

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details		Host: mag2, Sample ID: 15, Task ID: 40
Task ID:	40	
Risk Level:	10	
Date Processed:	2016-03-29 05:50:03 (UTC)	
Processing Time:	63.04 seconds	
Virtual Environment:	IntelliVM	
Execution Arguments:	"c:\windows\temp\spyeye_inj_ector_.exe"	
Sample ID:	15	
Type:	basic	
Owner:	admin	
Label:	spyeye%inj%ector%.exe	
Date Added:	2016-03-29 05:50:03 (UTC)	
File Type:	PE32:win32:gui	
File Size:	103936 bytes	
MD5:	b98bb6d7428c3dbffcfcab2414c6daa2	
SHA256:	fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029	
Description:	None	

Pattern Matching Results

6	Modifies registry autorun entries
7	Writes to memory of system processes
6	Writes to system32 folder
10	Suspicious writeprocess: Spyeye [Banking]
5	Abnormal sleep detected
5	Installs service
8	Possible kernel API resolver
3	HTTP connection - response code 200 (success)
3	Connects to local host
2	PE: Nonstandard section
4	Terminates process under Windows subfolder
4	Reads process memory
5	PE: Contains compressed section
6	Notifies system about Internet connection change
4	Connects to local IP
5	Packer: UPX
5	Adds autostart object
10	Creates malicious mutex: Spyeye [Banking]

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process:	C:\windows\temp\spyeye_inj_ector_.exe
["C:\windows\temp\spyeye_inj_ector_.exe"]	
Creates process:	C:\WinOldFileq\83A494219A6.exe ["C:\WinOldFileq\83A494219A6.exe"]
Creates process:	C:\Windows\system32\rundll32.exe ["C:\Windows\system32\rundll32.exe"
"C:\Windows\system32\WININET.dll",DispatchAPICall 1 1]	
Reads from process:	PID:2600 C:\Windows\System32\rundll32.exe
Reads from process:	PID:2680 C:\Windows\System32\calc.exe
Reads from process:	PID:2712 C:\Windows\System32\rundll32.exe
Reads from process:	PID:2792 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3076 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3128 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3180 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3228 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3284 C:\Windows\System32\rundll32.exe
Reads from process:	PID:3348 C:\Windows\System32\rundll32.exe
Writes to process:	PID:1180 C:\Windows\explorer.exe
Writes to process:	PID:360 C:\Windows\System32\wininit.exe
Writes to process:	PID:408 C:\Windows\System32\winlogon.exe
Writes to process:	PID:452 C:\Windows\System32\lsass.exe
Writes to process:	PID:460 C:\Windows\System32\lsm.exe
Writes to process:	PID:580 C:\Windows\System32\svchost.exe
Writes to process:	PID:644 C:\Windows\System32\svchost.exe
Writes to process:	PID:692 C:\Windows\System32\svchost.exe
Writes to process:	PID:808 C:\Windows\System32\svchost.exe
Writes to process:	PID:860 C:\Windows\System32\svchost.exe
Writes to process:	PID:976 C:\Windows\System32\svchost.exe
Writes to process:	PID:1164 C:\Windows\System32\dmw.exe
Writes to process:	PID:1248 C:\Windows\System32\spoolsv.exe
Writes to process:	PID:1284 C:\Windows\System32\taskhost.exe
Writes to process:	PID:1312 C:\Windows\System32\svchost.exe
Writes to process:	PID:1380 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Writes to process:	PID:1464 C:\Windows\System32\svchost.exe
Writes to process:	PID:1520 C:\Windows\System32\svchost.exe
Writes to process:	PID:1944 C:\Windows\System32\UI0Detect.exe
Writes to process:	PID:2032 C:\Windows\System32\svchost.exe
Writes to process:	PID:1716 C:\Windows\System32\mobsync.exe
Writes to process:	PID:1692 C:\Windows\System32\taskhost.exe
Writes to process:	PID:1804 C:\Windows\System32\wbem\unsecapp.exe
Writes to process:	PID:2104 C:\Windows\System32\wbem\WmiPrvSE.exe
Writes to process:	PID:2160 C:\Windows\System32\conhost.exe
Writes to process:	PID:2172 C:\Windows\Temp\spyeye_inj_ector_.exe
Writes to process:	PID:2600 C:\Windows\System32\rundll32.exe
Writes to process:	PID:2712 C:\Windows\System32\rundll32.exe
Writes to process:	PID:2792 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3076 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3128 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3180 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3228 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3284 C:\Windows\System32\rundll32.exe
Writes to process:	PID:3348 C:\Windows\System32\rundll32.exe
Terminates process:	C:\WinOldFileq\83A494219A6.exe
Terminates process:	C:\Windows\Temp\spyeye_inj_ector_.exe
Terminates process:	C:\Windows\System32\rundll32.exe
Terminates process:	C:\Windows\System32\mobsync.exe
Creates remote thread:	System

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\RPCController
Creates mutex:	\Sessions\1\BaseNamedObjects\zXeRY3a_PtW\00000000
Creates mutex:	\BaseNamedObjects\zXeRY3a_PtW\00000000
Creates mutex:	\BaseNamedObjects\M3wSKwK7maYcQA95g79Wq3uQs1gCA
Creates mutex:	\Sessions\1\BaseNamedObjects\!MSFTHISTORY!_
Creates mutex:	

```
\Sessions\1\BaseNamedObjects\c:\users\admin\appdata\local\microsoft\windows\temporary internet
files\content.ie5!
Creates mutex:
\Sessions\1\BaseNamedObjects\c:\users\admin\appdata\roaming\microsoft\windows\cookies!
Creates mutex:
\Sessions\1\BaseNamedObjects\c:\users\admin\appdata\local\microsoft\windows\history\history.ie5!
Creates mutex: \Sessions\1\BaseNamedObjects\WininetStartupMutex
Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex
Creates mutex: \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex
Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex: \Sessions\1\BaseNamedObjects\_!MSFTHISTORY!_LOW!_
Creates mutex:
\Sessions\1\BaseNamedObjects\c:\users\admin\appdata\local\microsoft\windows\temporary internet
files\low\content.ie5!
Creates mutex:
\Sessions\1\BaseNamedObjects\c:\users\admin\appdata\roaming\microsoft\windows\cookies\low!
Creates mutex:
\Sessions\1\BaseNamedObjects\c:\users\admin\appdata\local\microsoft\windows\history\low\history.ie5!
Creates mutex: \Sessions\1\BaseNamedObjects\IESQMMUTEX_0_208
Creates mutex: \Sessions\1\BaseNamedObjects\!IETId\Mutex
Creates event: \BaseNamedObjects\SvcctlStartEvent_A3752DX
Creates event: \KernelObjects\SuperFetchTracesReady
Creates event: \KernelObjects\SuperFetchParametersChanged
Creates event: \KernelObjects\PrefetchTracesReady
Creates event: \BaseNamedObjects\BFE_Notify_Event_{4c5d64bd-7721-4661-8bc5-
6cc92228969f}
Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED
Creates semaphore: \Sessions\1\BaseNamedObjects\4FBEA4B1
```

File System Events

```
Creates: C:\WinOldFileq
Creates: C:\WinOldFileq\
Creates: C:\WinOldFileq\83A494219A6.exe
Creates: C:\WinOldFileq\9C413B7B23C1D6D
Creates: C:\Users\Admin
Creates: C:\Users\Admin\AppData\Local
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Creates: C:\Users\Admin\AppData\Roaming
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Creates: C:\Windows\Prefetch\NTOSBOOT-B00DFAAD.pf
Creates: C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf
Creates: C:\Users\Admin\Favorites
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETIdCache
Creates: C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf
Creates:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[1].txt
Creates:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[2].txt
Creates: C:\Windows\System32\wfp\wfpdiag.etl
Opens: C:\Windows\Prefetch\SPYEE_INJ_ECTOR_.EXE-76AA8D3E.pf
Opens: C:\Windows\System32
Opens: C:\Windows\System32\sechost.dll
Opens: C:\Windows\System32\kernel32.dll
Opens: C:\
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\System32\ntdll.dll
Opens: C:\WinOldFileq
Opens: C:\WinOldFileq\
Opens: C:\Windows\Temp\spyeye_inj_ector_.exe
Opens: C:\WinOldFileq\83A494219A6.exe
Opens: C:\Windows\AppPatch\sysmain.sdb
Opens: C:\WinOldFileq\ui\SwDRM.dll
Opens: C:\Windows\Prefetch\83A494219A6.EXE-0D3DE1A1.pf
Opens: C:\Windows\System32\imm32.dll
Opens: C:\WinOldFileq\MSIMG32.dll
Opens: C:\Windows\System32\msimg32.dll
Opens: C:\WinOldFileq\9C413B7B23C1D6D
Opens: C:\Windows\MSIMG32.dll
Opens: C:\Windows\System32\user32.dll
Opens: C:\Windows\CSO\v2.0.6\namespace
Opens: C:\Windows\System32\wininet.dll
Opens: C:\Windows\System32\ws2_32.dll
Opens: C:\Windows\System32\advapi32.dll
Opens: C:\Windows\System32\crypt32.dll
Opens: C:\Windows\System32\tzres.dll
Opens: C:\Windows\System32\en-US\tzres.dll.mui
Opens: C:\Windows\System32\mswsock.dll
Opens: C:\Windows\System32\WSHTCPIP.DLL
Opens: C:\Windows\Explorer.EXE.Local\
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData\Local
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
Opens: C:\Users\Admin\AppData\Roaming
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
Opens: C:\Windows\Temp\MSIMG32.dll
Opens: C:\Windows\dnssapi.DLL
Opens: C:\Windows\System32\dnssapi.dll
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs
Opens: C:\Windows\Temp\spyeye_inj_ector_.exe
Opens: C:\Program Files\Adobe\Reader 9.0\Reader\MSIMG32.dll
Opens: C:\Windows\System32\dot3api.dll
```

Opens: C:\Windows\System32\eaappcfg.dll
Opens: C:\Windows\System32\wlanhlp.dll
Opens: C:\Windows\System32\wlanapi.dll
Opens: C:\Windows\System32\wlanutil.dll
Opens: C:\Windows\System32\onex.dll
Opens: C:\Windows\System32\eaappprxy.dll
Opens: C:\ProgramData\Microsoft\Network\Connections\Pbk\
Opens: C:\Windows\System32\ras
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
Opens: C:
Opens: C:\Windows\Prefetch
Opens: \\?\Volume{69d250e3-6c18-11e3-b3bc-806e6f6e6963}
Opens: \\?\Volume{69d250e3-6c18-11e3-b3bc-806e6f6e6963}\
Opens: C:\Windows\System32\en-US\sysmain.dll.mui
Opens: \\?\Volume{69d250e3-6c18-11e3-b3bc-806e6f6e6963}\ReadyBoostPerfTest.tmp
Opens: \\?\Volume{69d250e3-6c18-11e3-b3bc-806e6f6e6963}\ReadyBoost.sfcache
Opens: C:\ReadyBoostPerfTest.tmp
Opens: C:\ReadyBoost.sfcache
Opens: C:\Windows\Prefetch\AgG1GlobalHistory.db
Opens: C:\Windows\Prefetch\AgG1FaultHistory.db
Opens: C:\Windows\Prefetch\AgG1FgAppHistory.db
Opens: C:\Windows\Prefetch\AgAppLaunch.db
Opens: C:\Windows\Prefetch\MSIEXEC.EXE-A2D55CB6.pf
Opens: C:\Windows\Prefetch\IEXPLORE.EXE-908C99F8.pf
Opens: C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
Opens: C:\Windows\Prefetch\EXPLORER.EXE-A80E4F97.pf
Opens: C:\Windows\Prefetch\TASKHOST.EXE-7238F31D.pf
Opens: C:\Windows\Prefetch\SYSTEMPROPERTIESADVANCED.EXE-68C7C4F0.pf
Opens: C:\Windows\Prefetch\LOGONUI2.EXE-09140401.pf
Opens: C:\Windows\Prefetch\ACRORD32.EXE-172CF576.pf
Opens: C:\Windows\Prefetch\AgRobust.db
Opens: C:\Windows\Prefetch\LongTermHist.db
Opens: C:\Windows\System32\secur32.dll
Opens: C:\Windows\System32\credssp.dll
Opens: C:\Windows\Prefetch\PfSvcPerfStats.bin
Opens: C:\Windows\Prefetch\NTOSBOOT-B00DFAAD.pf
Opens: C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf
Opens: C:\Windows\Prefetch\PYTHONW.EXE-DD01C6BD.pf
Opens: C:\Windows\Prefetch\REG.EXE-E7E8BD26.pf
Opens: C:\Windows\RASAPI32.dll
Opens: C:\Windows\System32\rasapi32.dll
Opens: C:\Windows\rasman.dll
Opens: C:\Windows\System32\rasman.dll
Opens: C:\Windows\rtutils.dll
Opens: C:\Windows\System32\rtutils.dll
Opens: C:\Windows\sensapi.dll
Opens: C:\Windows\System32\SensApi.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows
Opens: C:\Users\Admin\AppData\Local\Microsoft
Opens: C:\Users\Admin\AppData
Opens: C:\Users
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows
Opens: C:\Users\Admin\AppData\Roaming\Microsoft
Opens: C:\Windows\System32\Sens.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low
Opens: C:\Windows\System32\stdole2.tlb
Opens: C:\Users\Admin\Favorites
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Virtualized
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE\Low
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache\Low
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\Low
Opens: C:\Users\Admin\AppData\Local\Temp\Low
Opens: C:\Users\Admin\AppData\Local\Temp
Opens: C:\Windows\System32\rundll32.exe
Opens: C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf
Opens: C:\Windows\rasadhlp.dll
Opens: C:\Windows\System32\rasadhlp.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5
Opens: C:\Windows
Opens: C:\Windows\AppPatch
Opens: C:\Windows\Globalization
Opens: C:\Windows\Globalization\Sorting
Opens: C:\Windows\System32\NapiNSP.dll
Opens: C:\Windows\System32\pnprpnsd.dll
Opens: C:\Windows\System32\en-US
Opens: C:\Windows\System32\apisetschema.dll
Opens: C:\Windows\System32\KernelBase.dll
Opens: C:\Windows\System32\locale.nls
Opens: C:\Windows\System32\gdi32.dll
Opens: C:\Windows\System32\lpk.dll
Opens: C:\Windows\System32\usp10.dll
Opens: C:\Windows\System32\msvcrt.dll
Opens: C:\Windows\System32\imagehlp.dll
Opens: C:\Windows\System32\winnr.dll
Opens: C:\Windows\System32\apphelp.dll
Opens: C:\Windows\AppPatch\AcLayers.dll
Opens: C:\Windows\System32\sspicli.dll
Opens: C:\Windows\System32\rpcrt4.dll
Opens: C:\Windows\System32\shell32.dll
Opens: C:\Windows\System32\shlwapi.dll
Opens: C:\Windows\System32\wship6.dll
Opens: C:\Windows\System32\ole32.dll
Opens: C:\Windows\System32\oleaut32.dll
Opens: C:\Windows\System32\userenv.dll
Opens: C:\Windows\System32\profapi.dll
Opens: C:\Windows\System32\winspool.drv
Opens: C:\Windows\System32\mpr.dll
Opens: C:\Windows\System32\msctf.dll
Opens: C:\Windows\System32\en-US\rundll32.exe.mui
Opens: C:\Windows\System32\urlmon.dll
Opens: C:\Windows\System32\msasn1.dll
Opens: C:\Windows\System32\iertutil.dll
Opens: C:\Windows\System32\uxtheme.dll
Opens: C:\Windows\System32\dwmapapi.dll
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens: C:\Windows\WindowsShell.Manifest

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5\index.dat
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
Opens: C:\Windows\System32\ansi.dll
Opens: C:\Windows\System32\IPHLPAPI.DLL
Opens: C:\Windows\System32\winnsi.dll
Opens: C:\Windows\System32\nlaapi.dll
Opens: C:\Windows\System32\cryptbase.dll
Opens: C:\Windows\System32\en-US\wininet.dll.mui
Opens: C:\Windows\System32\rpcss.dll
Opens: C:\Windows\System32\drivers\etc\hosts
Opens: C:\Windows\System32\FWPUCLNT.DLL
Opens: C:\Windows\System32\WININET.dll.manifest
Opens: C:\Windows\System32\rundll32.exe.Local\
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5\desktop.ini
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\desktop.ini
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\desktop.ini
Opens: C:\Windows\System32\drivers\etc\lmhosts
Opens: C:\Windows\System32\calc.exe
Opens: C:\dump.pcap
Opens: C:\Windows\System32\en-US\urlmon.dll.mui
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.microsoft[2].txt
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[1].txt
Opens: C:\Windows\Prefetch\ReadyBoot
Opens: C:\Windows\Prefetch\ReadyBoot\Trace3.fx
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[2].txt
Opens: C:\\$MFT
Opens: C:\\$Secure:\$SDS
Opens: C:\\$Extend\\$\UsnJrnl:\$J
Opens: C:\System Volume Information
Opens: C:\Windows\System32\CodeIntegrity\driver.stl
Opens: C:\ProgramData
Opens: C:\ProgramData\Microsoft
Opens: C:\ProgramData\Microsoft\MF\Active.GRL
Opens: C:\Windows\System32\drivers
Opens: C:\Windows\System32\drivers\cdrom.sys
Opens: C:\Windows\System32\CodeIntegrity\bootcat.cache
Opens: C:\Windows\System32\drivers\null.sys
Opens: C:\Windows\System32\drivers\beep.sys
Opens: C:\Windows\System32\drivers\vga.sys
Opens: C:\Windows\System32\drivers\videoprt.sys
Opens: C:\Windows\System32\drivers\watchdog.sys
Opens: C:\Windows\System32\drivers\RDPCDD.sys
Opens: C:\Windows\System32\drivers\RDPCNDD.sys
Opens: C:\Windows\System32\drivers\RDPPREFMP.sys
Opens: C:\Windows\System32\drivers\msfs.sys
Opens: C:\Windows\System32\drivers\npfs.sys
Opens: C:\Windows\System32\drivers\tdx.sys
Opens: C:\Windows\System32\drivers\tdi.sys
Opens: C:\Windows\System32\drivers\afd.sys
Opens: C:\Windows\System32\drivers\netbt.sys
Opens: C:\Windows\System32\drivers\wfplwf.sys
Opens: C:\Windows\System32\drivers\pacer.sys
Opens: C:\Windows\System32\drivers\netbios.sys
Opens: C:\Windows\System32\drivers\wanarp.sys
Opens: C:\Windows\System32\drivers\termdd.sys
Opens: C:\Windows\System32\drivers\rdbsp.sys
Opens: C:\Windows\System32\drivers\ntproxy.sys
Opens: C:\Windows\System32\drivers\msmbios.sys
Opens: C:\Windows\System32\drivers\discache.sys
Opens: C:\Windows\System32\drivers\csc.sys
Opens: C:\Windows\System32\drivers\dfsc.sys
Opens: C:\Windows\System32\drivers\blbdrive.sys
Opens: C:\Windows\bootstat.dat
Opens: C:\Windows\System32\smss.exe
Opens: C:\Windows\System32\drivers\tunnel.sys
Opens: C:\Windows\System32\drivers\i804prt.sys
Opens: C:\Windows\System32\drivers\kbdclass.sys
Opens: C:\Windows\System32\drivers\mouseclass.sys
Opens: C:\Windows\System32\drivers\parport.sys
Opens: C:\Windows\System32\drivers\vgapnp.sys
Opens: C:\Windows\System32\drivers\E1660I32.sys
Opens: C:\Windows\System32\drivers\CmBatt.sys
Opens: C:\Windows\System32\drivers\CompositeBus.sys
Opens: C:\Windows\System32\drivers\agilevpn.sys
Opens: C:\Windows\System32\drivers\rasl2tp.sys
Opens: C:\Windows\System32\drivers\ndistapi.sys
Opens: C:\Windows\System32\drivers\ndiswan.sys
Opens: C:\Windows\System32\drivers\rasppoe.sys
Opens: C:\Windows\System32\drivers\rasppptp.sys
Opens: C:\Windows\System32\drivers\rassstp.sys
Opens: C:\Windows\System32\drivers\rdpbus.sys
Opens: C:\Windows\System32\drivers\swenum.sys
Opens: C:\Windows\System32\drivers\ks.sys
Opens: C:\Windows\System32\drivers\umbus.sys
Opens: C:\Windows\System32\autochk.exe
Opens: C:\Windows\System32\drivers\ndproxy.sys
Opens: C:\Users\Admin\Documents
Opens: C:\Users\Default
Opens: C:\Users\Default\AppData\Local
Opens: C:\Users\Default\Documents
Opens: C:\Users\Public
Opens: C:\Users\Public\Documents
Opens: C:\Windows\System32\dxapi.dll
Opens: C:\Windows\System32\normaliz.dll
Opens: C:\Windows\System32\Wldap32.dll
Opens: C:\Windows\System32\clbcatq.dll
Opens: C:\Windows\System32\psapi.dll
Opens: C:\Windows\System32\setupapi.dll
Opens: C:\Windows\System32\cmdlg32.dll
Opens: C:\Windows\System32\devobj.dll
Opens: C:\Windows\System32\wintrust.dll
Opens: C:\Windows\System32\cfgmgr32.dll
Opens: C:\Windows\System32\comctl32.dll
Opens: C:\Windows\System32\config
Opens: C:\Windows\System32\config\SOFTWARE
Opens: C:\Windows\System32\LogFiles

Opens: C:\Windows\System32\LogFiles\WMI
Opens: C:\Windows\System32\LogFiles\WMI\RtBackup
Opens: C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTEventLog-Application.etl
Opens: C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTEventLog-System.etl
Opens: C:\Windows\System32\config\TxR
Opens: C:\Windows\System32\config\TxR\{6cccd301-6e01-11de-8bed-001e0bcd1824}.TM.b1f
001e0bcd1824}.TM.Container00000000000000000001.regtrans-ms
Opens: C:\Windows\System32\win32k.sys
Opens: C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTDiagLog.etl
Opens: C:\Windows\System32\drivers\dxapi.sys
Opens: C:\Windows\System32\config\DEFAULT
Opens: C:\Windows\System32\csrss.exe
Opens: C:\Windows\System32\csrssv.dll
Opens: C:\Windows\System32\basesrv.dll
Opens: C:\Windows\System32\winsrv.dll
Opens: C:\Windows\System32\en-US\csrss.exe.mui
Opens: C:\Windows\System32\en-US\winsrv.dll.mui
Opens: C:\Windows\System32\drivers\dxg.sys
Opens: C:\Windows\System32\FNTCACHE.DAT
Opens: C:\Windows\System32\en-US\win32k.sys.mui
Opens: C:\Windows\System32\drivers\monitor.sys
Opens: C:\Windows\AppPatch\drvmain.sdb
Opens: C:\Windows\System32\tsddd.dll
Opens: C:\Windows\Fonts
Opens: C:\Windows\Fonts\vgasys.fon
Opens: C:\Windows\Fonts\vgaoem.fon
Opens: C:\Windows\Fonts\vgafix.fon
Opens: C:\Windows\Fonts\dosapp.fon
Opens: C:\Windows\Fonts\cga40woa.fon
Opens: C:\Windows\Fonts\cga80woa.fon
Opens: C:\Windows\Fonts\ega40woa.fon
Opens: C:\Windows\Fonts\ega80woa.fon
Opens: C:\Windows\System32\sxssrv.dll
Opens: C:\Windows\System32\wininit.exe
Opens: C:\Windows\System32\en-US\wininit.exe.mui
Opens: C:\Windows\System32\RpcRtRemote.dll
Opens: C:\Windows\System32\vga.dll
Opens: C:\Windows\System32\framebuf.dll
Opens: C:\Windows\System32\vgaz56.dll
Opens: C:\Windows\System32\vgaz64k.dll
Opens: C:\Windows\System32\winlogon.exe
Opens: C:\Windows\System32\KBDUS.DLL
Opens: C:\Windows\Fonts\batang.ttc
Opens: C:\Windows\Fonts\gulim.ttc
Opens: C:\Windows\Fonts\malgun.ttf
Opens: C:\Windows\Fonts\malgunbd.ttf
Opens: C:\Windows\Fonts\meiryong.ttc
Opens: C:\Windows\Fonts\meiryob.ttc
Opens: C:\Windows\Fonts\msjhe.ttc
Opens: C:\Windows\Fonts\msjhebd.ttc
Opens: C:\Windows\Fonts\msyh.ttc
Opens: C:\Windows\Fonts\msyhebd.ttc
Opens: C:\Windows\Fonts\mingliu.ttc
Opens: C:\Windows\Fonts\mingliub.ttc
Opens: C:\Windows\Fonts\msgothic.ttc
Opens: C:\Windows\Fonts\msmincho.ttc
Opens: C:\Windows\Fonts\segoeui.ttc
Opens: C:\Windows\Fonts\segoeui.b.ttc
Opens: C:\Windows\Fonts\simsum.ttc
Opens: C:\Windows\Fonts\simsum.b.ttc
Opens: C:\Windows\Fonts\tahoma.ttf
Opens: C:\Windows\Fonts\microsf.ttf
Opens: C:\Windows\System32\en-US\user32.dll.mui
Opens: C:\Windows\Fonts\marlett.ttf
Opens: C:\Windows\Prefetch\ReadyBoot\ReadyBoot.etl
Opens: C:\Windows\Cursors
Opens: C:\Windows\Cursors\ aero_arrow.cur
Opens: C:\Windows\Cursors\ aero_busy.ani
Opens: C:\Windows\Cursors\ aero_up.cur
Opens: C:\Windows\Cursors\ aero_nwse.cur
Opens: C:\Windows\Cursors\ aero_nesw.cur
Opens: C:\Windows\Cursors\ aero_ew.cur
Opens: C:\Windows\Cursors\ aero_ns.cur
Opens: C:\Windows\Cursors\ aero_move.cur
Opens: C:\Windows\Cursors\ aero_unavail.cur
Opens: C:\Windows\Cursors\ aero_working.ani
Opens: C:\Windows\Cursors\ aero_helpsel.cur
Opens: C:\Windows\Cursors\ aero_pen.cur
Opens: C:\Windows\Cursors\ aero_link.cur
Opens: C:\Windows\System32\WIS0WinDH.dll
Opens: C:\Windows\System32\services.exe
Opens: C:\Windows\System32\services.dll
Opens: C:\Windows\winsxs
Opens: C:\Windows\winsxs\Manifests
Opens: C:\Windows\winsxs\Manifests\x86_microsoft.windows.systemcompatible_6595b64144ccf1df_6.0.7600.16385_none_49adccbbe8169a03.manifest
Opens: C:\Windows\assembly
Opens: C:\Windows\assembly\GAC_32
Opens: C:\Windows\winsxs\Manifests\x86_microsoft.windows.isolationautomation_6595b64144ccf1df_1.0.0.0_none_35d357a66c38ade4.manifest
Opens: C:\Windows\winsxs\Manifests\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80.manifest
Opens: C:\Windows\winsxs\Manifests\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af.manifest
Opens: C:\Windows\winsxs\Manifests\x86_microsoft.windows.i..otomation.proxystub_6595b64144ccf1df_1.0.7600.16385_none_9d148a8db8d32238.manifest
Opens: C:\Windows\winsxs\Manifests\x86_microsoft.windows.common-controls.resources_6595b64144ccf1df_5.82.7600.16385_en-us_020378a8991bbcc2.manifest
Opens: C:\Windows\System32\lsass.exe
Opens: C:\Windows\System32\lsme.exe
Opens: C:\Windows\System32\winsta.dll
Opens: C:\Windows\System32\en-US\winlogon.exe.mui
Opens: C:\Windows\System32\scext.dll
Opens: C:\Windows\System32\scsersv.dll
Opens: C:\Windows\System32\srvc1i.dll
Opens: C:\Windows\System32\en-US\services.exe.mui
Opens: C:\Windows\System32\aelupsvc.dll
Opens: C:\Windows\System32\en-US\aelupsvc.dll.mui
Opens: C:\Windows\System32\drivers\en-US
Opens: C:\Windows\System32\drivers\en-US\afd.sys.mui
Opens: C:\Windows\System32\alg.exe
Opens: C:\Windows\System32\en-US\alg.exe.mui
Opens: C:\Windows\System32\appidsv.dll
Opens: C:\Windows\System32\en-US\appidsv.dll.mui

Opens:	C:\Windows\System32\appinfo.dll
Opens:	C:\Windows\System32\en-US\appinfo.dll.mui
Opens:	C:\Windows\System32\appmgmts.dll
Opens:	C:\Windows\System32\en-US\appmgmts.dll.mui
Opens:	C:\Windows\System32\rascfg.dll
Opens:	C:\Windows\System32\en-US\rascfg.dll.mui
Opens:	C:\Windows\System32\audiosrv.dll
Opens:	C:\Windows\System32\en-US\AudioSrv.dll.mui
Opens:	C:\Windows\System32\AxInstSv.dll
Opens:	C:\Windows\System32\en-US\AxInstSv.dll.mui
Opens:	C:\Windows\System32\bdesvc.dll
Opens:	C:\Windows\System32\en-US\bdesvc.dll.mui
Opens:	C:\Windows\System32\BFE.DLL
Opens:	C:\Windows\System32\en-US\bfe.dll.mui
Opens:	C:\Windows\System32\qmgr.dll
Opens:	C:\Windows\System32\en-US\qmgr.dll.mui
Opens:	C:\Windows\System32\sysntfy.dll
Opens:	C:\Windows\System32\wmmsgapi.dll
Opens:	C:\Windows\System32\browser.dll
Opens:	C:\Windows\System32\en-US\browser.dll.mui
Opens:	C:\Windows\System32\bthserv.dll
Opens:	C:\Windows\System32\en-US\bthserv.dll.mui
Opens:	C:\Windows\System32\certprop.dll
Opens:	C:\Windows\System32\en-US\certprop.dll.mui
Opens:	C:\Windows\System32\clfs.sys
Opens:	C:\Windows\System32\en-US\clfs.sys.mui
Opens:	C:\Windows\System32\sspisrv.dll
Opens:	C:\Windows\System32\lsasrv.dll
Opens:	C:\Windows\System32\samsrv.dll
Opens:	C:\Windows\System32\cryptdll.dll
Opens:	C:\Windows\System32\wevtapi.dll
Opens:	C:\Windows\System32\cngaudit.dll
Opens:	C:\Windows\System32\authz.dll
Opens:	C:\Windows\System32\ncrypt.dll
Opens:	C:\Windows\System32\bcrypt.dll
Opens:	C:\Windows\System32\en-US\lsasrv.dll.mui
Opens:	C:\Windows\System32\comres.dll
Opens:	C:\Windows\System32\en-US\comres.dll.mui
Opens:	C:\Windows\System32\cryptsvc.dll
Opens:	C:\Windows\System32\en-US\cryptsvc.dll.mui
Opens:	C:\Windows\System32\cscsvc.dll
Opens:	C:\Windows\System32\en-US\cscsvc.dll.mui
Opens:	C:\Windows\System32\oleres.dll
Opens:	C:\Windows\System32\en-US\oleres.dll.mui
Opens:	C:\Windows\System32\defragsvc.dll
Opens:	C:\Windows\System32\config\SECURITY
Opens:	C:\Windows\System32\en-US\defragsvc.dll.mui
Opens:	C:\Windows\System32\dhcpcore.dll
Opens:	C:\Windows\System32\en-US\dhcpcore.dll.mui
Opens:	C:\Windows\System32\en-US\dnsapi.dll.mui
Opens:	C:\Windows\System32\dot3svc.dll
Opens:	C:\Windows\System32\en-US\dot3svc.dll.mui
Opens:	C:\Windows\Fonts\modern.fon
Opens:	C:\Windows\Fonts\roman.fon
Opens:	C:\Windows\Fonts\script.fon
Opens:	C:\Windows\Fonts\cours.fon
Opens:	C:\Windows\Fonts\serife.fon
Opens:	C:\Windows\Fonts\sserife.fon
Opens:	C:\Windows\Fonts\small.fon
Opens:	C:\Windows\Fonts\small.fon
Opens:	C:\Windows\System32\mspri.v
Opens:	C:\Windows\System32\netjoin.dll
Opens:	C:\Windows\System32\negoexts.dll
Opens:	C:\Windows\System32\kerberos.dll
Opens:	C:\Windows\System32\cryptsp.dll
Opens:	C:\Windows\System32\msv1_0.dll
Opens:	C:\Windows\System32\wdi
Opens:	C:\Windows\System32\wdi\LogFiles
Opens:	C:\Windows\System32\wdi\LogFiles\BootCKCL.etl
Opens:	C:\Windows\System32\netlogon.dll
Opens:	C:\Windows\System32\logoncli.dll
Opens:	C:\Windows\System32\schannel.dll
Opens:	C:\Windows\System32\wdigest.dll
Opens:	C:\Windows\System32\C_28591.NLS
Opens:	C:\Windows\System32\rsaenh.dll
Opens:	C:\Windows\System32\Tspkg.dll
Opens:	C:\Windows\System32\pku2u.dll
Opens:	C:\Windows\System32\bcryptprimitives.dll
Opens:	C:\Windows\System32\efslsaext.dll
Opens:	C:\Windows\System32\Microsoft\Protect\S-1-5-18
Opens:	C:\Windows\System32\Microsoft\Protect\S-1-5-18\User
Opens:	C:\Windows\System32\dps.dll
Opens:	C:\Windows\System32\en-US\dps.dll.mui
Opens:	C:\Windows\System32\eapsvc.dll
Opens:	C:\Windows\System32\en-US\eapsvc.dll.mui
Opens:	C:\Windows\System32\efssvc.dll
Opens:	C:\Windows\System32\en-US\efssvc.dll.mui
Opens:	C:\Windows\ehome
Opens:	C:\Windows\ehome\ehrecvr.exe
Opens:	C:\Windows\ehome\en-US
Opens:	C:\Windows\ehome\en-US\ehrecvr.exe.mui
Opens:	C:\Windows\System32\config\SAM
Opens:	C:\Windows\ehome\ehsched.exe
Opens:	C:\Windows\ehome\en-US\ehsched.exe.mui
Opens:	C:\Windows\System32\wevtstvc.dll
Opens:	C:\Windows\System32\en-US\wevtstvc.dll.mui
Opens:	C:\Windows\System32\FXSRESM.dll
Opens:	C:\Windows\System32\en-US\FXSRESM.dll.mui
Opens:	C:\Windows\System32\scecli.dll
Opens:	C:\Windows\System32\fdPHost.dll
Opens:	C:\Windows\System32\en-US\fdPHost.dll.mui
Opens:	C:\Windows\System32\FDResPub.dll
Opens:	C:\Windows\System32\en-US\fdrespub.dll.mui
Opens:	C:\Windows\System32\drivers\fileinfo.sys
Opens:	C:\Windows\System32\drivers\filetrace.sys
Opens:	C:\Windows\System32\drivers\fltMgr.sys
Opens:	C:\Windows\System32\drivers\en-US\fltmgr.sys.mui
Opens:	C:\Windows\System32\FntCache.dll
Opens:	C:\Windows\System32\en-US\FntCache.dll.mui
Opens:	C:\Windows\System32\PresentationHost.exe
Opens:	C:\Windows\System32\en-US\PresentationHost.exe.mui
Opens:	C:\Windows\System32\drivers\fsdepends.sys
Opens:	C:\Windows\System32\drivers\fvevol.sys
Opens:	C:\Windows\System32\drivers\en-US\fvevol.sys.mui
Opens:	C:\Windows\System32\gpapi.dll
Opens:	C:\Windows\System32\en-US\gpapi.dll.mui

