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

Run by kinderen at 2016-10-15 23:25:25

Microsoft Windows 10 Home

System drive C: has 390 GB (85%) free of 458 GB

Total RAM: 3988 MB (42% free)

Logfile of Trend Micro HijackThis v2.0.4

Scan saved at 23:25:29, on 15-10-2016

Platform: Unknown Windows (WinNT 6.02.1008)

MSIE: Internet Explorer v11.0 (11.00.14393.0000)

Boot mode: Normal

Running processes:

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

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

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

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 - HKCU\Software\Microsoft\Internet Explorer\Main,Local Page = %11%\blank.htm

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: Lync Click to Call BHO - {31D09BA0-12F5-4CCE-BE8A-2923E76605DA} - C:\Program Files (x86)\Microsoft Office\root\Office16\OCHelper.dll

O2 - BHO: Java(tm) Plug-In SSV Helper - {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} - C:\Program Files (x86)\Java\jre1.8.0\_101\bin\ssv.dll

O2 - BHO: Microsoft OneDrive for Business Browser Helper - {D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF} - C:\Program Files (x86)\Microsoft Office\root\Office16\GROOVEEX.DLL

O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files (x86)\Java\jre1.8.0\_101\bin\jp2ssv.dll

O4 - HKLM\..\Run: [Dropbox] "C:\Program Files (x86)\Dropbox\Client\Dropbox.exe" /systemstartup

O4 - HKLM\..\Run: [CCAV] "C:\Program Files (x86)\COMODO\COMODO Cloud Antivirus\ccavsrv.exe" -autorun

O4 - HKLM\..\Run: [IseUI] C:\Program Files (x86)\COMODO\Internet Security Essentials\vkise.exe

O4 - HKLM\..\Run: [SunJavaUpdateSched] "C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"

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

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

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')

O8 - Extra context menu item: E&xport to Microsoft Excel - res://C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE/3000

O8 - Extra context menu item: E&xporteren naar Microsoft Excel - res://C:\PROGRA~2\MICROS~1\Office12\EXCEL.EXE/3000

O8 - Extra context menu item: Se&nd to OneNote - res://C:\Program Files (x86)\Microsoft Office\Root\Office16\ONBttnIE.dll/105

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

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

O9 - Extra button: Lync Click to Call - {31D09BA0-12F5-4CCE-BE8A-2923E76605DA} - C:\Program Files (x86)\Microsoft Office\root\Office16\OCHelper.dll

O9 - Extra 'Tools' menuitem: Lync Click to Call - {31D09BA0-12F5-4CCE-BE8A-2923E76605DA} - C:\Program Files (x86)\Microsoft Office\root\Office16\OCHelper.dll

O9 - Extra button: OneNote Lin&ked Notes - {789FE86F-6FC4-46A1-9849-EDE0DB0C95CA} - C:\Program Files (x86)\Microsoft Office\root\Office16\ONBttnIELinkedNotes.dll

O9 - Extra 'Tools' menuitem: OneNote Lin&ked Notes - {789FE86F-6FC4-46A1-9849-EDE0DB0C95CA} - C:\Program Files (x86)\Microsoft Office\root\Office16\ONBttnIELinkedNotes.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

O15 - Trusted Zone: \*.ea-match.eu

O15 - Trusted Zone: http://\*.hola.org

O15 - ESC Trusted Zone: \*.ea-match.eu

O18 - Protocol: mso-minsb-roaming.16 - {83C25742-A9F7-49FB-9138-434302C88D07} - C:\Program Files (x86)\Microsoft Office\root\Office16\MSOSB.DLL

O18 - Protocol: mso-minsb.16 - {42089D2D-912D-4018-9087-2B87803E93FB} - C:\Program Files (x86)\Microsoft Office\root\Office16\MSOSB.DLL

O18 - Protocol: osf-roaming.16 - {42089D2D-912D-4018-9087-2B87803E93FB} - C:\Program Files (x86)\Microsoft Office\root\Office16\MSOSB.DLL

O18 - Protocol: osf.16 - {5504BE45-A83B-4808-900A-3A5C36E7F77A} - C:\Program Files (x86)\Microsoft Office\root\Office16\MSOSB.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

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

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

O23 - Service: Apple Mobile Device Service - Apple Inc. - C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe

O23 - Service: Bonjour-service (Bonjour Service) - Apple Inc. - C:\Program Files\Bonjour\mDNSResponder.exe

O23 - Service: ccavsrv - COMODO - C:\Program Files (x86)\COMODO\COMODO Cloud Antivirus\ccavsrv.exe

O23 - Service: Intel(R) Content Protection HECI Service (cphs) - Intel Corporation - C:\WINDOWS\SysWow64\IntelCpHeciSvc.exe

O23 - Service: Dropbox-update-service (dbupdate) (dbupdate) - Dropbox, Inc. - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe

O23 - Service: Dropbox-update-service (dbupdatem) (dbupdatem) - Dropbox, Inc. - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe

O23 - Service: DbxSvc - Unknown owner - C:\WINDOWS\system32\DbxSvc.exe (file missing)

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

O23 - Service: Genie Timeline Service (GenieTimelineService) - Genie9 - C:\Program Files\NETGEAR\ReadySHARE Vault\GenieTimelineService.exe

O23 - Service: Hola Better Internet Engine (hola\_svc) - Hola Networks Ltd. - C:\Program Files\Hola\app\hola\_svc.exe

O23 - Service: Hola Better Internet Updater (hola\_updater) - Hola Networks Ltd. - C:\Program Files\Hola\app\hola\_updater.exe

O23 - Service: Intel(R) HD Graphics Control Panel Service (igfxCUIService1.0.0.0) - Unknown owner - C:\WINDOWS\system32\igfxCUIService.exe (file missing)

O23 - Service: iPod-service (iPod Service) - Apple Inc. - C:\Program Files\iPod\bin\iPodService.exe

O23 - Service: isesrv - COMODO - C:\Program Files (x86)\COMODO\Internet Security Essentials\isesrv.exe

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

O23 - Service: Mozilla Maintenance Service (MozillaMaintenance) - Mozilla Foundation - C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe

O23 - Service: @comres.dll,-2797 (MSDTC) - Unknown owner - C:\WINDOWS\System32\msdtc.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: Realtek Audio Service (RtkAudioService) - Realtek Semiconductor - C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe

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

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

O23 - Service: Skype Updater (SkypeUpdate) - Skype Technologies - C:\Program Files (x86)\Skype\Updater\Updater.exe

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

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: SynTPEnh Caller Service (SynTPEnhService) - Synaptics Incorporated - C:\Program Files\Synaptics\SynTP\SynTPEnhService.exe

O23 - Service: TeamViewer 11 (TeamViewer) - TeamViewer GmbH - C:\Program Files (x86)\TeamViewer\TeamViewer\_Service.exe

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: @%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 - 10846 bytes

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

winlogon.exe

C:\WINDOWS\system32\lsass.exe

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

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

"dwm.exe"

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

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

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

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

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

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

C:\WINDOWS\system32\igfxCUIService.exe

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

"C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe"

"C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /SRSPS

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

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

C:\WINDOWS\System32\spoolsv.exe

"C:\Program Files (x86)\COMODO\Internet Security Essentials\isesrv.exe" -service

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

"C:\Program Files (x86)\COMODO\COMODO Cloud Antivirus\ccavsrv.exe" -service

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

"C:\Program Files\Synaptics\SynTP\SynTPEnhService.exe"

"C:\Program Files\Bonjour\mDNSResponder.exe"

"C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service

"C:\Program Files (x86)\TeamViewer\TeamViewer\_Service.exe"

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

C:\WINDOWS\system32\DbxSvc.exe

"C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe"

dashost.exe {8ae6a1c1-2a8a-4916-a3b90aa09ebc9a28}

"C:\Program Files\Hola\app\hola\_updater.exe" --service --run-as hola\_updater

"C:\Program Files\Hola\app\hola\_svc.exe" --service

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

sihost.exe

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

C:\WINDOWS\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe

C:\WINDOWS\Explorer.EXE

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

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

"C:\Program Files\NETGEAR\ReadySHARE Vault\GenieTimelineAgent.exe"

"C:\Program Files\Synaptics\SynTP\SynTPEnh.exe"

"C:\PROGRAM FILES\SYNAPTICS\SYNTP\SYNTPHELPER.EXE"

igfxEM.exe

igfxHK.exe

igfxTray.exe

"C:\WINDOWS\SystemApps\ShellExperienceHost\_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca

"C:\Program Files\WindowsApps\Microsoft.SkypeApp\_11.8.190.0\_x64\_\_kzf8qxf38zg5c\SkypeHost.exe" -ServerName:SkypeHost.ServerServer

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

C:\WINDOWS\system32\DllHost.exe /Processid:{49F6E667-6658-4BD1-9DE9-6AF87F9FAF85}

"C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe" -s

"C:\Program Files\Hola\app\hola.exe" --silent

"C:\Program Files\iTunes\iTunesHelper.exe"

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

"C:\Program Files\iPod\bin\iPodService.exe"

"C:\Program Files (x86)\Dropbox\Client\Dropbox.exe" /systemstartup

"C:\Program Files\Internet Explorer\iexplore.exe" -restart /WERRESTART

"C:\Program Files (x86)\COMODO\COMODO Cloud Antivirus\ccavsrv.exe" -autorun

"C:\Program Files (x86)\COMODO\Internet Security Essentials\vkise.exe"

"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6372 CREDAT:75009 /prefetch:2

"C:\Program Files\CCleaner\CCleaner64.exe" /MONITOR /uac

"C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"

"C:\Program Files\Internet Explorer\iexplore.exe" "http://tech-connect.biz/?ssid=1473634859&a=1051321&src=sh&uuid=8080add8-fb07-499d-9fa0-abed50da579f,1473634806583"

"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:7736 CREDAT:75009 /prefetch:2

"fontdrvhost.exe"

"C:\Windows\SystemApps\Microsoft.Windows.Cortana\_cw5n1h2txyewy\SearchUI.exe" -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca

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

"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:7736 CREDAT:140552 /prefetch:2

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

"C:\Program Files (x86)\Microsoft Office\root\Office16\msoia.exe" scan upload mininterval:2880

"C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps\_17.7369.40737.0\_x64\_\_8wekyb3d8bbwe\HxMail.exe" -ServerName:microsoft.windowslive.mail.AppX7fgs1v31b27fq9zen50wdw83aappcatm.mca

"C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps\_17.7369.40737.0\_x64\_\_8wekyb3d8bbwe\HxTsr.exe" -ServerName:Hx.IPC.Server

"C:\Program Files\NETGEAR\ReadySHARE Vault\GenieTimelineService.exe"

"C:\Program Files (x86)\Mozilla Firefox\firefox.exe"

C:\WINDOWS\system32\AUDIODG.EXE 0x420

"C:\WINDOWS\system32\backgroundTaskHost.exe" -ServerName:CortanaUI.AppXy7vb4pc2dr3kc93kfc509b1d0arkfb2x.mca

"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:7736 CREDAT:206094 /prefetch:2

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

"C:\Users\kinderen\AppData\Local\Microsoft\Windows\INetCache\IE\ILYL9TQ8\RSITx64.exe"

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

======Scheduled tasks folder======

C:\WINDOWS\tasks\Adobe Flash Player Updater.job - C:\WINDOWS\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe

C:\WINDOWS\tasks\DropboxUpdateTaskMachineCore.job - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe /c

C:\WINDOWS\tasks\DropboxUpdateTaskMachineUA.job - C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe /ua /installsource scheduler

=========Mozilla firefox=========

ProfilePath - C:\Users\kinderen\AppData\Roaming\Mozilla\Firefox\Profiles\l3jxgxtu.default

prefs.js - "browser.startup.homepage" - "about:home"

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@adobe.com/FlashPlayer]

"Description"=Adobe® Flash® Player 23.0.0.162 Plugin

"Path"=C:\WINDOWS\SysWOW64\Macromed\Flash\NPSWF32\_23\_0\_0\_162.dll

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@java.com/DTPlugin,version=11.101.2]

"Description"=Java™ Deployment Toolkit

"Path"=C:\Program Files (x86)\Java\jre1.8.0\_101\bin\dtplugin\npDeployJava1.dll

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@java.com/JavaPlugin,version=11.101.2]

"Description"=Oracle® Next Generation Java™ Plug-In

"Path"=C:\Program Files (x86)\Java\jre1.8.0\_101\bin\plugin2\npjp2.dll

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@microsoft.com/Lync,version=15.0]

"Description"=Microsoft Lync Plug-in for Firefox

"Path"=C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesX86\Mozilla Firefox\plugins\npmeetingjoinpluginoc.dll

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\MozillaPlugins\@microsoft.com/SharePoint,version=14.0]

"Description"=Microsoft SharePoint Plug-in for Firefox

"Path"=C:\Program Files (x86)\Microsoft Office\root\Office16\NPSPWRAP.DLL

[HKEY\_LOCAL\_MACHINE\SOFTWARE\MozillaPlugins\@adobe.com/FlashPlayer]

"Description"=Adobe® Flash® Player 23.0.0.162 Plugin

"Path"=C:\WINDOWS\system32\Macromed\Flash\NPSWF64\_23\_0\_0\_162.dll

C:\Users\kinderen\AppData\Roaming\Mozilla\Firefox\Profiles\l3jxgxtu.default\extensions\

jid1-4P0kohSJxU1qGg@jetpack

C:\Users\kinderen\AppData\Roaming\Mozilla\Firefox\Profiles\l3jxgxtu.default\searchplugins\

AdTrustMediaCCAV.xml

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

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{31D09BA0-12F5-4CCE-BE8A-2923E76605DA}]

Lync Browser Helper - C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesX64\Microsoft Office\Office16\OCHelper.dll [2016-09-05 215752]

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF}]

Microsoft OneDrive for Business Browser Helper - C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesX64\Microsoft Office\Office16\GROOVEEX.DLL [2016-09-05 2278192]

[HKEY\_LOCAL\_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{31D09BA0-12F5-4CCE-BE8A-2923E76605DA}]

Lync Browser Helper - C:\Program Files (x86)\Microsoft Office\root\Office16\OCHelper.dll [2016-09-05 157904]

[HKEY\_LOCAL\_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}]

Java(tm) Plug-In SSV Helper - C:\Program Files (x86)\Java\jre1.8.0\_101\bin\ssv.dll [2016-09-28 473152]

[HKEY\_LOCAL\_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF}]

Microsoft OneDrive for Business Browser Helper - C:\Program Files (x86)\Microsoft Office\root\Office16\GROOVEEX.DLL [2016-09-05 1658160]

[HKEY\_LOCAL\_MACHINE\SOFTWARE\wow6432node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{DBC80044-A445-435b-BC74-9C25C1C588A9}]

Java(tm) Plug-In 2 SSV Helper - C:\Program Files (x86)\Java\jre1.8.0\_101\bin\jp2ssv.dll [2016-09-28 186944]

[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

"RtHDVCpl"=C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe [2016-06-07 13196432]

"hola"=C:\Program Files\Hola\app\hola.exe [2016-09-18 2162864]

"iTunesHelper"=C:\Program Files\iTunes\iTunesHelper.exe [2016-09-09 176440]

"SynTPEnh"=C:\Program Files\Synaptics\SynTP\SynTPEnh.exe [2016-06-07 3954880]

[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run]

"OneDrive"=C:\Users\kinderen\AppData\Local\Microsoft\OneDrive\OneDrive.exe [2016-09-25 633024]

"CCleaner Monitoring"=C:\Program Files\CCleaner\CCleaner64.exe [2016-06-01 8722136]

[HKEY\_LOCAL\_MACHINE\Software\wow6432node\Microsoft\Windows\CurrentVersion\Run]

"Dropbox"=C:\Program Files (x86)\Dropbox\Client\Dropbox.exe [2016-10-06 25243040]

"CCAV"=C:\Program Files (x86)\COMODO\COMODO Cloud Antivirus\ccavsrv.exe [2016-09-30 5443720]

"IseUI"=C:\Program Files (x86)\COMODO\Internet Security Essentials\vkise.exe [2016-09-29 3382464]

"SunJavaUpdateSched"=C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe [2016-06-22 598552]

[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\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

