-07-18 17:19:56 ----D---- C:\WINDOWS\system32\sr-Latn-CS

2017-07-14 19:16:27 ----AC---- C:\WINDOWS\system32\MRT.exe

2017-07-14 19:16:18 ----SHD---- C:\Config.Msi

2017-07-14 19:16:17 ----D---- C:\ProgramData\Microsoft Help

2017-07-04 15:07:14 ----D---- C:\ProgramData\AVAST Software

2017-06-30 16:47:29 ----A---- C:\WINDOWS\SYSWOW64\FlashPlayerApp.exe

2017-06-30 15:34:36 ----SHD---- C:\System Volume Information

======List of drivers (R=Running, S=Stopped, 0=Boot, 1=System, 2=Auto, 3=Demand, 4=Disabled)======

R0 AsDsm;AsDsm; C:\WINDOWS\system32\drivers\AsDsm.sys [2010-03-20 35384]

R0 aswbidsh;aswbidsh; C:\WINDOWS\system32\drivers\aswbidsha.sys [2017-07-18 198976]

R0 aswblog;aswblog; C:\WINDOWS\system32\drivers\aswbloga.sys [2017-07-18 343288]

R0 aswbuniv;aswbuniv; C:\WINDOWS\system32\drivers\aswbuniva.sys [2017-07-18 57728]

R0 aswRvrt;aswRvrt; C:\WINDOWS\system32\drivers\aswRvrt.sys [2017-07-04 84392]

R0 aswVmm;aswVmm; C:\WINDOWS\system32\drivers\aswVmm.sys [2017-07-04 361336]

R0 iaStor;@oem34.inf,%*PNP0600.DeviceDesc%;Intel AHCI Controller; C:\WINDOWS\System32\drivers\iaStor.sys [2009-08-06 408600]

R0 iorate;@%SystemRoot%\system32\drivers\iorate.sys,-101; C:\WINDOWS\system32\drivers\iorate.sys [2017-03-18 49568]

R0 lullaby;lullaby; C:\WINDOWS\system32\DRIVERS\lullaby.sys [2009-06-18 15928]

R0 PxHlpa64;PxHlpa64; C:\WINDOWS\System32\Drivers\PxHlpa64.sys [2006-10-18 52760]

R1 aswbidsdriver;aswbidsdriver; C:\WINDOWS\system32\drivers\aswbidsdrivera.sys [2017-07-18 320008]

R1 aswKbd;aswKbd; C:\WINDOWS\system32\drivers\aswKbd.sys [2017-07-04 41800]

R1 aswRdr;aswRdr; C:\WINDOWS\system32\drivers\aswRdr2.sys [2017-07-04 110352]

R1 aswSnx;aswSnx; C:\WINDOWS\system32\drivers\aswSnx.sys [2017-07-04 1015848]

R1 aswSP;aswSP; C:\WINDOWS\system32\drivers\aswSP.sys [2017-07-04 585608]

R1 FileCrypt;@%systemroot%\system32\drivers\filecrypt.sys,-100; C:\WINDOWS\system32\drivers\filecrypt.sys [2017-03-18 54272]

R1 GpuEnergyDrv;@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-100; C:\WINDOWS\System32\drivers\gpuenergydrv.sys [2017-03-18 8192]

R2 ASMMAP64;ASMMAP64; \??\C:\Program Files\ATKGFNEX\ASMMAP64.sys [2007-07-24 14904]

R2 aswMonFlt;aswMonFlt; C:\WINDOWS\system32\drivers\aswMonFlt.sys [2017-07-18 146696]

R2 aswStm;aswStm; C:\WINDOWS\system32\drivers\aswStm.sys [2017-07-04 198768]

R2 clreg;@%SystemRoot%\system32\drivers\registry.sys,-100; C:\WINDOWS\System32\drivers\registry.sys [2017-03-18 14336]

R2 ghaio;ghaio; \??\C:\Program Files\ASUS\NB Probe\SPM\ghaio.sys [2007-08-03 17464]

R2 MMCSS;@%systemroot%\system32\drivers\mmcss.sys,-100; C:\WINDOWS\system32\drivers\mmcss.sys [2017-03-18 50688]

R2 storqosflt;@%SystemRoot%\System32\drivers\storqosflt.sys,-101; C:\WINDOWS\system32\drivers\storqosflt.sys [2017-03-18 79872]