Opens: C:\Windows\System32\hidserv.dll
Opens: C:\Windows\System32\en-US\hidserv.dll.mui
Opens: C:\Windows\System32\KMSVC.DLL
Opens: C:\Windows\System32\en-US\KMSVC.DLL.MUI
Opens: C:\Windows\System32\ListSvc.dll
Opens: C:\Windows\System32\en-US\listsvc.dll.mui
Opens: C:\Windows\System32\prosvsvc.dll
Opens: C:\Windows\System32\en-US\prosvsvc.dll.mui
Opens: C:\Windows\System32\drivers\http.sys
Opens: C:\Windows\System32\drivers\en-US\http.sys.mui
Opens: C:\Windows\System32\drivers\hwpolicy.sys
Opens: C:\Windows\Microsoft.NET
Opens: C:\Windows\Microsoft.NET\Framework
Opens: C:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication Foundation
Opens: C:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication
Foundation\ServiceModel\InstallIRC.dll
Opens: C:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication
Foundation\en-US\ServiceModel\InstallIRC.dll.mui
Opens: C:\Windows\System32\IKEEXT.DLL
Opens: C:\Windows\System32\en-US\ikeext.dll.mui
Opens: C:\Windows\System32\IPBusEnum.dll
Opens: C:\Windows\System32\en-US\IPBusEnum.dll.mui
Opens: C:\Windows\System32\iphlpvc.dll
Opens: C:\Windows\System32\en-US\iphlpvc.dll.mui
Opens: C:\Windows\System32\drivers\irenum.sys
Opens: C:\Windows\System32\keyiso.dll
Opens: C:\Windows\System32\en-US\keyiso.dll.mui
Opens: C:\Windows\System32\srsvvc.dll
Opens: C:\Windows\System32\en-US\srsvvc.dll.mui
Opens: C:\Windows\System32\wkssvc.dll
Opens: C:\Windows\System32\en-US\wkssvc.dll.mui
Opens: C:\Windows\System32\lltdres.dll
Opens: C:\Windows\System32\en-US\lltdres.dll.mui
Opens: C:\Windows\System32\lmhsvc.dll
Opens: C:\Windows\System32\en-US\lmhsvc.dll.mui
Opens: C:\Windows\System32\drivers\luaifv.sys
Opens: C:\Windows\System32\drivers\en-US\luaifv.sys.mui
Opens: C:\Windows\ehome\ehres.dll
Opens: C:\Windows\ehome\en-US\ehres.dll.mui
Opens: C:\Windows\System32\mmcscs.dll
Opens: C:\Windows\System32\en-US\mmcscs.dll.mui
Opens: C:\Windows\System32\drivers\mountmgr.sys
Opens: C:\Windows\System32\drivers\en-US\mountmgr.sys.mui
Opens: C:\Windows\System32\FirewallAPI.dll
Opens: C:\Windows\System32\en-US\FirewallAPI.dll.mui
Opens: C:\Windows\System32\WebClnt.dll
Opens: C:\Windows\System32\en-US\WebClnt.dll.mui
Opens: C:\Windows\Prefetch\CALC.EXE-77FDF17F.pf
Opens: C:\Windows\System32\drivers\mshidkmdf.sys
Opens: C:\Windows\System32\iscsidsc.dll
Opens: C:\Windows\System32\en-US\iscsidsc.dll.mui
Opens: C:\Windows\System32\msimgl.dll
Opens: C:\Windows\System32\en-US\msimgl.dll.mui
Opens: C:\Windows\System32\drivers\mup.sys
Opens: C:\Windows\System32\QAGENTRT.DLL
Opens: C:\Windows\System32\en-US\QAgentRT.dll.mui
Opens: C:\Windows\System32\drivers\ndis.sys
Opens: C:\Windows\System32\drivers\en-US\ndis.sys.mui
Opens: C:\Windows\System32\en-US\netlogon.dll.mui
Opens: C:\Windows\System32\netman.dll
Opens: C:\Windows\System32\en-US\netman.dll.mui
Opens: C:\Windows\System32\netprofm.dll
Opens: C:\Windows\System32\en-US\netprofm.dll.mui
Opens: C:\Windows\System32\nlasvc.dll
Opens: C:\Windows\System32\en-US\nlasvc.dll.mui
Opens: C:\Windows\System32\nsisvc.dll
Opens: C:\Windows\System32\en-US\nsisvc.dll.mui
Opens: C:\Windows\System32\pnprpsvc.dll
Opens: C:\Windows\System32\en-US\pnprpsvc.dll.mui
Opens: C:\Windows\System32\p2psvc.dll
Opens: C:\Windows\System32\en-US\p2psvc.dll.mui
Opens: C:\Windows\System32\drivers\partmgr.sys
Opens: C:\Windows\System32\drivers\en-US\partmgr.sys.mui
Opens: C:\Windows\System32\pcasvc.dll
Opens: C:\Windows\System32\en-US\pcasvc.dll.mui
Opens: C:\Windows\System32\PeerDistSvc.dll
Opens: C:\Windows\System32\en-US\PeerDistSvc.dll.mui
Opens: C:\Windows\System32\pla.dll
Opens: C:\Windows\System32\en-US\pla.dll.mui
Opens: C:\Windows\System32\umpnpgmgr.dll
Opens: C:\Windows\System32\en-US\umpnpgmgr.dll.mui
Opens: C:\Windows\System32\pnrpauto.dll
Opens: C:\Windows\System32\en-US\pnrpauto.dll.mui
Opens: C:\Windows\System32\polstore.dll
Opens: C:\Windows\System32\en-US\polstore.dll.mui
Opens: C:\Windows\System32\umpo.dll
Opens: C:\Windows\System32\en-US\umpo.dll.mui
Opens: C:\Windows\System32\profsvc.dll
Opens: C:\Windows\System32\en-US\profsvc.dll.mui
Opens: C:\Windows\System32\psbase.dll
Opens: C:\Windows\System32\en-US\psbase.dll.mui
Opens: C:\Windows\System32\drivers\en-US\pacer.sys.mui
Opens: C:\Windows\System32\qwave.dll
Opens: C:\Windows\System32\en-US\qwave.dll.mui
Opens: C:\Windows\System32\drivers\qwavedrv.sys
Opens: C:\Windows\System32\drivers\en-US\qwavedrv.sys.mui
Opens: C:\Windows\System32\rasauto.dll
Opens: C:\Windows\System32\en-US\rasauto.dll.mui
Opens: C:\Windows\System32\rasmans.dll
Opens: C:\Windows\System32\en-US\rasmans.dll.mui
Opens: C:\Windows\System32\ssstpsvc.dll
Opens: C:\Windows\System32\en-US\ssstpsvc.dll.mui
Opens: C:\Windows\System32\mprdim.dll
Opens: C:\Windows\System32\en-US\mprdim.dll.mui
Opens: C:\Windows\System32\regsvc.dll
Opens: C:\Windows\System32\en-US\regsvc.dll.mui
Opens: C:\Windows\System32\RpcEpMap.dll
Opens: C:\Windows\System32\en-US\RpcEpMap.dll.mui
Opens: C:\Windows\System32\Locator.exe
Opens: C:\Windows\System32\en-US\Locator.exe.mui
Opens: C:\Windows\System32\en-US\samsrv.dll.mui
Opens: C:\Windows\System32\SCardSvr.dll
Opens: C:\Windows\System32\en-US\SCardSvr.dll.mui
Opens: C:\Windows\System32\drivers\scfilter.sys
Opens: C:\Windows\System32\drivers\en-US\scfilter.sys.mui
Opens: C:\Windows\System32\schedsvc.dll

Opens: C:\Windows\System32\en-US\schedsvc.dll.mui
Opens: C:\Windows\System32\sdrsvc.dll
Opens: C:\Windows\System32\en-US\sdrsvc.dll.mui
Opens: C:\Windows\System32\seclogon.dll
Opens: C:\Windows\System32\en-US\seclogon.dll.mui
Opens: C:\Windows\System32\en-US\sens.dll.mui
Opens: C:\Windows\System32\sensrvc.dll
Opens: C:\Windows\System32\en-US\sensrvc.dll.mui
Opens: C:\Windows\System32\SessEnv.dll
Opens: C:\Windows\System32\en-US\sessenv.dll.mui
Opens: C:\Windows\System32\ipnathlp.dll
Opens: C:\Windows\System32\en-US\ipnathlp.dll.mui
Opens: C:\Windows\System32\shsvcs.dll
Opens: C:\Windows\System32\en-US\shsvcs.dll.mui
Opens: C:\Windows\System32\tcpipcfg.dll
Opens: C:\Windows\System32\en-US\tcpipcfg.dll.mui
Opens: C:\Windows\System32\snmptrap.exe
Opens: C:\Windows\System32\en-US\snmptrap.exe.mui
Opens: C:\Windows\System32\spoolsv.exe
Opens: C:\Windows\System32\en-US\spoolsv.exe.mui
Opens: C:\Windows\System32\spoolsv.exe
Opens: C:\Windows\System32\en-US\spoolsv.exe.mui
Opens: C:\Windows\System32\spuuinotify.dll
Opens: C:\Windows\System32\en-US\spuuinotify.dll.mui
Opens: C:\Windows\System32\ssdpsrv.dll
Opens: C:\Windows\System32\en-US\ssdpsrv.dll.mui
Opens: C:\Windows\System32\wiaservc.dll
Opens: C:\Windows\System32\en-US\wiaservc.dll.mui
Opens: C:\Windows\System32\vmstorfltres.dll
Opens: C:\Windows\System32\StorSvc.dll
Opens: C:\Windows\System32\en-US\StorSvc.dll.mui
Opens: C:\Windows\System32\swprv.dll
Opens: C:\Windows\System32\en-US\swprv.dll.mui
Opens: C:\Windows\System32\sysmain.dll
Opens: C:\Windows\System32\TabSvc.dll
Opens: C:\Windows\System32\en-US\TabSvc.dll.mui
Opens: C:\Windows\System32\tapisrv.dll
Opens: C:\Windows\System32\en-US\tapisrv.dll.mui
Opens: C:\Windows\System32\tbssvc.dll
Opens: C:\Windows\System32\en-US\tbssvc.dll.mui
Opens: C:\Windows\System32\termsrv.dll
Opens: C:\Windows\System32\en-US\termsrv.dll.mui
Opens: C:\Windows\System32\themeservice.dll
Opens: C:\Windows\System32\en-US\themeservice.dll.mui
Opens: C:\Windows\System32\trkwks.dll
Opens: C:\Windows\System32\en-US\trkwks.dll.mui
Opens: C:\Windows\servicing
Opens: C:\Windows\servicing\TrustedInstaller.exe
Opens: C:\Windows\servicing\en-US\TrustedInstaller.exe.mui
Opens: C:\Windows\System32\drivers\tssecsrv.sys
Opens: C:\Windows\System32\drivers\TsUsbFlt.sys
Opens: C:\Windows\System32\drivers\en-US\tsusbflt.sys.mui
Opens: C:\Windows\System32\UI0Detect.exe
Opens: C:\Windows\System32\en-US\ui0detect.exe.mui
Opens: C:\Windows\System32\umrpd.dll
Opens: C:\Windows\System32\en-US\umrpd.dll.mui
Opens: C:\Windows\System32\upnphost.dll
Opens: C:\Windows\System32\en-US\upnphost.dll.mui
Opens: C:\Windows\System32\dmw.exe
Opens: C:\Windows\System32\en-US\dmw.exe.mui
Opens: C:\Windows\System32\vaultsvc.dll
Opens: C:\Windows\System32\en-US\vaultsvc.dll.mui
Opens: C:\Windows\System32\vds.exe
Opens: C:\Windows\System32\en-US\vds.exe.mui
Opens: C:\Windows\System32\drivers\volmgrx.sys
Opens: C:\Windows\System32\drivers\en-US\volmgrx.sys.mui
Opens: C:\Windows\System32\VSSVC.exe
Opens: C:\Windows\System32\en-US\VSSVC.exe.mui
Opens: C:\Windows\System32\drivers\wwi fibus.sys
Opens: C:\Windows\System32\drivers\en-US\wwi fibus.sys.mui
Opens: C:\Windows\System32\w32time.dll
Opens: C:\Windows\System32\en-US\w32time.dll.mui
Opens: C:\Windows\System32\wbengine.exe
Opens: C:\Windows\System32\en-US\wbengine.exe.mui
Opens: C:\Windows\System32\wbiosrvc.dll
Opens: C:\Windows\System32\en-US\wbiosrvc.dll.mui
Opens: C:\Windows\System32\wcnscvc.dll
Opens: C:\Windows\System32\en-US\wcnscvc.dll.mui
Opens: C:\Windows\System32\WcsPlugInService.dll
Opens: C:\Windows\System32\en-US\WcsPlugInService.dll.mui
Opens: C:\Windows\System32\wdi.dll
Opens: C:\Windows\System32\en-US\wdi.dll.mui
Opens: C:\Windows\System32\wecsvc.dll
Opens: C:\Windows\System32\en-US\wecsvc.dll.mui
Opens: C:\Windows\System32\werclsupport.dll
Opens: C:\Windows\System32\en-US\werclsupport.dll.mui
Opens: C:\Windows\System32\wersvc.dll
Opens: C:\Windows\System32\en-US\wersvc.dll.mui
Opens: C:\Program Files
Opens: C:\Program Files\Windows Defender
Opens: C:\Program Files\Windows Defender\MsMpRes.dll
Opens: C:\Program Files\Windows Defender\en-US\MsMpRes.dll.mui
Opens: C:\Windows\System32\winhttp.dll
Opens: C:\Windows\System32\en-US\winhttp.dll.mui
Opens: C:\Windows\System32\wbem
Opens: C:\Windows\System32\wbem\WMIsvc.dll
Opens: C:\Windows\System32\wbem\en-US
Opens: C:\Windows\System32\wbem\en-US\WMIsvc.dll.mui
Opens: C:\Windows\System32\WsmSvc.dll
Opens: C:\Windows\System32\en-US\WsmSvc.dll.mui
Opens: C:\Windows\System32\wlansvc.dll
Opens: C:\Windows\System32\en-US\wlansvc.dll.mui
Opens: C:\Windows\System32\wbem\WmiApSrv.exe
Opens: C:\Windows\System32\wbem\en-US\WmiApSrv.exe.mui
Opens: C:\Program Files\Windows Media Player
Opens: C:\Program Files\Windows Media Player\wmpnetwk.exe
Opens: C:\Program Files\Windows Media Player\en-US
Opens: C:\Program Files\Windows Media Player\en-US\wmpnetwk.exe.mui
Opens: C:\Windows\System32\wpcsvc.dll
Opens: C:\Windows\System32\en-US\wpcsvc.dll.mui
Opens: C:\Windows\System32\wpd busenum.dll
Opens: C:\Windows\System32\en-US\wpd busenum.dll.mui
Opens: C:\Windows\System32\drivers\ws2ifsl.sys
Opens: C:\Windows\System32\drivers\en-US\ws2ifsl.sys.mui
Opens: C:\Windows\System32\wscsvc.dll
Opens: C:\Windows\System32\en-US\wscsvc.dll.mui

Opens: C:\Windows\System32\SearchIndexer.exe
Opens: C:\Windows\System32\en-US\SearchIndexer.exe.mui
Opens: C:\Windows\System32\wuaueng.dll
Opens: C:\Windows\System32\en-US\wuaueng.dll.mui
Opens: C:\Windows\System32\WUDFSvc.dll
Opens: C:\Windows\System32\en-US\wudfsvc.dll.mui
Opens: C:\Windows\System32\wmansvc.dll
Opens: C:\Windows\System32\en-US\wmansvc.dll.mui
Opens: C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTEventlog-Security.etl
Opens: C:\Windows\security
Opens: C:\Windows\System32\ubpm.dll
Opens: C:\Windows\System32\LogFiles\Scm
Opens: C:\Windows\System32\svchost.exe
Opens: C:\Windows\System32\SPInf.dll
Opens: C:\Windows\System32\devrtl.dll
Opens: C:\Windows\System32\en-US\svchost.exe.mui
Opens: C:\Windows\System32\pcwum.dll
Opens: C:\Windows\System32\en-US\setupapi.dll.mui
Opens: C:\Windows\System32\powrprof.dll
Opens: C:\Program Files\Common Files
Opens: C:\Windows\ServiceProfiles\NetworkService
Opens: C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
Opens: C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT{6cccd2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf
8bed-001e0bcd1824}.TM.blf
Opens: C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT{6cccd2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000001.regtrans-ms
Opens: C:\Windows\System32\en-US\wshtcpip.dll.mui
Opens: C:\Windows\System32\en-US\wship6.dll.mui
Opens: C:\Windows\System32\wshqos.dll
Opens: C:\Windows\System32\en-US\wshqos.dll.mui
Opens: C:\Windows\ServiceProfiles\LocalService
Opens: C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
Opens: C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT{6cccd2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf
8bed-001e0bcd1824}.TM.blf
Opens: C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT{6cccd2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000001.regtrans-ms
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local
Opens: C:\Windows\System32\version.dll
Opens: C:\Windows\System32\LogonUI.exe
Opens: C:\Windows\winsxs\Manifests\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2.manifest
Opens: C:\Windows\winsxs\Manifests\x86_microsoft.windows.c...-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9.manifest
Opens: C:\Windows\System32\en-US\lsm.exe.mui
Opens: C:\Windows\System32\ntmarta.dll
Opens: C:\Windows\System32\authui.dll
Opens: C:\Windows\System32\cryptui.dll
Opens: C:\Windows\en-US
Opens: C:\Windows\System32\shacct.dll
Opens: C:\Windows\System32\samlib.dll
Opens: C:\Windows\System32\propsys.dll
Opens: C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
Opens: C:\Windows\System32\dui70.dll
Opens: C:\Windows\System32\duser.dll
Opens: C:\Windows\System32\en-US\authui.dll.mui
Opens: C:\Windows\System32\SndVolSSO.dll
Opens: C:\Windows\System32\hid.dll
Opens: C:\Windows\System32\MMDevAPI.dll
Opens: C:\Windows\System32\xmlite.dll
Opens: C:\Windows\System32\imageres.dll
Opens: C:\Windows\System32\WindowsCodecs.dll
Opens: C:\Windows\System32\winbrand.dll
Opens: C:\Windows\Branding\Basebrd\basebrd.dll
Opens: C:\Windows\Branding\Basebrd\en-US\basebrd.dll.mui
Opens: C:\Windows\System32\wtsapi32.dll
Opens: C:\Windows\System32\VaultCredProvider.dll
Opens: C:\Windows\System32\SmartcardCredentialProvider.dll
Opens: C:\Windows\System32\BioCredProv.dll
Opens: C:\Windows\System32\winbio.dll
Opens: C:\Windows\System32\credui.dll
Opens: C:\Windows\System32\vaultcli.dll
Opens: C:\Windows\System32\netapi32.dll
Opens: C:\Windows\System32\netutils.dll
Opens: C:\Windows\System32\wkscli.dll
Opens: C:\Windows\System32\samcli.dll
Opens: C:\Windows\System32\certCredProvider.dll
Opens: C:\Windows\System32\rasplap.dll
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat
Opens: C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTUBPM.etl
Opens: C:\Windows\System32\input.dll
Opens: C:\Windows\System32\en-US\input.dll.mui
Opens: C:\Program Files\Common Files\Microsoft Shared
Opens: C:\Program Files\Common Files\Microsoft Shared\ink
Opens: C:\Program Files\Common Files\Microsoft Shared\ink\tipsf.dll
Opens: C:\Program Files\Common Files\Microsoft Shared\ink\en-US
Opens: C:\Program Files\Common Files\Microsoft Shared\ink\en-US\TipTsf.dll.mui
Opens: C:\Windows\IME\SPITIP.DLL
Opens: C:\Windows\IME\en-US\SpTip.dll.mui
Opens: C:\Program Files\Windows NT\TableTextService
Opens: C:\Program Files\Windows NT\TableTextService\TableTextService.dll
Opens: C:\Program Files\Windows NT\TableTextService\en-US\TableTextService.dll.mui
US\TableTextService.dll.mui
Opens: C:\Windows\System32\en-US\KernelBase.dll.mui
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive1.dat
Opens: C:\Windows\System32\winevt\Logs
Opens: C:\Windows\System32\winevt\Logs\System.evtx
Opens: C:\Windows\System32\winevt\Logs\Application.evtx
Opens: C:\Windows\System32\winevt\Logs\Security.evtx
Opens: C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx
Opens: C:\Windows\System32\winevt\Logs\Media Center.evtx
Opens: C:\Windows\System32\winevt\Logs\Key Management Service.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-User Profile
Service\Operational.evtx
Opens: C:\Windows\System32\adtschema.dll
Opens: C:\Windows\System32\winevt\Logs\Internet Explorer.evtx
Opens: C:\Windows\System32\winevt\Logs\HardwareEvents.evtx
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\System32\en-US\imageres.dll.mui
Opens: C:\Program Files\Windows Defender\MpEvMsg.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender\Operational.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender\WHC.evtx
Opens: C:\Windows\System32\radardt.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaustion-

Detector%40operational.evtx
Opens: C:\Windows\System32\diagperf.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-
Performance%40operational.evtx
Opens: C:\Windows\System32\avrt.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-
LocalSessionManager%4Admin.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-
LocalSessionManager%40operational.evtx
Opens: C:\Windows\setupact.log
Opens: C:\Windows\System32\microsoft-windows-kernel-power-events.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Power%4Thermal-
Operational.evtx
Opens: C:\Windows\System32\PSHED.DLL
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-
WHEA%4Errors.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-
WHEA%40operational.evtx
Opens: C:\Windows\System32\PeerDist.dll
Opens: C:\Windows\CSC\2.0.6
Opens: C:\Windows\System32\gpsvc.dll
Opens: C:\Windows\System32\Wdi\LogFiles\WdiContextLog.etl.002
Opens: C:\Windows\System32\atl.dll
Opens: C:\Windows\System32\taskschd.dll
Opens: C:\Windows\System32\mstask.dll
Opens: C:\Windows\System32\dsrole.dll
Opens: C:\Windows\System32\slc.dll
Opens: C:\Windows\System32\es.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-
GroupPolicy%40operational.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-
OfflineFiles%40operational.evtx
Opens: C:\Windows\System32\UXInit.dll
Opens: C:\Windows\Resources\Themes
Opens: C:\Windows\Resources\Themes\Aero\Aero.msstyles
Opens: C:\Windows\Resources\Themes\Aero\en-US\Aero.msstyles.mui
Opens: C:\ProgramData\Microsoft\User Account Pictures
Opens: C:\ProgramData\Microsoft\User Account Pictures\user.bmp
Opens: C:\Windows\System32\config\SAM.LOG1
Opens: C:\Users\Admin\NTUSER.DAT
Opens: C:\Users\Admin\NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf
Opens: C:\Users\Admin\NTUSER.DAT{6cced2f1-6e01-11de-8bed-
001e0bcd1824}.TMContainer00000000000000000001.regtrans-ms
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\UsrClass.dat
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\UsrClass.dat{976abdbf-
6c18-11e3-bf1c-080027ca8fe0}.TM.blf
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\UsrClass.dat{976abdbf-
6c18-11e3-bf1c-080027ca8fe0}.TMContainer00000000000000000001.regtrans-ms
Opens: C:\Windows\System32\dlhhost.exe
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dfa859149af\comctl32.dll
Opens: C:\ProgramData\Microsoft\Windows
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-
Winlogon%40operational.evtx
Opens: C:\Windows\System32\IDStore.dll
Opens: C:\Windows\System32\slui.exe
Opens: C:\Windows\System32\spppcmdlg.dll
Opens: C:\Windows\System32\spopc.dll
Opens: C:\Windows\System32\en-US\slui.exe.mui
Opens: C:\Windows\System32\spppcomapi.dll
Opens: C:\Windows\System32\spppcext.dll
Opens: C:\Windows\System32\WinSCard.dll
Opens: C:\Windows\System32\webio.dll
Opens: C:\Windows\System32\tapi32.dll
Opens: C:\Windows\System32\msi.dll
Opens: C:\Windows\System32\slwga.dll
Opens: C:\Windows\System32\uxsms.dll
Opens: C:\Windows\System32\drivers\l1tdio.sys
Opens: C:\Windows\System32\drivers\rsnpndr.sys
Opens: C:\Windows\System32\dmmdir.dll
Opens: C:\Windows\System32\dmncore.dll
Opens: C:\Windows\System32\d3d10_1.dll
Opens: C:\Windows\System32\d3d10_1core.dll
Opens: C:\Windows\System32\dxgi.dll
Opens: C:\Windows\System32\nrpsrv.dll
Opens: C:\Windows\System32\en-US\gpsvc.dll.mui
Opens: C:\Windows\System32\dhcpcore6.dll
Opens: C:\Windows\System32\dnsrslvr.dll
Opens: C:\Windows\System32\dnsextd.dll
Opens: C:\Windows\System32\dhcpcsvc6.dll
Opens: C:\Windows\System32\dhcpcsvc.dll
Opens: C:\Windows\System32\fvaeapi.dll
Opens: C:\Windows\System32\tbs.dll
Opens: C:\Windows\System32\fvcecerts.dll
Opens: C:\Windows\System32\wiarpc.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-
Client%4Admin.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Dhcpv6-
Client%4Admin.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-
BranchCacheSMB%40operational.evtx
Opens: C:\Windows\System32\ktmw32.dll
Opens: C:\Windows\System32\taskcomp.dll
Opens: C:\Windows\System32\en-US\taskcomp.dll.mui
Opens: C:\Windows\Tasks\SCHEDLGU.TXT
Opens: C:\Windows\System32\Tasks\Microsoft\Windows
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Autochk\Proxy
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\MUI\LPRemove
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media Center
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media
Center\RecordingRestart
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\SystemRestore\SR
Opens:
C:\Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient\SystemTask
Opens:
C:\Windows\System32\Tasks\Microsoft\Windows\AppID\VerifiedPublisherCertStoreCheck
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\SideShow
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\SideShow\SessionAgent
Opens:
C:\Windows\System32\Tasks\Microsoft\Windows\Shell\WindowsParentalControls
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\SideShow\SystemDataProviders
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\MobilePC\HotStart
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Active Directory Rights
Management Services Client
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Active Directory Rights
Management Services Client\AD RMS Rights Policy Template Management (Automated)

Opens: C:\Windows\System32\Tasks\Microsoft\Windows\SideShow\AutoWake
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\WindowsColorSystem\Calibration Loader
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Offline Files
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Offline Files\Logon
 Synchronization
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\Multimedia\SystemSoundsService
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\DiskDiagnostic
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\DiskDiagnostic\Microsoft-
 Windows-DiskDiagnosticResolver
 Opens: C:\Windows\System32\taskhost.exe
 Opens: C:\Windows\System32\en-US\taskhost.exe.mui
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Windows Error
 Reporting\QueueReporting
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient\UserTask
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Active Directory Rights
 Management Services Client\AD RMS Rights Policy Template Management (Manual)
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\Shell\WindowsParentalControlsMigration
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\TextServicesFramework\MsCtfMonitor
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media Center\PvrRecoveryTask
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Tcpip\IpAddressConflict1
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Diagnosis\Scheduled
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media
 Center\SqlLiteRecoveryTask
 Opens: C:\Windows\system32\wbem\MSIMG32.dll
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Time
 Synchronization\SynchronizeTime
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Tcpip\IpAddressConflict2
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Application
 Experience\ProgramDataUpdater
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Windows Media
 Sharing\UpdateLibrary
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\PerfTrack\BackgroundConfigSurveyor
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media
 Center\ReindexSearchRoot
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\MemoryDiagnostic\CorruptionDetector
 Opens: C:\Windows\System32\HotStart\UserAgent.dll
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows Defender\MpIdleTask
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Ras\MobilityManager
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media
 Center\ObjectStoreRecoveryTask
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\User Profile
 Service\HiveUploadTask
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\WindowsBackup\ConfigNotification
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Windows Filtering
 Platform\BfeOnServiceStartTypeChange
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\DiskDiagnostic\Microsoft-
 Windows-DiskDiagnosticDataCollector
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\AppID\PolicyConverter
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\WDI\ResolutionHost
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTask
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media Center\PBDADiscovery
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Power Efficiency
 Diagnostics\AnalyzeSystem
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media
 Center\ActivateWindowsSearch
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\RemoteAssistance\RemoteAssistanceTask
 Opens: C:\Windows\System32\PlaySndSrv.dll
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient\UserTask-Roam
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media Center\PvrScheduleTask
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\Bluetooth\UninstallDeviceTask
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Offline Files\Background
 Synchronization
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media Center\OCURDiscovery
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media
 Center\DispatchRecoveryTasks
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Customer Experience
 Improvement Program
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Customer Experience
 Improvement Program\KernelCeipTask
 Opens:
 C:\Windows\System32\Tasks\Microsoft\Windows\MemoryDiagnostic\DecompressionFailureDetector
 Opens: C:\Windows\System32\MsCtfMonitor.dll
 Opens: C:\Windows\System32\msutb.dll
 Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-
 StoreMgr%40operational.evtx
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\RAC\RacTask
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Maintenance\WinSAT
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Customer Experience
 Improvement Program\UsbCeip
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Customer Experience
 Improvement Program\Consolidator
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media Center\OCURActivate
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Defrag\ScheduledDefrag
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media
 Center\UpdateRecordPath
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media Center\PBDADiscoveryW2
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows Defender\MP Scheduled Scan
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media
 Center\PeriodicScanRetry
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Application
 Experience\AitAgent
 Opens: C:\Windows\system
 Opens: C:\Windows\System32\WindowsPowerShell\v1.0
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\UPnP\UPnPHostConfig
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media
 Center\MediaCenterRecoveryTask
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Registry\RegIdleBackup
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media
 Center\InstallPlayReady
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media
 Center\ConfigureInternetTimeService
 Opens: C:\Windows\System32\Tasks\Microsoft\Windows\NetTrace\GatherNetworkInfo
 Opens: C:\ProgramData\Microsoft\Windows\Caches
 Opens: C:\ProgramData\Microsoft\Windows\Caches\cversions.2.db