"EnableLinkedConnections"=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

"wave"=wdmaud.drv

"midi"=wdmaud.drv

"mixer"=wdmaud.drv

"aux"=wdmaud.drv

"wave1"=wdmaud.drv

"midi1"=wdmaud.drv

"mixer1"=wdmaud.drv

"aux1"=wdmaud.drv

"MSVideo8"=VfWWDM32.dll

"wave2"=wdmaud.drv

"midi2"=wdmaud.drv

"mixer2"=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======

2016-10-15 23:25:25 ----D---- C:\rsit

2016-10-15 23:25:25 ----D---- C:\Program Files\trend micro

2016-10-15 23:09:01 ----D---- C:\CCAV

2016-10-14 22:27:49 ----HD---- C:\$SysReset

2016-10-14 22:20:18 ----A---- C:\WINDOWS\system32\msfeeds.dll

2016-10-14 22:20:17 ----A---- C:\WINDOWS\system32\ieframe.dll

2016-10-14 22:20:16 ----A---- C:\WINDOWS\SYSWOW64\ieframe.dll

2016-10-14 22:20:15 ----A---- C:\WINDOWS\SYSWOW64\twinui.dll

2016-10-14 22:20:15 ----A---- C:\WINDOWS\system32\CertEnroll.dll

2016-10-14 22:20:14 ----A---- C:\WINDOWS\system32\wpncore.dll

2016-10-14 22:20:14 ----A---- C:\WINDOWS\system32\msxml6.dll

2016-10-14 22:20:13 ----A---- C:\WINDOWS\SYSWOW64\DWrite.dll

2016-10-14 22:20:13 ----A---- C:\WINDOWS\SYSWOW64\daxexec.dll

2016-10-14 22:20:13 ----A---- C:\WINDOWS\system32\wpx.dll

2016-10-14 22:20:13 ----A---- C:\WINDOWS\system32\ncsi.dll

2016-10-14 22:20:13 ----A---- C:\WINDOWS\system32\inetcomm.dll

2016-10-14 22:20:12 ----A---- C:\WINDOWS\SYSWOW64\ShareHost.dll

2016-10-14 22:20:12 ----A---- C:\WINDOWS\SYSWOW64\msfeeds.dll

2016-10-14 22:20:12 ----A---- C:\WINDOWS\system32\nlasvc.dll

2016-10-14 22:20:12 ----A---- C:\WINDOWS\system32\msdtctm.dll

2016-10-14 22:20:12 ----A---- C:\WINDOWS\system32\credprovs.dll

2016-10-14 22:20:11 ----A---- C:\WINDOWS\system32\UserDeviceRegistration.dll

2016-10-14 22:20:11 ----A---- C:\WINDOWS\system32\bcdedit.exe

2016-10-14 22:20:10 ----A---- C:\WINDOWS\system32\netshell.dll

2016-10-14 22:20:09 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.AllJoyn.dll

2016-10-14 22:20:09 ----A---- C:\WINDOWS\SYSWOW64\Windows.ApplicationModel.Wallet.dll

2016-10-14 22:20:09 ----A---- C:\WINDOWS\SYSWOW64\dsreg.dll

2016-10-14 22:20:09 ----A---- C:\WINDOWS\system32\drivers\mrxdav.sys

2016-10-14 22:20:08 ----A---- C:\WINDOWS\SYSWOW64\UserDeviceRegistration.dll

2016-10-14 22:20:08 ----A---- C:\WINDOWS\SYSWOW64\mspaint.exe

2016-10-14 22:20:08 ----A---- C:\WINDOWS\system32\UserMgrProxy.dll

2016-10-14 22:20:08 ----A---- C:\WINDOWS\system32\dsreg.dll

2016-10-14 22:20:07 ----A---- C:\WINDOWS\SYSWOW64\UserMgrProxy.dll

2016-10-14 22:20:07 ----A---- C:\WINDOWS\SYSWOW64\UserDeviceRegistration.Ngc.dll

2016-10-14 22:20:07 ----A---- C:\WINDOWS\SYSWOW64\AuthBroker.dll

2016-10-14 22:20:07 ----A---- C:\WINDOWS\system32\Windows.Networking.ServiceDiscovery.Dnssd.dll

2016-10-14 22:20:07 ----A---- C:\WINDOWS\system32\UserDeviceRegistration.Ngc.dll

2016-10-14 22:20:07 ----A---- C:\WINDOWS\system32\AuthBroker.dll

2016-10-14 22:20:06 ----A---- C:\WINDOWS\SYSWOW64\aadtb.dll

2016-10-14 22:20:06 ----A---- C:\WINDOWS\system32\urlmon.dll

2016-10-14 22:20:05 ----A---- C:\WINDOWS\system32\mshtml.dll

2016-10-14 22:20:05 ----A---- C:\WINDOWS\system32\edgehtml.dll

2016-10-14 22:20:04 ----A---- C:\WINDOWS\system32\shell32.dll

2016-10-14 22:20:02 ----A---- C:\WINDOWS\SYSWOW64\mshtml.dll

2016-10-14 22:19:59 ----A---- C:\WINDOWS\system32\Chakra.dll

2016-10-14 22:19:58 ----A---- C:\WINDOWS\SYSWOW64\edgehtml.dll

2016-10-14 22:19:58 ----A---- C:\WINDOWS\system32\iertutil.dll

2016-10-14 22:19:57 ----A---- C:\WINDOWS\SYSWOW64\Chakra.dll

2016-10-14 22:19:57 ----A---- C:\WINDOWS\system32\AppXDeploymentServer.dll

2016-10-14 22:19:56 ----A---- C:\WINDOWS\system32\jscript9.dll

2016-10-14 22:19:55 ----A---- C:\WINDOWS\system32\wininet.dll

2016-10-14 22:19:55 ----A---- C:\WINDOWS\system32\win32kbase.sys

2016-10-14 22:19:54 ----A---- C:\WINDOWS\SYSWOW64\mos.dll

2016-10-14 22:19:54 ----A---- C:\WINDOWS\SYSWOW64\iertutil.dll

2016-10-14 22:19:54 ----A---- C:\WINDOWS\system32\smartscreen.exe

2016-10-14 22:19:53 ----A---- C:\WINDOWS\system32\DWrite.dll

2016-10-14 22:19:53 ----A---- C:\WINDOWS\system32\drivers\MegaSas2i.sys

2016-10-14 22:19:52 ----A---- C:\WINDOWS\SYSWOW64\jscript9.dll

2016-10-14 22:19:52 ----A---- C:\WINDOWS\system32\ngcsvc.dll

2016-10-14 22:19:51 ----A---- C:\WINDOWS\SYSWOW64\GdiPlus.dll

2016-10-14 22:19:51 ----A---- C:\WINDOWS\system32\AppXDeploymentExtensions.onecore.dll

2016-10-14 22:19:50 ----A---- C:\WINDOWS\SYSWOW64\inetcomm.dll

2016-10-14 22:19:50 ----A---- C:\WINDOWS\SYSWOW64\fontdrvhost.exe

2016-10-14 22:19:50 ----A---- C:\WINDOWS\system32\vbscript.dll

2016-10-14 22:19:49 ----A---- C:\WINDOWS\SYSWOW64\msi.dll

2016-10-14 22:19:47 ----A---- C:\WINDOWS\SYSWOW64\offreg.dll

2016-10-14 22:19:47 ----A---- C:\WINDOWS\SYSWOW64\netshell.dll

2016-10-14 22:19:47 ----A---- C:\WINDOWS\SYSWOW64\credprovs.dll

2016-10-14 22:19:47 ----A---- C:\WINDOWS\SYSWOW64\apprepsync.dll

2016-10-14 22:19:47 ----A---- C:\WINDOWS\SYSWOW64\apprepapi.dll

2016-10-14 22:19:47 ----A---- C:\WINDOWS\system32\adsmsext.dll

2016-10-14 22:19:46 ----A---- C:\WINDOWS\SYSWOW64\efswrt.dll

2016-10-14 22:19:44 ----A---- C:\WINDOWS\SYSWOW64\dialclient.dll

2016-10-14 22:19:44 ----A---- C:\WINDOWS\SYSWOW64\Chakradiag.dll

2016-10-14 22:19:44 ----A---- C:\WINDOWS\system32\Windows.Web.Diagnostics.dll

2016-10-14 22:19:43 ----A---- C:\WINDOWS\system32\AppXDeploymentExtensions.desktop.dll

2016-10-14 22:19:43 ----A---- C:\WINDOWS\system32\aadtb.dll

2016-10-14 22:19:35 ----A---- C:\WINDOWS\system32\lsasrv.dll

2016-10-14 22:19:34 ----A---- C:\WINDOWS\SYSWOW64\shell32.dll

2016-10-14 22:19:33 ----A---- C:\WINDOWS\SYSWOW64\Windows.ApplicationModel.Store.dll

2016-10-14 22:19:32 ----A---- C:\WINDOWS\system32\Windows.ApplicationModel.Store.dll

2016-10-14 22:19:31 ----A---- C:\WINDOWS\SYSWOW64\urlmon.dll

2016-10-14 22:19:30 ----A---- C:\WINDOWS\SYSWOW64\wininet.dll

2016-10-14 22:19:30 ----A---- C:\WINDOWS\SYSWOW64\mstscax.dll

2016-10-14 22:19:30 ----A---- C:\WINDOWS\SYSWOW64\CertEnroll.dll

2016-10-14 22:19:29 ----A---- C:\WINDOWS\system32\wc\_storage.dll

2016-10-14 22:19:29 ----A---- C:\WINDOWS\system32\wbiosrvc.dll

2016-10-14 22:19:29 ----A---- C:\WINDOWS\system32\daxexec.dll

2016-10-14 22:19:28 ----A---- C:\WINDOWS\system32\WpcWebFilter.dll

2016-10-14 22:19:28 ----A---- C:\WINDOWS\system32\diagtrack.dll

2016-10-14 22:19:27 ----A---- C:\WINDOWS\SYSWOW64\WpcWebFilter.dll

2016-10-14 22:19:27 ----A---- C:\WINDOWS\system32\drivers\cng.sys

2016-10-14 22:19:26 ----A---- C:\WINDOWS\SYSWOW64\vbscript.dll

2016-10-14 22:19:26 ----A---- C:\WINDOWS\system32\Windows.Devices.Sensors.dll

2016-10-14 22:19:26 ----A---- C:\WINDOWS\system32\CloudExperienceHostCommon.dll

2016-10-14 22:19:25 ----A---- C:\WINDOWS\SYSWOW64\AzureSettingSyncProvider.dll

2016-10-14 22:19:24 ----A---- C:\WINDOWS\SYSWOW64\EmailApis.dll

2016-10-14 22:19:24 ----A---- C:\WINDOWS\SYSWOW64\ContactApis.dll

2016-10-14 22:19:24 ----A---- C:\WINDOWS\system32\Windows.Devices.AllJoyn.dll

2016-10-14 22:19:24 ----A---- C:\WINDOWS\system32\efswrt.dll

2016-10-14 22:19:23 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Logon.dll

2016-10-14 22:19:23 ----A---- C:\WINDOWS\SYSWOW64\UserDataAccountApis.dll

2016-10-14 22:19:23 ----A---- C:\WINDOWS\SYSWOW64\mstsc.exe

2016-10-14 22:19:23 ----A---- C:\WINDOWS\SYSWOW64\ChatApis.dll

2016-10-14 22:19:23 ----A---- C:\WINDOWS\SYSWOW64\AppointmentApis.dll

2016-10-14 22:19:23 ----A---- C:\WINDOWS\system32\dialclient.dll

2016-10-14 22:19:22 ----A---- C:\WINDOWS\SYSWOW64\MCRecvSrc.dll

2016-10-14 22:19:18 ----A---- C:\WINDOWS\system32\wmp.dll

2016-10-14 22:19:16 ----A---- C:\WINDOWS\SYSWOW64\mfcore.dll

2016-10-14 22:19:16 ----A---- C:\WINDOWS\system32\Windows.UI.Search.dll

2016-10-14 22:19:15 ----A---- C:\WINDOWS\SYSWOW64\wmp.dll

2016-10-14 22:19:15 ----A---- C:\WINDOWS\SYSWOW64\mfnetcore.dll

2016-10-14 22:19:14 ----A---- C:\WINDOWS\SYSWOW64\KernelBase.dll

2016-10-14 22:19:14 ----A---- C:\WINDOWS\system32\MSVidCtl.dll

2016-10-14 22:19:14 ----A---- C:\WINDOWS\system32\mstscax.dll

2016-10-14 22:19:13 ----A---- C:\WINDOWS\system32\KernelBase.dll

2016-10-14 22:19:13 ----A---- C:\WINDOWS\system32\AppxPackaging.dll

2016-10-14 22:19:12 ----A---- C:\WINDOWS\SYSWOW64\Windows.StateRepository.dll

2016-10-14 22:19:11 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.dll

2016-10-14 22:19:11 ----A---- C:\WINDOWS\system32\winload.exe

2016-10-14 22:19:10 ----A---- C:\WINDOWS\SYSWOW64\win32kfull.sys

2016-10-14 22:19:09 ----A---- C:\WINDOWS\SYSWOW64\AppxPackaging.dll

2016-10-14 22:19:09 ----A---- C:\WINDOWS\system32\winresume.exe

2016-10-14 22:19:09 ----A---- C:\WINDOWS\system32\TSWorkspace.dll

2016-10-14 22:19:08 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Search.dll

2016-10-14 22:19:07 ----A---- C:\WINDOWS\SYSWOW64\mfnetsrc.dll

2016-10-14 22:19:07 ----A---- C:\WINDOWS\system32\mfsensorgroup.dll

2016-10-14 22:19:06 ----A---- C:\WINDOWS\SYSWOW64\MSVidCtl.dll

2016-10-14 22:19:06 ----A---- C:\WINDOWS\system32\Windows.Web.dll

2016-10-14 22:19:05 ----A---- C:\WINDOWS\SYSWOW64\AppXDeploymentClient.dll

2016-10-14 22:19:05 ----A---- C:\WINDOWS\system32\Windows.Networking.dll

2016-10-14 22:19:05 ----A---- C:\WINDOWS\system32\drivers\tm.sys

2016-10-14 22:19:05 ----A---- C:\WINDOWS\system32\drivers\dfsc.sys

2016-10-14 22:19:05 ----A---- C:\WINDOWS\system32\apprepsync.dll

2016-10-14 22:19:04 ----A---- C:\WINDOWS\SYSWOW64\Windows.Web.dll

2016-10-14 22:19:04 ----A---- C:\WINDOWS\SYSWOW64\CloudExperienceHostCommon.dll

2016-10-14 22:19:04 ----A---- C:\WINDOWS\system32\Windows.Networking.HostName.dll

2016-10-14 22:19:04 ----A---- C:\WINDOWS\system32\offreg.dll

2016-10-14 22:19:04 ----A---- C:\WINDOWS\system32\CloudExperienceHost.dll

2016-10-14 22:19:04 ----A---- C:\WINDOWS\system32\apprepapi.dll

2016-10-14 22:19:03 ----A---- C:\WINDOWS\system32\Windows.Web.Http.dll

2016-10-14 22:19:03 ----A---- C:\WINDOWS\system32\msi.dll

2016-10-14 22:19:02 ----A---- C:\WINDOWS\SYSWOW64\Windows.Web.Http.dll

2016-10-14 22:19:02 ----A---- C:\WINDOWS\SYSWOW64\Windows.Networking.dll

2016-10-14 22:19:02 ----A---- C:\WINDOWS\SYSWOW64\Windows.Networking.Connectivity.dll

2016-10-14 22:19:02 ----A---- C:\WINDOWS\system32\Windows.Networking.Connectivity.dll

2016-10-14 22:19:02 ----A---- C:\WINDOWS\system32\Windows.ApplicationModel.Wallet.dll

2016-10-14 22:19:01 ----A---- C:\WINDOWS\SYSWOW64\Windows.StateRepositoryClient.dll

2016-10-14 22:19:01 ----A---- C:\WINDOWS\SYSWOW64\Windows.Networking.ServiceDiscovery.Dnssd.dll

2016-10-14 22:19:01 ----A---- C:\WINDOWS\SYSWOW64\Windows.Networking.HostName.dll

2016-10-14 22:19:01 ----A---- C:\WINDOWS\SYSWOW64\Windows.Networking.BackgroundTransfer.dll

2016-10-14 22:19:01 ----A---- C:\WINDOWS\SYSWOW64\ConfigureExpandedStorage.dll

2016-10-14 22:19:01 ----A---- C:\WINDOWS\system32\Windows.Networking.BackgroundTransfer.dll