R3 athr;@netathrx.inf,%ATHR.Service.DispName%;Qualcomm Atheros Extensible Wireless LAN device driver; C:\WINDOWS\System32\drivers\athwnx.sys [2017-03-18 4233728]

R3 CAD;@ChargeArbitration.inf,%CAD_DevDesc%;Charge Arbitration Driver; C:\WINDOWS\System32\drivers\CAD.sys [2017-03-18 53664]

R3 ETD;@oem5.inf,%PS2DeviceDesc%;ELAN Input Device; C:\WINDOWS\system32\DRIVERS\ETD.sys [2015-11-01 464472]

R3 igfx;igfx; C:\WINDOWS\system32\DRIVERS\igdkmd64.sys [2012-03-23 10627744]

R3 kbfiltr;@oem26.inf,%kbfiltr.SvcDesc%;Keyboard Filter; C:\WINDOWS\System32\drivers\kbfiltr.sys [2009-07-20 15416]

R3 L1E;@netl1e64.inf,%L1E.Service.DispName%;NDIS Miniport Driver for Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Controller; C:\WINDOWS\System32\drivers\L1E62x64.sys [2017-03-18 59904]

R3 MQAC;@mqutil.dll,-6101; C:\WINDOWS\system32\drivers\mqac.sys [2017-07-18 177664]

R3 MTsensor;@oem36.inf,%ATKACPI.DisplayName%;ATK0100 ACPI UTILITY; C:\WINDOWS\System32\drivers\ATK64AMD.sys [2009-05-13 15928]

S0 LSI_SAS2i;LSI_SAS2i; C:\WINDOWS\System32\drivers\lsi_sas2i.sys [2017-03-18 123808]

S0 LSI_SAS3i;LSI_SAS3i; C:\WINDOWS\System32\drivers\lsi_sas3i.sys [2017-03-18 103328]

S0 megasas2i;megasas2i; C:\WINDOWS\System32\drivers\MegaSas2i.sys [2017-03-18 64416]

S0 percsas2i;percsas2i; C:\WINDOWS\System32\drivers\percsas2i.sys [2017-03-18 58784]

S0 percsas3i;percsas3i; C:\WINDOWS\System32\drivers\percsas3i.sys [2017-03-18 61848]

S0 scmbus;@scmbus.inf,%scmbus.SvcDesc%;Microsoft Storage Class Memory Bus Driver; C:\WINDOWS\System32\drivers\scmbus.sys [2017-03-18 91040]

S0 storufs;@storufs.inf,%UfsServiceDesc%;Microsoft Universal Flash Storage (UFS) Driver; C:\WINDOWS\System32\drivers\storufs.sys [2017-03-18 36760]

S2 CldFlt;Windows Cloud Files Filter Driver; C:\WINDOWS\system32\drivers\cldflt.sys [2017-03-18 12288]

S3 AcpiDev;@acpidev.inf,%AcpiDev.SvcDesc%;ACPI Devices driver; C:\WINDOWS\System32\drivers\AcpiDev.sys [2017-03-18 20480]

S3 AmUStor;AM USB Stroage Driver; C:\WINDOWS\system32\drivers\AmUStor.SYS [2015-10-15 101040]

S3 applockerfltr;@%systemroot%\system32\srpapi.dll,-102; C:\WINDOWS\system32\drivers\applockerfltr.sys [2017-03-18 17920]

S3 aswHwid;aswHwid; C:\WINDOWS\system32\drivers\aswHwid.sys [2017-07-04 46984]

S3 buttonconverter;@buttonconverter.inf,%btnconv.SvcDesc%;Service for Portable Device Control devices; C:\WINDOWS\System32\drivers\buttonconverter.sys [2017-03-18 39424]

S3 CapImg;@capimg.inf,%CapImgHid_Service%;HID driver for CapImg touch screen; C:\WINDOWS\System32\drivers\capimg.sys [2017-03-18 122880]

S3 genericusbfn;@genericusbfn.inf,%genericusbfn.ServiceName%;Generic USB Function Class; C:\WINDOWS\System32\drivers\genericusbfn.sys [2017-03-18 21504]

S3 hidinterrupt;@hidinterrupt.inf,%HID_Interrupt.SvcDesc%;Common Driver for HID Buttons implemented with interrupts; C:\WINDOWS\System32\drivers\hidinterrupt.sys [2017-03-18 51104]