Opens: C:\ProgramData\Microsoft\Windows\Caches\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x0000000000000007.db
Opens: C:\ProgramData\Microsoft\Windows\Caches\{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0x0000000000000002.db
Opens: C:\Windows\System32\en-US\propsys.dll.mui
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media Center\mcupdate
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media Center\PBDADiscoveryW1
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media Center\ehDRMInit
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Location\Notifications
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Media Center\RegisterSearch
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\Task Manager\Interactive
Opens: C:\Windows\System32\drivers\bowser.sys
Opens: C:\Windows\System32\drivers\mrxsm.sys
Opens: C:\Windows\System32\drivers\mrxsm10.sys
Opens: C:\Windows\System32\drivers\mrxsm20.sys
Opens: C:\Windows\System32\drivers\parvdm.sys
Opens: C:\Windows\System32\vsapi.dll
Opens: C:\Windows\System32\vsstrace.dll
Opens: C:\Windows\System32\en-US\vsstrace.dll.mui
Opens: C:\Windows\System32\WSDApi.dll
Opens: C:\Windows\System32\webservices.dll
Opens: C:\Windows\System32\fundisc.dll
Opens: C:\Windows\System32\drivers\PEAuth.sys
Opens: C:\Windows\System32\drivers\secdrv.sys
Opens: C:\Windows\System32\drivers\srvtet.sys
Opens: C:\Windows\System32\ncsi.dll
Opens: C:\Windows\System32\ntoskrnl.exe
Opens: C:\Windows\System32\halacpi.dll
Opens: C:\Windows\System32\kdcom.dll
Opens: C:\Windows\System32\mcupdate_GenuineIntel.dll
Opens: C:\Windows\System32\B00TVID.DLL
Opens: C:\Windows\System32\ci.dll
Opens: C:\Windows\System32\drivers\Wdf01000.sys
Opens: C:\Windows\System32\drivers\WdfLdr.sys
Opens: C:\Windows\System32\drivers\acpi.sys
Opens: C:\Windows\System32\drivers\wmilib.sys
Opens: C:\Windows\System32\drivers\msisadrv.sys
Opens: C:\Windows\System32\drivers\pci.sys
Opens: C:\Windows\System32\drivers\vdrvroot.sys
Opens: C:\Windows\System32\drivers\compbatt.sys
Opens: C:\Windows\System32\drivers\battc.sys
Opens: C:\Windows\System32\drivers\volmgr.sys
Opens: C:\Windows\System32\drivers\intelide.sys
Opens: C:\Windows\System32\drivers\pciindex.sys
Opens: C:\Windows\System32\drivers\atapci.sys
Opens: C:\Windows\System32\drivers\ataport.sys
Opens: C:\Windows\System32\drivers\amdxta.sys
Opens: C:\Windows\System32\drivers\ntfs.sys
Opens: C:\Windows\System32\drivers\msrpc.sys
Opens: C:\Windows\System32\drivers\ksecdd.sys
Opens: C:\Windows\System32\drivers\cng.sys
Opens: C:\Windows\System32\drivers\pcw.sys
Opens: C:\Windows\System32\drivers\fs_rec.sys
Opens: C:\Windows\System32\drivers\netio.sys
Opens: C:\Windows\System32\drivers\ksecpkg.sys
Opens: C:\Windows\System32\drivers\tcpip.sys
Opens: C:\Windows\System32\drivers\FwPKCLNT.SYS
Opens: C:\Windows\System32\drivers\vmstorfl.sys
Opens: C:\Windows\System32\drivers\volsnap.sys
Opens: C:\Windows\System32\drivers\spldr.sys
Opens: C:\Windows\System32\drivers\rdyboost.sys
Opens: C:\Windows\System32\drivers\disk.sys
Opens: C:\Windows\System32\drivers\Classpnp.sys
Opens: C:\Windows\System32\ssdpapi.dll
Opens: C:\Windows\System32\vpnikeyapi.dll
Opens: C:\Windows\System32\httpapi.dll
Opens: C:\Windows\System32\msxml6.dll
Opens: C:\Windows\System32\msxml6r.dll
Opens: C:\Windows\System32\en-US\MsCtfMonitor.dll.mui
Opens: C:\Windows\System32\drivers\tcpipreg.sys
Opens: C:\Windows\System32\tlntsrvc.exe
C:\Windows\winsxs\Manifests\x86_policy.9.0.microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_f47ed0f6f6564d90.manifest
Opens: C:\Windows\winsxs\Manifests\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742.manifest
Opens: C:\Windows\System32\python27.dll
C:\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\msvcr90.dll
Opens: C:\Windows\System32\pywintypes27.dll
Opens: C:\Windows\System32\config\systemprofile
Opens: C:\Windows\System32\wbemcomn.dll
Opens: C:\Windows\System32\drivers\srvt2.sys
Opens: C:\Windows\System32\drivers\srvt.sys
Opens: C:\Windows\System32\sqmapi.dll
Opens: C:\Windows\System32\wdscore.dll
Opens: C:\Windows\System32\wbem\WmiDcPrv.dll
Opens: C:\Windows\System32\wbem\fastprox.dll
Opens: C:\Windows\System32\ntdsapi.dll
Opens: C:\Windows\System32\wbem\wbemprox.dll
Opens: C:\System Volume Information\tracking.log
Opens: C:\Windows\System32\wbem\WinMgmtR.dll
Opens: C:\Windows\System32\netmsg.dll
Opens: C:\Windows\System32\en-US\netmsg.dll.mui
Opens: C:\Windows\System32\netcfgx.dll
Opens: C:\Windows\System32\ipconfig.exe
Opens: C:\Windows\System32\wbem\wbemcore.dll
Opens: C:\Windows\System32\wbem\esscli.dll
Opens: C:\Windows\System32\wbem\wbemsvr.dll
Opens: C:\Windows\System32\conhost.exe
Opens: C:\Windows\System32\nci.dll
Opens: C:\Windows\System32\en-US\conhost.exe.mui
Opens: C:\Windows\System32\sscore.dll
Opens: C:\Windows\System32\clusapi.dll
Opens: C:\Windows\System32\resutils.dll
Opens: C:\Windows\System32\en-US\ipconfig.exe.mui
Opens: C:\Windows\System32\hnetcfg.dll
Opens: C:\Windows\System32\wbem\wmiutils.dll
Opens: C:\Windows\System32\wbem\repdrvfs.dll
Opens: C:\Windows\System32\wbem\Repository
Opens: C:\Windows\System32\wbem\Repository\MAPPING1.MAP
Opens: C:\Windows\System32\wbem\Repository\MAPPING2.MAP
Opens: C:\Windows\System32\wbem\Repository\MAPPING3.MAP
Opens: C:\Windows\System32\wbem\Repository\OBJECTS.DATA
Opens: C:\Windows\System32\wbem\Repository\INDEX.BTR
Opens: C:\Windows\System32\wbem\WmiPrvSD.dll
Opens: C:\Windows\System32\ncobjapi.dll

Opens: C:\Windows\System32\wbem\wbemess.dll
Opens: C:\Windows\System32\perftrack.dll
Opens: C:\Windows\System32\wer.dll
Opens: C:\Windows\System32\aeapic.dll
Opens: C:\Windows\System32\sfcd.dll
Opens: C:\Windows\System32\sfcd_os.dll
Opens: C:\Windows\System32\en-US\user.dll.mui
Opens: C:\Windows\winsxs\x86_microsoft.windows.c.-
controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui
Opens: C:\Windows\System32\icaapi.dll
Opens: C:\Windows\System32\lsmproxy.dll
Opens: C:\Windows\System32\winmm.dll
Opens: C:\Windows\System32\en-US\winmm.dll.mui
Opens: C:\Windows\System32\regapi.dll
Opens: C:\Windows\System32\rdpcorekmts.dll
Opens: C:\Windows\System32\rdpwsx.dll
Opens: C:\Windows\System32\tlscsp.dll
Opens: C:\Windows\System32\PortableDeviceApi.dll
Opens: C:\Windows\System32\dimsjob.dll
Opens: C:\Windows\System32\PortableDeviceConnectApi.dll
Opens: C:\Program Files\Windows Defender\MpSvc.dll
Opens: C:\Program Files\Windows Defender\MpClient.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
Opens: C:\Program Files\Windows Defender\MsMpLics.dll
Opens: C:\Windows\System32\IPSECVC.DLL
Opens: C:\Windows\System32\FwRemoteSvr.dll
Opens: C:\ProgramData\Microsoft\Windows Defender
Opens: C:\Windows\System32\drivers\rdpdr.sys
Opens: C:\Windows\System32\Applhpdn.dll
Opens: C:\Windows\System32\pnpts.dll
Opens: C:\Windows\System32\wdiasqmodule.dll
Opens: C:\Windows\System32\npmproxy.dll
Opens: C:\Windows\System32\drivers\tdtcp.sys
Opens: C:\Windows\System32\drivers\rdpwd.sys
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-NCSI%4Operational.evtx
Opens: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
Opens: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\686aace6942fb7f7cbe231212eef4a4_577c175f-2428-49fc-a95e-635c93546ef9
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4Operational.evtx
Opens: C:\Windows\System32\drivers\spsys.sys
Opens: C:\Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-manifest-signed.xrm-ms
Opens: C:\Windows\System32\sppwinob.dll
Opens: C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
Opens: C:\Windows\System32\LogFiles\SQM
Opens: C:\Windows\System32\LogFiles\SQM\SQMLogger.etl.003
Opens: C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
Opens: C:\Windows\System32\spp\plugin-manifests-signed\sppobjjs-spp-plugin-manifest-signed.xrm-ms
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx
Opens: C:\Windows\System32\en-US\crypt32.dll.mui
Opens: C:\Windows\System32\p2pcollab.dll
Opens: C:\Windows\System32\en-US\p2pcollab.dll.mui
Opens: C:\Windows\System32\fvui.dll
Opens: C:\Windows\System32\en-US\fvui.dll.mui
Opens: C:\ProgramData\Microsoft\Windows Defender\Support\MPLog-07132009-215552.log
Opens: C:\Windows\System32\sppobjjs.dll
Opens: C:\Windows\inf
Opens: C:\Windows\System32\DriverStore
Opens: C:\Windows\System32\DriverStore\en-US
Opens: C:\Windows\inf\netip6.PNF
Opens: C:\Windows\inf\netwif1.PNF
Opens: C:\Windows\inf\ndiscap.PNF
Opens: C:\Windows\inf\netserv.PNF
Opens: C:\Windows\inf\netrb.PNF
Opens: C:\Windows\inf\wfp1wf.PNF
Opens: C:\Windows\inf\netrass.PNF
Opens: C:\Windows\inf\netmscli.PNF
Opens: C:\Windows\inf\netavpnt.PNF
Opens: C:\Windows\inf\nettcpip.PNF
Opens: C:\Windows\inf\netrast.PNF
Opens: C:\Windows\inf\l1tdio.PNF
Opens: C:\Windows\inf\vspndr.PNF
Opens: C:\Windows\inf\netsstpt.PNF
Opens: C:\Windows\inf\ndisuio.PNF
Opens: C:\Windows\System32\ndiscapCfg.dll
Opens: C:\Windows\System32\mprapi.dll
Opens: C:\Windows\System32\mprmsg.dll
Opens: C:\Windows\System32\en-US\mprmsg.dll.mui
Opens: C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft
Opens: C:\Windows\System32\config\SYSTEM.LOG1
C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\SoftwareProtectionPlatform\tokens.dat
Opens: C:\Windows\System32\config\SYSTEM
Opens: C:\Windows\System32\umb.dll
Opens: C:\Program Files\Windows Defender\MpRTP.dll
Opens: C:\Windows\System32\wsnnetbs.dll
Opens: C:\Windows\System32\localspl.dll
Opens: C:\Windows\System32\spoolss.dll
Opens: C:\Windows\System32\PrintIsolationProxy.dll
Opens: C:\Windows\System32\en-US\localspl.dll.mui
Opens: C:\Windows\System32\FXSMON.dll
Opens: C:\Windows\System32\pautoenr.dll
Opens: C:\Windows\System32\certcli.dll
Opens: C:\Windows\System32\CertEnroll.dll
Opens: C:\Windows\System32\tpcomn.dll
Opens: C:\Windows\System32\snmpapi.dll
Opens: C:\Windows\System32\wsnmp32.dll
Opens: C:\Windows\System32\tcpbidi.xml
Opens: C:\Windows\System32\usbmon.dll
Opens: C:\Windows\System32\WSDMon.dll
Opens: C:\Windows\System32\en-US\WSDMon.dll.mui
Opens: C:\Windows\System32\fdPnp.dll
Opens: C:\Windows\System32\spool\prtprocs\w32x86\winprint.dll
Opens: C:\Windows\System32\win32spl.dll

Opens: C:\Windows\System32\en-US\win32spl.dll.mui
Opens: C:\Windows\System32\inetpp.dll
Opens: C:\Windows\System32\DriverStore\infpub.dat
Opens: C:\Windows\System32\DriverStore\infstrng.dat
Opens: C:\Windows\System32\DriverStore\infstor.dat
Opens: C:\Windows\inf\faxcn002.inf
Opens: C:\Windows\System32\en-US\inetpp.dll.mui
Opens: C:\Windows\System32\spool\drivers\w32x86\3
Opens: C:\Windows\System32\userinit.exe
Opens: C:\Windows\System32\cscapi.dll
Opens: C:\Windows\System32\en-US\userinit.exe.mui
Opens: C:\Windows\explorer.exe
Opens: C:\Windows\System32\ExplorerFrame.dll
Opens: C:\Windows\en-US\explorer.exe.mui
Opens: C:\Users\Admin\AppData\Local\IconCache.db
Opens: C:\Windows\System32\catroot2
Opens: C:\Windows\System32\EhStorShell.dll
Opens: C:\Windows\System32\cscui.dll
Opens: C:\Windows\System32\cscdll.dll
Opens: C:\Windows\System32\ntshrui.dll
Opens: C:\Windows\System32\esent.dll
Opens: C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb
Opens: C:\Windows\System32\netevent.dll
Opens: C:\Windows\System32\en-US\netevent.dll.mui
Opens: C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
Opens: C:\Windows\System32\catroot2\edb.log
Opens: C:\Windows\System32\IconCodecService.dll
Opens: C:\Windows\System32\wmploc.DLL
Opens: C:\Windows\System32\en-US\wmploc.DLL.mui
Opens: C:\Windows\System32\ie4uinit.exe
Opens: C:\Windows\System32\en-US\ie4uinit.exe.mui
Opens: C:\Windows\System32\iedkcs32.dll
Opens: C:\Windows\System32\en-US\iedkcs32.dll.mui
Opens: C:\Windows\System32\themeui.dll
Opens: C:\Windows\System32\en-US\themeui.dll.mui
Opens: C:\Windows\System32\en-US\shell32.dll.mui
Opens: C:\Windows\System32\catroot2\edb.chk
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-31bf3856ad364e35-x86~~6.1.7601.17514.cat
Opens: C:\Windows\System32\timedate.cpl
Opens: C:\Windows\System32\actxprxy.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000005.db
Opens: C:\Windows\System32\shdocvw.dll
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explorer.lnk
Opens: C:\Windows\System32\linkinfo.dll
Opens: C:\Program Files\Internet Explorer
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Explorer.lnk
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Media Player.lnk
Opens: C:\Windows\System32\unregmp2.exe
Opens: C:\Windows\System32\en-US\unregmp2.exe.mui
Opens: C:\Windows\System32\DriverStore\FileRepository
Opens: C:\Windows\System32\DriverStore\FileRepository\prnms001.inf_x86_neutral_a1ff1bc29207b04f
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
Opens: C:\ProgramData\Microsoft\Windows\Start Menu
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs
Opens: C:\Windows\System32\accessibilitycpl.dll
Opens: C:\Windows\System32\en-US\accessibilitycpl.dll.mui
Opens: C:\Windows\System32\sud.dll
Opens: C:\Windows\System32\en-US\sud.dll.mui
Opens: C:\Windows\System32\wucltux.dll
Opens: C:\Windows\System32\en-US\wucltux.dll.mui
Opens: C:\Program Files\Windows Sidebar
Opens: C:\Program Files\Windows Sidebar\sidebar.exe
Opens: C:\Program Files\Windows Sidebar\en-US\sidebar.exe.mui
Opens: C:\Windows\System32\WindowsAnytimeUpgradeui.exe
Opens: C:\Windows\System32\en-US\windowsanytimeupgradeui.exe.mui
Opens: C:\Program Files\DVD Maker
Opens: C:\Program Files\DVD Maker\DVDMaker.exe
Opens: C:\Program Files\DVD Maker\en-US\DVDMaker.exe.mui
Opens: C:\Program Files\Common Files\Microsoft Shared\ink\mip.exe
Opens: C:\Program Files\Common Files\Microsoft Shared\ink\en-US\mip.exe.mui
Opens: C:\Windows\System32\mb1ctr.exe
Opens: C:\Windows\System32\en-US\mb1ctr.exe.mui
Opens: C:\Windows\System32\NetProjW.dll
Opens: C:\Windows\System32\en-US\NetProjW.dll.mui
Opens: C:\Windows\System32\SoundRecorder.exe
Opens: C:\Windows\System32\en-US\SoundRecorder.exe.mui
Opens: C:\Windows\System32\SyncCenter.dll
Opens: C:\Windows\System32\en-US\SyncCenter.dll.mui
Opens: C:\Windows\System32\Speech\SpeechUX
Opens: C:\Windows\System32\Speech\SpeechUX\sapi.cpl
Opens: C:\Windows\System32\Speech\SpeechUX\en-us
Opens: C:\Windows\System32\Speech\SpeechUX\en-us\sapi.cpl.mui
Opens: C:\Windows\System32\dfrgui.exe
Opens: C:\Windows\System32\en-US\DfrgUI.exe.mui
Opens: C:\Windows\System32\wdc.dll
Opens: C:\Windows\System32\en-US\wdc.dll.mui
Opens: C:\Windows\System32\msinfo32.exe
Opens: C:\Windows\System32\en-US\msinfo32.exe.mui
Opens: C:\Windows\System32\rstrui.exe
Opens: C:\Windows\System32\en-US\rstrui.exe.mui
Opens: C:\Windows\System32\miguiresource.dll
Opens: C:\Windows\System32\en-US\miguiresource.dll.mui
Opens: C:\Windows\System32\migwiz
Opens: C:\Windows\System32\migwiz\wet.dll
Opens: C:\Windows\System32\migwiz\en-US\wet.dll.mui
Opens: C:\Program Files\Common Files\Microsoft Shared\ink\ShapeCollector.exe
Opens: C:\Windows\System32\en-US\explorerframe.dll.mui
Opens: C:\Program Files\Common Files\Microsoft Shared\ink\en-US\ShapeCollector.exe.mui
Opens: C:\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll
Opens: C:\Windows\System32\msftedit.dll
Opens: C:\Program Files\Windows Journal

Opens: C:\Program Files\Windows Journal\Journal.exe
Opens: C:\Program Files\Windows Journal\en-US
Opens: C:\Windows\System32\msls31.dll
Opens: C:\Windows\Fonts\segoeui.ttf
Opens: C:\Program Files\Windows Journal\en-US\Journal.exe.mui
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\en-US
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\en-US\powershell.exe.mui
Opens: C:\Windows\System32\mycomput.dll
Opens: C:\Windows\System32\en-US\mycomput.dll.mui
Opens: C:\Windows\System32\odbcbint.dll
Opens: C:\Windows\System32\en-US\odbcbint.dll.mui
Opens: C:\Windows\System32\iscsicpl.dll
Opens: C:\Windows\System32\en-US\iscsicpl.dll.mui
Opens: C:\Windows\System32\MdSched.exe
Opens: C:\Windows\System32\en-US\MdSched.exe.mui
Opens: C:\Windows\System32\pmcsnap.dll
Opens: C:\Windows\System32\en-US\pmcsnap.dll.mui
Opens: C:\Windows\System32\wsecedit.dll
Opens: C:\Windows\System32\en-US\wsecedit.dll.mui
Opens: C:\Windows\System32\filemgmt.dll
Opens: C:\Windows\System32\en-US\filemgmt.dll.mui
Opens: C:\Windows\System32\msconfig.exe
Opens: C:\Windows\System32\en-US\msconfig.exe.mui
Opens: C:\Windows\System32\AuthFWGP.dll
Opens: C:\Windows\System32\en-US\authfwgp.dll.mui
Opens: C:\Windows\System32\gameux.dll
Opens: C:\Windows\System32\en-US\gameux.dll.mui
Opens: C:\Windows\System32\sdcp1.dll
Opens: C:\Windows\System32\en-US\sdcp1.dll.mui
Opens: C:\Windows\System32\recdisc.exe
Opens: C:\Windows\System32\en-US\recdisc.exe.mui
Opens: C:\Windows\System32\msra.exe
Opens: C:\Windows\System32\en-US\msra.exe.mui
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories\Accessibility
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories\System Tools
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories\System Tools\Desktop.ini
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories
Opens: C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\Accessories\Desktop.ini
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative
Tools
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative
Tools\desktop.ini
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\System
Tools
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\System
Tools\Desktop.ini
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Tablet
PC
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows
PowerShell
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Python 2.7
Opens: C:\Windows\System32\msiltsf.dll
Opens: C:\Program Files\Microsoft Office\OFFICE11
Opens: C:\Windows\System32\DeviceCenter.dll
Opens: C:\Windows\System32\en-US\DeviceCenter.dll.mui
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms
Opens: C:\ProgramData\Microsoft\Windows\Caches\{7CD55808-3D38-4DD5-90C9-
62F0E6EE60D4}.2.ver0x0000000000000001.db
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms
Opens: C:\Windows\System32\thumbcache.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Explorer
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db
Opens: C:\Windows\System32\networkexplorer.dll
Opens: C:\Windows\System32\tdh.dll
Opens: C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{9013FD8F-
1A53-49C9-9847-FE4C4078D288}\mpengine.dll
Opens: C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{9013FD8F-
1A53-49C9-9847-FE4C4078D288}\mpasbase.vdm
Opens: C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{9013FD8F-
1A53-49C9-9847-FE4C4078D288}\mpasdlta.vdm
Opens: C:\Windows\System32\spool\drivers\w32x86\PCC
Opens: C:\Windows\System32\stobject.dll
Opens: C:\Windows\System32\batmeter.dll
Opens: C:\Windows\System32\en-US\stobject.dll.mui
Opens: C:\Windows\System32\prnfldr.dll
Opens: C:\Windows\System32\en-US\sndvol32.dll.mui
Opens: C:\Windows\System32\DXP.dll
Opens: C:\Windows\System32\Syncreg.dll
Opens: C:\Windows\ehome\ehSSO.dll
Opens: C:\Windows\System32\netshe11.dll
Opens: C:\Windows\System32\AltTab.dll
Opens: C:\Windows\System32\en-US\AltTab.dll.mui
Opens: C:\Windows\System32\WPDShServiceObj.dll
Opens: C:\Windows\System32\PortableDeviceTypes.dll
Opens: C:\Windows\System32\pnidui.dll
Opens: C:\Windows\System32\QUTIL.DLL
Opens: C:\Windows\System32\tquery.dll
Opens: C:\Windows\System32\msrch.dll
Opens: C:\Windows\System32\cscobj.dll
Opens: C:\Windows\System32\en-US\pnidui.dll.mui
Opens: C:\Windows\System32\srchadmin.dll
Opens: C:\Windows\System32\msidle.dll
Opens: C:\ProgramData\Microsoft\Search\Data\Applications\Windows
Opens: C:\Windows\System32\msprxy.dll
Opens: C:\Windows\System32\ActionCenter.dll
Opens: C:\Windows\System32\rasd1g.dll
Opens: C:\Windows\System32\en-US\rasd1g.dll.mui

Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex
Opens: C:\Windows\System32\en-US\query.dll.mui
Opens: C:\Windows\System32\en-US\ESent.dll.mui
Opens: C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.log
Opens: C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.chk
Opens: C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\SecStore\CIST0000.001
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\INDEX.001
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010001.wid
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010001.dir
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010002.wid
Opens: C:\Windows\System32\WwanAPI.dll
Opens: C:\Windows\System32\wwapi.dll
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010002.dir
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010003.wid
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010003.dir
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010004.wid
Opens: C:\Windows\System32\QAGENT.DLL
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010004.dir
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-
NetworkAccessProtection\Operational.evtx
Opens: C:\Windows\System32\bthprops.cpl
Opens: C:\Windows\System32\ieframe.dll
Opens: C:\Windows\System32\oleacc.dll
Opens: C:\Windows\System32\oleaccrc.dll
Opens: C:\Windows\System32\en-US\bthprops.cpl.mui
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010005.wid
Opens: C:\ProgramData\Microsoft\Search\Data\Applications\Windows\tmp.edb
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010005.dir
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010006.wid
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010006.dir
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010007.wid
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010007.dir
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010008.wid
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010008.dir
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010011.wid
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010011.dir
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\CiAD0001.002
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Windows
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows
Opens: C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft
Opens: C:\Windows\System32\webcheck.dll
Opens: C:\Windows\System32\mlang.dll
Opens: C:\Windows\System32\imapid2.dll
Opens: C:\Windows\System32\hgcp1.dll
Opens: C:\Windows\System32\mssitlb.dll
Opens: C:\Windows\System32\FXSST.dll
Opens: C:\Windows\System32\FXSAPI.dll
Opens: C:\Windows\System32\FXSVC.exe
Opens: C:\Windows\System32\SearchProtocolHost.exe
Opens: C:\Windows\System32\mshooks.dll
Opens: C:\Windows\System32\SearchFilterHost.exe
Opens: C:\Windows\System32\mscoree.dll
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727
Opens: C:\Windows\System32\mssvp.dll
Opens: C:\Windows\System32\mapis32.dll
Opens: C:\Windows\System32\wscapi.dll
Opens: C:\Windows\System32\wscisvif.dll
Opens: C:\Windows\System32\wscproxystub.dll
Opens: C:\Windows\System32\en-US\advapi32.dll.mui
Opens: C:\Windows\System32\en-US\prnflidr.dll.mui
Opens: C:\Windows\System32\en-US\netshell.dll.mui
Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\SoftwareProtectionPlatform\Cache\cache.dat
Opens: C:\Windows\Prefetch\ReadyBoot\Trace4.fx
Opens: C:\Windows\System32\wdi\LogFiles\WdiContextLog.etl.003
Opens: C:\Windows\System32\Tasks\Microsoft\Windows\SideShow\GadgetManager
Opens: C:\Windows\System32\ntkrnlpa.exe
Opens: C:\Windows\System32\en-US\cscui.dll.mui
Opens: C:\Windows\inf\setupapi.dev.log
Opens: C:\Windows\System32\drvinst.exe
Opens: C:\Windows\System32\en-US\drvinst.exe.mui
Opens: C:\Windows\System32\newdev.dll
Opens: C:\Windows\inf\setupapi.ev3
Opens: C:\Windows\inf\setupapi.ev1
Opens: C:\Windows\System32\en-US\newdev.dll.mui
Opens: C:\Windows\System32\DriverStore\INF\CACHE.1
Opens:
C:\Windows\System32\DriverStore\FileRepository\cdrom.inf_x86_neutral_6381e09675524225\cdrom.PNF
Opens: C:\Windows\inf\apps.inf
Opens:
C:\Windows\System32\DriverStore\FileRepository\battery.inf_x86_neutral_5752155055c5e2d7
Opens:
C:\Windows\System32\DriverStore\FileRepository\battery.inf_x86_neutral_5752155055c5e2d7\battery.PNF
Opens: C:\Windows\System32\dinotify.exe
Opens: C:\Windows\inf\defltbase.inf
Opens: C:\Windows\inf\dwup.inf
Opens: C:\Windows\inf\verrta.inf
Opens: C:\Windows\inf\fontsetup.inf
Opens: C:\Windows\winsxs\FileMaps

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_21f9a9c4a2f8b514.cdf-ms
Opens: C:\Windows\System32\pnpuil.dll
Opens: C:\Windows\System32\en-US\dinotify.exe.mui
Opens: C:\Windows\System32\en-US\pnpuil.dll.mui
Opens: C:\Windows\inf\lltdio.inf
Opens: C:\Windows\inf\ndiscap.inf
Opens: C:\Windows\inf\ndisuio.inf
Opens: C:\Windows\inf\netavpna.inf
Opens: C:\Windows\inf\netavpnt.inf
Opens: C:\Windows\inf\netbrdgm.inf
Opens: C:\Windows\inf\netbrdgs.inf
Opens: C:\Windows\inf\netip6.inf
Opens: C:\Windows\inf\netmscli.inf
Opens: C:\Windows\inf\netnb.inf
Opens: C:\Windows\inf\netnwifi.inf
Opens: C:\Windows\inf\netpacer.inf
Opens: C:\Windows\inf\netpgm.inf
Opens: C:\Windows\inf\netrasa.inf
Opens: C:\Windows\inf\netrass.inf
Opens: C:\Windows\inf\netrast.inf
Opens: C:\Windows\inf\netserv.inf
Opens: C:\Windows\inf\netsstpa.inf
Opens: C:\Windows\inf\netsstpt.inf
Opens: C:\Windows\inf\nettcpip.inf
Opens: C:\Windows\inf\netwifflt.inf
Opens: C:\Windows\inf\netwifimp.inf
Opens: C:\Windows\inf\printupg.inf
Opens: C:\Windows\inf\puwk.inf
Opens: C:\Windows\inf\rspndr.inf
Opens: C:\Windows\inf\scereglv1.inf
Opens: C:\Windows\inf\secrets.inf
Opens: C:\Windows\inf\wfpplw.inf
Opens: C:\Windows\inf\NET Data Provider for Oracle
Opens: C:\Windows\inf\MSDTC Bridge 3.0.0.0
Opens: C:\Windows\inf\ServiceModelEndpoint 3.0.0.0
Opens: C:\Windows\inf\ServiceModelOperation 3.0.0.0
Opens: C:\Windows\inf\ServiceModelService 3.0.0.0
Opens: C:\Windows\inf\SMSvcHost 3.0.0.0
Opens: C:\Windows\inf\Windows Workflow Foundation 3.0.0.0
Opens: C:\Windows\System32\batt.dll
Opens: C:\Windows\System32\Storprop.dll
Opens: C:\Windows\System32\en-US\batt.dll.mui
Opens: C:\Windows\System32\sysclass.dll
Opens: C:\Windows\inf\battery.PNF
Opens: C:\Windows\inf\battery.inf
Opens: C:\Windows\System32\spfileq.dll
Opens:
C:\Windows\System32\DriverStore\FileRepository\battery.inf_x86_neutral_5752155055c5e2d7\CmBatt.sys
Opens: C:\Windows\inf\setupapi.ev2
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-31bf3856ad364e35-x86--6.1.7601.17514.cat
Opens: C:\Windows\System32\cryptnet.dll
Opens:
C:\Windows\System32\DriverStore\FileRepository\battery.inf_x86_neutral_5752155055c5e2d7\battc.sys
Opens: C:\Windows\inf\cdrom.PNF
Opens: C:\Windows\inf\cdrom.inf
Opens:
C:\Windows\System32\DriverStore\FileRepository\cdrom.inf_x86_neutral_6381e09675524225\cdrom.sys
Opens: C:\Windows\System32\en-US\mpr.dll.mui
Opens: C:\Windows\System32\drprov.dll
Opens: C:\Windows\System32\ntlman.dll
Opens: C:\Windows\System32\davclnt.dll
Opens: C:\Windows\System32\davhlpr.dll
Opens: C:\Windows\System32\drivers\cdfs.sys
Opens: C:\System Volume Information\Syscache.hve
Opens: C:\Windows\AppCompat\Programs\RecentFileCache.bcf
Opens: C:\Program Files\Internet Explorer\iexplore.exe
Opens: C:\Program Files\Internet Explorer\en-US
Opens: C:\Program Files\Internet Explorer\en-US\iexplore.exe.mui
Opens: C:\Program Files\Windows Media Player\wmpplayer.exe
Opens: C:\Program Files\Windows Media Player\en-US\wmpplayer.exe.mui
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Welcome
Center.lnk
Opens: C:\Windows\Branding\ShellBrd\shellbrd.dll
Opens: C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\Accessories\displayswitch.lnk
Opens: C:\Windows\System32\DisplaySwitch.exe
Opens: C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\Accessories\Calculator.lnk
Opens: C:\Windows\System32\en-US\calc.exe.mui
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Sticky
Notes.lnk
Opens: C:\Windows\System32\StikyNot.exe
Opens: C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\Accessories\Snipping Tool.lnk
Opens: C:\Windows\System32\SnippingTool.exe
Opens: C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\Accessories\Paint.lnk
Opens: C:\Windows\System32\mspaint.exe
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\XPS Viewer.lnk
Opens: C:\Windows\System32\xpsrchw.exe
Opens: C:\Windows\System32\en-US\xpsrchw.exe.mui
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows Fax and
Scan.lnk
Opens: C:\Windows\System32\WFS.exe
Opens: C:\Windows\System32\WFSR.dll
Opens: C:\Windows\System32\en-US\WFSR.dll.mui
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Remote
Desktop Connection.lnk
Opens: C:\Windows\System32\mtsc.exe
Opens: C:\Windows\System32\en-US\mtsc.exe.mui
Opens: C:\Windows\System32\en-US\batmeter.dll.mui
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\PropMap\CiPT0000.002
Opens: C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS00004.log
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\INDEX.002
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\0001000C.wid
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\0001000C.dir
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\CiAD0002.002
Opens: C:\Users\Admin\AppData\Local\Microsoft\Internet Explorer
Opens: C:\Windows\System32\NaturalLanguage6.dll
Opens: C:\Windows\System32\NlsData0009.dll