2016-10-14 22:19:01 ----A---- C:\WINDOWS\system32\FrameServer.dll

2016-10-14 22:19:00 ----A---- C:\WINDOWS\SYSWOW64\UIRibbonRes.dll

2016-10-14 22:19:00 ----A---- C:\WINDOWS\system32\Windows.UI.Logon.dll

2016-10-14 22:19:00 ----A---- C:\WINDOWS\system32\UIRibbonRes.dll

2016-10-14 22:19:00 ----A---- C:\WINDOWS\system32\GamePanel.exe

2016-10-14 22:18:59 ----A---- C:\WINDOWS\system32\AzureSettingSyncProvider.dll

2016-10-14 22:18:58 ----A---- C:\WINDOWS\system32\SettingsHandlers\_nt.dll

2016-10-14 22:18:55 ----A---- C:\WINDOWS\system32\twinui.dll

2016-10-14 22:18:52 ----A---- C:\WINDOWS\system32\win32kfull.sys

2016-10-14 22:18:45 ----A---- C:\WINDOWS\system32\mfcore.dll

2016-10-14 22:18:44 ----A---- C:\WINDOWS\system32\ntoskrnl.exe

2016-10-14 22:18:43 ----A---- C:\WINDOWS\system32\mos.dll

2016-10-14 22:18:43 ----A---- C:\WINDOWS\system32\mfnetcore.dll

2016-10-14 22:18:41 ----A---- C:\WINDOWS\system32\Windows.StateRepository.dll

2016-10-14 22:18:41 ----A---- C:\WINDOWS\system32\FntCache.dll

2016-10-14 22:18:40 ----A---- C:\WINDOWS\SYSWOW64\msxml6.dll

2016-10-14 22:18:40 ----A---- C:\WINDOWS\system32\Windows.Media.dll

2016-10-14 22:18:39 ----A---- C:\WINDOWS\system32\fontdrvhost.exe

2016-10-14 22:18:38 ----A---- C:\WINDOWS\system32\GdiPlus.dll

2016-10-14 22:18:37 ----A---- C:\WINDOWS\system32\win32spl.dll

2016-10-14 22:18:37 ----A---- C:\WINDOWS\system32\drivers\ndis.sys

2016-10-14 22:18:36 ----A---- C:\WINDOWS\SYSWOW64\mfsensorgroup.dll

2016-10-14 22:18:36 ----A---- C:\WINDOWS\system32\drivers\tcpip.sys

2016-10-14 22:18:36 ----A---- C:\WINDOWS\system32\ContactApis.dll

2016-10-14 22:18:36 ----A---- C:\WINDOWS\system32\cloudAP.dll

2016-10-14 22:18:36 ----A---- C:\WINDOWS\system32\AppXDeploymentClient.dll

2016-10-14 22:18:35 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.Sensors.dll

2016-10-14 22:18:35 ----A---- C:\WINDOWS\system32\ShareHost.dll

2016-10-14 22:18:35 ----A---- C:\WINDOWS\system32\mfps.dll

2016-10-14 22:18:35 ----A---- C:\WINDOWS\system32\drivers\sdbus.sys

2016-10-14 22:18:35 ----A---- C:\WINDOWS\system32\drivers\dumpsd.sys

2016-10-14 22:18:34 ----A---- C:\WINDOWS\SYSWOW64\adsmsext.dll

2016-10-14 22:18:34 ----A---- C:\WINDOWS\system32\EmailApis.dll

2016-10-14 22:18:34 ----A---- C:\WINDOWS\system32\ChatApis.dll

2016-10-14 22:18:34 ----A---- C:\WINDOWS\system32\AppointmentApis.dll

2016-10-14 22:18:32 ----A---- C:\WINDOWS\system32\Windows.StateRepositoryClient.dll

2016-10-14 22:18:32 ----A---- C:\WINDOWS\system32\mspaint.exe

2016-10-14 22:18:32 ----A---- C:\WINDOWS\system32\ErrorDetails.dll

2016-10-14 22:18:31 ----A---- C:\WINDOWS\system32\Windows.StateRepositoryBroker.dll

2016-10-14 22:18:31 ----A---- C:\WINDOWS\system32\MCRecvSrc.dll

2016-10-14 18:32:04 ----D---- C:\Program Files (x86)\Microsoft Works

2016-10-14 18:31:11 ----D---- C:\WINDOWS\PCHEALTH

2016-10-14 18:27:14 ----D---- C:\Program Files\Microsoft Office

2016-10-14 18:26:21 ----D---- C:\WINDOWS\SHELLNEW

2016-10-14 18:26:00 ----D---- C:\ProgramData\Microsoft Help

2016-10-14 18:03:36 ----ASH---- C:\swapfile.sys

2016-10-14 18:03:36 ----ASH---- C:\pagefile.sys

2016-10-14 18:03:31 ----ASH---- C:\hiberfil.sys

2016-10-13 17:31:27 ----SHD---- C:\Config.Msi

2016-10-11 00:37:33 ----SHD---- C:\Recovery

2016-10-10 22:40:09 ----HD---- C:\$WINDOWS.~BT

2016-10-10 22:10:29 ----HD---- C:\$Windows.~WS

2016-10-10 21:47:24 ----D---- C:\ESD

2016-10-10 00:07:53 ----D---- C:\ProgramData\Shared Space

2016-10-06 23:06:30 ----A---- C:\WINDOWS\system32\DbxSvc.exe

2016-10-06 23:00:28 ----A---- C:\WINDOWS\system32\drivers\dbx-stable.sys

2016-10-06 23:00:28 ----A---- C:\WINDOWS\system32\drivers\dbx-dev.sys

2016-10-06 23:00:28 ----A---- C:\WINDOWS\system32\drivers\dbx-canary.sys

2016-10-05 20:22:30 ----A---- C:\WINDOWS\SYSWOW64\wlancfg.dll

2016-10-05 20:22:30 ----A---- C:\WINDOWS\SYSWOW64\tdh.dll

2016-10-05 20:22:30 ----A---- C:\WINDOWS\SYSWOW64\ReAgent.dll

2016-10-05 20:22:29 ----A---- C:\WINDOWS\SYSWOW64\tsmf.dll

2016-10-05 20:22:29 ----A---- C:\WINDOWS\SYSWOW64\SyncSettings.dll

2016-10-05 20:22:29 ----A---- C:\WINDOWS\SYSWOW64\msctf.dll

2016-10-05 20:22:26 ----A---- C:\WINDOWS\SYSWOW64\mprddm.dll

2016-10-05 20:22:25 ----A---- C:\WINDOWS\SYSWOW64\olepro32.dll

2016-10-05 20:22:25 ----A---- C:\WINDOWS\SYSWOW64\NaturalLanguage6.dll

2016-10-05 20:22:25 ----A---- C:\WINDOWS\SYSWOW64\MSAC3ENC.DLL

2016-10-05 20:22:24 ----A---- C:\WINDOWS\SYSWOW64\ieproxy.dll

2016-10-05 20:22:23 ----A---- C:\WINDOWS\SYSWOW64\NetworkCollectionAgent.dll

2016-10-05 20:22:23 ----A---- C:\WINDOWS\SYSWOW64\iedkcs32.dll

2016-10-05 20:22:22 ----A---- C:\WINDOWS\SYSWOW64\Windows.Data.Pdf.dll

2016-10-05 20:22:22 ----A---- C:\WINDOWS\SYSWOW64\setupugc.exe

2016-10-05 20:22:22 ----A---- C:\WINDOWS\SYSWOW64\clusapi.dll

2016-10-05 20:22:21 ----A---- C:\WINDOWS\SYSWOW64\CPFilters.dll

2016-10-05 20:22:20 ----A---- C:\WINDOWS\SYSWOW64\comsvcs.dll

2016-10-05 20:22:19 ----A---- C:\WINDOWS\SYSWOW64\SndVolSSO.dll

2016-10-05 20:22:17 ----A---- C:\WINDOWS\SYSWOW64\tquery.dll

2016-10-05 20:22:17 ----A---- C:\WINDOWS\SYSWOW64\SearchProtocolHost.exe

2016-10-05 20:22:16 ----A---- C:\WINDOWS\SYSWOW64\Windows.System.UserDeviceAssociation.dll

2016-10-05 20:22:16 ----A---- C:\WINDOWS\SYSWOW64\Windows.Storage.ApplicationData.dll

2016-10-05 20:22:16 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Speech.UXRes.dll

2016-10-05 20:22:16 ----A---- C:\WINDOWS\SYSWOW64\SearchIndexer.exe

2016-10-05 20:22:16 ----A---- C:\WINDOWS\SYSWOW64\Search.ProtocolHandler.MAPI2.dll

2016-10-05 20:22:16 ----A---- C:\WINDOWS\SYSWOW64\mssrch.dll

2016-10-05 20:22:15 ----A---- C:\WINDOWS\SYSWOW64\WinRtTracing.dll

2016-10-05 20:22:15 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Speech.dll

2016-10-05 20:22:15 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Ocr.dll

2016-10-05 20:22:15 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.FaceAnalysis.dll

2016-10-05 20:22:15 ----A---- C:\WINDOWS\SYSWOW64\Windows.Gaming.XboxLive.Storage.dll

2016-10-05 20:22:15 ----A---- C:\WINDOWS\SYSWOW64\Windows.Gaming.Input.dll

2016-10-05 20:22:15 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.Perception.dll

2016-10-05 20:22:15 ----A---- C:\WINDOWS\SYSWOW64\Windows.ApplicationModel.dll

2016-10-05 20:22:15 ----A---- C:\WINDOWS\SYSWOW64\Windows.ApplicationModel.Core.dll

2016-10-05 20:22:14 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Protection.PlayReady.dll

2016-10-05 20:22:14 ----A---- C:\WINDOWS\SYSWOW64\Windows.ApplicationModel.Background.SystemEventsBroker.dll

2016-10-05 20:22:14 ----A---- C:\WINDOWS\SYSWOW64\nshwfp.dll

2016-10-05 20:22:14 ----A---- C:\WINDOWS\SYSWOW64\ClipboardServer.dll

2016-10-05 20:22:14 ----A---- C:\WINDOWS\SYSWOW64\AppContracts.dll

2016-10-05 20:22:12 ----A---- C:\WINDOWS\SYSWOW64\xpsrchvw.exe

2016-10-05 20:22:12 ----A---- C:\WINDOWS\SYSWOW64\WWanAPI.dll

2016-10-05 20:22:12 ----A---- C:\WINDOWS\SYSWOW64\smphost.dll

2016-10-05 20:22:11 ----A---- C:\WINDOWS\SYSWOW64\wsp\_sr.dll

2016-10-05 20:22:11 ----A---- C:\WINDOWS\SYSWOW64\wsp\_health.dll

2016-10-05 20:22:11 ----A---- C:\WINDOWS\SYSWOW64\wsp\_fs.dll

2016-10-05 20:22:11 ----A---- C:\WINDOWS\SYSWOW64\mispace.dll

2016-10-05 20:22:10 ----A---- C:\WINDOWS\SYSWOW64\wintrust.dll

2016-10-05 20:22:10 ----A---- C:\WINDOWS\SYSWOW64\WindowsCodecs.dll

2016-10-05 20:22:10 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.dll

2016-10-05 20:22:10 ----A---- C:\WINDOWS\SYSWOW64\webio.dll

2016-10-05 20:22:08 ----A---- C:\WINDOWS\SYSWOW64\WwaApi.dll

2016-10-05 20:22:08 ----A---- C:\WINDOWS\SYSWOW64\ws2\_32.dll

2016-10-05 20:22:08 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Input.Inking.dll

2016-10-05 20:22:07 ----A---- C:\WINDOWS\SYSWOW64\WsmSvc.dll

2016-10-05 20:22:07 ----A---- C:\WINDOWS\SYSWOW64\WSManHTTPConfig.exe

2016-10-05 20:22:07 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.Scanners.dll

2016-10-05 20:22:07 ----A---- C:\WINDOWS\SYSWOW64\StoreAgent.dll

2016-10-05 20:22:07 ----A---- C:\WINDOWS\SYSWOW64\InstallAgentUserBroker.exe

2016-10-05 20:22:07 ----A---- C:\WINDOWS\SYSWOW64\InstallAgent.exe

2016-10-05 20:22:06 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Xaml.Phone.dll

2016-10-05 20:22:06 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Xaml.Maps.dll

2016-10-05 20:22:06 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Xaml.InkControls.dll

2016-10-05 20:22:06 ----A---- C:\WINDOWS\SYSWOW64\UIAutomationCore.dll

2016-10-05 20:22:05 ----A---- C:\WINDOWS\SYSWOW64\UserDataTimeUtil.dll

2016-10-05 20:22:04 ----A---- C:\WINDOWS\SYSWOW64\twinui.appcore.dll

2016-10-05 20:22:04 ----A---- C:\WINDOWS\SYSWOW64\twinapi.appcore.dll

2016-10-05 20:22:04 ----A---- C:\WINDOWS\SYSWOW64\TpmCoreProvisioning.dll

2016-10-05 20:22:04 ----A---- C:\WINDOWS\SYSWOW64\SessEnv.dll

2016-10-05 20:22:03 ----A---- C:\WINDOWS\SYSWOW64\LicenseManager.dll

2016-10-05 20:22:02 ----A---- C:\WINDOWS\SYSWOW64\storagewmi.dll

2016-10-05 20:22:01 ----A---- C:\WINDOWS\SYSWOW64\TokenBroker.dll

2016-10-05 20:22:01 ----A---- C:\WINDOWS\SYSWOW64\sppcext.dll

2016-10-05 20:22:00 ----A---- C:\WINDOWS\SYSWOW64\ngccredprov.dll

2016-10-05 20:22:00 ----A---- C:\WINDOWS\SYSWOW64\msv1\_0.dll

2016-10-05 20:22:00 ----A---- C:\WINDOWS\SYSWOW64\cryptngc.dll

2016-10-05 20:21:59 ----A---- C:\WINDOWS\SYSWOW64\Windows.Security.Authentication.Identity.Provider.dll

2016-10-05 20:21:59 ----A---- C:\WINDOWS\SYSWOW64\TempSignedLicenseExchangeTask.dll

2016-10-05 20:21:59 ----A---- C:\WINDOWS\SYSWOW64\LicenseManagerApi.dll

2016-10-05 20:21:58 ----A---- C:\WINDOWS\SYSWOW64\RTMediaFrame.dll

2016-10-05 20:21:58 ----A---- C:\WINDOWS\SYSWOW64\mprdim.dll

2016-10-05 20:21:57 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Playback.MediaPlayer.dll

2016-10-05 20:21:57 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Editing.dll

2016-10-05 20:21:57 ----A---- C:\WINDOWS\SYSWOW64\BackgroundMediaPolicy.dll

2016-10-05 20:21:56 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Playback.BackgroundMediaPlayer.dll

2016-10-05 20:21:56 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.BackgroundMediaPlayback.dll

2016-10-05 20:21:56 ----A---- C:\WINDOWS\SYSWOW64\Windows.Graphics.Printing.3D.dll

2016-10-05 20:21:55 ----A---- C:\WINDOWS\SYSWOW64\wpnapps.dll

2016-10-05 20:21:55 ----A---- C:\WINDOWS\SYSWOW64\Windows.Perception.Stub.dll

2016-10-05 20:21:55 ----A---- C:\WINDOWS\SYSWOW64\Windows.Graphics.Printing.dll

2016-10-05 20:21:55 ----A---- C:\WINDOWS\SYSWOW64\pwrshplugin.dll

2016-10-05 20:21:55 ----A---- C:\WINDOWS\SYSWOW64\PrintDialogs.dll

2016-10-05 20:21:55 ----A---- C:\WINDOWS\SYSWOW64\PlayToReceiver.dll

2016-10-05 20:21:55 ----A---- C:\WINDOWS\SYSWOW64\PlayToManager.dll

2016-10-05 20:21:55 ----A---- C:\WINDOWS\SYSWOW64\PlayToDevice.dll

2016-10-05 20:21:55 ----A---- C:\WINDOWS\SYSWOW64\pdh.dll

2016-10-05 20:21:54 ----A---- C:\WINDOWS\SYSWOW64\oleacc.dll

2016-10-05 20:21:54 ----A---- C:\WINDOWS\SYSWOW64\ntdll.dll

2016-10-05 20:21:54 ----A---- C:\WINDOWS\SYSWOW64\findnetprinters.dll

2016-10-05 20:21:52 ----A---- C:\WINDOWS\SYSWOW64\MSVPXENC.dll

2016-10-05 20:21:52 ----A---- C:\WINDOWS\SYSWOW64\msftedit.dll

2016-10-05 20:21:51 ----A---- C:\WINDOWS\SYSWOW64\mprapi.dll

2016-10-05 20:21:51 ----A---- C:\WINDOWS\SYSWOW64\MiracastReceiver.dll

2016-10-05 20:21:51 ----A---- C:\WINDOWS\SYSWOW64\mfreadwrite.dll

2016-10-05 20:21:51 ----A---- C:\WINDOWS\SYSWOW64\mfplat.dll

2016-10-05 20:21:51 ----A---- C:\WINDOWS\SYSWOW64\mfmpeg2srcsnk.dll

2016-10-05 20:21:49 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Import.dll

2016-10-05 20:21:49 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Audio.dll