S3 hvservice;@%SystemRoot%\system32\drivers\hvservice.sys,-16; C:\WINDOWS\system32\drivers\hvservice.sys [2017-03-18 74648]

S3 cht4iscsi;cht4iscsi; C:\WINDOWS\System32\drivers\cht4sx64.sys [2017-03-18 347032]

S3 cht4vbd;@cht4vx64.inf,%cht4vbd.generic%;Chelsio Virtual Bus Driver;
C:\WINDOWS\System32\drivers\cht4vx64.sys [2017-03-18 2104224]

S3 iagpio;@iagpio.inf,%iagpio.SVCDESC%;Intel Serial IO GPIO Controller Driver;
C:\WINDOWS\System32\drivers\iagpio.sys [2017-03-18 33280]

S3 iai2c;@iai2c.inf,%iai2c.SVCDESC%;Intel(R) Serial IO I2C Host Controller;
C:\WINDOWS\System32\drivers\iai2c.sys [2017-03-18 81408]

S3 iaLPSS2i_GPIO2;@iaLPSS2i_GPIO2_SKL.inf,%iaLPSS2i_GPIO2.SVCDESC%;Intel(R) Serial IO GPIO Driver v2; C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2.sys [2017-03-18 70656]

S3 iaLPSS2i_GPIO2_BXT_P;@iaLPSS2i_GPIO2_BXT_P.inf,%iaLPSS2i_GPIO2_BXT_P.SVCDESC%;Intel(R) Serial IO GPIO Driver v2; C:\WINDOWS\System32\drivers\iaLPSS2i_GPIO2_BXT_P.sys [2017-03-18 85504]

S3 iaLPSS2i_I2C;@iaLPSS2i_I2C_SKL.inf,%iaLPSS2i_I2C.SVCDESC%;Intel(R) Serial IO I2C Driver v2;
C:\WINDOWS\System32\drivers\iaLPSS2i_I2C.sys [2017-03-18 165376]

S3 iaLPSS2i_I2C_BXT_P;@iaLPSS2i_I2C_BXT_P.inf,%iaLPSS2i_I2C_BXT_P.SVCDESC%;Intel(R) Serial IO I2C Driver v2; C:\WINDOWS\System32\drivers\iaLPSS2i_I2C_BXT_P.sys [2017-03-18 168448]

S3 ibbus;@mlx4_bus.inf,%Ibbus.ServiceDesc%;Mellanox InfiniBand Bus/AL (Filter Driver);
C:\WINDOWS\System32\drivers\ibbus.sys [2017-03-18 526240]

S3 IndirectKmd;@%SystemRoot%\system32\drivers\IndirectKmd.sys,-100;
C:\WINDOWS\System32\drivers\IndirectKmd.sys [2017-03-18 36864]

S3 irda;IrDA; C:\WINDOWS\system32\drivers\irda.sys [2017-03-18 120320]

S3 mausbhost;@mausbhost.inf,%MAUSBHost.ServiceName%;MA-USB Host Controller Driver;
C:\WINDOWS\System32\drivers\mausbhost.sys [2017-03-18 405408]

S3 mausbip;@mausbhost.inf,%MAUSBIP.ServiceName%;MA-USB IP Filter Driver;
C:\WINDOWS\System32\drivers\mausbip.sys [2017-03-18 51104]

S3 mlx4_bus;@mlx4_bus.inf,%MLX4BUS.ServiceDesc%;Mellanox ConnectX Bus Enumerator;
C:\WINDOWS\System32\drivers\mlx4_bus.sys [2017-03-18 842656]

S3 ndfltr;@mlx4_bus.inf,%ndfltr.ServiceDesc%;NetworkDirect Service;
C:\WINDOWS\System32\drivers\ndfltr.sys [2017-03-18 108960]

S3 NetAdapterCx;Network Adapter Wdf Class Extension Library;
C:\WINDOWS\system32\drivers\NetAdapterCx.sys [2017-03-18 122368]

S3 nvdimmn;@nvdimmn.inf,%nvdimmn.SvcDesc%;Microsoft NVDIMM-N device driver;
C:\WINDOWS\System32\drivers\nvdimmn.sys [2017-03-18 80896]

S3 pmem;@pmem.inf,%pmem.SvcDesc%;Microsoft persistent memory disk driver;
C:\WINDOWS\System32\drivers\pmem.sys [2017-03-18 101376]