Opens: C:\Windows\System32\NlsLexicons0009.dll
Opens: C:\Windows\System32\ms sph.dll
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.10.gthr
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Known Folders API
Service.evtx
Opens: C:\Windows\System32\syncui.dll
Opens: C:\Windows\System32\synceng.dll
Opens: C:\Program Files\Internet Explorer\ieproxy.dll
Opens: C:\Windows\System32\wpdshext.dll
Opens: C:\Windows\System32\audiodev.dll
Opens: C:\Windows\System32\WMVCORE.DLL
Opens: C:\Windows\System32\WMASF.DLL
Opens: C:\Windows\System32\EhStorAPT.dll
Opens: C:\Users\Admin\Links\Downloads.lnk
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent
Opens: C:\Users\Admin\Downloads
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms
Opens: C:\Windows\System32\UIAnimation.dll
Opens: C:\Windows\System32\StructuredQuery.dll
Opens: C:\Windows\System32\BdeUnlockWizard.exe
Opens: C:\Windows\System32\en-US\BdeUnlockWizard.exe.mui
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin
Opens: C:\Windows\System32\SearchFolder.dll
Opens: C:\Windows\Media
Opens: C:\Windows\Media\Windows Navigation Start.wav
Opens: C:\Windows\System32\en-US\ntshrui.dll.mui
Opens: C:\Windows\System32\notepad.exe
Opens: C:\Windows\System32\en-US\notepad.exe.mui
Opens: C:\Windows\System32\zipfldr.dll
Opens: C:\Windows\System32\en-US\oleaccrc.dll.mui
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories\Accessibility\Magnify.lnk
Opens: C:\Windows\System32\Magnify.exe
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\5afe4de1b92fc382.customDestinations-
ms
Opens: C:\Windows\System32\en-US\searchfolder.dll.mui
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories\Command Prompt.lnk
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories\System Tools\Private Character Editor.lnk
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories\Accessibility\Ease of Access.lnk
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Media Center.lnk
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Python 2.7\Python
(command line).lnk
Opens: C:\Windows\Installer
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance\Create
Recovery Disc.lnk
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative
Tools\Component Services.lnk
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative
Tools\Computer Management.lnk
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative
Tools\System Configuration.lnk
Opens: C:\Users\Public\Libraries
Opens: C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\Accessories\Mobility Center.lnk
Opens: C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\Accessories\NetworkProjection.lnk
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Sync
Center.lnk
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\System
Tools\Character Map.lnk
Opens: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\System
Tools\Disk Cleanup.lnk
Opens: C:\Windows\System32\cmd.exe
Opens: C:\Windows\System32\en-US\cmd.exe.mui
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\0001000C.wsb
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\0001000C.ci
Opens: C:\Windows\System32\en-US\mssvp.dll.mui
Opens: C:\Users\Admin\Favorites\Links for United States
Opens: C:\Windows\System32\sc.exe
Opens: C:\Windows\Prefetch\ReadyBoot\Trace5.fx
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db
Opens:
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.11.gthr
Opens: C:\Program Files\Windows Media Player\wmpnscfg.exe
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking
Opens: C:\Program Files\Windows Media Player\en-US\wmpnscfg.exe.mui
Opens: C:\Program Files\Windows Media Player\wmpnssci.dll
Opens: C:\Windows\System32\wssock32.dll
Opens: C:\Windows\System32\wmrmdev.dll
Opens: C:\Windows\System32\drmv2clt.dll
Opens: C:\Windows\System32\mfplat.dll
Opens: C:\Windows\System32\wmp.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Media
Opens: C:\Users\Admin\AppData\Local\Microsoft\Media
Player\CurrentDatabase_372.wmdb
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Media-Format-Package-31bf3856ad364e35-x86~6.1.7601.17514.cat
Opens: C:\ProgramData\Microsoft\Windows\DRM\drmstore.hds
Opens: C:\Windows\System32\blackbox.dll
Opens: C:\Windows\System32\fdWSD.dll
Opens: C:\Windows\System32\fdSSDP.dll
Opens: C:\Windows\System32\fdProxy.dll
Opens: C:\ProgramData\Microsoft\Windows\DRM\v3ks.sec
Opens: C:\ProgramData\Microsoft\Windows\DRM\v3ks.bla
Opens: C:\Windows\System32\upnp.dll
Opens: C:\Windows\System32\P2P.dll
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Opens: C:\Windows\System32\P2PGraph.dll
Opens: C:\Windows\System32\wmpps.dll
Opens: C:\Windows\System32\wmpmde.dll
Opens: C:\Windows\System32\WinSATAPI.dll

Opens: C:\Windows\Performance\WinSAT
Opens: C:\Windows\System32\en-US\WinSATAPI.dll.mui
Opens: C:\Windows\System32\MSMPEG2ENC.DLL
Opens: C:\Windows\System32\devenum.dll
Opens: C:\Windows\System32\msdmo.dll
Opens: C:\Windows\System32\wbem\WmiPrivSE.exe
Opens: C:\Windows\System32\wbem\wmiprov.dll
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-HomeGroup Provider
Service%40operational.evtx
Opens: C:\Windows\System32\udhisapi.dll
Opens: C:\Windows\System32\msxml3.dll
Opens: C:\Windows\System32\msxml3r.dll
Opens: C:\Program Files\Windows Media Player\Network Sharing
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
Opens: C:\Program Files\Windows Media Player\Network
Sharing\ConnectionManager.xml
Opens: C:\Program Files\Windows Media Player\Network
Sharing\ContentDirectory.xml
Opens: C:\Program Files\Windows Media Player\Network
Sharing\MediaReceiverRegistrar.xml
Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\0758d43fe07c2439041ddb5e8144f0e2_577c175f-2428-
49fc-a95e-635c93546ef9
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\UPnP
Device Host\upnphost\udhisapi.dll
Opens: C:\Program Files\Windows Media Player\Network Sharing\wmpnss_color48.png
Opens:
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows Media Player
NSS\3.0\Icon Files\0aef9a97-98cd-4f89-b183-3db737149306.png
Opens: C:\Users\Public\Libraries\RecordedTV.library-ms
Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\c9b2a162fe2e8905ca66c1b53d166a01_577c175f-2428-
49fc-a95e-635c93546ef9
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\8d844364c535c5b5c8ba03cedd538a73.sst
Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\eb3bc6388b8f46d91ac65574d706a290_577c175f-2428-
49fc-a95e-635c93546ef9
Opens: C:\Windows\System32\dssenh.dll
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\01ED921B23B3B2074DA8E25F969F71FF3EDB116
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\8d4f95592ce335421d51fad8712f5c\grouping
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\8d4f95592ce335421d51fad8712f5c\grouping\edb.log
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\8d4f95592ce335421d51fad8712f5c\grouping\edb.chk
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\8d4f95592ce335421d51fad8712f5c\grouping\edb.mdb
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\65e9eda7bcb6088518aea0ddf13df80843a6ea25.HomeGroupClassifier\8d4f95592ce335421d51fad8712f5c\grouping\tmp.edb
Opens:
C:\Windows\winsxs\FileMaps\\$.cdf-ms
Opens: C:\Users\Public\Music\Sample Music
Opens: C:\Windows\System32\drtrtransport.dll
Opens: C:\Windows\System32\drt.dll
Opens: C:\Users\Public\Pictures\Sample Pictures
Opens: C:\Users\Public\Pictures\Sample Pictures\desktop.ini
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-
19\7e22207fe9846926e18c29d3e675240e_577c175f-2428-49fc-a95e-635c93546ef9
Opens: C:\Windows\Prefetch\WMPNSCFG.EXE-FC0D39BF.pf
Opens: C:\Windows\AppPatch\pcmain.sdb
Opens: C:\Windows\System32\wbem\cimwin32.dll
Opens: C:\Windows\System32\wbem\en-US\cimwin32.dll.mui
Opens: C:\Windows\System32\browcli.dll
Opens: C:\Windows\System32\framedynos.dll
Opens: C:\Windows\System32\schedcli.dll
Opens: C:\Windows\System32\wmi.dll
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\prnxx002.cat
Opens: C:\Users\Admin\AppData\Local\Temp\-DF1FDE99B5F239651.TMP
Opens: C:\Windows\System32\asycfilt.dll
Opens: C:\Windows\Fonts\arial1.ttf
Opens: C:\Windows\System32\aeevt.sdb
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-
Experience%4Program-Compatibility-Assistant.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-
Experience%4Program-Telemetry.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-
Experience%4Program-Inventory.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-
Experience%4Problem-Steps-Recorder.evtx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-
Experience%4Program-Compatibility-Troubleshooter.evtx
Opens: C:\Windows\Prefetch\ReadyBoot\Trace6.fx
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-
International%4operational.evtx
Opens: C:\Windows\System32\en-US\sppcommdlg.dll.mui
Opens: C:\Windows\System32\en-US\sic.dll.mui
Opens: C:\Program Files\Adobe\Reader 9.0
Opens: C:\Program Files\Adobe\Reader 9.0\Reader
Opens: C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Opens:
C:\Windows\winsxs\Manifests\x86_policy.8.0.microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_516d712b0f495a45.manifest
Opens:
C:\Windows\winsxs\Manifests\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc.manifest
Opens: C:\Users\Public\Desktop\Adobe Reader 9.lnk
Opens: C:\Program Files\Common Files\Adobe\ARM\1.0
Opens: C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe
Opens: C:\Program Files\Common Files\Java\Java Update
Opens:
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcp80.dll
Opens:
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
Opens: C:\Windows\System32\oledlg.dll
Opens: C:\Program Files\Common Files\Java\Java Update\jusched.exe
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Protect\S-1-5-21-2160590473-
689474908-1361669368-1002

Opens: C:\Users\Admin\AppData\Local\Temp\AdobeARM.log
Opens: C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
Opens: C:\Windows\System32\en-US\shlwapi.dll.mui
Opens: C:\Windows\System32\wsui.cpl
Opens:
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\d5671e75207216480e6ee946e1a6f31_577c175f-2428-49fc-a95e-635c93546ef9
Opens: C:\Windows\System32\appwiz.cpl
Opens: C:\Windows\System32\osbaseIn.dll
Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\7e4dca80246863e3.automaticDestinations-ms
Opens: C:\Windows\System32\en-US\appwiz.cpl.mui
Opens: C:\Windows\System32\Macromed\Flash
Opens: C:\Windows\Installer\41e90.msi
Opens: C:\Windows\Installer\41e62.msi
Opens: C:\Windows\Installer\41e68.msi
Opens: C:\Program Files\Java\jre7
Opens: C:\Program Files\Java\jre7\bin
Opens: C:\Windows\Installer\1d4ab.msi
Opens: C:\Windows\Installer\361e1.msi
Opens: C:\Windows\Installer\1d4a7.msi
Opens: C:\Windows\Installer\{95120000-003F-0409-0000-000000FF1CE}\xlwicon.exe
Opens: C:\Windows\Installer\{90120000-0020-0409-0000-000000FF1CE}\012ConvIcon.exe
Opens: C:\Windows\Installer\41e6c.msi
Opens: C:\Windows\System32\Macromed\Flash\FlashUtil10h_ActiveX.exe
Opens: C:\Windows\Installer\1d4c0.msi
Opens: C:\Windows\Installer\{90850409-6000-11D3-8CFE-0150048383C9}\wrdvicon.exe
Opens: C:\Program Files\Java\jre7\bin\javaws.exe
Opens: C:\Windows\Installer\{AC76BA86-7AD7-1033-7B44-A93000000001}
Opens: C:\Windows\Installer\{AC76BA86-7AD7-1033-7B44-A93000000001}\SC_Reader.ico
Opens: C:\Windows\Media\Windows Exclamation.wav
Opens: C:\Windows\System32\msiexec.exe
Opens: C:\Windows\AppPatch\AcGenral.dll
Opens: C:\Windows\System32\msacm32.dll
Opens: C:\Windows\System32\en-US\msiexec.exe.mui
Opens: C:\Windows\System32\srclient.dll
Opens: C:\Windows\System32\spp.dll
Opens: C:\Windows\System32\wolehlp.dll
Opens: C:\Windows\System32\virtdisk.dll
Opens: C:\Windows\System32\fltlib.dll
Opens: C:\Windows\System32\vss_ps.dll
Opens: C:\Windows\System32\catsrvut.dll
Opens: C:\Windows\System32\mfcsbcs.dll
Opens: C:\Windows\System32\eventcls.dll
Opens: C:\Windows\System32\SMI\Store\Machine
Opens: C:\Windows\winsxs\FileMaps\\$\$_addins_2452dff8cb692cdd.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_appcompat_programs_99c7f419bd54f4ca.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_apppatch_1143992cbbbecab.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_apppatch_en-us_098dc872781aebb9.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_dvd_pcat_de3c62295de3e26e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_dvd_pcat_en-us_80af7686f451a150.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_fonts_fee710f4f7b180e0.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_0f8924c0debe64e4.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_cs-cz_da8bfa0c28cad1cc.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_da-dk_da67f50e291bdec5.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_de-de_da67f5ee291bdcbb.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_el-gr_da43f0fe296cebfd.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_en-us_da440b72296cc45e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_es-es_da43ed1c296cf1c1.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_fi-fi_da1fe77a29be0007.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_fr-fr_da1fe64829be028f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_hu-hu_d9d7d7f62a602593.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_it-it_d9b3d122ab13661.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_ja-jp_d98fca962b0246de.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_ko-kr_d96bc3742b535818.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_nb-no_d8f7faee42c468adc.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_nl-nl_d8fafaf642c46898f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_pl-pl_d8b7a1782ce8abbb.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_pt-br_d8b7861c2ce8d537.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_pt-pt_d8b7a0682ce8adfb.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_ru-ru_d86f925a2d8ad06f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_sv-se_d84b8da62d8dbc6c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_tr-tr_d82784d42ec2f1c3.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_zh-cn_d74f2fe2301398dc.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_zh-hk_d74f39cc301389ac.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_boot_pcat_zh-tw_d74f4ee430136b4c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_branding_1728f5d8b15e5263.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_branding_basebrd_9ee9a176c9fadab4.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_branding_basebrd_en-us_51c0631d4347f350.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_branding_shellbrd_be1f632087fb0947.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_cursors_bff8b8b245707919.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_index_6f9ad1a80c4f7ad6.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_diagnostics_scheduled_maintenance_6bb1b174b39bb442.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_scheduled_maintenance_en-us_1c00802b579d904e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_aero_8b2c42561936b3f0.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_aero_en-us_1a668ac520a43d24.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_audio_9d2751b7c84ca0f1.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_audio_en-us_9fb258d76056760d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_devicecenter_0e1655bf357f4c22.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_devicecenter_en-us_63ad620434e90fd4.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_device_9d2d754600160183.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_device_en-us_3d982204ee3c99ad.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_homegroup_1909584eb21c73e3.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_homegroup_en-us_a38a598dd5f2b78b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_iebrowseweb_e2468f1fdde27cf7.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_iebrowseweb_en-us_ecd0995f1c154eaf.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_iesecurity_25644a5ef81c9ef5.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_iesecurity_en-us_bd38ea4838c17913.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_networking_29c6b61ce45e9171.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_networking_en-us_9db86426234993c3.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_pcw_2115168e47eaddb7.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_pcw_en-us_30a9ef1c7976423b.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_performance_d48bf95b5c828123.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_performance_en-us_0e192682c5b12037.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_power_9d457dc1c7c54838.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_power_en-us_721989d674f7bd04.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_printer_22190c3ab8798fd9.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_printer_en-us_211a053df7b8c611.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_search_9d4b5385ff8f1ef3.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_search_en-us_0b243b1f8544b909.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_windowsmediaplayerconfiguration_537e287f67955d9f.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_windowsmediaplayerconfiguration_en-us_b557b88758a93acd.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_windowsmediaplayermedialibrary_64611465e9119df8.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_windowsmediaplayermedialibrary_en-us_90086ff8e09d3732.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_windowsmediaplayerplaydvd_3aa04961f831b79d.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_windowsmediaplayerplaydvd_en-us_17d71967caf66a17.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_windowsupdate_0862ad88ff233b9d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_diagnostics_system_windowsupdate_en-us_6dbfbf04647c43f3.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_digitallocker_en-us_ff53d45933582902.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_ehome_40103e2da1d121de.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_components_ccfb52aef0c0f0151.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_components_tables_c2b8c3e0749098d8.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_ed3f8f2e7a4426af.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_filters_5fe1b967f204215a.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_sfxplugins_5b043573249413c8.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_sonicresources_7e22c968e006c522.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_styles_ntsc_c4d1e502f2c449b1.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_styles_ntsc_symphony_daaa4003771a0c78.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_styles_ntsc_symphony_symphony_97a43ae95f09b239.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_styles_pal_55d264f56641a00e.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_styles_pal_symphony_b9729623521ab9e5.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_styles_pal_symphony_symphony_f1d008156719fefe.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_ehome_createdisc_style_0d4521df11573950.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_ehome_en-us_1a0f218933093e9c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_ehome_mcx_022df17cf4546600.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_ehome_mcx_x02_7afb1a3b86c42e5e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_ehome_mediarenderer_923295b945ee30c7.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_en-us_40104e69a1d105cc.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_fonts_40104ba9a1d20dac.cdf-ms
Opens:

C:\Windows\winsxs\FileMaps\\$\$_globalization_els_transliteration_1547068d18bc2738.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_0b932a9a9cc9f99b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-au_theme_8b4e352268872029.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-au_wallpaper_6187684a82a84eda.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-ca_theme_8ade199269dd7453.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-ca_wallpaper_2a609fdb2b110530.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-gb_link_61442ee528aa6cdd.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-gb_rssfeed_29449ea7eb4c7797.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-gb_theme_8a4ff6a06b18c1d8.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-gb_wallpaper_e474064dc62e18eb.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-us_link_5f6dbb3b2c805e48.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-us_rssfeed_41d427d3ce5de0ec.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-us_theme_887982f66eeeb343.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-us_wallpaper_fd038f79a93f8240.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-za_theme_87a14dce71263ecc.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_globalization_mct_mct-

za_wallpaper_92a67a51c073d8f7.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_globalization_sorting_04883de290c6ef1b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_help_help_en-us_91e6e7979a9bf9c6.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_help_mui_0409_c7942094fabea651.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_help_windows_en-us_b594929e73669c5e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_ime_3f581be9a4c8cabd.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_ime_en-us_0d349188e45a5789.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_ime_imejp10_dicts_281006c600450618.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_ime_imejp10_help_280ffde19e779392.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_ime_imekr8_dicts_2ff7cb9394dec12.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_ime_imekr8_help_6edfa6f9f9cba42e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_ime_imesc5_dicts_32255cd579e8854e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_ime_imesc5_help_693c441c0201a8fa.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_ime_imetc10_dicts_31e93cd9cd8cc931.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_ime_imetc10_help_31e933f572191d05.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.netframework_0000_fd6b5f63492732f4.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.netframework_0409_fd6b70814927192f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.netframework_266880c2626e99c6.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_clr_data_0000_9334e121f0277e71.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_clr_data_0409_9334f23ff02764ac.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_clr_data_0864fda87da3c851.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_clr_networking_0000_417aaafa90927065.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_clr_networking_0409_417ab2a4909264b0.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_clr_networking_d061836896f4f29d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_data_provider_for_oracle_0000_1ac87488f00b2af0.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_data_provider_for_oracle_0409_1ac885a6f00b112b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_data_provider_for_oracle_07838adde9419766.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_data_provider_for_sqlserver_0000_22ef191981b08b2b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_data_provider_for_sqlserver_0409_22ef188981b08c78.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_.net_data_provider_for_sqlserver_7cfd5f3e72497ce1.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_3f581daba4c8c835.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_bits_0000_a03dbf7d63e833bd.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_bits_0409_a03dbeed63e8350a.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_bits_0ef6f148bde367d9.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_en-us_0ef70046e1d1b811.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_esent_0000_5aeb75e54bde718e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_esent_0409_5aeb87034bde57c9.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_esent_0ef70656e1d1b1ac.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_msdtc_0000_5b1b81b54f36c82e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_msdtc_0409_5b1b92d34f36ae69.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_msdtc_0ef70686e1d9b30c.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_msdtc_bridge_3.0.0.0_0000_5d60388d7f35c25e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_msdtc_bridge_3.0.0.0_0409_5d6037fd7f35c3ab.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_pnrpsvc_0000_43733b07fe2eb83f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_pnrpsvc_0409_437342b1fe2eac8a.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_pnrpsvc_3932681b8fb41c9d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_rdyboost_0000_50c61a1d7330c91d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_rdyboost_0409_50c6198d7330ca6a.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_rdyboost_95e76b07334dd353.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_remoteaccess_0000_86bc982ae65d5d49.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_remoteaccess_0409_86bc979ae65d5e96.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_remoteaccess_110554180baafc8b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_servicemodelendpoint_3.0.0.0_0000_1441b5e36e0dde07.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_servicemodelendpoint_3.0.0.0_0409_1441b5536e0ddf54.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_servicemodeloperation_3.0.0.0_0000_9b92bb9ad51f70d3.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_servicemodeloperation_3.0.0.0_0409_9b92ccb8d51f570e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_servicemodelservice_3.0.0.0_0000_2fd4d7f498bba769.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_servicemodelservice_3.0.0.0_0409_2fd4df9e98bb9bb4.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_smsvchost_3.0.0.0_0000_2d6d90735cb61780.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_smsvchost_3.0.0.0_0409_2d6da1915cb5fddb.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_tapisrv_0000_2e9995ea1b86323e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_tapisrv_0409_2e999d941b862689.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_tapisrv_20c65cafb424239c.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_termservice_0000_f96d5ce56bc76fc8.cdf-ms
ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_termservice_0409_f96d648f6bc76413.cdf-ms
ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_termservice_f0fb244350031192.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_ugatherer_0000_046b5203f9ca3f14.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_ugatherer_0409_046b6321f9ca254f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_ugatherer_9f1f9c5b6cd50d98.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_ugthrsvc_0000_8451c300df70be5f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_ugthrsvc_0409_8451c270df70bfac.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_ugthrsvc_9c5b081f28f83f11.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_usbhub_0000_1bec33bb3c8ba8f4.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_usbhub_0409_1bec32773c8babd1.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_usbhub_299dea1039e75d30.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_windows_workflow_foundation_3.0.0.0_0000_c87be1b3a75f787b.cdf-ms
ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_windows_workflow_foundation_3.0.0.0_0409_c87be95da75f6cc6.cdf-ms
ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_wsearchidxpi_0000_2e6e3f1caf9fca20.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_wsearchidxpi_0409_2e6e3e8ca9f9cb6d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_inf_wsearchidxpi_a2c41dc1731a4204.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_l2schemas_d7bb5637381de58c.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_media_401039ffa1d92906.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_media_afternoon_ae5d080a6a887942.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_calligraphy_7b7c7a996fa5cd3c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_characters_8ee06d90f7dead3a.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_cityscape_b0cbff7c81824cc5.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_delta_0f36d7d9b4f7293c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_festival_d2aa354bee3f11cc.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_garden_6cea56938e5bd6b1.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_heritage_bd7af0f60e3b0705.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_landscape_e9488ca8249a3acf.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_quirky_6baa21a590d24b57.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_raga_d0fd3c9ac0f8ab1b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_savanna_6b39e54d8ae1e5ca.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_media_sonata_6b55eb3f91aab49e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_3296b36dbe4c7fa3.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_authman_27829e1b3df01691.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_83386eac0379231b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v1.0.3705_b19cf3207984c497.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v2.0.50727_1033_7994eb100abd5435.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v2.0.50727_config_9a0d48f3c07d2a12.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v2.0.50727_e9368840261e60ee.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v2.0.50727_mui_0409_fbb44c0c63bd26c.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v2.0.50727_redistlist_2e6ab8b35e9ef953.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v2.0.50727_subsetlist_2a1589056b6db300.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v3.0_windows_communication_foundation_e07323de19ff1b52.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v3.0_windows_communication_foundation_en-us_ff3176905af82a92.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v3.0_wpf_b56a2354fbfa0c31.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v3.0_wpf_en-us_22092b638fc9de75.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v3.0_wpf_xamlviewer_97ff09273e68a809.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v3.5_1033_b573e20073d26166.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v3.5_5588a8293fdc4499.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_microsoft.net_framework_v3.5_sql_en_30e6a6afa3284c6e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_performance_02bd33cc045df684.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_performance_winsat_ac47b36afb2fa68e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_performance_winsat_datastore_34fe222e5de27d61.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_pla_reports_a2604845b2b380ca.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_pla_reports_en-us_04eb81229a78dfb4.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_pla_rules_0bde462ce96f215e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_pla_rules_en-us_8cd2a7c250e636a2.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_policydefinitions_89130cdfc4d9c27c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_policydefinitions_en-us_3b1c5b998da0d4ae.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_prefetch_1688e4e8b2f89473.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_prefetch_readyboot_925024bb73d7b5a6.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_resources_ease_of_access_themes_e29108c7f81ea04c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_resources_fbee56ab048ab239.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_resources_themes_4d0d4910e83c2273.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_resources_themes_aero_3fd78bf4cb5fa2c4.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_resources_themes_aero_en-us_ab16867f204414fa.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_resources_themes_aero_shell_a91dfa5124b343c4.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_resources_themes_aero_shell_normalcolor_10be8ec981b35fb6.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_resources_themes_aero_shell_normalcolor_en-us_8f1a9ecd4c3325e8.cdf-ms
Opens:
Opens: C:\Windows\winsxs\FileMaps\\$\$_schcache_f995a5d4decb8cc0.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_schemas_eaphost_52e2de002c0b1796.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_schemas_eapmethods_2935fdc1307d3ad6.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_schemas_tworkspace_8eac79c1e59127ee.cdf-ms
Opens:
Opens: C:\Windows\winsxs\FileMaps\\$\$_schemas_wcn_b437fb7b7751c8a8.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_security_audit_073f574e8f328f85.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_security_fe3ad40cd6e08c7c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_servicing_editions_596ea20ddafb9f7d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_servicing_en-us_62939e786cb82928.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_servicing_fc2045b9046cc796.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_servicing_gc32_972ee38cf65a9c2f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_servicing_version_6.1.7601.17514_a11608d70a47f4d5.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_shellnew_0394304acf469b24.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_speech_common_76cd6f1aaba6e83b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_speech_common_en-us_11ebcc5f3c902d23.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_speech_engines_lexicon_en-gb_bd71d721f658dd56.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_speech_engines_lexicon_en-us_bd71d54bf658e12b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_speech_engines_sr_en-gb_3201b387cd317f4d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_speech_engines_sr_en-us_3201cbb7cd315cd0.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_0409_06652563df2ff0c1.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_system32_advancedinstallers_dfe2cf200b391371.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ar-sa_3b02d130904371b4.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_bg-bg_3ce955ba8d69a9ab.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_boot_06654401df2fc50e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_boot_en-us_bd4746182a790f00.cdf-ms
ms
Opens:
C:\Windows\winsxs\FileMaps\\$\$_system32_codeintegrity_e9af9308cfc26dc2.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_com_066545e3d047e7c7.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_com_en-us_4019834316e68b9b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_cs-cz_3ecfeffb68a8fc3f6.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_da-dk_40b64d5e87b63595.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_de-de_40b64d5e87b647ef.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_dism_066548addf2fb4db.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_dism_en-us_064f3ab06d0848d3.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_driverstore_en-us_f6b4aaeeda14a371.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_drivers_dc1b782427b5ee1b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_drivers_en-us_4bb913fc5eb96bcf.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_drivers_etc_a531967eb3dfecbd.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_drivers_umdf_a531b5dc588477d3.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_drivers_umdf_en-us_b8ba9f5b7f1c3933.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_el-gr_429cd0b684dc71bd.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_429cd25484dc6f94.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_205e682c4ad0fe50.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_enterprise_758c84c10065b5be.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_enterprise_758c84d30065b56d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_enterprise_1f6aff8483fc8d55.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_homebasic_bf4c0782a00b4a92.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_homebasic_bf4c063ea00b4d6b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_homebasic_fa0efb1c1bd4a64f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_homepremium_26b2adb8fffe6aeb.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_homepremium_26b2adb8fffe6af4.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_homepremium_26b2adb8fffe6af4.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_professionale_d407bf8aae39fb3e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_professional_d407d0a0ae39e19d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_professional_5918bf2ee6a07e89.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_starter_f6228028229393f0.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_starter_f6228028229393f9.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_starter_f622802873b12085.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_ultimate_3692e229c097ae4c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_ultimate_3692f33fc09794ab.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_default_ultimate_fb35b2e019a373f7.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_enterprise_1d6f5a51fa30e848.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_enterprise_1d6f5a63fa30e7f7.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_enterprise_0a9aa7d44eee0b7f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_homebasic_aa7bafd26afcc8bc.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_homebasic_aa7bae8e6afcc95.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_homebasic_341b792f755543ad.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_homepremium_ce9583506532fca7.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_homepremium_ce9583506532fcb0.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_homepremium_ce95835012f5fa8a.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_professionale_9cb528bb523eb560.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_professional_9cb539d1523e9bbf.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_professional_00fb94bfbdd51045.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_starter_d5453e150472d334.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_starter_d5453e150472d33d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_starter_d5453e15283eab7b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_ultimate_709f603d1a184baa.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_ultimate_709f71531a183209.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_eval_ultimate_da5870ccfb82b33b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_enterprise_ff340ff929b60a6f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_enterprise_ff340eb529b60d48.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_enterprise_91ed40889f955d10.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_homebasic_65b9eb47628f590b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_homebasic_65b9fc5d628f3f6a.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_homebasic_254ee2d1432fe5da.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_homepremium_35794f97aba466da.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_homepremium_35794fa9aba46689.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_homepremium_703e4180a32e263d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_professionale_e0db4d0dc779aff1.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-