2016-10-05 20:21:49 ----A---- C:\WINDOWS\SYSWOW64\odbcconf.dll

2016-10-05 20:21:49 ----A---- C:\WINDOWS\SYSWOW64\mfsvr.dll

2016-10-05 20:21:48 ----A---- C:\WINDOWS\SYSWOW64\windows.storage.dll

2016-10-05 20:21:48 ----A---- C:\WINDOWS\SYSWOW64\MFMediaEngine.dll

2016-10-05 20:21:48 ----A---- C:\WINDOWS\SYSWOW64\mbsmsapi.dll

2016-10-05 20:21:48 ----A---- C:\WINDOWS\SYSWOW64\MbaeApiPublic.dll

2016-10-05 20:21:47 ----A---- C:\WINDOWS\SYSWOW64\LogonController.dll

2016-10-05 20:21:47 ----A---- C:\WINDOWS\SYSWOW64\AboveLockAppHost.dll

2016-10-05 20:21:45 ----A---- C:\WINDOWS\SYSWOW64\Windows.Internal.Bluetooth.dll

2016-10-05 20:21:45 ----A---- C:\WINDOWS\SYSWOW64\InputService.dll

2016-10-05 20:21:45 ----A---- C:\WINDOWS\SYSWOW64\imapi2.dll

2016-10-05 20:21:40 ----A---- C:\WINDOWS\SYSWOW64\Windows.Globalization.dll

2016-10-05 20:21:40 ----A---- C:\WINDOWS\SYSWOW64\Geolocation.dll

2016-10-05 20:21:40 ----A---- C:\WINDOWS\SYSWOW64\gdi32.dll

2016-10-05 20:21:39 ----A---- C:\WINDOWS\SYSWOW64\Windows.Energy.dll

2016-10-05 20:21:39 ----A---- C:\WINDOWS\SYSWOW64\uReFS.dll

2016-10-05 20:21:39 ----A---- C:\WINDOWS\SYSWOW64\gdi32full.dll

2016-10-05 20:21:39 ----A---- C:\WINDOWS\SYSWOW64\explorer.exe

2016-10-05 20:21:39 ----A---- C:\WINDOWS\SYSWOW64\dmenrollengine.dll

2016-10-05 20:21:38 ----A---- C:\WINDOWS\SYSWOW64\Windows.Internal.Management.dll

2016-10-05 20:21:38 ----A---- C:\WINDOWS\SYSWOW64\DolbyDecMFT.dll

2016-10-05 20:21:38 ----A---- C:\WINDOWS\SYSWOW64\dnsapi.dll

2016-10-05 20:21:38 ----A---- C:\WINDOWS\SYSWOW64\DisplayManager.dll

2016-10-05 20:21:38 ----A---- C:\WINDOWS\SYSWOW64\D3DCompiler\_47.dll

2016-10-05 20:21:37 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.WiFiDirect.dll

2016-10-05 20:21:37 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.WiFi.dll

2016-10-05 20:21:37 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.Usb.dll

2016-10-05 20:21:37 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.Radios.dll

2016-10-05 20:21:37 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.Midi.dll

2016-10-05 20:21:37 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.LowLevel.dll

2016-10-05 20:21:37 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.Bluetooth.dll

2016-10-05 20:21:37 ----A---- C:\WINDOWS\SYSWOW64\offlinesam.dll

2016-10-05 20:21:37 ----A---- C:\WINDOWS\SYSWOW64\devenum.dll

2016-10-05 20:21:36 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.SmartCards.dll

2016-10-05 20:21:36 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.SerialCommunication.dll

2016-10-05 20:21:36 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.PointOfService.dll

2016-10-05 20:21:36 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.Picker.dll

2016-10-05 20:21:36 ----A---- C:\WINDOWS\SYSWOW64\Windows.Devices.HumanInterfaceDevice.dll

2016-10-05 20:21:36 ----A---- C:\WINDOWS\SYSWOW64\mfksproxy.dll

2016-10-05 20:21:36 ----A---- C:\WINDOWS\SYSWOW64\dwmapi.dll

2016-10-05 20:21:36 ----A---- C:\WINDOWS\SYSWOW64\DataExchange.dll

2016-10-05 20:21:36 ----A---- C:\WINDOWS\SYSWOW64\d2d1.dll

2016-10-05 20:21:36 ----A---- C:\WINDOWS\SYSWOW64\CryptoWinRT.dll

2016-10-05 20:21:35 ----A---- C:\WINDOWS\SYSWOW64\WinTypes.dll

2016-10-05 20:21:35 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.CredDialogController.dll

2016-10-05 20:21:35 ----A---- C:\WINDOWS\SYSWOW64\credprovslegacy.dll

2016-10-05 20:21:35 ----A---- C:\WINDOWS\SYSWOW64\credprovhost.dll

2016-10-05 20:21:35 ----A---- C:\WINDOWS\SYSWOW64\CredProvDataModel.dll

2016-10-05 20:21:35 ----A---- C:\WINDOWS\SYSWOW64\CoreUIComponents.dll

2016-10-05 20:21:35 ----A---- C:\WINDOWS\SYSWOW64\cdp.dll

2016-10-05 20:21:34 ----A---- C:\WINDOWS\SYSWOW64\Windows.AccountsControl.dll

2016-10-05 20:21:34 ----A---- C:\WINDOWS\SYSWOW64\biwinrt.dll

2016-10-05 20:21:34 ----A---- C:\WINDOWS\SYSWOW64\AudioSes.dll

2016-10-05 20:21:33 ----A---- C:\WINDOWS\SYSWOW64\Windows.ApplicationModel.LockScreen.dll

2016-10-05 20:21:32 ----A---- C:\WINDOWS\SYSWOW64\dlnashext.dll

2016-10-05 20:21:32 ----A---- C:\WINDOWS\SYSWOW64\CoreMessaging.dll

2016-10-05 20:21:32 ----A---- C:\WINDOWS\SYSWOW64\BcastDVRHelper.dll

2016-10-05 20:21:31 ----A---- C:\WINDOWS\SYSWOW64\bcastdvr.exe

2016-10-05 20:17:02 ----A---- C:\WINDOWS\system32\tquery.dll

2016-10-05 20:17:02 ----A---- C:\WINDOWS\system32\SearchProtocolHost.exe

2016-10-05 20:17:02 ----A---- C:\WINDOWS\system32\drivers\vpci.sys

2016-10-05 20:17:01 ----A---- C:\WINDOWS\system32\Windows.Networking.Vpn.dll

2016-10-05 20:17:01 ----A---- C:\WINDOWS\system32\StructuredQuery.dll

2016-10-05 20:17:01 ----A---- C:\WINDOWS\system32\SearchIndexer.exe

2016-10-05 20:17:01 ----A---- C:\WINDOWS\system32\SearchFilterHost.exe

2016-10-05 20:17:01 ----A---- C:\WINDOWS\system32\Search.ProtocolHandler.MAPI2.dll

2016-10-05 20:17:01 ----A---- C:\WINDOWS\system32\mssrch.dll

2016-10-05 20:17:01 ----A---- C:\WINDOWS\system32\mssprxy.dll

2016-10-05 20:17:01 ----A---- C:\WINDOWS\system32\cmintegrator.dll

2016-10-05 20:17:00 ----A---- C:\WINDOWS\system32\Windows.System.UserDeviceAssociation.dll

2016-10-05 20:17:00 ----A---- C:\WINDOWS\system32\Windows.Storage.ApplicationData.dll

2016-10-05 20:17:00 ----A---- C:\WINDOWS\system32\VPNv2CSP.dll

2016-10-05 20:16:59 ----A---- C:\WINDOWS\system32\Windows.Media.Speech.UXRes.dll

2016-10-05 20:16:59 ----A---- C:\WINDOWS\system32\Windows.Media.Speech.dll

2016-10-05 20:16:59 ----A---- C:\WINDOWS\system32\Windows.Media.Ocr.dll

2016-10-05 20:16:58 ----A---- C:\WINDOWS\system32\Windows.Media.FaceAnalysis.dll

2016-10-05 20:16:58 ----A---- C:\WINDOWS\system32\Windows.Gaming.XboxLive.Storage.dll

2016-10-05 20:16:58 ----A---- C:\WINDOWS\system32\Windows.Gaming.Input.dll

2016-10-05 20:16:58 ----A---- C:\WINDOWS\system32\Windows.Devices.Perception.dll

2016-10-05 20:16:58 ----A---- C:\WINDOWS\system32\Windows.ApplicationModel.dll

2016-10-05 20:16:58 ----A---- C:\WINDOWS\system32\Windows.ApplicationModel.Background.SystemEventsBroker.dll

2016-10-05 20:16:58 ----A---- C:\WINDOWS\system32\ffbroker.dll

2016-10-05 20:16:58 ----A---- C:\WINDOWS\system32\drivers\stornvme.sys

2016-10-05 20:16:58 ----A---- C:\WINDOWS\system32\AppContracts.dll

2016-10-05 20:16:56 ----A---- C:\WINDOWS\system32\nshwfp.dll

2016-10-05 20:16:55 ----A---- C:\WINDOWS\system32\Windows.Media.Protection.PlayReady.dll

2016-10-05 20:16:55 ----A---- C:\WINDOWS\system32\drivers\storahci.sys

2016-10-05 20:16:50 ----A---- C:\WINDOWS\system32\XblAuthManager.dll

2016-10-05 20:16:48 ----A---- C:\WINDOWS\system32\xpsrchvw.exe

2016-10-05 20:16:47 ----A---- C:\WINDOWS\system32\WWanAPI.dll

2016-10-05 20:16:47 ----A---- C:\WINDOWS\system32\smphost.dll

2016-10-05 20:16:46 ----A---- C:\WINDOWS\system32\wsp\_sr.dll

2016-10-05 20:16:46 ----A---- C:\WINDOWS\system32\wsp\_health.dll

2016-10-05 20:16:46 ----A---- C:\WINDOWS\system32\wsp\_fs.dll

2016-10-05 20:16:46 ----A---- C:\WINDOWS\system32\wkssvc.dll

2016-10-05 20:16:46 ----A---- C:\WINDOWS\system32\mispace.dll

2016-10-05 20:16:45 ----A---- C:\WINDOWS\system32\wlancfg.dll

2016-10-05 20:16:45 ----A---- C:\WINDOWS\system32\wintrust.dll

2016-10-05 20:16:45 ----A---- C:\WINDOWS\system32\winsrv.dll

2016-10-05 20:16:45 ----A---- C:\WINDOWS\system32\winlogon.exe

2016-10-05 20:16:45 ----A---- C:\WINDOWS\system32\Windows.UI.dll

2016-10-05 20:16:45 ----A---- C:\WINDOWS\system32\ReAgent.dll

2016-10-05 20:16:44 ----A---- C:\WINDOWS\system32\WindowsCodecs.dll

2016-10-05 20:16:44 ----A---- C:\WINDOWS\system32\webio.dll

2016-10-05 20:16:44 ----A---- C:\WINDOWS\system32\WebcamUi.dll

2016-10-05 20:16:42 ----A---- C:\WINDOWS\system32\WsmSvc.dll

2016-10-05 20:16:42 ----A---- C:\WINDOWS\system32\WSManHTTPConfig.exe

2016-10-05 20:16:42 ----A---- C:\WINDOWS\system32\ws2\_32.dll

2016-10-05 20:16:42 ----A---- C:\WINDOWS\system32\Windows.UI.Input.Inking.dll

2016-10-05 20:16:42 ----A---- C:\WINDOWS\system32\Windows.Devices.Scanners.dll

2016-10-05 20:16:41 ----A---- C:\WINDOWS\system32\UIAutomationCore.dll

2016-10-05 20:16:41 ----A---- C:\WINDOWS\system32\StoreAgent.dll

2016-10-05 20:16:41 ----A---- C:\WINDOWS\system32\InstallAgent.exe

2016-10-05 20:16:40 ----A---- C:\WINDOWS\system32\Windows.UI.Xaml.Phone.dll

2016-10-05 20:16:40 ----A---- C:\WINDOWS\system32\Windows.UI.Xaml.Maps.dll

2016-10-05 20:16:40 ----A---- C:\WINDOWS\system32\Windows.UI.Xaml.InkControls.dll

2016-10-05 20:16:37 ----A---- C:\WINDOWS\system32\PimIndexMaintenance.dll

2016-10-05 20:16:36 ----A---- C:\WINDOWS\system32\UserDataTimeUtil.dll

2016-10-05 20:16:36 ----A---- C:\WINDOWS\system32\dsregcmd.exe

2016-10-05 20:16:34 ----A---- C:\WINDOWS\system32\twinui.appcore.dll

2016-10-05 20:16:34 ----A---- C:\WINDOWS\system32\twinapi.appcore.dll

2016-10-05 20:16:34 ----A---- C:\WINDOWS\system32\TpmCoreProvisioning.dll

2016-10-05 20:16:34 ----A---- C:\WINDOWS\system32\tdh.dll

2016-10-05 20:16:33 ----A---- C:\WINDOWS\system32\SessEnv.dll

2016-10-05 20:16:32 ----A---- C:\WINDOWS\system32\systemreset.exe

2016-10-05 20:16:32 ----A---- C:\WINDOWS\system32\ResetEngine.dll

2016-10-05 20:16:32 ----A---- C:\WINDOWS\system32\reseteng.dll

2016-10-05 20:16:32 ----A---- C:\WINDOWS\system32\msctf.dll

2016-10-05 20:16:32 ----A---- C:\WINDOWS\system32\lsm.dll

2016-10-05 20:16:31 ----A---- C:\WINDOWS\system32\SyncSettings.dll

2016-10-05 20:16:31 ----A---- C:\WINDOWS\system32\sbe.dll

2016-10-05 20:16:31 ----A---- C:\WINDOWS\system32\LicenseManager.dll

2016-10-05 20:16:30 ----A---- C:\WINDOWS\system32\storagewmi.dll

2016-10-05 20:16:30 ----A---- C:\WINDOWS\system32\SpeechPal.dll

2016-10-05 20:16:29 ----A---- C:\WINDOWS\system32\drivers\srv2.sys

2016-10-05 20:16:29 ----A---- C:\WINDOWS\system32\drivers\mrxsmb20.sys

2016-10-05 20:16:28 ----A---- C:\WINDOWS\system32\SharedStartModel.dll

2016-10-05 20:16:28 ----A---- C:\WINDOWS\system32\Family.Client.dll

2016-10-05 20:16:27 ----A---- C:\WINDOWS\system32\SensorService.dll

2016-10-05 20:16:26 ----A---- C:\WINDOWS\system32\Windows.Security.Authentication.Web.Core.dll

2016-10-05 20:16:26 ----A---- C:\WINDOWS\system32\TokenBroker.dll

2016-10-05 20:16:26 ----A---- C:\WINDOWS\system32\sppsvc.exe

2016-10-05 20:16:26 ----A---- C:\WINDOWS\system32\Sens.dll

2016-10-05 20:16:26 ----A---- C:\WINDOWS\system32\nltest.exe

2016-10-05 20:16:26 ----A---- C:\WINDOWS\system32\EditionUpgradeManagerObj.dll

2016-10-05 20:16:25 ----A---- C:\WINDOWS\system32\sppcext.dll

2016-10-05 20:16:25 ----A---- C:\WINDOWS\system32\NgcCtnr.dll

2016-10-05 20:16:25 ----A---- C:\WINDOWS\system32\ngccredprov.dll

2016-10-05 20:16:25 ----A---- C:\WINDOWS\system32\msv1\_0.dll

2016-10-05 20:16:25 ----A---- C:\WINDOWS\system32\manage-bde.exe

2016-10-05 20:16:25 ----A---- C:\WINDOWS\system32\LsaIso.exe

2016-10-05 20:16:25 ----A---- C:\WINDOWS\system32\fveui.dll

2016-10-05 20:16:25 ----A---- C:\WINDOWS\system32\bdeunlock.exe

2016-10-05 20:16:25 ----A---- C:\WINDOWS\system32\bdeui.dll

2016-10-05 20:16:24 ----A---- C:\WINDOWS\system32\fvenotify.exe

2016-10-05 20:16:24 ----A---- C:\WINDOWS\system32\fveapibase.dll

2016-10-05 20:16:24 ----A---- C:\WINDOWS\system32\fveapi.dll

2016-10-05 20:16:24 ----A---- C:\WINDOWS\system32\bdesvc.dll

2016-10-05 20:16:23 ----A---- C:\WINDOWS\system32\sppobjs.dll

2016-10-05 20:16:23 ----A---- C:\WINDOWS\system32\BitLockerDeviceEncryption.exe

2016-10-05 20:16:23 ----A---- C:\WINDOWS\system32\aadcloudap.dll

2016-10-05 20:16:22 ----A---- C:\WINDOWS\system32\spaceman.exe

2016-10-05 20:16:22 ----A---- C:\WINDOWS\system32\SpaceControl.dll

2016-10-05 20:16:22 ----A---- C:\WINDOWS\system32\OneBackupHandler.dll

2016-10-05 20:16:22 ----A---- C:\WINDOWS\system32\drivers\fvevol.sys

2016-10-05 20:16:21 ----A---- C:\WINDOWS\system32\SystemSettings.DeviceEncryptionHandlers.dll