S3 ReFSv1;ReFSv1; C:\WINDOWS\system32\drivers\ReFSv1.sys [2017-03-18 936864]

S3 SDFRd;@SDFRd.inf,%SDFRd.ServiceDesc%;SDF Reflector; C:\WINDOWS\System32\drivers\SDFRd.sys [2017-03-18 31128]

S3 SpatialGraphFilter;Holographic Spatial Graph Filter; C:\WINDOWS\System32\drivers\SpatialGraphFilter.sys [2017-03-20 40352]

======List of services (R=Running, S=Stopped, 0=Boot, 1=System, 2=Auto, 3=Demand, 4=Disabled)======

R2 602XML Updater;602Updater; C:\Program Files (x86)\Common Files\soft602\602updsvc\602updsvc.exe [2011-10-10 85344]

R2 AFBAgent;AFBAgent; C:\Windows\system32\FBAgent.exe [2009-12-08 379520]

R2 AppHostSvc;@%windir%\system32\inetsrv\iisres.dll,-30011; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

R2 ASLDRService;ASLDR Service; C:\Program Files (x86)\ASUS\ATK Hotkey\ASLDRSrv.exe [2009-06-16 84536]

R2 ATKGFNEXSrv;ATKGFNEX Service; C:\Program Files\ATKGFNEX\GFNEXSrv.exe [2007-08-08 94208]

R2 avast! Antivirus;Avast Antivirus; C:\Program Files\AVAST Software\Avast\AvastSvc.exe [2017-07-18 263312]

R2 CDPSvc;@%SystemRoot%\system32\cdpsvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

R2 CDPUserSvc_625e8e;Uživatelská služba platformy připojených zařízení_625e8e; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

R2 CoreMessagingRegistrar;@%SystemRoot%\system32\coremessaging.dll,-1; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

R2 DiagTrack;@%SystemRoot%\system32\diagtrack.dll,-3001; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

R2 DusmSvc;@%SystemRoot%\System32\dusmsvc.dll,-1; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

R2 ETDService;Elan Service; C:\Program Files\Elantech\ETDService.exe [2015-11-01 144104]

R2 MSMQ;@mqutil.dll,-6102; C:\WINDOWS\system32\mqsvc.exe [2017-07-18 26112]

R2 NetMsmqActivator;@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallR

C.dll,-8195; C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe [2017-03-18 136360]

R2 NetPipeActivator;@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll,-8197; C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe [2017-03-18 136360]

R2 OneSyncSvc_625e8e;Hostitel synchronizace_625e8e; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

R2 SecurityHealthService;@%systemroot%\system32\SecurityHealthAgent.dll,-1002; C:\WINDOWS\system32\SecurityHealthService.exe [2017-07-18 336320]

R3 ADSMService;ADSM Service; C:\Program Files (x86)\ASUS\ASUS Data Security Manager\ADSMSrv.exe [2008-03-31 225280]

R3 aswbIDSAgent;aswbIDSAgent; C:\Program Files\AVAST Software\Avast\x64\aswidsagenta.exe [2017-07-18 7430992]

R3 DsSvc;@%SystemRoot%\system32\dssvc.dll,-10003; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

R3 LicenseManager;@%SystemRoot%\system32\licensemanagersvc.dll,-200; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

R3 NgcCtnrSvc;@%SystemRoot%\System32\NgcCtnrSvc.dll,-1; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

R3 NgcSvc;@%SystemRoot%\System32\ngcsvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

R3 PimIndexMaintenanceSvc_625e8e;Data kontaktů_625e8e; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

R3 RmSvc;@%SystemRoot%\system32\RMapi.dll,-1001; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

R3 spmgr;spmgr; C:\Program Files\ASUS\NB Probe\SPM\spmgr.exe [2007-08-03 125496]

R3 StateRepository;@%SystemRoot%\system32\windows.staterepository.dll,-1; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S2 CDPUserSvc;@%SystemRoot%\system32\cdpusersvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S2 DoSvc;@%systemroot%\system32\dosvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S2 gupdate;Služba Google Update (gupdate); C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2015-08-30 144200]

S2 MapsBroker;@%SystemRoot%\System32\moshost.dll,-100; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

S2 NetTcpActivator;@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll,-8199; C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe [2017-03-18 136360]