us_licenses_oem_professionaln_e0db4d0dc779affa.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_professional_e0db4d0dc7ac2dac.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_startere_3099b13c9201d0f3.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_startern_3099b14e9201d0a2.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_starter_151ea2a70dab9296.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_ultimatee_1ea73fcb54424f75.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_ultimaten_1ea73fcb54424f7e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en-us_licenses_oem_ultimate_1ea73fcaaf270754.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_en_9da4492827ac64e5.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_es-es_429cd1a084dc7119.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_et-ee_429cb6e884dc9948.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_fi-fi_448337a68202d703.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_fr-fr_448347788202c03b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_he-il_48502d1c7c4f6669.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_hr-hr_485036ac7c4f596f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_hu-hu_48503bf27c4f51d7.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ias_0665534bd047d20d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_icsxml_1f8f393b196e65ae.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ime_imejp10_aead4918eed09977.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ime_imejp10_applets_bad04da37647b46c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ime_imekr8_46a67c6e42ef3b99.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ime_imekr8_applets_4b4e797746aa967c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ime_imekr8_dicts_4b36d5aba5194cae.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ime_imesc5_46a6606042ef6565.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ime_imesc5_applets_7ab7847ddb9a9a48.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ime_imetc10_aead306aead0be86.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ime_imetc10_applets_93adac07b5e841fb.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ime_shared_5a5b3a5824d8fee4.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ime_shared_res_791e6438104a0cf8.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_inetsrv_e6240a381854fe3d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_it-it_4a36b1ca7975a0f9.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ja-jp_4c1d2478769bf2f4.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ko-kr_4e039de673c23e4a.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_logfiles_wudf_082845cc19e06817.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_lt-lt_4fea189870e886c7.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_lv-lv_4fea1c1c70e881b7.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_manifeststore_7d35b12f9be4c20e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migration_927a21df1acd7c18.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migration_en-us_815d10948a0810a2.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migration_wsmt_rras_dlmanifests_3797d36d4dbe18ed.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migration_wsmt_rras_dlmanifests_microsoft-windows-rasserver-migplugin_60ef4b1ac8368ae4.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migration_wsmt_rras_replacementmanifests_475f557ec0a59abb.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migration_wsmt_rras_replacementmanifests_microsoft-windows-rasapi-migplugin_4c5c5fbc1ceebb383.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migration_wsmt_rras_replacementmanifests_microsoft-windows-rasserver-migplugin_b1d9b81e0b884bcc.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_2650d8d30fee1fe9.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_bitsextensions-server_7d542a16c26409f3.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_f1386c432966667b.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-activedirectory-webseervices-dl_b2cdce29afb29e47.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-adfs-dl_893986f097ae8ea9.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-bluetooth-config_40d5c57bfa898bfd.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-com-complus-setup-dl_1ee4026d5f5876ce.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-com-dtc-setup-dl_a3b468532c03dbe0.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-dhcpservermigplugin-dl_0534ab06e10ae139.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-directoryservices-adam-dl_6c3018cc6f347ede.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-iasserver-migplugin_96e6769f772696e5.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-ie-esc_881b20a0d277648.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-iis-dl_8822f736d253acda.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-international-core-dl_d66e65e1080457e5.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-mediaplayer-drm-dl_552be0fd1dd444d0.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-mediaplayer_644fa9f0de4025eb.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-ndis_f0ef0c61452d5b28.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-rasapi_86cec7cd5753cec.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-rasconnectionmanager_2597396f593c1559.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-rasserver-migplugin_9fbe397ae34120be.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-shmig-dl_45622e527f470963.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-storagemigration_d55783f2ccb4b27.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-sxs_214556d37cabee6c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-tapisetup_0be6007940c10533.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-textservicesframework-migration-dl_549205906affe6bf.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-unimodem-config_2000ab316115550f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_microsoft-windows-wmi-core_0fa6ec0ad029fddb.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_dlmanifests_networking-mpssvc-svc_e23ab12e0e23ec55.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_en-us_b32d907252d3e073.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_postmigres_data_8383ed297796e30e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_postmigres_web_997c3ff186280ede.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_postmigres_web_base_images_0e64dea9756e1d4c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_174c7b92bb7d581f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_microsoft-activedirectory-webservices_fbf8031b6420fb6.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_microsoft-international-core_05a14960964e6af4.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_microsoft-windows-audio-mmecore-other_5137bedd30b4e5d8.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_microsoft-windows-gameuxmig_726077238a45fd4a.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_microsoft-windows-iis-rm_9ee468490d6de347.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_microsoft-windows-ndis_b44547c729f73574.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_microsoft-windows-offlinefiles-core_3b64983f65339578.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_microsoft-windows-shmig_9ef85dcb89d16c58.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_microsoft-windows-terminalservices-appserver-licensing_10d3d9d862990d9c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_microsoft-windows-terminalservices-licenseserver_cff2bf5f876a8fcd.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_usb_395978177bf6d5e1.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_migwiz_replacementmanifests_windowssearchengine_145004789b880a4a.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_msdtc_trace_f33466dc5bf36670.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_mui_0409_ecc96e0e9498d62e.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_mui_dispec_d93de566344a36d0.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_nb-no_53b700d66b352886.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_networklist_029a4846a59cac56.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_networklist_icons_2b49083c03963dec.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_networklist_icons_stockicons_c7f9dde8d52dc62c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_n1-n1_53b6f9bc6b35343b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_oobe_06655c95ddf2fa06f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_oobe_en-us_e44fe14df02b3595.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_pl-pl_5783e8f06581cd6f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_printing_admin_scripts_en-us_f242a041737eb912.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_pt-br_5783f3346581bed3.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_pt-pt_5783f7006581b92f.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ras_06656461d047b86c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ro-ro_5b50dd6a5fce5f0b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_ru-ru_5b50e7f65fce4fdb.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_setup_5d3758a05cf4a445.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_setup_en-us_afa35959583f5dbd.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_sk-sk_5d374dfc5cf4b5c5.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_sl-si_5d374a0c5cf4bbc8.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_slmgr_0409_c09c721c0002fb96.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_smi_schema_b445cd341d59fadc.cdf-ms
ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_speech_common_8c297630658eaa3d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_speech_engines_sr-en-us_50079c0208866964.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_speech_engines_sr_f5f77fb9283237d8.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_speech_speechux_bf4b53e8d47da913.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_speech_speechux_en-gb_84f7bae6593a3452.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_speech_speechux_en-us_84f7db2c593a03f7.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spool_drivers_color_714407f67ff2f9d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spool_drivers_w32x86_3_8416c27bd490b8bd.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spool_drivers_w32x86_3_en-us_cc27677906e15f61.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spool_drivers_w32x86_3_mui_0409_b123c2e8e96d758d.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spool_prtrprocs_w32x86_ef52e6aef2b8011c.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spool_prtrprocs_w32x86_en-us_5b08a36c001a2d60.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spool_tools_e03b2d8f300154a4.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spool_tools_en-us_103725fe114f4888.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spool_tools_microsoft_xps_document_writer_6c795755c36cebb.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_sppui_5d3749c25cf4bbd3.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spp_plugin-manifests-signed_d1e9d31c180bebd2.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spp_tokens_channels_ocur_c1b54526a616e8b6.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spp_tokens_identity_11b267e2f2add041.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spp_tokens_issuance_2c48fd0ccc1c41cc.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spp_tokens_pkeyconfig_d8fc0830c525895a.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spp_tokens_ppdlic_0f09ba294211a24b.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_spp_tokens_skus_security-spp-component-sku-professional_b76e8f28df7dd879.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_sr-latn-cs_36d1c3d11e65ce00.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_sv-se_5d37410c5cf4ca56.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_sysprep_en-us_ed807a30a752749a.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_sysprep_f7b45b8dfed1b768.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_tasks_5f1dd67a5a1ae70e.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_tasks_microsoft_b7abd682baafefc2.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_tasks_microsoft_windows_media_center_ad67db1bbb2dd336.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_tasks_microsoft_windows_media_center_extender_02bff096ccf79441.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_tasks_microsoft_windows_remoteapp_and_desktop_connections_update_c0beaecbfc21a5e1.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_tasks_microsoft_windows_synccenter_6c995d37b2976a17.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_th-th_5f1dc0505a1b09f7.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_tr-tr_5f1dd1e45a1af0a7.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_uk-ua_61042a3457416b73.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_wbem_06656d9fdf2f8577.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_wbem_en-us_4555b1beb1c13883.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_wbem_tmf_026f0fb07227ea72.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_wbem_xml_026f0f207227ebbc.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_wcn_06656d8dd047aafe.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_wcn_en-us_f42897ed07859b3c.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_wdi_perftrack_e5904ddd3f58b556.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_wdi_perftrack_traces_0af2b48360b94cec.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_winbiодatabase_8ca29eba075c22c3.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_winbioplugins_071a28c5b510fb6a.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_winbioplugins_en-us_4600b46a9eff5ffa.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_windowspowershell_v1.0_3f102d555ee05d33.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_windowspowershell_v1.0_en-us_028e6949cac04f1d.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_windowspowershell_v1.0_modules_applocker_b50db0a500311141.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_windowspowershell_v1.0_modules_applocker_en-us_0185315044ae185f.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_windowspowershell_v1.0_modules_bitstransfer_935cce3b0456eb87.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_windowspowershell_v1.0_modules_bitstransfer_en-us_8f6d5322d8d680dd.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_windowspowershell_v1.0_modules_troubleshootingpack_aa01ee5573cb1655.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_windowspowershell_v1.0_modules_troubleshootingpack_en-us_53560fea81cb8acf.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_winrm_0409_a9926295fab42c40.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_zh-cn_6a8499504900c466.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_zh-hk_6a84939e4900ccf6.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system32_zh-tw_6a84aa664900aad6.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_system_4c3aa2308f9f8f41.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_temp_401038c9a18c18c0.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_tracing_bca9e27848ac4cc0.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_twain_32_209f76caa35c9a77.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_web_3f580d25a4c8e0a0.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_web_wallpaper_architecture_7e5377d6faf00937.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_web_wallpaper_characters_a0a6ad47bc54d5d2.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_web_wallpaper_landscapes_dd1321c96ffce30a.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_web_wallpaper_nature_be2d0c211d1167a9.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_web_wallpaper_scenes_bd7cd5771e94d62b.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\\$\$_web_wallpaper_windows_bcf8a09f6400ad61.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\programdata_microsoft_crypto_dss_machinekeys_43de8c451bf80cb4.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\programdata_microsoft_crypto_keys_584b284368b25bef.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\programdata_microsoft_crypto_rsa_machinekeys_aa739417efae0d58.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\programdata_microsoft_devicesync_d6b7928aa153816d.cdf-ms

Opens: C:\Windows\winsxs\FileMaps\programdata_microsoft_device_stage_device_113527a4-45d4-4b6f-b567-

97838f1b04b0__5d055d2c3e7e3719.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_device_stage_device_8702d817-5aad-4674-9ef3-4d3dec87120__8740ea4a07ab72cd.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_device_stage_task_07deb856-fc6e-4fb9-8add-d8f2cf8722c9-en-us_66e939cf450318c4.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_device_stage_task_07deb856-fc6e-4fb9-8add-d8f2cf8722c9__0ce7c057892d5774.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_device_stage_task_e35be42d-f742-4d96-a50a-1775fb1a7a42-en-us_98bc184903c637fe.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_identitycr1_9ceb7e1568e6c6e7.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_network_connections_2e5c3accd04dd407.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_user_account_pictures_default_pictures_e70ab2484087f163.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_windows_ait_140a03828e6ffe97.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_windows_devicemetastore_en-us_cc94fe8746890b55.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_windows_drm_1409f63e8e701274.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_windows_drm_cache_0462a9ca8b56f2bc.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_windows_nt_msfax_common_coverpages_642a277e0ccb775c.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_windows_nt_msfax_common_coverpages_en-us_eec635e583fac604.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_windows_nt_msfax_virtualinbox_en-us_9c5e5cbcf8e8df85.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_windows_nt_msscan_549c401cd5c756f4.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_windows_power_efficiency_diagnostics_acddb9fca5769337.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_windows_start_menu_programs_accessories_tablet_pc_0ed3cc98382d9d9a.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_windows_start_menu_programs_tablet_pc_55463303c7fe1328.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_wwansvc_b22df3b43960e1d3.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\programdata_microsoft_wwansvc_profiles_d39df26c249b675d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_d7a65bb2f0e854e7.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_818c5a0e45020fba.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_dao_3c86dc390b3b2f48.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_1.0_c96a7f20e8d9af65.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_1.7_c96a7f2ee8d9af65.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_3c86e3db0b3b254c.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_ar-sa_827c11e62573e02c.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_bg-bg_84629670229a1823.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_cs-cz_8649306c1fc0326e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_da-dk_882f8e141ce6a40d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_de-de_882f82201ce6b667.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_el-gr_8a16116c1a0ce035.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_en-us_8a16130a1a0cde0c.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_es-es_8a1612561a0cdf91.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_et-ee_8a15f79e1a0d07c0.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_fi-fi_8bfc785c1733457b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_fr-fr_8bfc882e17332eb3.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_fsdefinitions_oskmenu_4ada925d6aba5911.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_fsdefinitions_oskumpad_ee37ed195958108b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_fsdefinitions_oskpred_4ada71c56aba89ef.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_fsdefinitions_symbols_4eaf815d64e8ecbc.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_fsdefinitions_web_310c2550dac9ac6b.cdf-

ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_he-
il_8fc96dd2117fd4e1.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_hr-
hr_8fc97762117fc7e7.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_hu-
hu_8fc97ca8117fc04f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_hwrcustomization_198fbc0f379ad82.cdf-
ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_it-
it_91aff2800ea60f71.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_ja-
jp_9396652e0bcc616c.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_ko-
kr_957cde9c08f2acc2.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_lt-
lt_9763594e0618f53f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_lv-
lv_97635cd20618f02f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_nb-
no_9b30418c006596fe.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_nl-
nl_9b303a720065a2b3.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_pl-
pl_9efd29a5fab23be7.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_pt-
br_9efd33e9fab22d4b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_pt-
pt_9efd37b5fab227a7.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_ro-
ro_a2ca1e1ff4fec83.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_ru-
ru_a2ca28abf4febe53.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_sk-
sk_a4b08eb1f225243d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_sl-
sl_a4b08ac1f2252a40.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_sr-latn-
cs_c779913ce1dfaa20.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_sv-
se_a4b081c1f22538ce.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_th-
th_a6970105ef4b786f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_tr-
tr_a6971299ef4b5f1f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_uk-
ua_a87d6ae9ec71d9eb.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_zh-
cn_b1fdda05de3132de.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_ink_zh-
tw_b1fdeb1bde31194e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_msinfo_817ad0c7c1c8e490.cdf-
ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_msinfo_en-
us_98319174bb92bc08.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_stationery_3f6c21eb4ac66a56.cdf-
ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_textconv_dfb016a4185c8725.cdf-
ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_textconv_en-
us_c7ff7b7c6290f6ab.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_triedit_en-
us_59ae2daa07429081.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_microsoft_shared_vgx_3c86fd9f0b3afd9b.cdf-
ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_services_e36ba211a9258e5f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_speechengines_microsoft_tts20_01244a1856097a63.cdf-
ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_speechengines_microsoft_tts20_en-
us_d560227d1a443333.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_speechengines_microsoft_tts20_en-us-enu-
dsk_bd3acd2fa8162df2.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_system_ado_149a784bc852a2c0.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_system_ado_en-
us_9c12689ac1360dc2.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_system_b13078daf1286f60.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_system_en-
us_48bd774a3f1387ec.cdf-ms

Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_system_msadc_48cda3763ecb3874.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\program_files_common_files_system_msadc_en-us_58bb034fa66b57cc.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_common_files_system_ole_db_48d1b11cd4e5cabe.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\program_files_common_files_system_ole_db_en-us_5ff73071fce05070.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\program_files_dvd_maker_405775de8763ce75.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\program_files_dvd_maker_en-us_5c61cfeeb9f5061.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_a54613779b918be2.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_5fb67e37dd207bb6.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_babyboy_c89d1dc244d4409a.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_babygirl_08d06a5a64874f02.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_flippage_f73c094c7f16edbe.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_full_8bfb7c162731e4e9.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_huecycle_de51e7f0a4721fb8.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_layeredtitles_c4062449752ea4b1.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_memories_f44b6a98846b15a5.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_oldage_c6de81a917a8cf68.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_performance_62d38a628f8404ee.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_pets_8bfb87d82731d4bc.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_push_8bfb73162731f37e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_rectangles_5bea48dc003ff122.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_resizingpanels_d3ead0ed83352928.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_shatter_c6467e7e49f697fb.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_specialoccasion_e32b316f8a75bd6e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_sports_c6567ebf18c8e989.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_stacking_dcc38bcea7f2f1e4.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_travel_c63680851907e918.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_videowall_3cbc91699310ec3d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_dvd_maker_shared_dvdstyles_vignette_f1288c9089f4958a.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\program_files_ffd0cbfc813cc4f1.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_internet_explorer_a421d1bfaf856e2b.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\program_files_internet_explorer_en-us_2650c83f8a48b821.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_msbuild_microsoft_windows_workflow_foundation_v3.5_06f0ac2a38886194.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_reference_assemblies_microsoft_framework_v3.0_44577d982216c291.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_reference_assemblies_microsoft_framework_v3.0_subsetlist_717872f9b222111.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_reference_assemblies_microsoft_framework_v3.5_44577da22216c264.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_reference_assemblies_microsoft_framework_v3.5_redistlist_bd550cc45cc12a27.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_reference_assemblies_microsoft_framework_v3.5_subsetlist_76650e039bf95764.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_defender_3e33901162166ae9.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\program_files_windows_defender_en-us_a607fb510b9fff95.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_journal_ada99bf7bc9c9733.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\program_files_windows_journal_en-us_ff6188d8bb083f5.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_journal_templates_b0a4d1151554acfa.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_mail_e07902f329fe05e9.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\program_files_windows_mail_en-us_4eecf28483baad93.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_media_player_da4e5f6eb3198de9.cdf-ms
Opens: C:\Windows\winsxs\FileMaps\program_files_windows_media_player_en-us_94ff97943fc617cd.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_media_player_icons_94ff7ddc3fca431d.cdf-ms

Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_media_player_media_renderer_5001a1a5de706f6e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_media_player_network_sharing_aed05552f451fd7d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_media_player_skins_94ff8de43fd42ce5.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_media_player_visualizations_e380711fc66b5d12.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_nt_6101456faac5015c.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_nt_accessories_156d2b9b22040474.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_nt_accessories_en-us_4cfa7c92c2470350.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_nt_tabletextservice_9475b2de2d92bc74.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_nt_tabletextservice_en-us_0e46adde4b3af550.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_photo_viewer_6eb173d8debcda9a.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_photo_viewer_en-us_bb1893748d4240dc.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_portable_devices_8ef3f2c72e8bb2ba.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_8d6dbc4becba56da.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_en-us_467d8a71f43f36ce.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_2652ddfd4d58a723.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_calendar.gadget_b054eca667f3063.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_calendar.gadget_en-us_css_4d83524d9d6217bc.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_calendar.gadget_en-us_e8aa0ae297615c6d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_calendar.gadget_en-us_js_45a8e205c0b938de.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_calendar.gadget_images_e8b234ae384ba7b1.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_clock.gadget_85cde96256fb59df.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_clock.gadget_en-us_b92194be8e78846b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_clock.gadget_en-us_css_2690e0e99412a2f4.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_clock.gadget_en-us_js_2690dfedc0f833b4.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_clock.gadget_images_11f95cf60938de7b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_cpu.gadget_3ea229fc96d38c13.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_cpu.gadget_en-us_268aa9af5ba2d05f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_cpu.gadget_en-us_css_25b24cc85d6f7250.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_cpu.gadget_en-us_js_e0a0cbba78d6d4d6.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_cpu.gadget_images_987b0ad259a4806b.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_currency.gadget_964bdce27d2d6734.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_currency.gadget_en-us_8182ef952052028a.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_currency.gadget_en-us_css_cf9198f7f6b7f8df.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_currency.gadget_en-us_js_9037510893ce6463.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_currency.gadget_images_818b19610434093a.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_mediacycenter.gadget_css_8dda2b51661abc9.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_mediacycenter.gadget_en-us_0eda41e17d8c829e.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_mediacycenter.gadget_f08b590d17819d36.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_mediacycenter.gadget_images_15a18af15dc71ee0.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_mediacycenter.gadget_js_8dda2a54ef707137.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_picturepuzzle.gadget_284c80f2b12171b5.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_picturepuzzle.gadget_en-us_40e1f69776c7e3c9.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_picturepuzzle.gadget_en-

us_css_ee4c58e41ef91b16.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_picturepuzzle.gadget_en-us_js_ee4c57e840f5e5a0.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_picturepuzzle.gadget_images_113209543e53c7d7.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_rssfeeds.gadget_22ec6b16cd2d39ce.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_rssfeeds.gadget_en-us_42036cf020e8a972.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_rssfeeds.gadget_en-us_css_adeac7d6c2b30bf7.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_rssfeeds.gadget_en-us_js_eebbf22d9f05f549.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_rssfeeds.gadget_images_420b96bc9fb8ab54.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_slideshow.gadget_1d53bb9c29c0aa6d.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_slideshow.gadget_en-us_23311f020fdd83c5.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_slideshow.gadget_en-us_css_ca39ca876b477a1a.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_slideshow.gadget_en-us_js_ca39c98b64be74a4.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_slideshow.gadget_images_db83d22ffb6579d1.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_slideshow.gadget_images_in_sidebar_845277d664af085f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_slideshow.gadget_images_on_desktop_8c4fbdc6458a98d1.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_weather.gadget_a4898b91b8575c47.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_weather.gadget_en-us_css_863292ab8d2936a8.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_weather.gadget_en-us_d90b1afcc77a7607.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_weather.gadget_en-us_js_4f0bf75a094013ae.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_weather.gadget_images_120dpi_12fb0c15aed95ff3.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_weather.gadget_images_144dpi_12b2fa65af7b87ad.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\program_files_windows_sidebar_gadgets_weather.gadget_images_585d106689450aab.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\users_default_appdata_roaming_media_center_programs_b8fc97cb3886dd3f.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\users_public_recorded_tv_a6d3315b447834ed.cdf-ms
Opens:
C:\Windows\winsxs\FileMaps\users_public_recorded_tv_sample_media_273d5f336c167723.cdf-ms
Opens: C:\Windows\Microsoft.NET\Framework\v3.5
Opens: C:\Windows\Microsoft.NET\Framework\v3.0\WPF
Opens: C:\Windows\Microsoft.NET\Framework\v3.0\Windows Workflow
Foundation\SQL\en
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\Browsers
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Security
Opens: C:\Windows\System32\wfp
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Security\Wizard
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Security\Wizard\AppDataLocalResources
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Security\Users
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Security\Users\AppDataLocalResources
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Security\Roles
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Security\Permissions
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Security\AppDataLocalResources
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Providers
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Providers\AppDataLocalResources
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Images
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\AppDataLocalResources
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\App_Code
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\AppConfig
Opens:
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\AppConfig\AppDataLocalResources
Opens: C:\Windows\Microsoft.NET\Framework\v1.0.3705
Opens: C:\Windows\Vss\Writers\System
Opens: C:\Windows\Vss\Writers\System\Obada1de-01a9-4625-8278-69e735f39dd2.xml
Opens: C:\Windows\Vss\Writers\System\75DFB225-E2E4-4d39-9AC9-FFAF65DDF06.xml
Opens: C:\Windows\Vss\Writers\System\D61D61C8-D73A-4EEE-8CDD-F6F9786B7124.xml
Opens: C:\Program Files\Common Files\System
Opens: C:\Program Files\DVD Maker\Shared


```

Opens: C:\Windows\ehome\CreateDisc
Opens: C:\Windows\System32\en-US\Licenses\OEM
Opens: C:\Windows\System32\IME\IMEJP10
Opens: C:\Windows\Web\Wallpaper
Opens: C:\Program Files\Windows Sidebar\Gadgets
Opens: C:\Windows\diagnostics\system
Opens: C:\Windows\System32\en-US\Licenses\eval
Opens: C:\Program Files\DVD Maker\Shared\DVDStyles
Opens: C:\Windows\diagnostics\system\AERO
Opens: C:\Windows\System32\spp\tokens
Opens: C:\Windows\System32\en-US\Licenses\_Default
Opens: C:\Windows\System32\migwiz\dlmanifests
Opens: C:\Windows\schemas
Opens: C:\Windows\System32\IME\shared
Opens: C:\Windows\PolicyDefinitions
Opens: C:\Windows\System32\oobe
Opens: C:\Windows\System32\spool\tools
Opens: C:\Windows\diagnostics\system\IEBrowseWeb
Opens: C:\Windows\PLA\Rules
Opens: C:\Windows\diagnostics\system\Power
Opens: C:\Windows\System32\migwiz\replacementmanifests
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\Modules
Opens: C:\Windows\diagnostics\scheduled\Maintenance
Opens: C:\Windows\PLA\Reports
Opens: C:\Program Files\Windows Sidebar\Gadgets\MediaCenter.Gadget
Opens: C:\Windows\System32\migration
Opens: C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-
d8f2cf8722c9}
Opens: C:\Windows\diagnostics\system\IESecurity
Opens: C:\Program Files\Common Files\Microsoft shared\ink\fsdefinitions
Opens: C:\Windows\diagnostics\system\HomeGroup
Opens: C:\Windows\System32\DisM
Opens: C:\Windows\System32\IME\IMESC5
Opens: C:\Program Files\Windows Sidebar\Gadgets\Weather.Gadget\images
Opens: C:\Windows\System32\NetworkList\Icons
Opens: C:\Program Files\Common Files\System\ado
Opens: C:\Windows\diagnostics\system\Audio
Opens: C:\Windows\System32\migration\WSMT\rras\replacementmanifests
Opens: C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.5
Opens: C:\Program Files\Windows Sidebar\Gadgets\SlideShow.Gadget\images
Opens: C:\Windows\Boot\PCAT
Opens: C:\ProgramData\Microsoft\Windows NT\MSFax
Opens: C:\Windows\diagnostics\system\Networking
Opens: C:\Windows\diagnostics\system\Device
Opens: C:\Windows\diagnostics\system\Search
Opens: C:\Program Files\Windows Photo Viewer
Opens: C:\Windows\diagnostics\system\Performance
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer
Opens: C:\Windows\diagnostics\system\WindowsMediaPlayerPlayDVD
Opens: C:\Windows\diagnostics\system\WindowsMediaPlayerMediaLibrary
Opens: C:\Program Files\Common Files\System\msadc
Opens: C:\Program Files\Common Files\System\OLE DB
Opens: C:\ProgramData\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-
1775fb1a7a2}
Opens: C:\Windows\diagnostics\system\DeviceCenter
Opens: C:\Windows\diagnostics\system\Printer
Opens: C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0
Opens: C:\Windows\diagnostics\system\WindowsMediaPlayerConfiguration
Opens: C:\Windows\System32\com
Opens: C:\Windows\diagnostics\system\PCW
Opens: C:\Windows\System32\migration\WSMT\rras\dlmanifests
Opens: C:\Program Files\Windows Mail
Opens: C:\System Volume Information\SPP\OnlineMetadataCache
Opens: C:\System Volume Information\SPP\OnlineMetadataCache\{4f2dcf97-2c63-
4554-a51c-bf0ab965d1e0}_OnDiskSnapshotProp
Opens: C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT.LOG1
Opens: C:\Users\Admin\ntuser.dat.LOG1
Opens: C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT.LOG1
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
Opens: C:\Windows\System32\config\SOFTWARE.LOG1
Opens: C:\Windows\System32\config\DEFAULT.LOG1
Opens: C:\Windows\System32\config\SECURITY.LOG1
Opens: C:\System Volume Information\Syscache.hve.LOG1
Opens: C:\Windows\System32\Microsoft\Protect\S-1-5-19
Opens: C:\Windows\AppPatch\msmain.sdb
Opens: C:\Windows\System32\en-US\sxs.dll.mui
Opens: C:\Windows\System32\ar-SA
Opens: C:\Windows\System32\cs-CZ
Opens: C:\Windows\System32\da-DK
Opens: C:\Windows\System32\de-DE
Opens: C:\Windows\System32\el-GR
Opens: C:\Windows\System32\es-ES
Opens: C:\Windows\System32\fi-FI
Opens: C:\Windows\System32\fr-FR
Opens: C:\Windows\System32\he-IL
Opens: C:\Windows\System32\hu-HU
Opens: C:\Windows\System32\it-IT
Opens: C:\Windows\System32\ja-JP
Opens: C:\Windows\System32\ko-KR
Opens: C:\Windows\System32\nb-NO
Opens: C:\Windows\System32\nl-NL
Opens: C:\Windows\System32\pl-PL
Opens: C:\Windows\System32\pt-BR
Opens: C:\Windows\System32\pt-PT
Opens: C:\Windows\System32\ru-RU
Opens: C:\Windows\System32\sr-Latn-CS
Opens: C:\Windows\System32\sv-SE
Opens: C:\Windows\System32\tr-TR
Opens: C:\Windows\System32\zh-CN
Opens: C:\Windows\System32\zh-TW
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.dll
Opens: C:\Windows\System32\RstrMgr.dll
Opens: C:\Windows\Installer\$\PatchCache\Managed
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-
RestartManager%40operational.evtx
Opens: C:\Windows\System32\msisip.dll
Opens: C:\Windows\System32\en-US\DisplaySwitch.exe.mui
Opens: C:\Windows\System32\en-US\SnippingTool.exe.mui
Opens: C:\Windows\System32\SNTSearch.dll
Opens: C:\Windows\System32\en-US\sntsearch.dll.mui
Opens: C:\Windows\System32\OobeFldr.dll
Opens: C:\Windows\System32\en-US\oobefldr.dll.mui
Opens: C:\Windows\System32\adslpc.dll
Opens: C:\Windows\Prefetch\ReadyBoot\Trace7.fx
Opens: C:\Windows\System32\security.dll
Opens: C:\Windows\System32\pythoncom27.dll

```

Opens: C:\Windows\System32\syssetup.dll
Opens: C:\Windows\System32\wbem\wbemdisp.dll
Opens: C:\Windows\System32\wbem\wbemdisp.tlb
Opens: C:\Windows\System32\spwmi.dll
Opens: C:\Windows\System32\drivers\asynccmac.sys
Opens: C:\Windows\System32\cscrip.exe
Opens: C:\Windows\System32\en-US\cscrip.exe.mui
Opens: C:\Windows\System32\vbscript.dll
Opens: C:\Windows\System32\slmgr.vbs
Opens: C:\Windows\System32\wshect.dll
Opens: C:\Windows\System32\scrobj.dll
Opens: C:\Windows\System32\scrrun.dll
Opens: C:\Windows\System32\slmgr\0409\slmgr.ini
Opens: C:\Windows\System32\winevt\Logs\Microsoft-Windows-ReadyBoost%40operational.evtx
Opens: C:\\$Extend
Writes to: C:\WinOldFileq\83A494219A6.exe
Writes to: C:\WinOldFileq\9C413B7B23C1D6D
Writes to: C:\Windows\Prefetch\NTOSBOOT-B00DFAAD.pf
Writes to: C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf
Writes to: C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf
Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[2].txt
Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[1].txt
Writes to: C:\Windows\System32\wfp\wfpdiag.etl
Writes to: C:\Windows\System32\winevt\Logs\Microsoft-Windows-ReadyBoost%40operational.evtx
Reads from: C:\Windows\System32\ntdll.dll
Reads from: C:\Windows\Temp\spyeye_inj_ector_.exe
Reads from: C:\WinOldFileq\83A494219A6.exe
Reads from: C:\WinOldFileq\9C413B7B23C1D6D
Reads from: C:\Windows\System32\user32.dll
Reads from: C:\Windows\System32\wininet.dll
Reads from: C:\Windows\System32\ws2_32.dll
Reads from: C:\Windows\System32\advapi32.dll
Reads from: C:\Windows\System32\crypt32.dll
Reads from: C:\Windows\Prefetch\AgGlobalHistory.db
Reads from: C:\Windows\Prefetch\AgGlobalFaultHistory.db
Reads from: C:\Windows\Prefetch\AgGlobalFgAppHistory.db
Reads from: C:\Windows\System32\Sens.dll
Reads from: C:\Windows\System32\stdole2.tlb
Reads from: C:\Windows\Prefetch\RUNDLL32.EXE-1304AE86.pf
Reads from: C:\Windows\System32\drivers\etc\hosts
Reads from:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@www.microsoft[2].txt
Reads from:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[1].txt
Reads from: C:\Windows\Prefetch\ReadyBoot\Trace3.fx
Reads from: C:\Windows\Prefetch\ReadyBoot\Trace4.fx
Reads from: C:\Windows\Prefetch\ReadyBoot\Trace5.fx
Reads from: C:\Windows\Prefetch\ReadyBoot\Trace6.fx
Reads from: C:\Windows\Prefetch\ReadyBoot\Trace7.fx
Reads from: C:\Windows\Prefetch\ReadyBoot\ReadyBoot.etl
Reads from: C:\Windows\System32\winevt\Logs\Microsoft-Windows-ReadyBoost%40operational.evtx
Deletes: C:\Windows\Temp\spyeye_inj_ector_.exe
Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[1].txt
Deletes:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@microsoft[2].txt
Deletes: C:\Windows\Prefetch\ReadyBoot\ReadyBoot.etl