2016-10-05 20:16:21 ----A---- C:\WINDOWS\system32\SettingsHandlers\_Flights.dll

2016-10-05 20:16:21 ----A---- C:\WINDOWS\system32\NgcCtnrGidsHandler.dll

2016-10-05 20:16:21 ----A---- C:\WINDOWS\system32\fvewiz.dll

2016-10-05 20:16:21 ----A---- C:\WINDOWS\system32\fvecpl.dll

2016-10-05 20:16:20 ----A---- C:\WINDOWS\system32\Family.SyncEngine.dll

2016-10-05 20:16:20 ----A---- C:\WINDOWS\system32\Family.Authentication.dll

2016-10-05 20:16:20 ----A---- C:\WINDOWS\system32\easwrt.dll

2016-10-05 20:16:18 ----A---- C:\WINDOWS\system32\SpaceAgent.exe

2016-10-05 20:16:17 ----A---- C:\WINDOWS\system32\Windows.Security.Authentication.Identity.Provider.dll

2016-10-05 20:16:17 ----A---- C:\WINDOWS\system32\sppwinob.dll

2016-10-05 20:16:17 ----A---- C:\WINDOWS\system32\RDXTaskFactory.dll

2016-10-05 20:16:15 ----A---- C:\WINDOWS\system32\RTMediaFrame.dll

2016-10-05 20:16:15 ----A---- C:\WINDOWS\system32\RMapi.dll

2016-10-05 20:16:15 ----A---- C:\WINDOWS\system32\RelPost.exe

2016-10-05 20:16:15 ----A---- C:\WINDOWS\system32\PsmServiceExtHost.dll

2016-10-05 20:16:15 ----A---- C:\WINDOWS\system32\drivers\rdbss.sys

2016-10-05 20:16:14 ----A---- C:\WINDOWS\system32\rdpudd.dll

2016-10-05 20:16:14 ----A---- C:\WINDOWS\system32\rasmans.dll

2016-10-05 20:16:14 ----A---- C:\WINDOWS\system32\rascustom.dll

2016-10-05 20:16:14 ----A---- C:\WINDOWS\system32\mprdim.dll

2016-10-05 20:16:14 ----A---- C:\WINDOWS\system32\mprddm.dll

2016-10-05 20:16:13 ----A---- C:\WINDOWS\system32\Windows.Media.Playback.MediaPlayer.dll

2016-10-05 20:16:13 ----A---- C:\WINDOWS\system32\Windows.Media.Playback.BackgroundMediaPlayer.dll

2016-10-05 20:16:13 ----A---- C:\WINDOWS\system32\Windows.Media.Editing.dll

2016-10-05 20:16:13 ----A---- C:\WINDOWS\system32\Windows.Media.BackgroundMediaPlayback.dll

2016-10-05 20:16:13 ----A---- C:\WINDOWS\system32\BackgroundMediaPolicy.dll

2016-10-05 20:16:12 ----A---- C:\WINDOWS\system32\RDXService.dll

2016-10-05 20:16:12 ----A---- C:\WINDOWS\system32\qedit.dll

2016-10-05 20:16:12 ----A---- C:\WINDOWS\system32\provops.dll

2016-10-05 20:16:12 ----A---- C:\WINDOWS\system32\profsvc.dll

2016-10-05 20:16:11 ----A---- C:\WINDOWS\system32\Windows.Graphics.Printing.dll

2016-10-05 20:16:11 ----A---- C:\WINDOWS\system32\Windows.Graphics.Printing.3D.dll

2016-10-05 20:16:11 ----A---- C:\WINDOWS\system32\usbmon.dll

2016-10-05 20:16:11 ----A---- C:\WINDOWS\system32\spoolsv.exe

2016-10-05 20:16:11 ----A---- C:\WINDOWS\system32\PrintWSDAHost.dll

2016-10-05 20:16:11 ----A---- C:\WINDOWS\system32\PlayToReceiver.dll

2016-10-05 20:16:11 ----A---- C:\WINDOWS\splwow64.exe

2016-10-05 20:16:10 ----A---- C:\WINDOWS\system32\wpnapps.dll

2016-10-05 20:16:10 ----A---- C:\WINDOWS\system32\Windows.Perception.Stub.dll

2016-10-05 20:16:10 ----A---- C:\WINDOWS\system32\PlayToManager.dll

2016-10-05 20:16:10 ----A---- C:\WINDOWS\system32\PlayToDevice.dll

2016-10-05 20:16:10 ----A---- C:\WINDOWS\system32\drivers\partmgr.sys

2016-10-05 20:16:09 ----A---- C:\WINDOWS\system32\pwrshplugin.dll

2016-10-05 20:16:09 ----A---- C:\WINDOWS\system32\pdh.dll

2016-10-05 20:16:09 ----A---- C:\WINDOWS\system32\localspl.dll

2016-10-05 20:16:08 ----A---- C:\WINDOWS\system32\puiobj.dll

2016-10-05 20:16:07 ----A---- C:\WINDOWS\system32\ntdll.dll

2016-10-05 20:16:06 ----A---- C:\WINDOWS\system32\NfcRadioMedia.dll

2016-10-05 20:16:06 ----A---- C:\WINDOWS\system32\NetworkUXBroker.dll

2016-10-05 20:16:06 ----A---- C:\WINDOWS\system32\nettrace.dll

2016-10-05 20:16:05 ----A---- C:\WINDOWS\system32\NaturalLanguage6.dll

2016-10-05 20:16:05 ----A---- C:\WINDOWS\system32\drivers\WdiWiFi.sys

2016-10-05 20:16:04 ----A---- C:\WINDOWS\system32\MSVPXENC.dll

2016-10-05 20:16:04 ----A---- C:\WINDOWS\system32\MSVideoDSP.dll

2016-10-05 20:16:03 ----A---- C:\WINDOWS\system32\SensorsApi.dll

2016-10-05 20:16:03 ----A---- C:\WINDOWS\system32\msftedit.dll

2016-10-05 20:16:03 ----A---- C:\WINDOWS\system32\MSAudDecMFT.dll

2016-10-05 20:16:03 ----A---- C:\WINDOWS\system32\MSAC3ENC.DLL

2016-10-05 20:16:03 ----A---- C:\WINDOWS\system32\mprapi.dll

2016-10-05 20:16:03 ----A---- C:\WINDOWS\system32\modernexecserver.dll

2016-10-05 20:16:03 ----A---- C:\WINDOWS\system32\MiracastReceiver.dll

2016-10-05 20:16:01 ----A---- C:\WINDOWS\system32\mfreadwrite.dll

2016-10-05 20:16:01 ----A---- C:\WINDOWS\system32\mfplat.dll

2016-10-05 20:16:00 ----A---- C:\WINDOWS\system32\mfmpeg2srcsnk.dll

2016-10-05 20:16:00 ----A---- C:\WINDOWS\system32\mfmp4srcsnk.dll

2016-10-05 20:15:59 ----A---- C:\WINDOWS\system32\wmpps.dll

2016-10-05 20:15:59 ----A---- C:\WINDOWS\system32\mfsvr.dll

2016-10-05 20:15:58 ----A---- C:\WINDOWS\system32\Windows.Media.Streaming.dll

2016-10-05 20:15:58 ----A---- C:\WINDOWS\system32\Windows.Media.Import.dll

2016-10-05 20:15:58 ----A---- C:\WINDOWS\system32\Windows.Media.Devices.dll

2016-10-05 20:15:58 ----A---- C:\WINDOWS\system32\Windows.Media.Audio.dll

2016-10-05 20:15:58 ----A---- C:\WINDOWS\system32\odbcconf.dll

2016-10-05 20:15:58 ----A---- C:\WINDOWS\system32\AccountsRt.dll

2016-10-05 20:15:56 ----A---- C:\WINDOWS\system32\windows.storage.dll

2016-10-05 20:15:56 ----A---- C:\WINDOWS\system32\MFMediaEngine.dll

2016-10-05 20:15:56 ----A---- C:\WINDOWS\system32\mbsmsapi.dll

2016-10-05 20:15:56 ----A---- C:\WINDOWS\system32\MbaeApiPublic.dll

2016-10-05 20:15:55 ----A---- C:\WINDOWS\system32\drivers\dxgmms2.sys

2016-10-05 20:15:55 ----A---- C:\WINDOWS\system32\drivers\dxgmms1.sys

2016-10-05 20:15:55 ----A---- C:\WINDOWS\system32\appinfo.dll

2016-10-05 20:15:54 ----A---- C:\WINDOWS\system32\LogonController.dll

2016-10-05 20:15:54 ----A---- C:\WINDOWS\system32\drivers\dxgkrnl.sys

2016-10-05 20:15:54 ----A---- C:\WINDOWS\system32\AboveLockAppHost.dll

2016-10-05 20:15:52 ----A---- C:\WINDOWS\system32\Windows.Internal.Bluetooth.dll

2016-10-05 20:15:52 ----A---- C:\WINDOWS\system32\imapi2.dll

2016-10-05 20:15:49 ----A---- C:\WINDOWS\system32\ieproxy.dll

2016-10-05 20:15:48 ----A---- C:\WINDOWS\system32\iedkcs32.dll

2016-10-05 20:15:47 ----A---- C:\WINDOWS\system32\NetworkCollectionAgent.dll

2016-10-05 20:15:43 ----A---- C:\WINDOWS\system32\drivers\http.sys

2016-10-05 20:15:42 ----A---- C:\WINDOWS\system32\Windows.Globalization.dll

2016-10-05 20:15:42 ----A---- C:\WINDOWS\system32\hal.dll

2016-10-05 20:15:42 ----A---- C:\WINDOWS\system32\gpsvc.dll

2016-10-05 20:15:42 ----A---- C:\WINDOWS\system32\Geolocation.dll

2016-10-05 20:15:41 ----A---- C:\WINDOWS\system32\gdi32full.dll

2016-10-05 20:15:41 ----A---- C:\WINDOWS\system32\gdi32.dll

2016-10-05 20:15:41 ----A---- C:\WINDOWS\system32\fhcfg.dll

2016-10-05 20:15:39 ----A---- C:\WINDOWS\system32\resutils.dll

2016-10-05 20:15:39 ----A---- C:\WINDOWS\system32\clusapi.dll

2016-10-05 20:15:37 ----A---- C:\WINDOWS\system32\uReFS.dll

2016-10-05 20:15:36 ----A---- C:\WINDOWS\system32\WpAXHolder.dll

2016-10-05 20:15:36 ----A---- C:\WINDOWS\system32\Windows.Energy.dll

2016-10-05 20:15:36 ----A---- C:\WINDOWS\system32\wevtsvc.dll

2016-10-05 20:15:36 ----A---- C:\WINDOWS\system32\enrollmentapi.dll

2016-10-05 20:15:36 ----A---- C:\WINDOWS\system32\dmenrollengine.dll

2016-10-05 20:15:36 ----A---- C:\WINDOWS\explorer.exe

2016-10-05 20:15:35 ----A---- C:\WINDOWS\system32\Windows.Internal.Management.dll

2016-10-05 20:15:35 ----A---- C:\WINDOWS\system32\DolbyDecMFT.dll

2016-10-05 20:15:35 ----A---- C:\WINDOWS\system32\dnsapi.dll

2016-10-05 20:15:34 ----A---- C:\WINDOWS\system32\DisplayManager.dll

2016-10-05 20:15:34 ----A---- C:\WINDOWS\system32\D3DCompiler\_47.dll

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\Windows.Devices.WiFiDirect.dll

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\Windows.Devices.WiFi.dll

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\Windows.Devices.Usb.dll

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\Windows.Devices.Radios.dll

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\Windows.Devices.Printers.dll

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\Windows.Devices.Midi.dll

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\Windows.Devices.LowLevel.dll

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\Windows.Devices.Bluetooth.dll

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\samsrv.dll

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\offlinesam.dll

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\DeviceCensus.exe

2016-10-05 20:15:33 ----A---- C:\WINDOWS\system32\devenum.dll

2016-10-05 20:15:32 ----A---- C:\WINDOWS\system32\Windows.Devices.HumanInterfaceDevice.dll

2016-10-05 20:15:32 ----A---- C:\WINDOWS\system32\Windows.Data.Pdf.dll

2016-10-05 20:15:32 ----A---- C:\WINDOWS\system32\setupugc.exe

2016-10-05 20:15:32 ----A---- C:\WINDOWS\system32\discan.dll

2016-10-05 20:15:32 ----A---- C:\WINDOWS\system32\DataExchange.dll

2016-10-05 20:15:32 ----A---- C:\WINDOWS\system32\d2d1.dll

2016-10-05 20:15:31 ----A---- C:\WINDOWS\system32\Windows.Devices.SmartCards.Phone.dll

2016-10-05 20:15:31 ----A---- C:\WINDOWS\system32\Windows.Devices.PointOfService.dll

2016-10-05 20:15:31 ----A---- C:\WINDOWS\system32\mfksproxy.dll

2016-10-05 20:15:31 ----A---- C:\WINDOWS\system32\FontProvider.dll

2016-10-05 20:15:31 ----A---- C:\WINDOWS\system32\dwmapi.dll

2016-10-05 20:15:30 ----A---- C:\WINDOWS\system32\Windows.Devices.SmartCards.dll

2016-10-05 20:15:30 ----A---- C:\WINDOWS\system32\Windows.Devices.Picker.dll

2016-10-05 20:15:30 ----A---- C:\WINDOWS\system32\enterprisecsps.dll

2016-10-05 20:15:29 ----A---- C:\WINDOWS\system32\Windows.UI.CredDialogController.dll

2016-10-05 20:15:29 ----A---- C:\WINDOWS\system32\Windows.Devices.SerialCommunication.dll

2016-10-05 20:15:29 ----A---- C:\WINDOWS\system32\CryptoWinRT.dll

2016-10-05 20:15:29 ----A---- C:\WINDOWS\system32\credprovhost.dll

2016-10-05 20:15:28 ----A---- C:\WINDOWS\system32\generaltel.dll

2016-10-05 20:15:28 ----A---- C:\WINDOWS\system32\CPFilters.dll

2016-10-05 20:15:28 ----A---- C:\WINDOWS\system32\CoreUIComponents.dll

2016-10-05 20:15:28 ----A---- C:\WINDOWS\system32\ConsoleLogon.dll

2016-10-05 20:15:28 ----A---- C:\WINDOWS\system32\CompatTelRunner.exe

2016-10-05 20:15:28 ----A---- C:\WINDOWS\system32\appraiser.dll

2016-10-05 20:15:27 ----A---- C:\WINDOWS\system32\WinTypes.dll

2016-10-05 20:15:27 ----A---- C:\WINDOWS\system32\CloudExperienceHostBroker.dll

2016-10-05 20:15:27 ----A---- C:\WINDOWS\system32\ci.dll

2016-10-05 20:15:27 ----A---- C:\WINDOWS\system32\cdpusersvc.dll

2016-10-05 20:15:27 ----A---- C:\WINDOWS\system32\cdpsvc.dll

2016-10-05 20:15:27 ----A---- C:\WINDOWS\system32\cdp.dll

2016-10-05 20:15:27 ----A---- C:\WINDOWS\system32\CastLaunch.dll

2016-10-05 20:15:19 ----A---- C:\WINDOWS\system32\drivers\wcifs.sys

2016-10-05 20:15:19 ----A---- C:\WINDOWS\system32\drivers\cmimcext.sys

2016-10-05 20:15:19 ----A---- C:\WINDOWS\system32\credprovslegacy.dll

2016-10-05 20:15:19 ----A---- C:\WINDOWS\system32\ContentDeliveryManager.Utilities.dll

2016-10-05 20:15:19 ----A---- C:\WINDOWS\system32\comsvcs.dll

2016-10-05 20:15:17 ----A---- C:\WINDOWS\system32\Windows.Cortana.Desktop.dll

2016-10-05 20:15:17 ----A---- C:\WINDOWS\system32\qmgr.dll

2016-10-05 20:15:17 ----A---- C:\WINDOWS\system32\BthRadioMedia.dll

2016-10-05 20:15:17 ----A---- C:\WINDOWS\system32\browserbroker.dll

2016-10-05 20:15:17 ----A---- C:\WINDOWS\system32\bootux.dll

2016-10-05 20:15:17 ----A---- C:\WINDOWS\system32\BootMenuUX.dll

2016-10-05 20:15:17 ----A---- C:\WINDOWS\system32\bisrv.dll

2016-10-05 20:15:13 ----A---- C:\WINDOWS\system32\biwinrt.dll

2016-10-05 20:15:12 ----A---- C:\WINDOWS\system32\Windows.Media.MediaControl.dll

2016-10-05 20:15:12 ----A---- C:\WINDOWS\system32\SndVolSSO.dll

2016-10-05 20:15:12 ----A---- C:\WINDOWS\system32\audiosrv.dll

2016-10-05 20:15:11 ----A---- C:\WINDOWS\system32\AudioSes.dll

2016-10-05 20:15:11 ----A---- C:\WINDOWS\system32\ACPBackgroundManagerPolicy.dll

2016-10-05 20:15:10 ----A---- C:\WINDOWS\system32\rshx32.dll

2016-10-05 20:15:09 ----A---- C:\WINDOWS\system32\Windows.AccountsControl.dll

2016-10-05 20:15:09 ----A---- C:\WINDOWS\system32\devinv.dll

2016-10-05 20:15:09 ----A---- C:\WINDOWS\system32\aeinv.dll

2016-10-05 20:15:08 ----A---- C:\WINDOWS\system32\Windows.ApplicationModel.LockScreen.dll