S2 OneSyncSvc;@%SystemRoot%\system32\APHostRes.dll,-10002; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 AdobeFlashPlayerUpdateSvc;Adobe Flash Player Update Service; C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe [2017-07-19 273408]

S3 AJRouter;@%SystemRoot%\system32\AJRouter.dll,-2; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 BthHFSrv;@%SystemRoot%\System32\BthHFSrv.dll,-103; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

S3 ClipSVC;@%SystemRoot%\system32\ClipSVC.dll,-103; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

S3 DevicesFlowUserSvc;@%SystemRoot%\system32\DevicesFlowBroker.dll,-103; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 DevicesFlowUserSvc_625e8e;Tok zařízení_625e8e; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 DevQueryBroker;@%SystemRoot%\system32\DevQueryBroker.dll,-100; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 diagnosticshub.standardcollector.service;@%SystemRoot%\system32\DiagSvcs\DiagnosticsHub.StandardCollector.ServiceRes.dll,-1000; C:\WINDOWS\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe [2017-03-18 86528]

S3 DmEnrollmentSvc;@%systemroot%\system32\Windows.Internal.Management.dll,-100; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 dmwappushservice;@%SystemRoot%\system32\dmwappushsvc.dll,-200; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 embeddedmode;@%SystemRoot%\system32\embeddedmodesvc.dll,-201; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

S3 EntAppSvc;@EnterpriseAppMgmtSvc.dll,-1; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 FontCache3.0.0.0;@%SystemRoot%\system32\PresentationHost.exe,-3309; C:\WINDOWS\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe [2017-02-10 43696]

S3 FrameServer;@%systemroot%\system32\FrameServer.dll,-100; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

S3 gupdatem;Služba Google Update (gupdatem); C:\Program Files (x86)\Google\Update\GoogleUpdate.exe [2015-08-30 144200]

S3 HvHost;@%SystemRoot%\system32\hvhostsvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 icssvc;@%SystemRoot%\System32\tetheringservice.dll,-4097; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 IDriverT;InstallDriver Table Manager; C:\Program Files (x86)\Common Files\InstallShield\Driver\1150\Intel 32\IDriverT.exe [2005-11-14 69632]

S3 IpxlatCfgSvc;@%Systemroot%\system32\ipxlatcfg.dll,-500; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

S3 irmon;@%SystemRoot%\System32\irmon.dll,-2000; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 MessagingService;@%SystemRoot%\system32\MessagingService.dll,-100; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 MessagingService_625e8e;Služba zasílání zpráv_625e8e; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 Microsoft Office Groove Audit Service;Microsoft Office Groove Audit Service; C:\Program Files (x86)\Microsoft Office\Office12\GrooveAuditService.exe [2009-02-26 64856]

S3 NaturalAuthentication;@%systemroot%\system32\NaturalAuth.dll,-100; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 NetSetupSvc;@%SystemRoot%\system32\NetSetupSvc.dll,-3; C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

S3 odserv;Microsoft Office Diagnostics Service; C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\ODSERV.EXE [2011-07-20 440696]

S3 ose;Office Source Engine; C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE [2006-10-26 145184]

S3 PhoneSvc;@%SystemRoot%\system32\PhoneserviceRes.dll,-10000; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 PimIndexMaintenanceSvc;@%SystemRoot%\system32\UserDataAccessRes.dll,-15001; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 RetailDemo;@%SystemRoot%\System32\RDXService.dll,-256;
C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

S3 SEMgrSvc;@%SystemRoot%\System32\SEMgrSvc.dll,-1001; C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 SensorDataService;@%SystemRoot%\system32\SensorDataService.exe,-101;
C:\WINDOWS\System32\SensorDataService.exe [2017-03-18 1284608]

S3 SensorService;@%SystemRoot%\System32\sensorservice.dll,-1000;
C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 SmsRouter;@%SystemRoot%\System32\SmsRouterSvc.dll,-10001;
C:\WINDOWS\system32\svchost.exe [2017-03-18 47664]

S3 spectrum;@%systemroot%\system32\spectrum.exe,-101; C:\WINDOWS\system32\spectrum.exe [2017-03-18 891904]

S4 aspnet_state;@%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\aspnet_rc.dll,-1;
C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe [2017-03-18 52920]

S4 shpamsvc;@%SystemRoot%\System32\Windows.SharedPC.AccountManager.dll,-100;
C:\WINDOWS\System32\svchost.exe [2017-03-18 47664]

----------EOF----------