Network Events

DNS query: alexeyartemov.com
DNS query: wpad
DNS query: www.microsoft.com
DNS query: teredo.ipv6.microsoft.com
DNS response: alexeyartemov.com ⇒ 198.105.244.11
DNS response: alexeyartemov.com ⇒ 104.239.213.7
DNS response: e10088.dspb.akamaiedge.net ⇒ 23.7.35.22
DNS response: e10088.dspb.akamaiedge.net ⇒ 184.86.231.62
DNS response: e10088.dspb.akamaiedge.net ⇒ 23.221.10.57
DNS response: e10088.dspb.akamaiedge.net ⇒ 104.84.156.166
DNS response: e10088.dspb.akamaiedge.net ⇒ 95.101.192.8
Connects to: 88.198.13.147:443
Connects to: 8.8.8.8:53
Connects to: 10.74.9.255:138
Connects to: 4.2.2.1:53
Connects to: 224.0.0.252:5355
Connects to: 198.105.244.11:80
Connects to: 127.0.0.1:80
Connects to: 23.221.10.57:80
Connects to: 23.7.35.22:80
Connects to: 104.239.213.7:80
Connects to: 95.101.192.8:80
Sends data to: 8.8.8.8:53
Sends data to: 88.198.13.147:443
Sends data to: 10.74.9.255:138
Sends data to: 4.2.2.1:53
Sends data to: 224.0.0.252:5355
Sends data to: alexeyartemov.com:80 (198.105.244.11)
Sends data to: e10088.dspb.akamaiedge.net:80 (23.221.10.57)
Sends data to: e10088.dspb.akamaiedge.net:80 (23.7.35.22)
Sends data to: e10088.dspb.akamaiedge.net:80 (95.101.192.8)
Receives data from: 88.198.13.147:443
Receives data from: 10.74.9.100:138
Receives data from: 4.2.2.1:53
Receives data from: alexeyartemov.com:80 (198.105.244.11)
Receives data from: 8.8.8.8:53
Receives data from: e10088.dspb.akamaiedge.net:80 (23.221.10.57)
Receives data from: e10088.dspb.akamaiedge.net:80 (23.7.35.22)
Receives data from: e10088.dspb.akamaiedge.net:80 (95.101.192.8)

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\run
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\1

Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Creates key: HKCU\software\microsoft\internet explorer\phishingfilter
Creates key: HKCU\software\microsoft\internet explorer\recovery
Creates key: HKLM\software\microsoft\windows nt\currentversion\networklist\nla\cache
Creates key: HKLM\software\microsoft\windows
nt\currentversion\networklist\nla\cache\intranet
Creates key: HKLM\software\microsoft\windows
nt\currentversion\networklist\nla\cache\intranet\
Creates key: HKCU\software\microsoft\systemcertificates\my
Creates key: HKCU\software\microsoft windows
Creates key: HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection
Creates key: HKU\S-1-5-21-2160590473-689474908-1361669368-1002\software\microsoft\ras
autodial
Creates key: HKU\S-1-5-21-2160590473-689474908-1361669368-1002\software\microsoft\ras
autodial\default
Creates key: HKLM\software\microsoft\ras autodial
Creates key: HKLM\software\microsoft\ras autodial\default
Creates key: HKLM\software\microsoft\windows nt\currentversion\emdmgmt
Creates key: HKLM\system\currentcontrolset\services\rdyboost\parameters
Creates key: HKLM\software\microsoft\windows
nt\currentversion\superfetch\diskassessment
Creates key: HKLM\software\microsoft\windows nt\currentversion\prefetcher
Creates key: HKLM\software\microsoft\windows\currentversion\optimallayout
Creates key: HKLM\system\currentcontrolset\control\deviceclasses
Creates key: HKLM\system\currentcontrolset\services\rdyboost\attachstate
Creates key: HKLM\software\microsoft\windows nt\currentversion\ncache
Creates key: HKLM\system\currentcontrolset\control\session manager\memory
management\prefetchparameters
Creates key: HKLM\software\microsoft\tracing
Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\connections
Creates key: HKLM\software\classes
Creates key: HKCU\software\appdatalow
Creates key: HKCU\software\microsoft\internet explorer\internetregistry
Creates key: HKCU\software\microsoft\internet explorer\lowregistry
Creates key: HKCU\software\microsoft\internet
explorer\lowregistry\dontshowmethisdialagain
Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache
Creates key: HKCU\software\microsoft\internet explorer\intelliforms
Creates key: HKCU\software\microsoft\internet explorer\toolbar
Creates key: HKCU\software\microsoft\internet explorer\toolbar\webbrowser
Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\menuorder\favorites
Creates key: HKCU\software\microsoft\internet explorer\pagesetup
Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\passport\lowdamap
Creates key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\lowregistry
Creates key: HKCU\software\microsoft\internet explorer\zoom
Creates key: HKCU\software\microsoft\internet explorer\browseremulation\lowmic
Creates key: HKCU\software\microsoft\internet explorer\ietyl\lowmic
Creates key: HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key: HKLM\software
Creates key: HKLM\software\microsoft
Creates key:
HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp
Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{7bf7ed91-f442-458a-abea-c661d1bd5efb}
Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{7bf7ed91-f442-458a-abea-c661d1bd5efb}\82-da-ad-19-17-f7
Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\82-da-ad-19-17-f7
Creates key: HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history
Creates key: HKLM\software\microsoft\wbem\cimom
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007
Creates key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
Deletes value: HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
Deletes value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpnameserver]
Deletes value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpnameserver]
Deletes value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpdomain]
Deletes value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpdomain]
Deletes value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{128919e8-8a5e-41d1-
ac17-c19ce8a73253}[dhcpnameserverlist]
Deletes value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpsubnetmaskopt]
Deletes value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpdefaultgateway]
Deletes value: HKLM\system\currentcontrolset\services\netbt\parameters[dhcpscopeid]
Deletes value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{128919e8-8a5e-41d1-
ac17-c19ce8a73253}[dhcplibiosoptions]
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gpdll
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control_panel\desktop
Opens key: HKCU\control_panel\desktop\mui\cached
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\83a494219a6.exe
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell_folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\83a494219a6.exe
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\hardware\devicemap\video
Opens key: HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-fd27e3774e32}\0000
Opens key: HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\38267a616a&0&10
Opens key: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000
Opens key: HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-0d8e74595f78}\0000
Opens key: HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-8ed0c8eb59a8}\0000
Opens key: HKLM\system\currentcontrolset\control\error_message_instrument\
Opens key: HKLM\system\currentcontrolset\control\error_message_instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime_compatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\ole
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\windows\currentversion\internet_settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKLM\software\policies\microsoft\power\powerrequestoverride
Opens key: HKLM\system\currentcontrolset\control\power\powerrequestoverride
Opens key: HKLM\system\currentcontrolset\control\power\powerrequestoverride\driver
Opens key: HKLM\software\microsoft\internet_explorer
Opens key: HKCU\software\microsoft\windows\currentversion\internet_settings\user
agent
Opens key: HKLM\software\microsoft\windows\currentversion\internet_settings\user
agent
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user_agent
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user_agent
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\user_agent
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\user_agent
Opens key: HKLM\software\microsoft\windows\currentversion\internet_settings\user
agent\lua_tokens
Opens key: HKCU\software\microsoft\windows\currentversion\internet_settings
Opens key: HKLM\software\microsoft\windows\currentversion\internet_settings\user
agent\pre_platform
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user_agent\pre_platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user_agent\pre_platform
Opens key: HKLM\software\microsoft\windows\currentversion\internet_settings\user
agent\post_platform
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user_agent\post_platform
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user_agent\post_platform
Opens key: HKLM\software\microsoft\internet_explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet_explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
Opens key: HKLM\software\policies\microsoft\sqlclient\windows
Opens key: HKLM\software\microsoft\sqlclient\windows
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\psched\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup_migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\policies
Opens key: HKCU\software\policies
Opens key: HKCU\software
Opens key: HKLM\software
Opens key: HKLM\software\policies\microsoft\internet_explorer
Opens key: HKLM\software\policies\microsoft\internet_explorer\main
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKLM\software\policies\microsoft\internet_explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet_explorer\main\featurecontrol
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user_shell
folders
Opens key: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
Opens key: HKCU\appevents\schemes\
Opens key: HKCU\appevents\schemes\apps\.default\open\.current
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
Opens key: HKCU\appevents\schemes\apps\.default\open\.current\active
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
Opens key: HKCU\software\microsoft\internet
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{f3229805-869e-479e-ba76-dd643f1d1b80}
Opens key: HKLM\software\microsoft\cryptography\oid
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\#16
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\ldap
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\certdllopenstoreprov
Opens key: HKCU\software\microsoft\systemcertificates\my\physicalstores

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2160590473-689474908-1361669368-1002

Opens key: HKCU\software\microsoft\systemcertificates\my

Opens key: HKCU\software\microsoft\systemcertificates\my\

Opens key: HKCU\software\microsoft\systemcertificates\my\certificates

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{f3229805-869e-479e-ba76-dd643f1d1b80}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{72dd97a9-e544-4915-88d8-44e829c34f68}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{72dd97a9-e544-4915-88d8-44e829c34f68}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{0aab3bce-41ed-11e5-bf5b-080027dfc114}

Opens key: HKCU\software\microsoft\systemcertificates\my\crls

Opens key: HKCU\software\microsoft\systemcertificates\my\ctls

Opens key: HKCU\software\microsoft\systemcertificates\my\keys

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{0aab3bce-41ed-11e5-bf5b-080027dfc114}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{69d2510e-6c18-11e3-b3bc-a199dcc7ccd3}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{69d2510e-6c18-11e3-b3bc-a199dcc7ccd3}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{7c5653f0-144a-4534-9e34-28ac99cba85e}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}

Opens key: HKCU\appevents\schemes\apps\default\close\current

Opens key: HKCU\appevents\schemes\apps\default\close\current\active

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\compatibility assistant

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7c5653f0-144a-4534-9e34-28ac99cba85e}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{69d2510f-6c18-11e3-b3bc-a199dcc7ccd3}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{69d2510f-6c18-11e3-b3bc-a199dcc7ccd3}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-1709a0196aed}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-a68f334c8d34}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6fe-7037-11de-816d-001c23e25b76}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6fe-7037-11de-816d-001c23e25b76}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac701-7037-11de-816d-001c23e25b76}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac701-7037-11de-816d-001c23e25b76}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac700-7037-11de-816d-001c23e25b76}

Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac700-7037-11de-816d-001c23e25b76}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{db2b4279-b5cf-4626-9dba-32d0ece44c87}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{db2b4279-b5cf-4626-9dba-32d0ece44c87}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e2f8a220-af88-446c-9a55-453e58dd3a33}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e28d896f-9ea8-433a-9c10-66c97c19a921}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e28d896f-9ea8-433a-9c10-66c97c19a921}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{dcb14c61-690d-46f7-8a89-150432fa5c44}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{483c9ff8-503d-414b-b402-e4c1f1f568cb}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{483c9ff8-503d-414b-b402-e4c1f1f568cb}

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{c0de3e38-8ba7-479f-8b75-833f294c5aa8}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{c0de3e38-8ba7-479f-8b75-833f294c5aa8}

Opens key: HKLM\system\currentcontrolset\control\cryptography\providers

Opens key: HKLM\system\currentcontrolset\control\cryptography\configuration

Opens key: HKLM\system\currentcontrolset\enum\bth

Opens key: HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0001\ndi\interfaces
Opens key: HKLM\system\currentcontrolset\enum\root*isatap\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0009
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0009\ndi\interfaces
Opens key: HKLM\system\currentcontrolset\enum\root\ms_12tpminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0002\ndi\interfaces
Opens key: HKLM\system\currentcontrolset\enum\root*teredo\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0011\ndi\interfaces
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006\ndi\interfaces
Opens key: HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi\interfaces
Opens key: HKLM\system\currentcontrolset\control\network
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi
Opens key: HKLM\software\microsoft\network\media
Opens key: HKCU\software\classes\
Opens key: HKLM\software\classes\
Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\implemented
categories\{00000003-0000-0000-c000-000000000046}
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi\interfaces
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip6\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005\ndi\interfaces
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ppoeminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004\ndi\interfaces
Opens key: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003\ndi\interfaces
Opens key: HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000\ndi\interfaces
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKU\
Opens key: HKU\s-1-5-21-2160590473-689474908-1361669368-1002\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKU\s-1-5-21-2160590473-689474908-1361669368-1002
Opens key: HKU\s-1-5-21-2160590473-689474908-1361669368-1002\control
panel\international
Opens key: HKLM\software\microsoft\windows
nt\currentversion\networklist\profiles\{7bf7ed91-f442-458a-abea-c661d1bd5efb}
Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\classes\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
Opens key: HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-1069-a2dd-08002b30309d}
Opens key: HKU\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-1069-a2dd-08002b30309d}
Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
Opens key: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\controlpanel\namespace\namecustomizations
Opens key: HKLM\system\currentcontrolset\control\mui\stringcachesettings
Opens key: HKCU\software\classes\local settings\muicache\27\52c64b7e
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\system\currentcontrolset\control\network\showwirelessconnectingonstart
Opens key: HKLM\system\currentcontrolset\control\wmi\autologger\readyboot
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{7f108a28-9833-4b3b-b780-2c6b5fa5c062}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#ide#cdromhl-dt-st_dvd-rom_gdr-t10n_____.02____#5&28836b88&0&0.0.0#\53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-

[illegible]

[illegible]

[illegible]

94f2-00a0c91efb8b}\\##7#scsi\\disk&ven_dell&prod_virtual_disk#6&3af2ddc5&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\\#\\control
Opens key: HKLM\\system\\currentcontrolset\\control\\deviceclasses\\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\\properties
Opens key: HKLM\\system\\currentcontrolset\\enum\\ide\\diskhitachi_____3.5.1.9_\\5&394c0ad3&0&0.0.0\\device
parameters
Opens key: HKLM\\software\\microsoft\\rpc\\securityservice
Opens key: HKLM\\system\\currentcontrolset\\control\\lsaextensionconfig\\sspicli
Opens key: HKLM\\system\\currentcontrolset\\control\\securityproviders
Opens key: HKLM\\system\\currentcontrolset\\control\\lsa\\sspicache
Opens key: HKLM\\system\\currentcontrolset\\control\\lsa\\sspicache\\credssp.dll
Opens key: HKLM\\system\\currentcontrolset\\control\\securityproviders\\saslpfiles
Opens key: HKLM\\software\\microsoft\\tracing\\explorer_rasapi32
Opens key: HKLM\\software\\microsoft\\tracing\\explorer_rasmancs
Opens key: HKCR\\clsid\\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}
Opens key: HKCR\\clsid\\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\\treatas
Opens key: HKCR\\clsid\\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\\progid
Opens key: HKCR\\clsid\\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\\inprocserver32
Opens key: HKCU\\software\\classes\\autoproxytypes
Opens key: HKCR\\autoproxytypes
Opens key: HKCU\\software\\classes\\autoproxytypes\\application/x-internet-signup
Opens key: HKCR\\autoproxytypes\\application/x-internet-signup
Opens key: HKCR\\clsid\\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\\inprochandler32
Opens key: HKCR\\clsid\\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\\inprochandler
Opens key: HKCU\\software\\classes\\autoproxytypes\\application/x-ns-proxy-autoconfig
Opens key: HKCR\\autoproxytypes\\application/x-ns-proxy-autoconfig
Opens key: HKLM\\software\\microsoft\\eventssystem\\{26c409cc-ae86-11d1-b616-00805fc79216}\\eventclasses\\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}-\\{00000000-0000-0000-000000000000}
Opens key: HKCR\\interface\\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\\typelib
Opens key: HKCR\\typelib
Opens key: HKCR\\typelib\\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}
Opens key: HKCR\\typelib\\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\\2.0
Opens key: HKCR\\typelib\\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\\2.0\\0
Opens key: HKCR\\typelib\\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\\2.0\\0\\win32
Opens key: HKCR\\interface\\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}
Opens key: HKCR\\typelib\\{00020430-0000-0000-c000-000000000046}
Opens key: HKCR\\typelib\\{00020430-0000-0000-c000-000000000046}\\2.0
Opens key: HKCR\\typelib\\{00020430-0000-0000-c000-000000000046}\\2.0\\0
Opens key: HKCR\\typelib\\{00020430-0000-0000-c000-000000000046}\\2.0\\0\\win32
Opens key: HKLM\\software\\microsoft\\windows nt\\currentversion\\image file execution
options\\rundll32.exe
Opens key: HKLM\\software\\microsoft\\windows nt\\currentversion\\appcompatflags\\custom\\rundll32.exe
Opens key: HKCU\\software\\microsoft\\internet explorer\\main\\featurecontrol\\feature_include_port_in_spn_kb908209
Opens key: HKLM\\software\\microsoft\\internet explorer\\main\\featurecontrol\\feature_include_port_in_spn_kb908209
Opens key: HKCU\\software\\microsoft\\internet explorer\\main\\featurecontrol\\feature_mime_handling
Opens key: HKLM\\software\\microsoft\\internet explorer\\main\\featurecontrol\\feature_mime_handling
Opens key: HKLM\\sam\\sam\\domains\\account\\groups\\000003ea
Opens key: HKLM\\sam\\sam\\domains\\account\\aliases\\000003ea
Opens key: HKLM\\sam\\sam\\domains\\account\\users\\000003ea
Opens key: HKLM\\system\\currentcontrolset\\services\\winsock2\\parameters
Opens key: HKLM\\system\\currentcontrolset\\services\\dnscache\\parameters
Opens key: HKLM\\software\\policies\\microsoft\\windows nt\\dnscclient
Opens key: HKLM\\system\\currentcontrolset\\services\\dns
Opens key: HKLM\\software\\policies\\microsoft\\system\\dnscclient
Opens key: HKLM\\system\\currentcontrolset\\services\\winsock\\setup
migration\\providers\\tcpip6
Opens key: HKCU\\software\\microsoft\\windows nt\\currentversion\\appcompatflags
Opens key: HKLM\\system\\currentcontrolset\\control\\cmf\\config
Opens key: HKLM\\system\\currentcontrolset\\control\\networkprovider\\hworder
Opens key: HKCU\\software\\microsoft\\windows\\currentversion\\internet settings\\wpad\\{7bf7ed91-f442-458a-abea-c661d1bd5efb}
Opens key: HKLM\\software\\microsoft\\rpc
Opens key: HKLM\\software\\policies\\microsoft\\windows nt\\rpc
Opens key: HKCU\\software\\microsoft\\windows\\currentversion\\internet settings\\5.0\\lowcache
Opens key: HKCU\\software\\microsoft\\windows\\currentversion\\internet settings\\5.0\\lowcache\\content
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\folderdescriptions
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\folderdescriptions\\{352481e8-33be-4251-ba85-6007caedcf9d}
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\folderdescriptions\\{352481e8-33be-4251-ba85-6007caedcf9d}\\propertybag
Opens key:
Opens key: HKCU\\software\\microsoft\\windows\\currentversion\\explorer
Opens key: HKLM\\software\\policies\\microsoft\\windows\\explorer
Opens key: HKCU\\software\\policies\\microsoft\\windows\\explorer
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\folderdescriptions\\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\folderdescriptions\\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\\propertybag
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\folderdescriptions\\{5e6c858f-0e22-4760-9afe-ea3317b67173}
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\folderdescriptions\\{5e6c858f-0e22-4760-9afe-ea3317b67173}\\propertybag
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\knownfoldersettings
Opens key: HKCU\\software\\microsoft\\windows\\currentversion\\internet settings\\5.0\\lowcache\\cookies
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\folderdescriptions\\{2b0f765d-c0e9-4171-908e-08a611b84ff6}
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\folderdescriptions\\{2b0f765d-c0e9-4171-908e-08a611b84ff6}\\propertybag
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\folderdescriptions\\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key:
HKLM\\software\\microsoft\\windows\\currentversion\\explorer\\folderdescriptions\\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\\propertybag
Opens key: HKCU\\software\\microsoft\\windows\\currentversion\\internet settings\\5.0\\lowcache\\history
Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld
Opens key: HKLM\system\currentcontrolset\services\netbt\linkage
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\307bda19-07de87e0
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\307bda19
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\000000019
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
Opens key: HKLM\software\microsoft\sqlclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqlclient\windows\disabledsessions\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\connections
Opens key:
HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{128919e8-8a5e-41d1-ac17-c19ce8a73253}
Opens key: HKLM\system\currentcontrolset\services\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\parameters\tcpip
Opens key: HKLM\system\currentcontrolset\services\netbt\adapters\{128919e8-8a5e-41d1-ac17-c19ce8a73253}
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnsolicyconfig
Opens key:
HKLM\system\currentcontrolset\services\dnsache\parameters\dnsolicyconfig
Opens key: HKCU\software\classes\applications\calc.exe
Opens key: HKCR\applications\calc.exe
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key: HKLM\software\policies\microsoft\internet explorer\security
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
Opens key:
HKLM\software\policies\microsoft\windows\networkconnectivitystatusindicator
Opens key: HKLM\system\currentcontrolset\services\olasvc\parameters\internet
Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\connections
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key: HKCU\software\microsoft\internet explorer\ietld
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history\microsoft.com
Opens key: HKLM\software\microsoft\ctf\knownclasses
Opens key: HKLM\software\policies\microsoft\windows nt\reliability
Opens key: HKLM\system\currentcontrolset\services\eventlog\system
Opens key: HKLM\software\microsoft\windows\currentversion\winevt\publishers
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0063715b-eeda-4007-9429-ad526f62696e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01090065-b467-4503-9b28-533766761087}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01578f96-c270-4602-ade0-578d9c29fc0c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{017247f2-7e96-11dc-8314-0800200c9a66}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{017ba13c-9a55-4f1f-8200-323055aac810}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01979c6a-42fa-414c-b8aa-eee2c8202018}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{02012a8a-adf5-4fab-92cb-ccb7bb3e689a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{030f2f57-abd0-4427-bcf1-3a3587d7dc7d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{04268430-d489-424d-b914-0cff741d6684}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{04d66358-c4a1-419b-8023-23b73902de2c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{05921578-2261-42c7-a0d3-26ddbce6c50d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{059c3e04-5535-4929-85e1-93030e78f47b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{05d7b0f0-2121-4eff-bf6b-ed3f69b894d7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06184c97-5201-480e-92af-3a3626c5b140}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06edcfcb-0fd0-4e53-acca-a6f8bbf81bcb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{07de7879-1c96-41ce-afbd-c659a0e8e643}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{08466062-aed4-4834-8b04-cddb414504e5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0888e5ef-9b98-4695-979d-e92ce4247224}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{093da50c-0bb9-4d7d-b95c-3bb9fcd5ee8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{09608c12-c1da-4104-a6fe-b959cf57560a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{099614a5-5dd7-4788-8bc9-e29f43db28fc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{09ec9687-d7ad-40ca-9c5e-78a04a5ae993}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0a88862d-20a3-4c1f-b76f-162c55adb93}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0bd3506a-9030-4f76-9b88-3e8fe1f7cfeb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0c478c5b-0351-41b1-8c58-4a6737da32e3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0d4fcd09-8c27-494a-bda0-505e4fd8adae}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0d759f0f-cff9-4902-8867-eb9e29d7a98b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0dd4d48e-2bbf-452f-a7ec-ba3dba8407ae}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0f177893-4a9c-4709-b921-f432d67f43d5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0f67e49f-fe51-4e9f-b490-6f2948cc6027}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11a377e3-be1e-4ee7-abda-81c6eda62e71}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11a75546-3234-465e-bec8-2d301cb501ac}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{122ee297-bb47-41ae-b265-1ca8d1886d40}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{127e0dc5-e13b-4935-985e-78fd508b1d80}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{13480a22-d79f-4334-9d32-aa239398ad3c}

Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{134ea407-755d-4a93-b8a6-f290cd155023}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{13b197bd-7cee-4b4e-8dd0-59314ce374ce}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1418ef04-b0b4-4623-bf7e-d74ab47bbdaa}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{155cb334-3d7f-4ff1-b107-df8afc3c0363}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{15a7a4f8-0072-4eab-abad-f98a4d666aed}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{15ca44ff-4d7a-4baa-bba5-0998955e531e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17d6e590-f5fe-11dc-95ff-0800200c9a66}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17e92e2a-3d08-413e-baeb-a79a262bf486}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17f14a23-551d-40cc-a086-e4194d64ed4c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{18f4a5fd-fd3b-40a5-8fc2-e5d261c5d02e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{192ede41-9175-4c86-ac02-9d003c9d43ab}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{199fe037-2b82-40a9-82ac-e1d46c792b99}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{19d2c934-ee9b-49e5-aaeb-9cce721d2c65}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a396961-5f3c-4c71-8310-44c653c0bf8a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a772f65-be1e-4fc6-96bb-248e03fa60f5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a9443d4-b099-44d6-8eb1-829b9c2fe290}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1b562e86-b7aa-4131-badc-b6f3a001407e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1b8b402d-78dc-46fb-bf71-46e64aedf165}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1be1a88d-8e34-4170-9123-f503375bbcef}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1c95126e-7eea-49a9-a3fe-a378b03ddb4d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1d75856d-36a7-4ecb-a3f5-b1315222d29}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1db28f2e-8f80-4027-8c5a-a11f7f10f62d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1edeee53-0afe-4609-b846-d8c0b2075b1f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1f678132-5938-4686-9fdc-c8ff68f15c85}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1f84007d-19ce-4b15-9e81-8a3dd8eb9ecb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{206f6dea-d3c5-4d10-bc72-989f03c8b84b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{21b7c16e-c5af-4a69-a74a-7245481c1b97}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{22b6d684-fa63-4578-87c9-efcbe6643c7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{22fb2cd6-0e7b-422b-a0c7-2fad1fd0e716}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{239cfb83-cbb7-4bbc-a02e-9bdb496aa7c2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{271c5228-c3fe-4e47-831f-48c3652ce5ac}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{272a979b-34b5-48ec-94f5-7225a59c85a0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{27a8c1e2-eb19-463e-8424-b399df27a216}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{28aa95bb-d444-4719-a36f-40462168127e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2992e9cf-4f99-48f5-a0b6-b99b11cd387d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{29d13147-1c2e-48ec-9994-e29dfe496eb3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2a274310-42d5-4019-b816-e4b8c7abe95c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2d318b91-e6e7-4c46-bd04-bfe6db412cf9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2e35aaeb-857f-4beb-a418-

2e6c0e54d988}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2ed6006e-4729-4609-b423-3ee7bcd678ef}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2f07e2ee-15db-40f1-90ef-9d7ba282188a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2fd7a9a5-b1a1-4fc7-b95c-c32fed818f30}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2ff3e6b7-cb90-4700-9621-443f389734ed}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{30336ed4-e327-447c-9de0-51b652c86108}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{314b2bd0-81ee-4474-b6e0-c2aaec0ddbde}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{314de49f-ce63-4779-ba2b-d616f6963a88}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{319122a9-1485-4e48-af35-7db2d93b8ad2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{31f60101-3703-48ea-8143-451f8de779d2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3239eb6f-c7fc-4953-aa15-646829a4ca4c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{331c3b3a-2005-44c2-ac5e-77220c37d6b4}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{355c44fe-0c8e-4bf8-be28-8bc7b5a42720}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{35ac6ce8-6104-411d-976c-877f183d2d32}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3663a992-84be-40ea-bba9-90c7ed544222}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{36c23e18-0e66-11d9-bbeb-505054503030}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{37945dc2-899b-44d1-b79c-dd4a9e57ff98}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3aa52b8b-6357-4c18-a92e-b53fb177853b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3c6c422b-019b-4f48-b67b-f79a3fa8b4ed}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cb2a168-fe19-4a4e-bdad-dcf422f13473}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cb40aaa-1145-4fb8-b27b-7e30f0454316}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cc2d4af-da5e-4ed4-bcbe-3cf995940483}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3df0c2c1-5a04-4966-9790-df6ef0ccde9c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3f7b2ff99-b863-4045-ad05-f6afb62e7af1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3f9e07bd-0e26-4241-a5a5-28cafa150a75}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{40ab57c2-1c53-4df9-9324-ff7cf898a02c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{40ae003c-6f3d-4590-ae1c-0e8be526b50f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4214dcd2-7c33-4f74-9898-719ccceec20f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{422088e6-cd0c-4f99-bd0b-6985fa290bdf}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{43d1a55c-76d6-4f7e-995c-64c711e5cafe}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{43e63da5-41d1-4fbf-aded-1bbcd98fdd1d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{46098845-8a94-442d-9095-366a6bcfe9a9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{49c2c27c-fe2d-40bf-8c4e-c3fb518037e7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4a933674-fb3d-4e8d-b01d-17ee14e91a3e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4b7eac67-fc53-448c-a49d-7cc6db524da7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ba32972-6fc5-488a-8368-5da620d05127}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4cb314df-c11f-47d7-9c04-65fb0051561b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4cec9c95-a65f-4591-b5c4-30100e51d870}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4edbe902-9ed3-4cf0-93e8-b8b5fa920299}
Opens key:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ef850d8-bf30-4e64-a917-ee21b9be1f0a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4f768be8-9c69-4bbc-87fc-95291d3f9d0c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4fba1227-f606-4e5f-b9e8-fab9ab5740f3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4fcbf664-a33a-4652-b436-9d558983d955}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{50b3e73c-9370-461d-bb9f-26f32d68887d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{50bd1bfd-936b-4db3-86be-e25b96c25898}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{51480c1a-90aa-416e-98fd-4c11f735349b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5322d61a-9efa-4bc3-a3f9-14be95c144f8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{538cbbad-4877-4eb2-b26e-7cae8f0f8cb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54164045-7c50-4905-963f-e5bc1eef0cca}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5444519f-2484-45a2-991e-953e4b54c8e0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{546549be-9d63-46aa-9154-4f6eb9526378}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54732ee5-61ca-4727-9da1-10be5a4f773d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54d5ac20-e14f-4fda-92da-ebf7556ff176}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54fffd262-99fe-4576-96e7-1adb500370dc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{57e0b31d-de8c-4181-bcd1-f70e880b49fc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5857d6ca-9732-4454-809b-2a87b70881f8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{588c5c5a-ffc5-44a2-9a7f-d5e8dbe6efd7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{588cd2e4-a5b0-492d-a59b-f6dd3e7681c6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5a24fcd8-1cf3-477b-b422-ef4909d51223}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b004607-1087-4f16-b10e-979685a8d131}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b0a651a-8807-45cc-9656-7579815b6af0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b93cdfa-5f51-45e0-9fde-296983129e6c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5bbca4a8-b209-48dc-a8c7-b23d3e5216fb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5c8bb950-959e-4309-8908-67961a1205d5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5c9be3e0-3593-4dcd-8f6d-63840923ffee}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d674230-ca9f-11da-a94d-0800200c9a66}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d896912-022d-40aa-a3a8-4fa5515c76d7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d9e0020-3761-4f36-90c8-38ce6511bd12}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5ec13d8e-4b3f-422e-a7e7-3121a1d90c7a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5f92bc59-248f-4111-86a9-e393e12c6139}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{606a6a38-70ec-4309-b3a3-82ff86f73329}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{614696c9-85af-4e64-b389-d2c0db4ff87b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{617853d6-728b-4b59-8a78-c3a9a5eade92}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{61f044af-9104-4ca5-81ee-cb6c51bb01ab}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63b530f8-29c9-4880-a5b4-b8179096e7b8}

Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63d1e632-95cc-4443-9312-af927761d52a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63d2bb1d-e39a-41b8-9a3d-52d06677588}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{651df93b-5053-4d1e-94c5-f6e6d25908d0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{65d341f3-baaa-4c6e-8b20-23d4f1574004}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{65d99466-7a8e-489c-b8e1-962bc945031e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6600e712-c3b6-44a2-8a48-935c511f28c8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{66a5c15c-4f8e-4044-bf6e-71d896038977}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{676f167f-f72c-446e-a498-eda43319a5e3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67bd1fef-afb2-458d-bcde-3758beb84dec}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67fe2216-727a-40cb-94b2-c02211edb34a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6863e644-dd5d-43a2-a8b5-7a81b46672e6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{699e309c-e782-4400-98c8-e21d162d7b7b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a1f2b00-6a90-4c38-95a5-5cab3b056778}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a2dc7c1-930a-4fb5-bb44-80b30aebd6c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a502821-ab44-40c8-b32f-37315d9d52e0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ad52b32-d609-4be9-ae07-ce8dae937e39}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6addabf4-8c54-4eab-bf4f-fbe6f1b62eb0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b1ffe48-5b1e-4793-9f7f-ae926454499d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b4db0bc-9a3d-467d-81b9-a84c6f2f3d40}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b93bf66-a922-4c11-a617-cf60d95c133d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ba132c4-da49-415b-a7f4-31870dc9fe25}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6c260f2c-049a-43d8-bf4d-d350a4e6611a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6d8a3a60-40af-445a-98ca-99359e500146}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6e400999-5b82-475f-b800-cef6fe361539}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6eb8db94-fe96-443f-a366-5fe0cee7fb1c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ece3302-fee1-4ea9-8b88-086d459ed976}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{70eb4f03-c1de-4f73-a051-33d13d5413bd}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{712abb2d-d806-4b42-9682-26da01d8b307}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{719be4ed-e9bc-4dd8-a7cf-c85ce8e4975d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7237fff9-a08a-4804-9c79-4a8704b70b87}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7288c9f8-d63c-4932-a345-89d6b060174d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{728b8c72-0f0f-4071-9bcc-27cb3b6dache}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{72d211e1-4c54-4a93-9520-4901681b2271}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{73370bd6-85e5-430b-b60a-fea1285808a7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{73e9c9de-a148-41f7-b1db-4da051fdc327}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{741fc222-44ed-4ba7-98e3-f405b2d2c4b4}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7426a56b-e2d5-4b30-bdef-b31815c1a74a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{747ef6fd-e535-4d16-b510-

42c90f6873a1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74b4a4b1-2302-4768-ac5b-9773dd456b08}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74b655a2-8958-410e-80e2-3457051b8dff}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74c2135f-cc76-45c3-879a-ef3bb1eeaf86}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0870-49e5-bdce-9d7028279489}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0936-4a55-9d26-5f298f3180bf}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0cc6-49da-8cd9-8903a5222aa0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-77b8-4ba8-9474-4f4a9db2f5c6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-8670-4eb6-b535-3b9d6bb222fd}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-997f-49cf-b49f-ecc50184b75d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-c8ae-4f93-9ca1-683a53e20cb6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-d017-4d0f-93ab-0b4f86579164}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75f48521-4131-4ac3-9887-65473224fcb2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{777ba8fe-2498-4875-933a-3067de883070}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{78168022-eca5-41e8-9e17-e8c7fd77aae1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7839bb2a-2ea3-4eca-a00f-b558ba678bec}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7a67066e-193f-4d3a-82d3-322fee5259de}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b563579-53c8-44e7-8236-0f87b9fe6594}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b6bc78c-898b-4170-bbf8-1a469ea43fc5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b7838a3-6562-4269-bb7a-97b0d9593882}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7bb5af18-cb16-4007-b813-9d88e9d6f8ef}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7bfcf102-7378-431c-9284-0b968258991a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7c314e58-8246-47d1-8f7a-4049dc543e0b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d29d58a-931a-40ac-8743-48c733045548}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d44233d-3055-4b9c-ba64-0d47ca40a232}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d5387b0-cbe0-11da-a94d-0800200c9a66}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d7b0c39-93f6-4100-bd96-4dda859652c5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7da4fe0e-fd42-4708-9aa5-89b77a224885}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7dd42a49-5329-4832-8dfd-43d979153a88}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7eafc7f9-06a7-460b-8a55-bd0a0c9248aa}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f2bd991-ae93-454a-b219-0bc23f02262a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f912b92-21ad-496e-b97a-88622a72bc42}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f9d83de-8abb-457f-98e8-4ad161449ecc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{802ec45a-1e99-4b83-9920-87c98277ba9d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8085cb91-900e-4d15-a7d1-921ddce641d8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8115579e-2bea-4c9e-9ab1-821cc2c98ab0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{820a42d8-38c4-465d-b64e-d7d56ea1d612}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{835b79e2-e76a-44c4-9885-26ad122d3b4d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8360bd0f-a7dc-4391-91a7-a457c5c381e4}
Opens key:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{83ed54f0-4d48-4e45-b16e-726ffd1fa4af}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{84051b98-f508-4e54-82fa-8865c697c3b1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8429e243-345b-47c1-8a91-2c94caf0daab}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8443ccb7-feb0-4b8d-8e28-8d4c7cb814e8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{85fe7609-ff4a-48e9-9d50-12918e43e1da}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{86133982-63d7-4741-928e-ef1349b80219}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{869fb599-80aa-485d-bca7-db18d72b7219}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{86efff39-2bdd-4efd-bd0b-853d71b2a9dc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{87d476fe-1a0f-4370-b785-60b028019693}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8939299f-2315-4c5c-9b91-abb86aa0627d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{899daace-4868-4295-afcd-9eb8fb497561}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89a2278b-c662-4aff-a06c-46ad3f220bca}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89b1e9f0-5aff-44a6-9b44-0a07a7ce5845}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8a93b54b-c75a-49b5-a5be-9060715b1a33}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8c63b5a5-b484-4381-892d-edd424582df7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8c9dd1ad-e6e5-4b07-b455-684a9d879900}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8ce93926-bdae-4409-9155-2fe4799ef4d3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{914ed502-b70d-4add-b758-95692854f8a3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{91f42016-0b4e-4a4b-9bbb-825d06cbcd35}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{91f5fb12-fdea-4095-85d5-614b495cd9de}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{92ae46d7-6d9c-4727-9ed5-e49af9c24cbf}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9363ccd9-d429-4452-9adb-2501e704b810}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{93c05d69-51a3-485e-877f-1806a8731346}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{945a8954-c147-4acd-923f-40c45405a658}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9485fa1e-23cd-49a1-84e3-11d8bc550cb7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{952773bf-c2b7-49bc-88f4-920744b82c43}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{95353826-4fbc-41d4-9c42-f521c6e86360}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{959f1fac-7ca8-4ed1-89dc-cdfa7e093cb0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{968f313b-097f-4e09-9cdd-bc62692d138b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{96ac7637-5950-4a30-b8f7-e07e8e5734c1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{96f4a050-7e31-453c-88be-9634f4e02139}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{973143dd-f3c7-4ef5-b156-544ac38c39b6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98583af0-fc93-4e71-96d5-9f8da716c6b8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98bf1cd3-583e-4926-95ee-a61bf3f46470}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98e6cfcb-ee0a-41e0-a57b-622d4e1b30b1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{99806515-9f51-4c2f-b918-1eae407aa8cb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9988748e-c2e8-4054-85f6-0c3e1cad2470}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9b307223-4e4d-4bf5-9be8-995cd8e7420b}

Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9b6123dc-9af6-4430-80d7-7d36f054fb9f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9c205a39-1250-487d-abd7-e831c6290539}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9d55b53d-449b-4824-a637-24f9d69aa02f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9db0fdb5-3b21-440e-a94b-63738a4be5de}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e03f75a-bcbe-428a-8f3c-d46f2a444935}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e3b3947-ca5d-4614-91a2-7b624e0e7244}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e6ae157-d9f7-47e5-8c6d-b17bb6c82a27}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e95e4d0-4cb4-4b5d-a936-c972d7d08d90}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9f0c4ea8-ec01-4200-a00d-b9701cbea5d8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9f650c63-9409-453c-a652-83d7185a2e83}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a0c1853b-5c40-4b15-8766-3cf1c58f985a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a0e3d8ea-c34f-4419-a1db-90435b8b21d0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a319d300-015c-48be-acdb-47746e154751}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a3e1697b-a12c-46b9-84d1-7ffe73c4b678}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a402fe09-da6e-45f2-82af-3cb37170ee0c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a50b09f8-93eb-4396-84c9-dc921259f952}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a615acb9-d5a4-4738-b561-1df301d207f8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a68ca8b7-004f-d7b6-a698-07e2de0f1f5d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a6ad76e3-867a-4635-91b3-4904ba6374d7}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a6f32731-9a38-4159-a220-3d9b7fc5fe5d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a7364e1a-894f-4b3d-a930-2ed9c8c4c811}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a7975c8f-ac13-49f1-87da-5a984a4ab417}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a8106e5c-293a-4cd0-9397-2e6fac7f9749}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a82fda5d-745f-409c-b0fe-18ae0678a0e0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a8a1f2f6-a13a-45e9-b1fe-3419569e5ef2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a97524f6-064c-4c4e-b74b-1acc87c3700d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aabf8b86-7936-4fa2-acb0-63127f879dbf}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aaf44901-5c64-4014-8b6c-a80813937293}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ab0d8ef9-866d-4d39-b83f-453f3b8f6325}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{abce23e7-de45-4366-8631-84fa6c525952}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ac43300d-5fcc-4800-8e99-1bd3f85f0320}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ad5162d8-daf0-4a25-88a7-01cbeb33902e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ad8aa069-a01b-40a0-ba40-948d1d8dedc5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ae4bd3be-f36f-45b6-8d21-bdd6fb832853}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aea1b4fa-97d1-45f2-a64c-4d69fffd92c9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af0a5a6d-e009-46d4-8867-42f2240f8a72}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af2e340c-0743-4f5a-b2d3-2f7225d215de}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af9cc194-e9a8-42bd-b0d1-834e9cfab799}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b03d4051-3564-4e93-93db-

3c34f1b5b503}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b059b83f-d946-4b13-87ca-4292839dc2f2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1bebb9a-24aa-4b83-9e4a-38c2a9a44377}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1c94ed9-ac9b-410e-aa48-4ffc5e45f4e3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1f90b27-4551-49d6-b2bd-dfc6453762a6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b240f1f-a05a-4dfd-886a-4c4f18c4334c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b3eee223-d0a9-40cd-adfc-50f1888138ab}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b44aec44-38f4-4b59-8df3-10306abf19b2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b5fd844a-01d4-4b10-a57f-58b13b561582}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b65471e1-019d-436f-bc38-e15fa8e87f53}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b675ec37-bdb6-4648-bc92-f3fdc74d3ca2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b92cf7fd-dc10-4c6b-a72d-1613bf25e597}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b977cf02-76f6-df84-cc1a-6a4b232322b6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b98f0db6-26e2-4a66-89fc-32a9a6a9af61}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b9da9fe6-ae5f-4f3e-b2fa-8e623c11dc75}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ba093605-3909-4345-990b-26b746adee0a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bbe94f36-f8dc-4c33-8227-81602b7a3d53}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bc2eeec-b77a-4a52-b6a4-dffb1b1370cb}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bc97b970-d001-482f-8745-b8d7d5759f99}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd12f3b8-fc40-4a61-a307-b7a013a069c1}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd2d1dae-d678-4e10-9667-21cba2aa70c3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd2f4252-5e1e-49fc-9a30-f3978ad89ee2}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bdb462fc-a297-49a2-bf2e-4f1809e12abc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{be69781c-b63b-41a1-8e24-a4fc7b3fc498}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{be932b00-0f8e-4386-ab89-873f7d0274aa}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bf406804-6afa-46e7-8a48-6c357e1d6d61}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c02afc2b-e24e-4449-ad76-bcc2c2575ead}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c06ed57a-a7bd-42d7-b5ff-77a9dec5732d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c100becc-d33a-4a4b-bf23-bbef4663d017}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c100becf-d33a-4a4b-bf23-bbef4663d017}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c26c4f3c-3f66-4e99-8f8a-39405cfed220}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c2fa0899-8a10-412b-a42e-9e5b284a2437}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c4636a1e-7986-4646-bf10-7bc3b4a76e8e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c514638f-7723-485b-bcfc-96565d735d4a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c6bf6832-f7bd-4151-ac21-753ce4707453}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c76baa63-ae81-421c-b425-340b4b24157f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c7bde69a-e1e0-4177-b6ef-283ad1525271}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c882ff1d-7585-4b33-b135-95c577179137}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c88a4ef5-d048-4013-9408-e04b7db2814a}
Opens key:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c89b991e-3b48-49b2-80d3-ac000dfc9749}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c8f7689f-3692-4d66-b0c0-9536d21082c9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c914f0df-835a-4a22-8c70-732c9a80c634}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c91ef675-842f-4fcf-a5c9-6ea93f2e4f8b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c9bdb4eb-9287-4c8e-8378-6896f0d1c5ef}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ca4e628d-8567-4896-ab6b-835b221f373f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ca5ba219-c0d4-4efa-9ceb-72aff92672b0}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cab2b8a5-49b9-4eec-b1b0-fac21da05a3b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cad2d809-03d9-4f46-9cf4-72aa4f04b6b9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cb070027-1534-4cf3-98ea-b9751f508376}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cb587ad1-cc35-4ef1-ad93-36cc82a2d319}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cbda4dbf-8d5d-4f69-9578-be14aa540d22}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cd032e15-15ad-4da4-afc6-03bf83516195}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cdc05e28-c449-49c6-b9d2-88cf761644df}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cdead503-17f5-4a3e-b7ae-df8cc2902eb9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ce20d1c3-a247-4c41-bcb8-3c7f52c8b805}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ce8dee0b-d539-4000-b0f8-77bed049c590}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cf3f502e-b40d-4071-996f-00981edf938e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfaa5446-c6c4-4f5c-866f-31c9b55b962d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622caee05b0a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d02a9c27-79b8-40d6-9b97-cf3f8b7b5d60}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d1bc9aff-2abf-4d71-9146-ecb2a986eb85}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d1d93ef7-e1f2-4f45-9943-03d245fe6c00}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d4263c98-310c-4d97-ba39-b55354f08584}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d53270e3-c8cf-4707-958a-dad20c90073c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d5c25f9a-4d47-493e-9184-40dd397a004d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d6f68875-cdf5-43a5-a3e3-53ffd683311c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d8975f88-7ddb-4ed0-91bf-3adf48c48e0c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dab065a9-620f-45ba-b5d6-d6bb8efedee9}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dab3b18c-3c0f-43e8-80b1-e44bc0dad901}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{db00dfb6-29f9-4a9c-9b3b-1f4f9e7d9770}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dbe9b383-7cf3-4331-91cc-a3cb16a3b538}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d5ef90a-6398-47a4-ad34-4dcecdf795f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dd70bc80-ef44-421b-8ac3-cd31da613a4e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dd85457f-4e2d-44a5-a7a7-6253362e34dc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{de513a55-c345-438b-9a74-e18cac5c5cc5}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dea07764-0790-44de-b9c4-49677b17174f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ded165cf-485d-4770-a3e7-9c5f0320e80c}

Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{df32a572-0b4b-44be-b09b-72084fdbf879}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e01b1a7c-c5c9-4e67-99a9-5e85acfb2e10}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e04fe2e0-c6cf-4273-b59d-5c97c9c374a4}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e0a40b26-30c4-4656-bc9a-74a5c3a0b2ec}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e104fb41-6b04-4f3a-b47d-f0df2f02b954}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e1dd7e52-621d-44e3-a1ad-0370c2b25946}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfa0f156}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e2816346-87f4-4f85-95c3-0c79409aa89d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e4480490-85b6-11dd-ad8b-0800200c9a66}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e46eead8-0c54-4489-9898-8fa79d059e0e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e4d53f84-7de3-11d8-9435-505054503030}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e53c6823-7bb8-44bb-90dc-3f86090d48a6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e595f735-b42a-494b-afcd-b68666945cd3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e5ba83f6-07d0-46b1-8bc7-7e669a1d31dc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e6307a09-292c-497e-aad6-498f68e2b619}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e670a5a2-ce74-4ab4-9347-61b815319f4c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e7558269-3fa5-46ed-9f4d-3c6e282dde55}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e7ef96be-969f-414f-97d7-3ddb7b558ccc}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e8316a2d-0d94-4f52-85dd-1e15b66c5891}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e837619c-a2a8-4689-833f-47b48ebd2442}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e856c26a-e105-4683-a948-6920dcc42e45}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e978f84e-582d-4167-977e-32af52706888}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eb3deb18-d1de-4897-8502-a230ad03db8a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ed6b3ba8-95b2-4cf5-a317-d4af7003884c}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{edd08927-9cc4-4e65-b970-c2560fb5c289}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ee4f43b5-03eb-41d2-a28c-ba8bee529247}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ef1cc15b-46c1-414e-bb95-e76b077bd51e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f0db7ef8-b6f3-4005-9937-feb77b9e1b43}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f230d19a-5d93-47d9-a83f-53829edfb8df}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f2c628ae-d26c-4352-9c45-74754e1e2f9f}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f3c5e28e-63f6-49c7-a204-e48a1bc4b09d}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f3f14ff3-7b80-4868-91d0-d77e497b025e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f404b94e-27e0-4384-bfe8-1d8d390b0aa3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f4aed7c7-a898-4627-b053-44a7caa12fcd}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f5344219-87a4-4399-b14a-e59cd118abb8}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f557ace2-bcf8-4994-8e4b-42368a6f078a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f5d05b38-80a6-4653-825d-c414e4ab3c68}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f61cefc0-aa2e-11da-a746-

0800200c9a66}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f6da35ce-d312-41c8-9828-5a2e173c91b6}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f82fb576-e941-4956-a2c7-a0cf83f6450a}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f997cd11-0fc9-4ab4-acba-bc742a4c0dd3}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fbcfac3f-8459-419f-8e48-1f0b49cdb85e}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc3bc8a7-2f61-449c-a8b4-22ac22058f92}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc65ddd8-d6ef-4962-83d5-6e5cfe9ce148}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc6f77dd-769a-470e-bcf9-1b6555a118be}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fd771d53-8492-4057-8e35-8c02813af49b}
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ffdb9886-80f3-4540-aa8b-b85192217ddf}
Opens key: HKLM\system\currentcontrolset\services\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\application\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\hardwareevents\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\internet
explorer\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\key management
service\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\media center\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\security\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\system\eventlog
Opens key: HKLM\software\policies\microsoft\netlogon\parameters
Opens key: HKLM\system\currentcontrolset\services\netlogon\parameters
Opens key: HKLM\system\currentcontrolset\services\fileinfo\instances
Opens key: HKLM\system\currentcontrolset\services\fileinfo\instances\fileinfo
Opens key: HKLM\system\currentcontrolset\services\luaflv\instances
Opens key: HKLM\system\currentcontrolset\services\luaflv\instances\luaflv
Opens key: HKLM\system\currentcontrolset\services\lsm\instances
Opens key: HKLM\system\currentcontrolset\control\minint
Opens key: HKLM\system\currentcontrolset\control\timezoneinformation
Opens key: HKLM\software\policies\microsoft\windows\reliability analysis\wmi
Opens key: HKLM\software\microsoft\reliability analysis\wmi
Opens key: HKLM\software\policies\microsoft\windows\ipsec\gptipsecpolicy
Opens key: HKLM\software\policies\microsoft\windows\ipsec\policy\local
Opens key: HKLM\software\microsoft\windows\currentversion\winevt
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
readyboost\operational
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-
readyboost\operational
Opens key: HKLM\system\currentcontrolset\services\eventlog\microsoft-windows-
readyboost\analytic
Opens key:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-
readyboost\analytic
Opens key: HKLM\system\currentcontrolset\control\wmi\security
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\linkage
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006\linkage
Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKCU\control panel\desktop\preferreduilanguages
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside\preferexternalmanifest
Queries value: HKLM\system\currentcontrolset\control\lsl\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup\systemsetupinprogress
Queries value: HKLM\system\currentcontrolset\control\lsl\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\lsl\extendedlocale[en-us]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\layers[c:\winddfileq\83a494219a6.exe]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\hardware\devicemap\video[maxobjectnumber]
Queries value: HKLM\hardware\devicemap\video[\device\video3]
Queries value: HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-fd27e3774e32}\0000[pruningmode]
Queries value: HKLM\hardware\devicemap\video[\device\video0]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[pruningmode]
Queries value: HKLM\hardware\devicemap\video[\device\video1]
Queries value: HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-0d8e74595f78}\0000[pruningmode]
Queries value: HKLM\hardware\devicemap\video[\device\video2]
Queries value: HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-8ed0c8eb59a8}\0000[pruningmode]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[83a494219a6]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheapisprivate]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
Queries value: HKLM\software\microsoft\internet explorer[version]

Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[user
agent]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[explorer.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-
a3fe-553973d0b723]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce4]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasiccoverclearchannel]
Queries value: HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

```
folders[history]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
  Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[lsass]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheopath]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[spyeye_inj_ector_]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheopath]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheopath]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
  Queries value: HKCU\appevents\schemes[]
  Queries value: HKCU\appevents\schemes\apps\default\open\current[]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheopath]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheopath]
  Queries value: HKCU\appevents\schemes\apps\default\open\current[default flags]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie[cachelimit]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie[cacheoptions]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcservername]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbscapiforcrack]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernames]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmprauth]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
```

```
settings[scavengecachelowerbound]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[explorer.exe]
  Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttptnocachecheck]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttptnocachecheck]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocheck]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocheck]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[mineexclusionlistforcache]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrevving]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[tcpautotuning]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\wpadoverride]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
  Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disablebranchcache]
  Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[explorer.exe]
  Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
  Queries value: HKLM\system\currentcontrolset\services\crypt32[diaglevel]
  Queries value: HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
  Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002[profileimagepath]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[searchlist]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registeradapternam]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
```

```
c19ce8a73253}{dhcpdomain}
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}{dhcpv6domain}
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}{nameserver}
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}{nameserver}
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}{dhcpnameserver}
  Queries value: HKCU\appevents\schemes\apps\default\close\current[]
  Queries value: HKCU\appevents\schemes\apps\default\close\current[default flags]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\appcompat\flags\compatibility assistant[logignoremonitorreason]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}{enabledhcp}
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}{registrationenabled}
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}{registeradaptername}
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}{domain}
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}{dhcpdomain}
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}{nameserver}
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}{dhcpnameserver}
  Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:
HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000[phantom]
  Queries value: HKLM\system\currentcontrolset\enum\root\ms_agilevpnminiport\0000[driver]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001[componentid]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi\interfaces[upprange]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi\interfaces[lowerrange]
  Queries value: HKLM\system\currentcontrolset\enum\root\*isatap\0000[phantom]
  Queries value: HKLM\system\currentcontrolset\enum\root\*isatap\0000[driver]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009[componentid]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009\ndi\interfaces[upprange]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009\ndi\interfaces[lowerrange]
  Queries value: HKLM\system\currentcontrolset\enum\root\ms_12tpminiport\0000[phantom]
  Queries value: HKLM\system\currentcontrolset\enum\root\ms_12tpminiport\0000[driver]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002[componentid]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002\ndi\interfaces[upprange]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002\ndi\interfaces[lowerrange]
  Queries value: HKLM\system\currentcontrolset\enum\root\*teredo\0000[phantom]
  Queries value: HKLM\system\currentcontrolset\enum\root\*teredo\0000[driver]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011[componentid]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\ndi\interfaces[upprange]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011\ndi\interfaces[lowerrange]
  Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000[phantom]
  Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000[driver]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[componentid]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\ndi\interfaces[upprange]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\ndi\interfaces[lowerrange]
  Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[phantom]
  Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[driver]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[componentid]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi\interfaces[upprange]
  Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[capabilities]
  Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&0&18[configflags]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[netcfginstanceid]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[characteristics]
  Queries value: HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[mediasubtype]
  Queries value: HKLM\system\currentcontrolset\control\network[config]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi\clsid]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi[service]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi[coservices]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi[bindform]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi[helptext]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi[filterclass]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi[filtertype]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\ndi[timestamp]
  Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
```

08002be10318}\0007\ndi\filterruntime]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi\interfaces\lowerrange]
08002be10318}\0007\ndi\interfaces\lowerrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi\interfaces\lowerexclude]
08002be10318}\0007\ndi\interfaces\lowerexclude]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0007\ndi\interfaces\filtermediatypes]
08002be10318}\0007\ndi\interfaces\filtermediatypes]
Queries value: HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a0&18[friendlyname]
08002be10318}\0007\ndi\interfaces\lowerrange]
Queries value: HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a0&18[devicedesc]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\software\microsoft\network\media\mediamanager]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5f31090b-d990-4e91-b16d-46121d0255aa]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5b23f342-8421-42ef-87eb-3b686f5a1b2a]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[253f4cd1-9475-4642-88e0-6790d7a86cde]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[7076bf7a-db99-4a63-8afe-0bb2ab92997a]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[ab0d8ef9-866d-4d39-b83f-453f3b8f6325]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[phantom]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[driver]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008[componentid]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi\interfaces\upperrange]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0008\ndi\interfaces\lowerrange]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip6\0000[phantom]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip6\0000[driver]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005[componentid]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005\ndi\interfaces\upperrange]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0005\ndi\interfaces\lowerrange]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pppoeiniport\0000[phantom]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pppoeiniport\0000[driver]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004[componentid]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004\ndi\interfaces\upperrange]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004\ndi\interfaces\lowerrange]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[phantom]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[driver]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003[componentid]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003\ndi\interfaces\upperrange]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003\ndi\interfaces\lowerrange]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000[phantom]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_sstpminiport\0000[driver]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000[componentid]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000\ndi\interfaces\upperrange]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000\ndi\interfaces\lowerrange]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKU\S-1-5-21-2160590473-689474908-1361669368-1002\software\microsoft\windows\currentversion\explorer\user_shell_folders[appdata]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKU\S-1-5-21-2160590473-689474908-1361669368-1002\control
panel\international[localename]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKU\S-1-5-21-2160590473-689474908-1361669368-1002\software\microsoft\ras
autodial\default[defaultinternet]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\software\microsoft\ras_autodial\default[defaultinternet]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\networklist\profiles\{7bf7ed91-f442-458a-abea-c661d1bd5efb}[category]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\networklist\profiles\{7bf7ed91-f442-458a-abea-c661d1bd5efb}[profilename]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32[]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32[loadwithoutcom]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}[sortorderindex]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[sortorderindex]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[b725f130-47ef-101a-a5f1-02608c9eebac] 10]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKCU\software\classes\local
settings\mui\cache\27\52c64b7e[@:\windows\system32\prnfltr.dll,-8036]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[system.itemnamedisplay]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[b725f130-47ef-101a-a5f1-02608c9eebac] 10]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKCU\software\classes\local
settings\mui\cache\27\52c64b7e[@:\windows\system32\netshell.dll,-1200]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\superfetch[migrateddata]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\emdmgmt[grouppolicydisallowcaches]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\superfetch\diskassessment[volumeserialnumber]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\software\microsoft\windows\currentversion\optimallayout[enableautolayout]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[default1]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#(9f129fb0-41e7-11e5-935f-806e6f6e963)#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\#\control[linked]
08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[name]
Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#(9f129fb0-41e7-11e5-935f-806e6f6e963)#000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\#\symboliclink]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{9f129fb0-41e7-11e5-935f-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\#\control[linked]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{9f129fb0-41e7-11e5-935f-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\#[symboliclink]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{9f129fb0-41e7-11e5-935f-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#storage#volume#{9f129fb0-41e7-11e5-935f-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]

Queries value: HKLM\system\currentcontrolset\services\rdyboost\attachstate[pv-4--]

Queries value: HKLM\system\currentcontrolset\services\rdyboost\attachstate[pv-v--]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\superfetch[processortime]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\superfetch[rebalancerflags]

Queries value: HKLM\software\microsoft\windows nt\currentversion\superfetch[pfpddata]

Queries value: HKLM\software\microsoft\windows nt\currentversion\ncache[testflags]

Queries value: HKLM\software\microsoft\windows nt\currentversion\ncache[serviceflags]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}[default]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?

#ide#diskhitachi_____3.5.1.9_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#\control[linked]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?

#ide#diskhitachi_____3.5.1.9_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\#[symboliclink]

Queries value: HKLM\system\currentcontrolset\control\deviceclasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?

#ide#diskhitachi_____3.5.1.9_#5&394c0ad3&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}[deviceinstance]

Queries value: HKLM\software\microsoft\rpc\securityservice[10]

Queries value:

HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignedll]

Queries value:

HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureoutline]

Queries value:

HKLM\system\currentcontrolset\control\securityproviders[securityproviders]

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]

Queries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]

Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]

HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]

Queries value: HKLM\software\microsoft\tracing[enableconsoletracing]

Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[enablefiletracing]

Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[filetracingmask]

Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[enableconsoletracing]

Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[consoletracingmask]

Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[maxfilesize]

Queries value: HKLM\software\microsoft\tracing\explorer_rasapi32[filedirectory]

Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[enablefiletracing]

Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[filetracingmask]

Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[enableconsoletracing]

Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[consoletracingmask]

Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[maxfilesize]

Queries value: HKLM\software\microsoft\tracing\explorer_rasmancs[filedirectory]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[appdata]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet

settings[proxysettingsperuser]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[migrateproxy]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyenable]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyserver]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyoverride]

Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}[]

Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[autoconfigurl]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\connections[savedlegacysettings]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\connections[defaultconnectionsettings]

Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[autoconfigcustomua]

Queries value: HKCR\autoproxytypes\application/x-internet-signup[dllfile]

Queries value: HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[threadingmodel]

Queries value: HKCR\autoproxytypes\application/x-internet-signup[fileextensions]

Queries value: HKCR\autoproxytypes\application/x-internet-signup[default]

Queries value: HKCR\autoproxytypes\application/x-internet-signup[flags]

Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}[eventclassname]

Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[dllfile]

Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[fileextensions]

Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[default]

Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[flags]

Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}[ownersid]

Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}[firinginterfacedid]

Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}[customconfigclsid]

Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}[description]

Queries value: HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-000000000000}[typeib]

Queries value: HKLM\software\microsoft\eventssystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-\{00000000-0000-0000-0000-000000000000}\{00000000-0000-0000-0000-000000000000}[publisherid]

Queries value: HKLM\software\microsoft\eventssystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-\{00000000-0000-0000-0000-0000-0000-0000-000000000000}[multiinterfacepublisherfilterclsid]

Queries value: HKLM\software\microsoft\eventssystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-\{00000000-0000-0000-0000-0000-0000-0000-000000000000}[allowinprocactivation]

Queries value: HKLM\software\microsoft\eventssystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-\{00000000-0000-0000-0000-0000-0000-0000-000000000000}[fireinparallel]

Queries value: HKLM\software\microsoft\eventssystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-\{00000000-0000-0000-0000-0000-0000-0000-000000000000}[eventclasspartitionid]

Queries value: HKLM\software\microsoft\eventssystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-\{00000000-0000-0000-0000-0000-0000-0000-000000000000}[eventclassapplicationid]

Queries value: HKLM\software\microsoft\eventssystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-\{00000000-0000-0000-0000-0000-0000-0000-000000000000}[parallelfiringtimeout]

Queries value: HKLM\software\microsoft\eventssystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-\{00000000-0000-0000-0000-0000-0000-0000-000000000000}[allowloweruserinprocactivation]

Queries value: HKLM\software\microsoft\eventssystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-\{00000000-0000-0000-0000-0000-0000-0000-000000000000}[allowperuseractivateasactivator]

Queries value: HKLM\software\microsoft\eventssystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-\{00000000-0000-0000-0000-0000-0000-0000-000000000000}[allowlowerusermoniker]

Queries value: HKLM\software\microsoft\eventssystem\{26c409cc-ae86-11d1-b616-00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-\{00000000-0000-0000-0000-0000-0000-0000-000000000000}[serialfiringtimeout]

Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[]

Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[version]

Queries value: HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0\win32[]

Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\interfacehelperdisabletypelib

Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\interfacehelperdisableall

Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\interfacehelperperuser

Queries value: HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[explorer.exe]

Queries value: HKLM\sam\sam\domains\account\users\000003ea[v]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodiald11]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[queryadaptername]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[usedomainnamedevolution]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[domainnamedevolutionlevel]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[prioritizerecorddata]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[allowunqualifiedquery]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[appendtomultilabelname]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[screenbadtlids]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[screenunreachableservers]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[screndefaultservers]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[dynamicserverqueryorder]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[filterclusterip]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[waitfornameerroronall]

Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usedns]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[dnssecurenamequeryfallback]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[enabledforallnetworks]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[directaccessqueryorder]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[queryipmatching]

Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usehostsfile]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[addrconfigcontrol]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationenabled]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registerprimaryname]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registeradaptername]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registerreverselookup]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registerwanadapters]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]

Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationttl]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]

Queries value:

```
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddresstoregister]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[updatesecuritylevel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[updateopleveldomainzones]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[downcasespncauseapiowneristoolazy]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationoverwrite]
  Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachesize]
  Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[maxnegativecachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[adaptertimeoutlimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[serverprioritytimelimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachedsockets]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[enablemulticast]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastresponderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsenderflags]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsendermaxtimeout]
  Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[dnstest]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[usecompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[cacheallcompartments]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[usenewregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistrationonly]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6\winsock 2.0 provider id]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[maxnumberofaddresstoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[enablemulticast]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enableadapterdomainnameregistration]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[maxnumberofaddresstoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enablemulticast]
  Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[rundll32]
  Queries value: HKLM\system\currentcontrolset\control\cmf\config\system]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\wpadlastnetwork]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[autoproxydetecttype]
  Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache[signature]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
```