2016-10-05 20:15:06 ----A---- C:\WINDOWS\system32\usermgr.dll

2016-10-05 20:15:06 ----A---- C:\WINDOWS\system32\deviceaccess.dll

2016-10-05 20:15:06 ----A---- C:\WINDOWS\system32\AppReadiness.dll

2016-10-05 20:15:05 ----A---- C:\WINDOWS\system32\skci.dll

2016-10-05 20:15:05 ----A---- C:\WINDOWS\system32\securekernel.exe

2016-10-05 20:15:05 ----A---- C:\WINDOWS\system32\NotificationController.dll

2016-10-05 20:15:05 ----A---- C:\WINDOWS\system32\drivers\winhvr.sys

2016-10-05 20:15:05 ----A---- C:\WINDOWS\system32\CoreMessaging.dll

2016-10-05 20:15:02 ----A---- C:\WINDOWS\system32\vmrdvcore.dll

2016-10-05 20:15:01 ----A---- C:\WINDOWS\system32\hvloader.exe

2016-10-05 20:15:01 ----A---- C:\WINDOWS\system32\hvix64.exe

2016-10-05 20:15:01 ----A---- C:\WINDOWS\system32\hvax64.exe

2016-10-05 20:15:00 ----A---- C:\WINDOWS\system32\icsvcext.dll

2016-10-05 20:15:00 ----A---- C:\WINDOWS\system32\icsvc.dll

2016-10-05 20:15:00 ----A---- C:\WINDOWS\system32\ClipUp.exe

2016-10-05 20:14:54 ----A---- C:\WINDOWS\system32\drivers\tpm.sys

2016-10-05 20:14:54 ----A---- C:\WINDOWS\system32\drivers\spaceport.sys

2016-10-05 20:14:54 ----A---- C:\WINDOWS\system32\drivers\pci.sys

2016-10-05 20:14:54 ----A---- C:\WINDOWS\system32\drivers\kbdhid.sys

2016-09-30 07:01:12 ----A---- C:\WINDOWS\system32\CcavGuard64.dll

2016-09-30 07:01:06 ----A---- C:\WINDOWS\SYSWOW64\CcavGuard32.dll

2016-09-30 07:00:48 ----A---- C:\WINDOWS\system32\drivers\CmdCCAV.sys

2016-09-28 21:40:55 ----D---- C:\Users\kinderen\AppData\Roaming\Sun

2016-09-28 21:36:58 ----A---- C:\WINDOWS\SYSWOW64\WindowsAccessBridge-32.dll

2016-09-28 21:36:26 ----D---- C:\ProgramData\Oracle

2016-09-28 21:36:20 ----D---- C:\Program Files (x86)\Java

2016-09-27 01:02:25 ----AD---- C:\Program Files (x86)\Mozilla Firefox

2016-09-25 17:31:34 ----D---- C:\ProgramData\Microsoft OneDrive

2016-09-25 17:28:58 ----D---- C:\ProgramData\USOShared

2016-09-24 05:31:29 ----DC---- C:\WINDOWS\Panther

2016-09-24 05:09:09 ----A---- C:\WINDOWS\SYSWOW64\winmde.dll

2016-09-24 05:09:09 ----A---- C:\WINDOWS\SYSWOW64\SettingSyncPolicy.dll

2016-09-24 05:09:09 ----A---- C:\WINDOWS\SYSWOW64\SettingSync.dll

2016-09-24 05:09:09 ----A---- C:\WINDOWS\SYSWOW64\msmpeg2vdec.dll

2016-09-24 05:09:09 ----A---- C:\WINDOWS\SYSWOW64\jsproxy.dll

2016-09-24 05:09:09 ----A---- C:\WINDOWS\SYSWOW64\hevcdecoder.dll

2016-09-24 05:09:09 ----A---- C:\WINDOWS\SYSWOW64\GamePanel.exe

2016-09-24 05:09:09 ----A---- C:\WINDOWS\SYSWOW64\CloudBackupSettings.dll

2016-09-24 05:09:09 ----A---- C:\WINDOWS\system32\msmpeg2vdec.dll

2016-09-24 05:09:09 ----A---- C:\WINDOWS\system32\hevcdecoder.dll

2016-09-24 05:09:09 ----A---- C:\WINDOWS\system32\encapi.dll

2016-09-24 05:09:09 ----A---- C:\WINDOWS\system32\CloudBackupSettings.dll

2016-09-24 05:08:56 ----A---- C:\WINDOWS\SYSWOW64\mfsrcsnk.dll

2016-09-24 05:08:56 ----A---- C:\WINDOWS\SYSWOW64\mfps.dll

2016-09-24 05:08:56 ----A---- C:\WINDOWS\SYSWOW64\mfmp4srcsnk.dll

2016-09-24 05:08:56 ----A---- C:\WINDOWS\system32\mfsrcsnk.dll

2016-09-24 05:08:56 ----A---- C:\WINDOWS\system32\mfnetsrc.dll

2016-09-24 05:08:56 ----A---- C:\WINDOWS\system32\MFCaptureEngine.dll

2016-09-24 05:08:54 ----A---- C:\WINDOWS\SYSWOW64\FSClient.dll

2016-09-24 05:08:53 ----A---- C:\WINDOWS\system32\FSClient.dll

2016-09-24 05:08:52 ----A---- C:\WINDOWS\SYSWOW64\wmpmde.dll

2016-09-24 05:08:52 ----A---- C:\WINDOWS\SYSWOW64\WebcamUi.dll

2016-09-24 05:08:52 ----A---- C:\WINDOWS\system32\wwansvc.dll

2016-09-24 05:08:52 ----A---- C:\WINDOWS\system32\wwanprotdim.dll

2016-09-24 05:08:52 ----A---- C:\WINDOWS\system32\wwanmm.dll

2016-09-24 05:08:52 ----A---- C:\WINDOWS\system32\wwanconn.dll

2016-09-24 05:08:52 ----A---- C:\WINDOWS\system32\wmpmde.dll

2016-09-24 05:08:52 ----A---- C:\WINDOWS\system32\SettingSyncPolicy.dll

2016-09-24 05:08:52 ----A---- C:\WINDOWS\system32\SettingSync.dll

2016-09-24 05:08:52 ----A---- C:\WINDOWS\system32\drivers\srv.sys

2016-09-24 05:08:52 ----A---- C:\WINDOWS\system32\drivers\mrxsmb10.sys

2016-09-24 05:08:51 ----A---- C:\WINDOWS\SYSWOW64\wlanhlp.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\SYSWOW64\wlanapi.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\SYSWOW64\wfdprov.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\SYSWOW64\eappprxy.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\SYSWOW64\eapphost.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\SYSWOW64\eappgnui.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\SYSWOW64\eappcfg.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\SYSWOW64\eapp3hst.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\wpninprc.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\wlansvcpal.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\wlansvc.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\wlansec.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\wlanmsm.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\wlanhlp.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\wlanapi.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\wifiprofilessettinghandler.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\WiFiConfigSP.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\wfdprov.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\rdpcorets.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\drivers\pdc.sys

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\drivers\FWPKCLNT.SYS

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\deviceassociation.dll

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\dasHost.exe

2016-09-24 05:08:51 ----A---- C:\WINDOWS\system32\das.dll

2016-09-24 05:08:50 ----A---- C:\WINDOWS\SYSWOW64\WMPDMC.exe

2016-09-24 05:08:50 ----A---- C:\WINDOWS\SYSWOW64\evr.dll

2016-09-24 05:08:50 ----A---- C:\WINDOWS\system32\wmploc.DLL

2016-09-24 05:08:50 ----A---- C:\WINDOWS\system32\WMPDMC.exe

2016-09-24 05:08:50 ----A---- C:\WINDOWS\system32\spwmp.dll

2016-09-24 05:08:50 ----A---- C:\WINDOWS\system32\pnidui.dll

2016-09-24 05:08:50 ----A---- C:\WINDOWS\system32\evr.dll

2016-09-24 05:08:50 ----A---- C:\WINDOWS\system32\dxmasf.dll

2016-09-24 05:08:50 ----A---- C:\WINDOWS\system32\dlnashext.dll

2016-09-24 05:08:49 ----A---- C:\WINDOWS\SYSWOW64\wmploc.DLL

2016-09-24 05:08:49 ----A---- C:\WINDOWS\SYSWOW64\spwmp.dll

2016-09-24 05:08:49 ----A---- C:\WINDOWS\SYSWOW64\dxmasf.dll

2016-09-24 05:08:48 ----A---- C:\WINDOWS\SYSWOW64\jscript9diag.dll

2016-09-24 05:08:48 ----A---- C:\WINDOWS\system32\jscript9diag.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\SYSWOW64\Windows.Internal.UI.Logon.ProxyStub.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\SYSWOW64\mshtmled.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\SYSWOW64\indexeddbserver.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\SYSWOW64\iesetup.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\SYSWOW64\iernonce.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\SYSWOW64\ieapfltr.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\SYSWOW64\Chakrathunk.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\sspicli.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\rpcrt4.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\mshtmled.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\lsass.exe

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\indexeddbserver.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\iesetup.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\iernonce.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\ieapfltr.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\ie4uinit.exe

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\drivers\ntfs.sys

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\drivers\ksecdd.sys

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\drivers\Classpnp.sys

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\csrsrv.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\Chakrathunk.dll

2016-09-24 05:08:47 ----A---- C:\WINDOWS\system32\Chakradiag.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Immersive.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\Windows.Shell.Search.UriHandler.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\usercpl.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\tcpipcfg.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\sspicli.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\sppc.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\slcext.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\slc.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\rpcrt4.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\resutils.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\ole32.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\netiougc.exe

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\LockAppHost.exe

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\LaunchWinApp.exe

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\DscCoreConfProv.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\authui.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\SYSWOW64\aclui.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\system32\tsmf.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\system32\NetworkMobileSettings.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\system32\msxml6r.dll

2016-09-24 05:08:39 ----A---- C:\WINDOWS\system32\mstsc.exe

2016-09-24 05:08:39 ----A---- C:\WINDOWS\system32\drivers\srvnet.sys

2016-09-24 05:08:39 ----A---- C:\WINDOWS\system32\drivers\mrxsmb.sys

2016-09-24 05:08:39 ----A---- C:\WINDOWS\system32\acmigration.dll

2016-09-24 05:08:31 ----A---- C:\WINDOWS\system32\SettingsHandlers\_WorkAccess.dll

2016-09-24 05:08:30 ----A---- C:\WINDOWS\system32\usercpl.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\SYSWOW64\pidgenx.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\Windows.UI.Shell.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\Windows.UI.Immersive.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\Windows.Shell.Search.UriHandler.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\Windows.Management.Provisioning.ProxyStub.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\Windows.Internal.UI.Logon.ProxyStub.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\wifitask.exe

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\wifinetworkmanager.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\wificonnapi.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\w32time.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\tcpipcfg.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\SystemSettingsThresholdAdminFlowUI.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\SystemSettingsAdminFlows.exe

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\SysResetErr.exe

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\StorSvc.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\StorageUsage.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\sppc.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\slcext.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\slc.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\SensorDataService.exe

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\ResetEngine.exe

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\RemovableMediaProvisioningPlugin.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\provtool.exe

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\ProvPluginEng.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\provisioningcsp.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\provhandlers.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\provengine.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\provdatastore.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\pidgenx.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\PhoneServiceRes.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\PhoneService.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\PhoneProviders.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\ole32.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\NFCProvisioningPlugin.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\netiougc.exe

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\MediaFoundation.DefaultPerceptionProvider.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\LockAppHost.exe

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\LaunchWinApp.exe

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\KnobsCsp.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\KnobsCore.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\jsproxy.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\invagent.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\IdCtrls.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\GenValObj.exe

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\EncDec.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\drivers\dam.sys

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\dosvc.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\domgmt.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\DeveloperOptionsSettingsHandlers.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\DataSenseHandlers.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\CredProvDataModel.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\C\_IS2022.DLL

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\c\_GSM7.DLL

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\C\_G18030.DLL

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\bcastdvr.exe

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\BarcodeProvisioningPlugin.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\authui.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\AppXApplicabilityBlob.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\AppCapture.dll

2016-09-24 05:08:29 ----A---- C:\WINDOWS\system32\aclui.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\WWAHost.exe

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Cred.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.BlockedShutdown.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.BioFeedback.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\Windows.Media.Streaming.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\Windows.ApplicationModel.Store.TestingFramework.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\VCardParser.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\UserDataTypeHelperUtil.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\UserDataPlatformHelperUtil.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\UserDataLanguageUtil.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\UserDataAccessRes.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\POSyncServices.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\PhoneutilRes.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\Phoneutil.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\NmaDirect.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\mfpmp.exe

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\mf.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\MapRouter.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\ExtrasXmlParser.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\ExSMime.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\ContactActivation.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\AppointmentActivation.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\SYSWOW64\AddressParser.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\XamlTileRender.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\WWAHost.exe

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\wuuhext.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\wups2.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\wuaueng.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\wuauclt.exe

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\winmde.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\Windows.UI.Cred.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\Windows.UI.BlockedShutdown.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\Windows.UI.BioFeedback.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\Windows.ApplicationModel.Store.TestingFramework.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\WinBioDataModelOOBE.exe

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\WinBioDataModel.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\VCardParser.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\usocore.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\UserDataTypeHelperUtil.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\UserDataPlatformHelperUtil.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\UserDataLanguageUtil.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\UserDataAccessRes.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\updatepolicy.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\shutdownux.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\SettingsHandlers\_Bluetooth.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\POSyncServices.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\PhoneutilRes.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\Phoneutil.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\MusUpdateHandlers.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\MusNotification.exe

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\mfpmp.exe

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\mf.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\MDEServer.exe

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\LicenseManagerSvc.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\InstallAgentUserBroker.exe

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\ExtrasXmlParser.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\ExSMime.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\DscCoreConfProv.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\DscCore.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\DMRServer.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\DbgModel.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\dbgeng.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\dafpos.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\ContactActivation.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\AppointmentActivation.dll

2016-09-24 05:08:25 ----A---- C:\WINDOWS\system32\AddressParser.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\user32.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\NMAA.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\MosStorage.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\MosResource.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\MosHostClient.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\Microsoft-Windows-MosTrace.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\Microsoft-Windows-MosHost.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\Microsoft-Windows-MapControls.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\MapsBtSvc.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\MapGeocoder.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\MapControlStringsRes.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\MapControlCore.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\MapConfiguration.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\JpMapControl.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\D3D12.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\BingOnlineServices.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\SYSWOW64\BingMaps.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\win32u.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\win32k.sys

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\user32.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\NmaDirect.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\NMAA.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\nativemap.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MosStorage.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MosResource.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\moshostcore.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MosHostClient.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\moshost.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\Microsoft-Windows-MosTrace.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\Microsoft-Windows-MosHost.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\Microsoft-Windows-MapControls.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\mapsupdatetask.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\mapstoasttask.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MapsStore.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MapsCSP.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MapsBtSvcProxy.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MapsBtSvc.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MapRouter.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MapGeocoder.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MapControlStringsRes.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MapControlCore.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\MapConfiguration.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\kdhvcom.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\JpMapControl.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\InputService.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\drivers\hvservice.sys

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\D3D12.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\cdd.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\BingOnlineServices.dll

2016-09-24 05:08:09 ----A---- C:\WINDOWS\system32\BingMaps.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Xaml.Resources.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\Windows.UI.Xaml.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\wincorlib.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\win32u.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\win32k.sys

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\wevtapi.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\updatepolicy.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\tzres.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\storagewmi\_passthru.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\SettingSyncHost.exe

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\SettingSyncCore.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\schannel.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\samlib.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\qdvd.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\OneDriveSettingSyncProvider.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\oleaut32.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\offlinelsa.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\msxml6r.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\MSAJApi.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\kerberos.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\encapi.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\dwmcore.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\DeviceFlows.DataModel.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\deviceassociation.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\delegatorprovider.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\DbgModel.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\dbgeng.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\container.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\combase.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\CloudExperienceHostUser.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\C\_IS2022.DLL

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\c\_GSM7.DLL

2016-09-24 05:08:08 ----A---- C:\WINDOWS\SYSWOW64\C\_G18030.DLL

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\Windows.UI.Xaml.Resources.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\Windows.UI.Xaml.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\wincorlib.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\wevtapi.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\tzres.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\tzautoupdate.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\storagewmi\_passthru.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\SettingSyncHost.exe

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\SettingSyncCore.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\schannel.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\samlib.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\OneDriveSettingSyncProvider.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\oleaut32.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\offlinelsa.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\MSAJApi.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\kerberos.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\facecredentialprovider.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\eappprxy.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\eapphost.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\eappgnui.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\eappcfg.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\eapp3hst.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\dwmcore.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\drivers\xinputhid.sys

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\drivers\usbvideo.sys

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\drivers\ksecpkg.sys

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\drivers\hidusb.sys

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\drivers\hidparse.sys

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\drivers\hidclass.sys

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\drivers\EhStorTcgDrv.sys

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\drivers\ClipSp.sys

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\DeviceFlows.DataModel.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\delegatorprovider.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\container.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\combase.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\CloudExperienceHostUser.dll

2016-09-24 05:08:08 ----A---- C:\WINDOWS\system32\ClipboardServer.dll

2016-09-24 05:03:23 ----D---- C:\WINDOWS\system32\Microsoft

2016-09-24 05:02:35 ----SHD---- C:\ProgramData\Application Data

2016-09-24 05:00:34 ----D---- C:\WINDOWS\SYSWOW64\XPSViewer

2016-09-24 05:00:31 ----D---- C:\Program Files\Reference Assemblies

2016-09-24 05:00:31 ----D---- C:\Program Files\MSBuild

2016-09-24 05:00:31 ----D---- C:\Program Files (x86)\Reference Assemblies

2016-09-24 05:00:31 ----D---- C:\Program Files (x86)\MSBuild

2016-09-24 04:59:36 ----A---- C:\WINDOWS\SYSWOW64\TsWpfWrp.exe

2016-09-24 04:59:36 ----A---- C:\WINDOWS\SYSWOW64\PresentationNative\_v0300.dll

2016-09-24 04:59:36 ----A---- C:\WINDOWS\SYSWOW64\PresentationCFFRasterizerNative\_v0300.dll

2016-09-24 04:59:21 ----A---- C:\WINDOWS\system32\TsWpfWrp.exe

2016-09-24 04:59:21 ----A---- C:\WINDOWS\system32\PresentationNative\_v0300.dll

2016-09-24 04:59:21 ----A---- C:\WINDOWS\system32\PresentationCFFRasterizerNative\_v0300.dll

2016-09-24 04:59:05 ----A---- C:\WINDOWS\system32\drivers\wof.sys

2016-09-24 04:55:27 ----A---- C:\WINDOWS\system32\emptyregdb.dat

2016-09-24 04:41:11 ----SD---- C:\Users\kinderen\AppData\Roaming\Microsoft

2016-09-24 04:37:04 ----D---- C:\WINDOWS\system32\SRSLabs

2016-09-24 04:37:01 ----D---- C:\Program Files\Realtek

2016-09-24 04:37:00 ----D---- C:\WINDOWS\SYSWOW64\RTCOM

2016-09-24 04:36:56 ----A---- C:\WINDOWS\SYSWOW64\OpenCL.DLL

2016-09-24 04:36:56 ----A---- C:\WINDOWS\system32\OpenCL.DLL

2016-09-24 04:36:45 ----D---- C:\Program Files\Intel

2016-09-24 04:35:44 ----D---- C:\Program Files\Synaptics

2016-09-24 04:34:47 ----A---- C:\WINDOWS\SYSWOW64\PrintConfig.dll

2016-09-24 04:34:43 ----AS---- C:\WINDOWS\bootstat.dat

2016-09-24 04:33:22 ----D---- C:\WINDOWS\Prefetch

2016-09-24 04:33:21 ----D---- C:\WINDOWS\system32\SleepStudy

2016-09-24 04:33:21 ----D---- C:\WINDOWS\ServiceProfiles

2016-09-24 04:33:07 ----A---- C:\WINDOWS\system32\FNTCACHE.DAT

2016-09-16 10:12:51 ----A---- C:\WINDOWS\system32\drivers\ccavsfi.dat

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

2016-10-15 23:25:28 ----D---- C:\WINDOWS\system32\drivers\etc

2016-10-15 23:25:28 ----D---- C:\WINDOWS\system32\drivers

2016-10-15 23:25:28 ----D---- C:\WINDOWS\System32

2016-10-15 23:25:28 ----D---- C:\WINDOWS

2016-10-15 23:25:25 ----RD---- C:\Users

2016-10-15 23:25:25 ----RD---- C:\Program Files

2016-10-15 23:24:43 ----D---- C:\WINDOWS\Temp

2016-10-15 23:10:31 ----D---- C:\WINDOWS\AppReadiness

2016-10-15 23:01:51 ----RD---- C:\WINDOWS\Microsoft.NET

2016-10-15 23:01:07 ----RD---- C:\WINDOWS\assembly

2016-10-15 22:53:08 ----SD---- C:\ProgramData\Microsoft

2016-10-15 22:52:39 ----A---- C:\WINDOWS\system32\PerfStringBackup.INI

2016-10-15 22:51:36 ----D---- C:\WINDOWS\system32\sru

2016-10-15 22:02:04 ----D---- C:\WINDOWS\system32\config

2016-10-15 21:55:54 ----SHDC---- C:\WINDOWS\Installer

2016-10-15 21:55:49 ----D---- C:\WINDOWS\SysWOW64

2016-10-15 21:53:04 ----D---- C:\WINDOWS\system32\catroot2

2016-10-15 21:29:17 ----D---- C:\WINDOWS\WinSxS

2016-10-15 21:28:11 ----D---- C:\WINDOWS\system32\DriverStore

2016-10-15 02:17:47 ----D---- C:\WINDOWS\SYSWOW64\nl-NL

2016-10-15 02:17:32 ----D---- C:\WINDOWS\system32\WinBioPlugIns

2016-10-15 02:17:32 ----D---- C:\WINDOWS\system32\wbem

2016-10-15 02:17:32 ----D---- C:\WINDOWS\system32\sr-Latn-CS

2016-10-15 02:17:32 ----D---- C:\WINDOWS\system32\nl-NL

2016-10-15 02:17:32 ----D---- C:\WINDOWS\system32\migwiz

2016-10-15 02:17:31 ----SD---- C:\WINDOWS\system32\DiagSvcs

2016-10-15 02:17:31 ----D---- C:\WINDOWS\system32\Boot

2016-10-15 02:17:22 ----D---- C:\WINDOWS\ShellExperiences

2016-10-15 02:17:21 ----RD---- C:\WINDOWS\ImmersiveControlPanel

2016-10-15 02:17:21 ----D---- C:\WINDOWS\INF

2016-10-15 02:17:21 ----D---- C:\Program Files\Windows Photo Viewer

2016-10-15 02:17:21 ----D---- C:\Program Files\Windows Mail

2016-10-15 02:17:21 ----D---- C:\Program Files (x86)\Windows Photo Viewer

2016-10-15 02:03:19 ----D---- C:\WINDOWS\rescache

2016-10-15 01:15:45 ----SHD---- C:\System Volume Information

2016-10-14 23:44:05 ----D---- C:\WINDOWS\system32\MRT

2016-10-14 23:34:46 ----D---- C:\WINDOWS\debug

2016-10-14 23:34:29 ----AC---- C:\WINDOWS\system32\MRT.exe

2016-10-14 23:26:44 ----D---- C:\WINDOWS\CbsTemp

2016-10-14 22:24:59 ----HD---- C:\Program Files\WindowsApps

2016-10-14 18:51:36 ----D---- C:\WINDOWS\system32\WinBioDatabase

2016-10-14 18:51:36 ----D---- C:\WINDOWS\system32\Recovery

2016-10-14 18:33:07 ----D---- C:\WINDOWS\system32\Tasks

2016-10-14 18:33:07 ----AD---- C:\Program Files (x86)\TeamViewer

2016-10-14 18:32:04 ----RD---- C:\Program Files (x86)

2016-10-14 18:31:49 ----AD---- C:\Program Files (x86)\Microsoft Office

2016-10-14 18:31:29 ----RSD---- C:\WINDOWS\Fonts

2016-10-14 18:29:29 ----AD---- C:\Program Files\Common Files\microsoft shared

2016-10-14 18:26:00 ----HD---- C:\ProgramData

2016-10-10 21:46:31 ----D---- C:\WINDOWS\Logs

2016-10-10 00:07:53 ----D---- C:\ProgramData\COMODO

2016-10-09 00:12:53 ----D---- C:\WINDOWS\system32\drivers\UMDF

2016-10-09 00:05:40 ----D---- C:\Program Files (x86)\Dropbox

2016-10-06 02:34:20 ----D---- C:\WINDOWS\system32\WDI

2016-10-06 01:48:14 ----D---- C:\WINDOWS\SYSWOW64\wbem

2016-10-06 01:48:13 ----SD---- C:\WINDOWS\SYSWOW64\F12

2016-10-06 01:48:13 ----D---- C:\WINDOWS\SYSWOW64\sr-Latn-CS

2016-10-06 01:48:13 ----D---- C:\WINDOWS\SYSWOW64\setup

2016-10-06 01:48:12 ----D---- C:\WINDOWS\SYSWOW64\en-US

2016-10-06 01:48:12 ----D---- C:\WINDOWS\SYSWOW64\Dism

2016-10-06 01:47:28 ----D---- C:\WINDOWS\system32\Sysprep

2016-10-06 01:47:28 ----D---- C:\WINDOWS\system32\sr-Latn-RS

2016-10-06 01:47:28 ----D---- C:\WINDOWS\system32\setup

2016-10-06 01:47:28 ----D---- C:\WINDOWS\system32\oobe

2016-10-06 01:47:26 ----SD---- C:\WINDOWS\system32\F12

2016-10-06 01:47:24 ----D---- C:\WINDOWS\system32\en-US

2016-10-06 01:47:24 ----D---- C:\WINDOWS\system32\drivers\nl-NL

2016-10-06 01:47:24 ----D---- C:\WINDOWS\system32\Dism

2016-10-06 01:47:24 ----D---- C:\WINDOWS\system32\appraiser

2016-10-06 01:46:39 ----D---- C:\WINDOWS\Provisioning

2016-10-06 01:46:37 ----D---- C:\WINDOWS\bcastdvr

2016-10-06 01:46:37 ----D---- C:\WINDOWS\AppPatch

2016-10-06 01:46:36 ----D---- C:\Program Files (x86)\Internet Explorer

2016-10-06 01:46:35 ----D---- C:\Program Files\Internet Explorer

2016-10-03 22:09:37 ----A---- C:\WINDOWS\SYSWOW64\FlashPlayerApp.exe

2016-10-02 16:59:44 ----D---- C:\Program Files (x86)\COMODO

2016-09-29 16:05:03 ----A---- C:\WINDOWS\system32\iseguard64.dll

2016-09-29 16:04:57 ----A---- C:\WINDOWS\SYSWOW64\iseguard32.dll

2016-09-28 21:49:55 ----D---- C:\WINDOWS\SYSWOW64\Macromed

2016-09-28 21:37:08 ----D---- C:\Program Files (x86)\Common Files

2016-09-28 00:33:37 ----D---- C:\Program Files (x86)\Mozilla Maintenance Service

2016-09-26 22:30:37 ----D---- C:\WINDOWS\system32\FxsTmp

2016-09-26 22:29:45 ----D---- C:\Program Files (x86)\SamsungPrinterLiveUpdateInstaller

2016-09-26 20:37:12 ----D---- C:\WINDOWS\appcompat

2016-09-25 17:38:41 ----D---- C:\WINDOWS\system32\restore

2016-09-25 17:28:59 ----D---- C:\ProgramData\USOPrivate

2016-09-25 17:28:12 ----A---- C:\WINDOWS\system32\{F33C3B9B-72AF-418A-B3FD-560646F7CDA2}.bat

2016-09-24 05:24:08 ----D---- C:\Windows.old(1)

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\zh-TW

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\zh-HK

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\zh-CN

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\uk-UA

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\tr-TR

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\th-TH

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\sv-SE

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\sl-SI

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\sk-SK

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\ru-RU

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\ro-RO

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\pt-PT

2016-09-24 05:10:22 ----D---- C:\WINDOWS\system32\pt-BR

2016-09-24 05:10:21 ----SD---- C:\WINDOWS\system32\dsc

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\pl-PL

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\nb-NO

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\migration

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\lv-LV

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\lt-LT

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\ko-KR

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\ja-jp

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\it-IT

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\hu-HU

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\hr-HR

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\he-IL

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\fr-FR

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\fr-CA

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\fi-FI

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\et-EE

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\es-MX

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\es-ES

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\en-GB

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\el-GR

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\de-DE

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\da-DK

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\cs-CZ

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\bg-BG

2016-09-24 05:10:21 ----D---- C:\WINDOWS\system32\ar-SA

2016-09-24 05:10:18 ----RD---- C:\Program Files\Windows Defender

2016-09-24 05:10:18 ----D---- C:\Program Files\Windows Media Player

2016-09-24 05:10:18 ----D---- C:\Program Files (x86)\Windows Media Player

2016-09-24 05:10:18 ----D---- C:\Program Files (x86)\Windows Mail

2016-09-24 05:10:18 ----D---- C:\Program Files (x86)\Windows Defender

2016-09-24 05:02:35 ----D---- C:\Program Files\Windows NT

2016-09-24 05:02:10 ----D---- C:\WINDOWS\SoftwareDistribution

2016-09-24 05:00:34 ----D---- C:\WINDOWS\SYSWOW64\MUI

2016-09-24 05:00:34 ----D---- C:\WINDOWS\system32\MUI

2016-09-24 05:00:28 ----D---- C:\WINDOWS\Registration

2016-09-24 05:00:05 ----D---- C:\WINDOWS\system32\Tasks\_Migrated

2016-09-24 04:59:46 ----D---- C:\WINDOWS\system32\LogFiles

2016-09-24 04:59:43 ----D---- C:\WINDOWS\Tasks

2016-09-24 04:48:14 ----D---- C:\WINDOWS\system32\CatRoot

2016-09-24 04:48:05 ----AD---- C:\ProgramData\regid.1991-06.com.microsoft

2016-09-24 04:44:51 ----D---- C:\WINDOWS\SYSWOW64\migration

2016-09-24 04:44:42 ----D---- C:\WINDOWS\system32\spool

2016-09-24 04:44:38 ----D---- C:\WINDOWS\system32\Macromed

2016-09-24 04:43:45 ----D---- C:\Program Files (x86)\Microsoft.NET

2016-09-24 04:43:43 ----D---- C:\Program Files\Common Files

2016-09-24 04:42:58 ----D---- C:\WINDOWS\system32\CodeIntegrity

2016-09-24 04:37:33 ----RD---- C:\WINDOWS\PrintDialog

2016-09-24 04:37:32 ----RD---- C:\WINDOWS\MiracastView

======List of drivers (R=Running, S=Stopped, 0=Boot, 1=System, 2=Auto, 3=Demand, 4=Disabled)======

S0 cmdccav;cmdccav; C:\WINDOWS\system32\drivers\CmdCCAV.sys [2016-09-30 155232]

S0 iaStor;@oem24.inf,%\*PNP0600.DeviceDesc%;Intel AHCI Controller; C:\WINDOWS\System32\drivers\iaStor.sys [2011-11-30 568600]

S0 iorate;@%SystemRoot%\system32\drivers\iorate.sys,-100; C:\WINDOWS\system32\drivers\iorate.sys [2016-07-16 45920]

S0 iusb3hcs;@oem28.inf,%XHCI\_svcdesc%;Intel(R) USB 3.0 hostcontrollerswitch-stuurprogramma; C:\WINDOWS\System32\drivers\iusb3hcs.sys [2012-01-05 16152]

S0 LSI\_SAS2i;LSI\_SAS2i; C:\WINDOWS\System32\drivers\lsi\_sas2i.sys [2016-07-16 105824]

S0 LSI\_SAS3i;LSI\_SAS3i; C:\WINDOWS\System32\drivers\lsi\_sas3i.sys [2016-07-16 101216]

S0 megasas2i;megasas2i; C:\WINDOWS\System32\drivers\MegaSas2i.sys [2016-10-05 64352]

S0 percsas2i;percsas2i; C:\WINDOWS\System32\drivers\percsas2i.sys [2016-07-16 58720]

S0 percsas3i;percsas3i; C:\WINDOWS\System32\drivers\percsas3i.sys [2016-07-16 61792]

S0 scmbus;@scmbus.inf,%scmbus.SvcDesc%;Microsoft Storage Class Memory Bus Driver; C:\WINDOWS\System32\drivers\scmbus.sys [2016-07-16 88416]

S0 storufs;@storufs.inf,%UfsServiceDesc%;Microsoft Universal Flash Storage (UFS) Driver; C:\WINDOWS\System32\drivers\storufs.sys [2016-07-16 32096]

S0 TVALZ;@oem20.inf,%TVALZ.SvcDesc%;TOSHIBA ACPI-Based Value Added Logical and General Purpose Device Driver; C:\WINDOWS\System32\drivers\TVALZ\_O.SYS [2016-07-21 53888]

S1 FileCrypt;@%systemroot%\system32\drivers\filecrypt.sys,-100; C:\WINDOWS\system32\drivers\filecrypt.sys [2016-07-16 88576]

S1 GpuEnergyDrv;@%SystemRoot%\system32\drivers\gpuenergydrv.sys,-100; C:\WINDOWS\System32\drivers\gpuenergydrv.sys [2016-07-16 8192]

S1 isedrv;Internet Security Essentials; C:\WINDOWS\system32\drivers\isedrv.sys [2016-09-29 50392]

S2 clreg;@%SystemRoot%\system32\drivers\registry.sys,-100; C:\WINDOWS\System32\drivers\registry.sys [2016-07-16 70144]

S2 MMCSS;@%systemroot%\system32\drivers\mmcss.sys,-100; C:\WINDOWS\system32\drivers\mmcss.sys [2016-07-16 48128]

S2 storqosflt;@%SystemRoot%\System32\drivers\storqosflt.sys,-101; C:\WINDOWS\system32\drivers\storqosflt.sys [2016-07-16 78336]

S3 AcpiDev;@acpidev.inf,%AcpiDev.SvcDesc%;ACPI Devices driver; C:\WINDOWS\System32\drivers\AcpiDev.sys [2016-07-16 18432]

S3 applockerfltr;@%systemroot%\system32\srpapi.dll,-102; C:\WINDOWS\system32\drivers\applockerfltr.sys [2016-07-16 15360]

S3 bcmfn;@bcmfn.inf,%bcmfn.SVCDESC%;bcmfn Service; C:\WINDOWS\System32\drivers\bcmfn.sys [2016-07-16 9728]

S3 buttonconverter;@buttonconverter.inf,%btnconv.SvcDesc%;Service for Portable Device Control devices; C:\WINDOWS\System32\drivers\buttonconverter.sys [2016-07-16 38912]

S3 CapImg;@capimg.inf,%CapImgHid\_Service%;HID driver for CapImg touch screen; C:\WINDOWS\System32\drivers\capimg.sys [2016-07-16 117248]

S3 cht4iscsi;cht4iscsi; C:\WINDOWS\System32\drivers\cht4sx64.sys [2016-07-16 346976]

S3 cht4vbd;@cht4vx64.inf,%cht4vbd.generic%;Chelsio Virtual Bus Driver; C:\WINDOWS\System32\drivers\cht4vx64.sys [2016-07-16 2104160]

S3 dbx;dbx; C:\WINDOWS\system32\DRIVERS\dbx.sys []

S3 genericusbfn;@genericusbfn.inf,%genericusbfn.ServiceName%;Generic USB Function Class; C:\WINDOWS\System32\drivers\genericusbfn.sys [2016-07-16 20480]

S3 hidinterrupt;@hidinterrupt.inf,%HID\_Interrupt.SvcDesc%;Common Driver for HID Buttons implemented with interrupts; C:\WINDOWS\System32\drivers\hidinterrupt.sys [2016-07-16 50016]

S3 hvservice;@%SystemRoot%\system32\drivers\hvservice.sys,-16; C:\WINDOWS\system32\drivers\hvservice.sys [2016-09-24 73568]

S3 iagpio;@iagpio.inf,%iagpio.SVCDESC%;Intel Serial IO GPIO Controller Driver; C:\WINDOWS\System32\drivers\iagpio.sys [2016-07-16 33280]

S3 iai2c;@iai2c.inf,%iai2c.SVCDESC%;Intel(R) Serial IO I2C Host Controller; C:\WINDOWS\System32\drivers\iai2c.sys [2016-07-16 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 [2016-07-16 64512]

S3 iaLPSS2i\_I2C;@iaLPSS2i\_I2C\_SKL.inf,%iaLPSS2i\_I2C.SVCDESC%;Intel(R) Serial IO I2C Driver v2; C:\WINDOWS\System32\drivers\iaLPSS2i\_I2C.sys [2016-07-16 176384]

S3 ibbus;@mlx4\_bus.inf,%Ibbus.ServiceDesc%;Mellanox InfiniBand Bus/AL (Filter Driver); C:\WINDOWS\System32\drivers\ibbus.sys [2016-07-16 526176]

S3 igfx;igfx; C:\WINDOWS\system32\DRIVERS\igdkmd64.sys [2016-05-03 3811288]

S3 IndirectKmd;@%SystemRoot%\system32\drivers\IndirectKmd.sys,-100; C:\WINDOWS\System32\drivers\IndirectKmd.sys [2016-07-16 35840]

S3 intaud\_WaveExtensible;@oem6.inf,%INTAUD\_WEX.SvcDesc%;Intel WiDi Audio Device; C:\WINDOWS\system32\drivers\intelaud.sys [2015-12-01 50160]

S3 IntcAzAudAddService;Service for Realtek HD Audio (WDM); C:\WINDOWS\system32\drivers\RTKVHD64.sys [2012-09-27 4155536]

S3 IntcDAud;@oem10.inf,%IntcDAud.SvcDesc%;Intel(R) Display Audio; C:\WINDOWS\system32\DRIVERS\IntcDAud.sys [2015-08-21 463112]

S3 irda;IrDA; C:\WINDOWS\system32\drivers\irda.sys [2016-07-16 120320]

S3 iusb3hub;Intel(R) USB 3.0 hub-stuurprogramma; C:\WINDOWS\System32\drivers\iusb3hub.sys [2012-01-05 355096]

S3 iusb3xhc;Intel(R) USB 3.0 uitbreidbare hostcontroller-stuurprogramma; C:\WINDOWS\System32\drivers\iusb3xhc.sys [2012-01-05 786200]

S3 iwdbus;@oem31.inf,%iwdbus.SVCDESC%;IWD Bus Enumerator; C:\WINDOWS\System32\drivers\iwdbus.sys [2015-12-01 38896]

S3 MEIx64;@oem18.inf,%HECI\_SvcDesc%;Intel(R) Management Engine Interface ; C:\WINDOWS\System32\drivers\HECIx64.sys [2012-07-17 62784]

S3 mlx4\_bus;@mlx4\_bus.inf,%MLX4BUS.ServiceDesc%;Mellanox ConnectX Bus Enumerator; C:\WINDOWS\System32\drivers\mlx4\_bus.sys [2016-07-16 842584]

S3 ndfltr;@mlx4\_bus.inf,%ndfltr.ServiceDesc%;NetworkDirect Service; C:\WINDOWS\System32\drivers\ndfltr.sys [2016-07-16 108896]

S3 NetAdapterCx;Network Adapter Wdf Class Extension Library; C:\WINDOWS\system32\drivers\NetAdapterCx.sys [2016-07-16 90624]

S3 ReFSv1;ReFSv1; C:\WINDOWS\system32\drivers\ReFSv1.sys [2016-07-16 928608]

S3 RSUSBSTOR;@oem30.inf,%RSUSBSTOR.SvcDesc%;RtsUStor.Sys Realtek USB Card Reader; C:\WINDOWS\System32\Drivers\RtsUStor.sys [2011-08-17 251496]

S3 rt640x64;@rt640x64.inf,%rt640.Service.DispName%;Realtek RT640 NT Driver; C:\WINDOWS\System32\drivers\rt640x64.sys [2016-07-16 589824]

S3 rtwlane\_13;@netrtwlane\_13.inf,%rtwlane\_13.DeviceDesc.DispName%;Realtek Wireless LAN 802.11n PCI-E Network Adapter; C:\WINDOWS\System32\drivers\rtwlane\_13.sys [2016-07-16 3717120]

S3 scmdisk0101;@scmdisk0101.inf,%scmdisk0101.SvcDesc%;Microsoft NVDIMM-N disk driver; C:\WINDOWS\System32\drivers\scmdisk0101.sys [2016-07-16 123904]

S3 SmbDrv;SmbDrv; C:\WINDOWS\System32\drivers\Smb\_driver\_AMDASF.sys [2015-10-08 50880]

S3 SmbDrvI;SmbDrvI; C:\WINDOWS\system32\DRIVERS\Smb\_driver\_Intel.sys [2015-10-08 51392]

S3 SynTP;@oem19.inf,%SynTP.SvcDesc%;Synaptics TouchPad Driver; C:\WINDOWS\system32\DRIVERS\SynTP.sys [2015-10-08 627392]

S3 Thotkey;@oem40.inf,%Thotkey%;Toshiba Hotkey Driver; C:\WINDOWS\System32\drivers\Thotkey.sys [2015-12-31 45720]

S3 UcmCx0101;USB Connector Manager KMDF Class Extension; C:\WINDOWS\System32\Drivers\UcmCx.sys [2016-07-16 95744]

S3 UcmTcpciCx0101;UCM-TCPCI KMDF Class Extension; C:\WINDOWS\System32\Drivers\UcmTcpciCx.sys [2016-07-16 108544]

S3 UcmUcsi;@UcmUcsi.inf,%UcmUcsi.ServiceName%;USB Connector Manager UCSI Client; C:\WINDOWS\System32\drivers\UcmUcsi.sys [2016-07-16 50688]

S3 UdeCx;USB Device Emulation Support Library; C:\WINDOWS\system32\drivers\udecx.sys [2016-07-16 45568]

S3 Ufx01000;USB Function Class Extension; C:\WINDOWS\system32\drivers\ufx01000.sys [2016-07-16 263008]

S3 UfxChipidea;@ufxchipidea.inf,%UfxChipidea.ServiceName%;USB Chipidea Controller; C:\WINDOWS\System32\drivers\UfxChipidea.sys [2016-07-16 96608]

S3 ufxsynopsys;@ufxsynopsys.inf,%ufxsynopsys.ServiceName%;USB Synopsys Controller; C:\WINDOWS\System32\drivers\ufxsynopsys.sys [2016-07-16 137056]

======List of services (R=Running, S=Stopped, 0=Boot, 1=System, 2=Auto, 3=Demand, 4=Disabled)======

S2 Apple Mobile Device Service;Apple Mobile Device Service; C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe [2016-08-05 83768]

S2 Bonjour Service;Bonjour-service; C:\Program Files\Bonjour\mDNSResponder.exe [2015-08-12 462096]

S2 ccavsrv;ccavsrv; C:\Program Files (x86)\COMODO\COMODO Cloud Antivirus\ccavsrv.exe [2016-09-30 5443720]

S2 CDPSvc;@%SystemRoot%\system32\cdpsvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S2 CDPUserSvc;@%SystemRoot%\system32\cdpusersvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S2 CDPUserSvc\_9f7ba;CDPUserSvc\_9f7ba; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S2 ClickToRunSvc;Microsoft Office Click-to-Run Service; C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe [2016-09-05 2980032]

S2 CoreMessagingRegistrar;@%SystemRoot%\system32\coremessaging.dll,-1; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S2 dbupdate;Dropbox-update-service (dbupdate); C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [2016-06-12 143144]

S2 DbxSvc;DbxSvc; C:\WINDOWS\system32\DbxSvc.exe [2016-10-06 42792]

S2 DiagTrack;@%SystemRoot%\system32\diagtrack.dll,-3001; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S2 DoSvc;@%systemroot%\system32\dosvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S2 GenieTimelineService;Genie Timeline Service; C:\Program Files\NETGEAR\ReadySHARE Vault\GenieTimelineService.exe [2014-06-18 673856]

S2 hola\_svc;Hola Better Internet Engine; C:\Program Files\Hola\app\hola\_svc.exe [2016-09-18 5618864]

S2 hola\_updater;Hola Better Internet Updater; C:\Program Files\Hola\app\hola\_updater.exe [2016-06-08 5615280]

S2 igfxCUIService1.0.0.0;Intel(R) HD Graphics Control Panel Service; C:\WINDOWS\system32\igfxCUIService.exe [2016-06-07 337888]

S2 isesrv;isesrv; C:\Program Files (x86)\COMODO\Internet Security Essentials\isesrv.exe [2016-09-29 118464]

S2 MapsBroker;@%SystemRoot%\System32\moshost.dll,-100; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S2 OneSyncSvc;@%SystemRoot%\system32\APHostRes.dll,-10002; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S2 OneSyncSvc\_9f7ba;Host synchroniseren\_9f7ba; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S2 RtkAudioService;Realtek Audio Service; C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe [2016-06-07 201360]

S2 SkypeUpdate;Skype Updater; C:\Program Files (x86)\Skype\Updater\Updater.exe [2016-03-23 327808]

S2 SynTPEnhService;SynTPEnh Caller Service; C:\Program Files\Synaptics\SynTP\SynTPEnhService.exe [2016-06-07 255168]

S2 TeamViewer;TeamViewer 11; C:\Program Files (x86)\TeamViewer\TeamViewer\_Service.exe [2016-09-20 7500048]

S2 tiledatamodelsvc;@%SystemRoot%\system32\tileobjserver.dll,-1; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 AdobeFlashPlayerUpdateSvc;Adobe Flash Player Update Service; C:\WINDOWS\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe [2016-09-13 270016]

S3 AJRouter;@%SystemRoot%\system32\AJRouter.dll,-2; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 BthHFSrv;@%SystemRoot%\System32\BthHFSrv.dll,-103; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S3 ClipSVC;@%SystemRoot%\system32\ClipSVC.dll,-103; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S3 cphs;Intel(R) Content Protection HECI Service; C:\WINDOWS\SysWow64\IntelCpHeciSvc.exe [2016-06-07 299488]

S3 dbupdatem;Dropbox-update-service (dbupdatem); C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe [2016-06-12 143144]

S3 DcpSvc;@%SystemRoot%\system32\dcpsvc.dll,-3001; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S3 DevQueryBroker;@%SystemRoot%\system32\DevQueryBroker.dll,-100; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 diagnosticshub.standardcollector.service;@%SystemRoot%\system32\DiagSvcs\DiagnosticsHub.StandardCollector.ServiceRes.dll,-1000; C:\WINDOWS\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe [2016-07-16 93184]

S3 DmEnrollmentSvc;@%systemroot%\system32\Windows.Internal.Management.dll,-100; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 dmwappushservice;@%SystemRoot%\system32\dmwappushsvc.dll,-200; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 DsSvc;@%SystemRoot%\system32\dssvc.dll,-10003; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S3 embeddedmode;@%SystemRoot%\system32\embeddedmodesvc.dll,-201; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S3 EntAppSvc;@EnterpriseAppMgmtSvc.dll,-1; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 FontCache3.0.0.0;@%SystemRoot%\system32\PresentationHost.exe,-3309; C:\WINDOWS\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe [2016-05-25 43696]

S3 FrameServer;@%systemroot%\system32\FrameServer.dll,-100; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S3 HvHost;@%SystemRoot%\system32\hvhostsvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 icssvc;@%SystemRoot%\System32\tetheringservice.dll,-4097; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 iPod Service;iPod-service; C:\Program Files\iPod\bin\iPodService.exe [2016-09-09 651576]

S3 irmon;@%SystemRoot%\System32\irmon.dll,-2000; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 LicenseManager;@%SystemRoot%\system32\licensemanagersvc.dll,-200; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S3 MessagingService;@%SystemRoot%\system32\MessagingService.dll,-100; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 MessagingService\_9f7ba;MessagingService\_9f7ba; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 MozillaMaintenance;Mozilla Maintenance Service; C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe [2016-09-27 172488]

S3 NetSetupSvc;@%SystemRoot%\system32\NetSetupSvc.dll,-3; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S3 NgcCtnrSvc;@%SystemRoot%\System32\NgcCtnrSvc.dll,-1; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 NgcSvc;@%SystemRoot%\System32\ngcsvc.dll,-100; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

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 [2016-09-05 209104]

S3 PhoneSvc;@%SystemRoot%\system32\PhoneserviceRes.dll,-10000; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 PimIndexMaintenanceSvc;@%SystemRoot%\system32\UserDataAccessRes.dll,-15001; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 PimIndexMaintenanceSvc\_9f7ba;Contact Data\_9f7ba; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 RetailDemo;@%SystemRoot%\System32\RDXService.dll,-256; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S3 RmSvc;@%SystemRoot%\system32\RMapi.dll,-1001; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S3 SensorDataService;@%SystemRoot%\system32\SensorDataService.exe,-101; C:\WINDOWS\System32\SensorDataService.exe [2016-09-24 1312768]

S3 SensorService;@%SystemRoot%\System32\sensorservice.dll,-1000; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 SmsRouter;@%SystemRoot%\System32\SmsRouterSvc.dll,-10001; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 StateRepository;@%SystemRoot%\system32\windows.staterepository.dll,-1; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S3 TieringEngineService;@%SystemRoot%\system32\TieringEngineService.exe,-702; C:\WINDOWS\system32\TieringEngineService.exe [2016-07-16 287744]

S3 TimeBrokerSvc;@%windir%\system32\TimeBrokerServer.dll,-1001; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

S4 shpamsvc;@%SystemRoot%\System32\Windows.SharedPC.AccountManager.dll,-100; C:\WINDOWS\System32\svchost.exe [2016-07-16 44496]

S4 tzautoupdate;@%SystemRoot%\system32\tzautoupdate.dll,-200; C:\WINDOWS\system32\svchost.exe [2016-07-16 44496]

-----------------EOF-----------------