[illegible]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\content[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\content[cache limit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\cookies[peruseritem]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable]
Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[initfolderhandler]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsingsname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\cookies[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\cookies[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\history[peruseritem]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parsingsname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresource]

Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[localdirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\history[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\history[cacheLimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cacheRepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cachePath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cachePrefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cacheLimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cacheOptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cacheRepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cachePath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cachePrefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cacheLimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cacheOptions]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cacheRepair]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cachePath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cachePrefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cacheLimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cacheOptions]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[1540ff4c-3fd7-4bba-9938-1dbf31573a7]
Queries value: HKLM\system\currentcontrolset\services\netbt\linkage[export]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[rundll32.exe]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]

[illegible]

Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value: HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp[collection]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultttl]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableipsourcerouting]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[arpretrycount]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[igmpvlevel]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[igmpversion]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableicmredirect]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableaddrmaskreply]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabletaskoffload]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enablebcstarpreply]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledhcpmediasense]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablemediasenseeventlog]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enablemulticastforwarding]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enablepmtudiscovery]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[tcpuserfc1122urgentpointer]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[tcpmaxdatatransmissions]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[keepalivetime]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[keepaliveinterval]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[tcpimedwaitdelay]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[tcpfinwait2delay]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enablepmtubhddetect]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[tcp1323opts]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enabletcpsa]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableedca]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[minimumpacketsizetodma]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableconnectionratelimiting]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enablewsd]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[qualifyingdestinationthreshold]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationenabled]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationsubnet]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[ipautoconfigurationmask]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[ipenablerouter]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[arpuseethersnap]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[overridedefaultaddressselection]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxuserport]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[ipaddress]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[subnetmask]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[ipautoconfigurationaddress]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[ipautoconfigurationenabled]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[performrouterdiscovery]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[defaultgateway]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[defaultgatewaymetric]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[solicitationaddressbcst]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[usezerobroadcast]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[typeofinterface]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[mtu]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[interfacemetric]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[tcpackfrequency]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[tcpdelackticks]
Queries value: HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[explorer.exe]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2101]
Queries value: HKLM\software\policies\microsoft\windows\networkconnectivitystatusindicator[noactiveprobe]
Queries value: HKLM\system\currentcontrolset\services\nlasvc\parameters\internet[activewebprobehost]
Queries value:

HKLM\system\currentcontrolset\services\nlasvc\parameters\internet[activexwebprobeopath]
Queries value:
HKLM\system\currentcontrolset\services\nlasvc\parameters\internet[activexwebprobecontent]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\connections[winhttpsettings]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{q6523100-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
Queries value:
HKLM\software\microsoft\windows\currentversion\reliability[timestampinterval]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[type]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[filemax]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[filecounter]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[buffer size]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[minbuffers]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[maxbuffers]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[latency]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[clocktype]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[level]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[controlguid]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[maxsize]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[maxsizeupper]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[retention]
Queries value:
HKLM\system\currentcontrolset\services\eventlog\system[autobackuplogfiles]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[file]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[flags]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[filterid]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[owningpublisher]
Queries value: HKLM\system\currentcontrolset\services\eventlog\system[customsd]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0063715b-eeda-4007-9429-
ad526f62696e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01090065-b467-4503-9b28-
533766761087}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01578f96-c270-4602-ade0-
578d9c29fc0c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{017247f2-7e96-11dc-8314-
0800200c9a66}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{017ba13c-9a55-4f1f-8200-
323055aac810}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{01979c6a-42fa-414c-b8aa-
eee2c8202018}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{02012a8a-adf5-4fab-92cb-
ccb7bb3e689a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{030f2f57-abd0-4427-bcf1-
3a3587d7dc7d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{04268430-d489-424d-b914-
0cff741d6684}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{04d66358-c4a1-419b-8023-
23b73902de2c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{05921578-2261-42c7-a0d3-
26ddbc6c50d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{059c3e04-5535-4929-85e1-
93030e78f47b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{05d7b0f0-2121-4eff-bf6b-
ed3f69b894d7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06184c97-5201-480e-92af-
3a3626c5b140}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{06edcfcb-0fd0-4e53-acca-
a6f8bbf81bcb}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{07de7879-1c96-41ce-afbd-
c659a0e8e643}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{08466062-aed4-4834-8b04-
cddb414504e5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0888e5ef-9b98-4695-979d-
e92ce4247224}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{093da50c-0bb9-4d7d-b95c-
3bb9fcd5ee8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{09608c12-c1da-4104-a6fe-
b959cf57560a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{099614a5-5dd7-4788-8bc9-
e29f43db28fc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{09ec9687-d7ad-40ca-9c5e-
78a04a5ae993}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0a88862d-20a3-4c1f-b76f-
162c55adb9f3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0bd3506a-9030-4f76-9b88-
3e8fe1f7c7fb6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0c478c5b-0351-41b1-8c58-
4a6737da32e3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0d4fd0c9-8c27-494a-bda0-
505e4fd8adae}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0d759f0f-cff9-4902-8867-eb9e29d7a98b}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0dd4d48e-2bbf-452f-a7ec-ba3dba8407ae}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0f177893-4a9c-4709-b921-f432d67f43d5}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{0f67e49f-fe51-4e9f-b490-6f2948cc6027}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11a377e3-be1e-4ee7-abda-81c6eda62e71}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11a75546-3234-465e-bec8-2d301cb501ac}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{122ee297-bb47-41ae-b265-1ca8d1886d40}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{127e0dc5-e13b-4935-985e-78fd508b1d80}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{13480a22-d79f-4334-9d32-aa239398ad3c}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{134ea407-755d-4a93-b8a6-f290cd155023}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{13b197bd-7cee-4b4e-8dd0-59314ce374ce}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1418ef04-b0b4-4623-bf7e-d74ab47bbdaa}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{155cb334-3d7f-4ff1-b107-df8afc3c0363}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{15a7a4f8-0072-4eab-abad-f98a4d666aed}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{15ca44ff-4d7a-4baa-bba5-0998955e531e}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17d6e590-f5fe-11dc-95ff-0800200c9a66}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17e92e2a-3d08-413e-baeb-a79a262bf486}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{17f14a23-551d-40cc-a086-e4194d64ed4c}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{18f4a5fd-fd3b-40a5-8fc2-e5d261c5d02e}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{192ede41-9175-4c86-ac02-9d003c9d43ab}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{199fe037-2b82-40a9-82ac-e1d46c792b99}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{19d2c934-ee9b-49e5-aaeb-9cce721d2c65}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a396961-5f3c-4c71-8310-44c653c0bf8a}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a772f65-be1e-4fc6-96bb-248e03fa60f5}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1a9443d4-b099-44d6-8eb1-829b9c2fe290}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1b562e86-b7aa-4131-badc-b6f3a001407e}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1b8b402d-78dc-46fb-bf71-46e64aedf165}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1be1a88d-8e34-4170-9123-f503375bbcef}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1c95126e-7eea-49a9-a3fe-a378b03ddb4d}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1d75856d-36a7-4ecb-a3f5-b1315222d29}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1db28f2e-8f80-4027-8c5a-a11f7f10f62d}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1edee53-0afe-4609-b846-d8c0b2075b1f}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1f678132-5938-4686-9fdc-c8ff68f15c85}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{1f84007d-19ce-4b15-9e81-8a3dd8eb9ecb}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{206f6dea-d3c5-4d10-bc72-989f03c8b84b}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{21b7c16e-c5af-4a69-a74a-7245481c1b97}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{22b6d684-fa63-4578-87c9-effcbe6643c7}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{22fb2cd6-0e7b-422b-a0c7-

2fad1fd0e716}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{239cfb83-cbb7-4bbc-a02e-9bdb496aa7c2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{271c5228-c3fe-4e47-831f-48c3652ce5ac}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{272a979b-34b5-48ec-94f5-7225a59c85a0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{27a8c1e2-eb19-463e-8424-b399df27a216}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{28aa95bb-d444-4719-a36f-40462168127e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2992e9cf-4f99-48f5-a0b6-b99b11cd387d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{29d13147-1c2e-48ec-9994-e29dfe496eb3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2a274310-42d5-4019-b816-e4b8c7abe95c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2d318b91-e6e7-4c46-bd04-bfe6db412cf9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2e35aaeb-857f-4beb-a418-2e6c0e54d988}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2ed6006e-4729-4609-b423-3ee7bcd678ef}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2f07e2ee-15db-40f1-90ef-9d7ba282188a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2fd7a9a5-b1a1-4fc7-b95c-c32fed818f30}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{2ff3e6b7-cb90-4700-9621-443f389734ed}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{30336ed4-e327-447c-9de0-51b652c86108}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{314b2b0d-81ee-4474-b6e0-c2aaec0ddbde}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{314de49f-ce63-4779-ba2b-d616f6963a88}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{319122a9-1485-4e48-af35-7db2d93b8ad2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{31f60101-3703-48ea-8143-451f8de779d2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3239eb6f-c7fc-4953-aa15-646829a4ca4c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{331c3b3a-2005-44c2-ac5e-77220c37d6b4}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{355c44fe-0c8e-4bf8-be28-8bc7b5a42720}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{35ac6ce8-6104-411d-976c-877f183d2d32}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3663a992-84be-40ea-bba9-90c7ed544222}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{36c23e18-0e66-11d9-bbeb-505054503030}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{37945dc2-899b-44d1-b79c-dd4a9e57ff98}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3aa52b8b-6357-4c18-a92e-b53fb177853b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3c6c422b-019b-4f48-b67b-f79a3fa8b4ed}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cb2a168-fe19-4a4e-bdad-dcf422f13473}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cb40aaa-1145-4fb8-b27b-7e30f0454316}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3cc2d4af-da5e-4ed4-bcbe-3cf995940483}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3df0c2c1-5a04-4966-9790-df6ef0ccde9c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3f7b2f99-b863-4045-ad05-f6afb62e7af1}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{3f9e07bd-0e26-4241-a5a5-28cfa150a75}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{40ab57c2-1c53-4df9-9324-ff7cf898a02c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{40ae003c-6f3d-4590-ae1c-0e8be526b50f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4214dcd2-7c33-4f74-9898-719ccceec20f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{422088e6-cd0c-4f99-bd0b-6985fa290bdf}[]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{43d1a55c-76d6-4f7e-995c-64c711e5cafe}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{43e63da5-41d1-4fbf-aded-1bbcd98fdd1d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{46098845-8a94-442d-9095-366a6bcfefa9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{49c2c27c-fe2d-40bf-8c4e-c3fb518037e7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4a933674-fb3d-4e8d-b01d-17ee14e91a3e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4b7eac67-fc53-448c-a49d-7cc6db524da7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ba32972-6fc5-488a-8368-5da620d05127}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4cb314df-c11f-47d7-9c04-65fb0051561b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4cec9c95-a65f-4591-b5c4-30100e51d870}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4edbe902-9ed3-4cf0-93e8-b8b5fa920299}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ee76bd8-3cf4-44a0-a0ac-3937643e37a3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4ef850d8-bf30-4e64-a917-ee21b9be1f0a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4f768be8-9c69-4bbc-87fc-95291d3f9d0c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4fba1227-f606-4e5f-b9e8-fab9ab5740f3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{4fcbf664-a33a-4652-b436-9d558983d955}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{50b3e73c-9370-461d-bb9f-26f32d68887d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{50bd1bfd-936b-4db3-86be-e25b96c25898}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{51480c1a-90aa-416e-98fd-4c11f735349b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5322d61a-9efa-4bc3-a3f9-14be95c144f8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{538cbbad-4877-4eb2-b26e-7caee8f0f8cb}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54164045-7c50-4905-963f-e5bc1eef0cca}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5444519f-2484-45a2-991e-953e4b54c8e0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{546549be-9d63-46aa-9154-4f6eb9526378}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54732ee5-61ca-4727-9da1-10be5a4f773d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54849625-5478-4994-a5ba-3e3b0328c30d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54d5ac20-e14f-4fda-92da-ebf7556ff176}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{54ffd262-99fe-4576-96e7-1adb500370dc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{555908d1-a6d7-4695-8e1e-26931d2012f4}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{57e0b31d-de8c-4181-bcd1-f70e880b49fc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5857d6ca-9732-4454-809b-2a87b70881f8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{588c5c5a-ffc5-44a2-9a7f-d5e8dbe6efd7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{588cd2e4-a5b0-492d-a59b-f6dd3e7681c6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5a24fcd8-1cf3-477b-b422-ef4909d51223}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b004607-1087-4f16-b10e-979685a8d131}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b0a651a-8807-45cc-9656-7579815b6af0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5b93cdfa-5f51-45e0-9fde-296983129e6c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5bbca4a8-b209-48dc-a8c7-b23d3e5216fb}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5c8bb950-959e-4309-8908-67961a1205d5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5c9be3e0-3593-4dcd-8f6d-63840923ffee}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d674230-ca9f-11da-a94d-0800200c9a66}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d896912-022d-40aa-a3a8-4fa5515c76d7}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5d9e0020-3761-4f36-90c8-38ce6511bd12}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5ec13d8e-4b3f-422e-a7e7-3121a1d90c7a}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{5f92bc59-248f-4111-86a9-e393e12c6139}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{606a6a38-70ec-4309-b3a3-82ff86f73329}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{614696c9-85af-4e64-b389-d2c0db4ff87b}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{617853d6-728b-4b59-8a78-c3a9a5eade92}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{61f044af-9104-4ca5-81ee-cb6c51bb01ab}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63b530f8-29c9-4880-a5b4-b8179096e7b8}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63d1e632-95cc-4443-9312-af927761d52a}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{63d2bb1d-e39a-41b8-9a3d-52dd06677588}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{651df93b-5053-4d1e-94c5-f6e6d25908d0}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{65d341f3-baaa-4c6e-8b20-23d4f1574004}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{65d99466-7a8e-489c-b8e1-962bc945031e}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6600e712-c3b6-44a2-8a48-935c511f28c8}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{66a5c15c-4f8e-4044-bf6e-71d896038977}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{676f167f-f72c-446e-a498-eda43319a5e3}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67bd1fef-afb2-458d-bcde-3758beb84dec}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{67fe2216-727a-40cb-94b2-c02211edb34a}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6863e644-dd5d-43a2-a8b5-7a81b46672e6}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{699e309c-e782-4400-98c8-e21d162d7b7b}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a1f2b00-6a90-4c38-95a5-5cab3b056778}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a2dc7c1-930a-4fb5-bb44-80b30aebd6c}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6a502821-ab44-40c8-b32f-37315d9d52e0}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ad52b32-d609-4be9-ae07-ce8dae937e39}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6addabf4-8c54-4eab-bf4f-fbef61b62eb0}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b1ffe48-5b1e-4793-9f7f-ae926454499d}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b4db0bc-9a3d-467d-81b9-a84c6f2f3d40}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6b93bf66-a922-4c11-a617-cf60d95c133d}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ba132c4-da49-415b-a7f4-31870dc9fe25}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6bba3851-2c7e-4dea-8f54-31e5afd029e3}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6c260f2c-049a-43d8-bf4d-d350a4e6611a}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6d8a3a60-40af-445a-98ca-99359e500146}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6e400999-5b82-475f-b800-cef6fe361539}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6eb8db94-fe96-443f-a366-5fe0cee7fb1c}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{6ece3302-fee1-4ea9-8b88-086d459ed976}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{70eb4f03-c1de-4f73-a051-33d13d5413bd}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{712abb2d-d806-4b42-9682-

26da01d8b307}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{719be4ed-e9bc-4dd8-a7cf-c85ce8e4975d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7237fff9-a08a-4804-9c79-4a8704b70b87}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7288c9f8-d63c-4932-a345-89d6b060174d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{728b8c72-0f0f-4071-9bcc-27cb3b6dacbe}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{72d211e1-4c54-4a93-9520-4901681b2271}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{73370bd6-85e5-430b-b60a-fea1285808a7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{73e9c9de-a148-41f7-b1db-4da051fdc327}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{741fc222-44ed-4ba7-98e3-f405b2d2c4b4}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7426a56b-e2d5-4b30-bdef-b31815c1a74a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{747ef6fd-e535-4d16-b510-42c90f6873a1}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74b4a4b1-2302-4768-ac5b-9773dd456b08}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74b655a2-8958-410e-80e2-3457051b8dff}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{74c2135f-cc76-45c3-879a-ef3bb1eeaf86}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0870-49e5-bdce-9d7028279489}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0936-4a55-9d26-5f298f3180bf}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-0cc6-49da-8cd9-8903a5222aa0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-77b8-4ba8-9474-4f4a9db2f5c6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-8670-4eb6-b535-3b9d6bb222fd}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-997f-49cf-b49f-ecc50184b75d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-c8ae-4f93-9ca1-683a53e20cb6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75ebc33e-d017-4d0f-93ab-0b4f86579164}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{75f48521-4131-4ac3-9887-65473224fcb2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{777ba8fe-2498-4875-933a-3067de883070}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{78168022-eca5-41e8-9e17-e8c7fd77aae1}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7839bb2a-2ea3-4eca-a00f-b558ba678bec}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7a67066e-193f-4d3a-82d3-322fee5259de}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b563579-53c8-44e7-8236-0f87b9fe6594}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b6bc78c-898b-4170-bbf8-1a469ea43fc5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7b7838a3-6562-4269-bb7a-97b0d9593882}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7bb5af18-cb16-4007-b813-9d88e9d6f8ef}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7bfcf102-7378-431c-9284-0b968258991a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7c314e58-8246-47d1-8f7a-4049dc543e0b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d29d58a-931a-40ac-8743-48c733045548}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d44233d-3055-4b9c-ba64-0d47ca40a232}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d5387b0-cbe0-11da-a94d-0800200c9a66}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7d7b0c39-93f6-4100-bd96-4dda859652c5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7da4fe0e-fd42-4708-9aa5-89b77a224885}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7dd42a49-5329-4832-8dfd-43d979153a88}[]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7eafc79-06a7-460b-8a55-bd0a0c9248aa}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f2bd991-ae93-454a-b219-0bc23f02262a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f912b92-21ad-496e-b97a-88622a72bc42}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{7f9d83de-8abb-457f-98e8-4ad161449ecc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{802ec45a-1e99-4b83-9920-87c98277ba9d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8085cb91-900e-4d15-a7d1-921ddce641d8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8115579e-2bea-4c9e-9ab1-821cc2c98ab0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{820a42d8-38c4-465d-b64e-d7d56ea1d612}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{835b79e2-e76a-44c4-9885-26ad122d3b4d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8360bd0f-a7dc-4391-91a7-a457c5c381e4}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{83ed54f0-4d48-4e45-b16e-726ffd1fa4af}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{84051b98-f508-4e54-82fa-8865c697c3b1}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8429e243-345b-47c1-8a91-2c94caf0daab}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8443ccb7-feb0-4b8d-8e28-8d4c7cb814e8}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{85fe7609-ff4a-48e9-9d50-12918e43e1da}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{86133982-63d7-4741-928e-ef1349b80219}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{869fb599-80aa-485d-bca7-db18d72b7219}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{86efff39-2bdd-4efd-bd0b-853d71b2a9dc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{87d476fe-1a0f-4370-b785-60b028019693}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8939299f-2315-4c5c-9b91-abb86aa0627d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{899daace-4868-4295-afcd-9eb8fb497561}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89a2278b-c662-4aff-a06c-46ad3f220bca}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{89b1e9f0-5aff-44a6-9b44-0a07a7ce5845}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8a93b54b-c75a-49b5-a5be-9060715b1a33}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8c63b5a5-b484-4381-892d-edd424582df7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8c9dd1ad-e6e5-4b07-b455-684a9d879900}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{8ce93926-bdae-4409-9155-2fe4799ef4d3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{914ed502-b70d-4add-b758-95692854f8a3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{91f42016-0b4e-4a4b-9bbb-825d06cbcd35}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{91f5fb12-fdea-4095-85d5-614b495cd9de}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{92ae46d7-6d9c-4727-9ed5-e49af9c24cbf}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9363ccd9-d429-4452-9adb-2501e704b810}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{93c05d69-51a3-485e-877f-1806a8731346}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{945a8954-c147-4acd-923f-40c45405a658}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9485fa1e-23cd-49a1-84e3-11d8bc550cb7}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{952773bf-c2b7-49bc-88f4-920744b82c43}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{95353826-4fbe-41d4-9c42-f521c6e86360}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9580d7dd-0379-4658-9870-d5be7d52d6de}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{959f1fac-7ca8-4ed1-89dc-cdfa7e093cb0}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{968f313b-097f-4e09-9cdd-bc62692d138b}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{96ac7637-5950-4a30-b8f7-e07e8e5734c1}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{96f4a050-7e31-453c-88be-9634f4e02139}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{973143dd-f3c7-4ef5-b156-544ac38c39b6}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98583af0-fc93-4e71-96d5-9f8da716c6b8}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98bf1cd3-583e-4926-95ee-a61bf3f46470}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{98e6cfc6-ee0a-41e0-a57b-622d4e1b30b1}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{99806515-9f51-4c2f-b918-1eae407aa8cb}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9988748e-c2e8-4054-85f6-0c3e1cad2470}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9b307223-4e4d-4bf5-9be8-995cd8e7420b}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9b6123dc-9af6-4430-80d7-7d36f054fb9f}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9c205a39-1250-487d-abd7-e831c6290539}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9d55b53d-449b-4824-a637-24f9d69aa02f}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9db0fdb5-3b21-440e-a94b-63738a4be5de}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e03f75a-bcbe-428a-8f3c-d46f2a444935}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e3b3947-ca5d-4614-91a2-7b624e0e7244}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e6ae157-d9f7-47e5-8c6d-b17bb6c82a27}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9e95e4d0-4cb4-4b5d-a936-c972d7d08d90}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9f0c4ea8-ec01-4200-a00d-b9701cbea5d8}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{9f650c63-9409-453c-a652-83d7185a2e83}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a0c1853b-5c40-4b15-8766-3cf1c58f985a}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a0e3d8ea-c34f-4419-a1db-90435b8b21d0}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a319d300-015c-48be-acdb-47746e154751}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a3e1697b-a12c-46b9-84d1-7ffe73c4b678}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a402fe09-da6e-45f2-82af-3cb37170ee0c}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a50b09f8-93eb-4396-84c9-dc921259f952}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a615acb9-d5a4-4738-b561-1df301d207f8}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a68ca8b7-004f-d7b6-a698-07e2de0f1f5d}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a6ad76e3-867a-4635-91b3-4904ba6374d7}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a6f32731-9a38-4159-a220-3d9b7fc5fe5d}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a7364e1a-894f-4b3d-a930-2ed9c8c4c811}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a7975c8f-ac13-49f1-87da-5a984a4ab417}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a8106e5c-293a-4cd0-9397-2e6fac7f9749}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a82fda5d-745f-409c-b0fe-18ae0678a0e0}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a8a1f2f6-a13a-45e9-b1fe-3419569e5ef2}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{a97524f6-064c-4c4e-b74b-1acc87c3700d}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aabf8b86-7936-4fa2-acb0-63127f879dbf}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aaf44901-5c64-4014-8b6c-a80813937293}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ab0d8ef9-866d-4d39-b83f-

453f3b8f6325}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{abce23e7-de45-4366-8631-84fa6c525952}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ac43300d-5fcc-4800-8e99-1bd3f85f0320}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ad5162d8-daf0-4a25-88a7-01cbeb33902e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ad8aa069-a01b-40a0-ba40-948d1d8dedc5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ae4bd3be-f36f-45b6-8d21-bdd6fb832853}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{aea1b4fa-97d1-45f2-a64c-4d69fffd92c9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af0a5a6d-e009-46d4-8867-42f2240f8a72}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af2e340c-0743-4f5a-b2d3-2f7225d215de}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{af9cc194-e9a8-42bd-b0d1-834e9cfab799}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b03d4051-3564-4e93-93db-3c34f1b5b503}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b059b83f-d946-4b13-87ca-4292839dc2f2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1bebb9a-24aa-4b83-9e4a-38c2a9a44377}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1c94ed9-ac9b-410e-aa48-4ffc5e45f4e3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b1f90b27-4551-49d6-b2bd-dfc6453762a6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b2a40f1f-a05a-4dfd-886a-4c4f18c4334c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b3eee223-d0a9-40cd-adfc-50f1888138ab}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b44ac44-38f4-4b59-8df3-10306abf19b2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b5fd844a-01d4-4b10-a57f-58b13b561582}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b65471e1-019d-436f-bc38-e15fa8e87f53}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b675ec37-bdb6-4648-bc92-f3fdc74d3ca2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b92cf7fd-dc10-4c6b-a72d-1613bf25e597}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b977cf02-76f6-df84-cc1a-6a4b232322b6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b98f0db6-26e2-4a66-89fc-32a9a6a9af61}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{b9da9fe6-ae5f-4f3e-b2fa-8e623c11dc75}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ba093605-3909-4345-990b-26b746adee0a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bbe94f36-f8dc-4c33-8227-81602b7a3d53}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bc2eeec-b77a-4a52-b6a4-dffb1b1370cb}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bc97b970-d001-482f-8745-b8d7d5759f99}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd12f3b8-fc40-4a61-a307-b7a013a069c1}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd2d1dae-d678-4e10-9667-21cba2aa70c3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bd2f4252-5e1e-49fc-9a30-f3978ad89ee2}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bdb462fc-a297-49a2-bf2e-4f1809e12abc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{be69781c-b63b-41a1-8e24-a4fc7b3fc498}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{be932b00-0f8e-4386-ab89-873f7d0274aa}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{bf406804-6afa-46e7-8a48-6c357e1d6d61}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c02af2cb-e24e-4449-ad76-bcc2c2575ead}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c06ed57a-a7bd-42d7-b5ff-77a9dec5732d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c100becc-d33a-4a4b-bf23-bbef4663d017}[]
Queries value:

HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c100becf-d33a-4a4b-bf23-bbef4663d017}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c26c4f3c-3f66-4e99-8f8a-39405cfd220}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c2fa0899-8a10-412b-a42e-9e5b284a2437}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c4636a1e-7986-4646-bf10-7bc3b4a76e8e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c514638f-7723-485b-bcfc-96565d735d4a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c6bf6832-f7bd-4151-ac21-753ce4707453}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c76baa63-ae81-421c-b425-340b4b24157f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c7bde69a-e1e0-4177-b6ef-283ad1525271}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c882ff1d-7585-4b33-b135-95c577179137}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c88a4ef5-d048-4013-9408-e04b7db2814a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c89b991e-3b48-49b2-80d3-ac00dfc9749}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c8f7689f-3692-4d66-b0c0-9536d21082c9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c914f0df-835a-4a22-8c70-732c9a80c634}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c91ef675-842f-4fcf-a5c9-6ea93f2e4f8b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{c9bdb4eb-9287-4c8e-8378-6896f0d1c5ef}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ca4e628d-8567-4896-ab6b-835b221f373f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ca5ba219-c0d4-4efa-9ceb-72aff92672b0}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cab2b8a5-49b9-4eec-b1b0-fac21da05a3b}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cad2d809-03d9-4f46-9cf4-72aa4f04b6b9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cb070027-1534-4cf3-98ea-b9751f508376}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cb587ad1-cc35-4ef1-ad93-36cc82a2d319}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cbda4dbf-8d5d-4f69-9578-be14aa540d22}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cd032e15-15ad-4da4-afc6-03bf83516195}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cdc05e28-c449-49c6-b9d2-88cf761644df}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cdead503-17f5-4a3e-b7ae-df8cc2902eb9}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ce20d1c3-a247-4c41-bcb8-3c7f52c8b805}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ce8dee0b-d539-4000-b0f8-77bed049c590}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cf3f502e-b40d-4071-996f-00981edf938e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfaa5446-c6c4-4f5c-866f-31c9b55b962d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{cfc18ec0-96b1-4eba-961b-622cae05b0a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d02a9c27-79b8-40d6-9b97-cf3f8b7b5d60}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d1bc9aff-2abf-4d71-9146-ecb2a986eb85}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d1d93ef7-e1f2-4f45-9943-03d245fe6c00}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d4263c98-310c-4d97-ba39-b55354f08584}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d53270e3-c8cf-4707-958a-dad20c90073c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d5c25f9a-4d47-493e-9184-40dd397a004d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d6f68875-cdf5-43a5-a3e3-53ffdf683311c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{d8975f88-7ddb-4ed0-91bf-3adf48c48e0c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dab065a9-620f-45ba-b5d6-d6bb8efedee9}[]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dab3b18c-3c0f-43e8-80b1-e44bc0dad901}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{db00dfb6-29f9-4a9c-9b3b-1f4f9e7d9770}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dbe9b383-7cf3-4331-91cc-a3cb16a3b538}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dd5ef90a-6398-47a4-ad34-4dcecddef795f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dd70bc80-ef44-421b-8ac3-cd31da613a4e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dd85457f-4e2d-44a5-a7a7-6253362e34dc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{de513a55-c345-438b-9a74-e18cac5c5cc5}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{dea07764-0790-44de-b9c4-49677b17174f}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ded165cf-485d-4770-a3e7-9c5f0320e80c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{df32a572-0b4b-44be-b09b-72084fdbf879}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e01b1a7c-c5c9-4e67-99a9-5e85acfb2e10}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e04fe2e0-c6cf-4273-b59d-5c97c9c374a4}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e0a40b26-30c4-4656-bc9a-74a5c3a0b2ec}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e104fb41-6b04-4f3a-b47d-f0df2f02b954}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e1dd7e52-621d-44e3-a1ad-0370c2b25946}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e23b33b0-c8c9-472c-a5f9-f2bdfea0f156}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e2816346-87f4-4f85-95c3-0c79409aa89d}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e4480490-85b6-11dd-ad8b-0800200c9a66}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e46eead8-0c54-4489-9898-8fa79d059e0e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e4d53f84-7de3-11d8-9435-505054503030}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e53c6823-7bb8-44bb-90dc-3f86090d48a6}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e595f735-b42a-494b-afcd-b68666945cd3}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e5ba83f6-07d0-46b1-8bc7-7e669a1d31dc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e6307a09-292c-497e-aad6-498f68e2b619}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e670a5a2-ce74-4ab4-9347-61b815319f4c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e7558269-3fa5-46ed-9f4d-3c6e282dde55}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e7ef96be-969f-414f-97d7-3ddb7b558ccc}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e8316a2d-0d94-4f52-85dd-1e15b66c5891}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e837619c-a2a8-4689-833f-47b48ebd2442}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e856c26a-e105-4683-a948-6920dcc42e45}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e978f84e-582d-4167-977e-32af52706888}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eb3deb18-d1de-4897-8502-a230ad03db8a}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ed6b3ba8-95b2-4cf5-a317-d4af7003884c}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{edd08927-9cc4-4e65-b970-c2560fb5c289}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ee4f43b5-03eb-41d2-a28c-ba8bee529247}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{eef54e71-0661-422d-9a98-82fd4940b820}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ef1cc15b-46c1-414e-bb95-e76b077bd51e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f0db7ef8-b6f3-4005-9937-

```

feb779e1b43][
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f230d19a-5d93-47d9-a83f-53829edfb8df}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f26c28ae-d26c-4352-9c45-74754e1e2f9f}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f3c5e28e-63f6-49c7-a204-e48a1bc4b09d}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f3f14ff3-7b80-4868-91d0-d77e497b025e}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f404b94e-27e0-4384-bfe8-1d8d390b0aa3}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f4aed7c7-a898-4627-b053-44a7caa12fcd}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f5344219-87a4-4399-b14a-e59cd118abb8}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f557ace2-bcf8-4994-8e4b-42368a6f078a}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f5d05b38-80a6-4653-825d-c414e4ab3c68}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f61cef0c-aa2e-11da-a746-0800200c9a66}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f6da35ce-d312-41c8-9828-5a2e173c91b6}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f82fb576-e941-4956-a2c7-a0cf83f6450a}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{f997cd11-0fc9-4ab4-acba-bc742a4c0dd3}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fbcfac3f-8459-419f-8e48-1f0b49c9b85e}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc3bc8a7-2f61-449c-a8b4-22ac22058f92}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc65dd8d-d6ef-4962-83d5-6e5cfe9ce148}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fc6f77dd-769a-470e-bcf9-1b6555a118be}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{fd771d53-8492-4057-8e35-8c02813af49b}[
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{ffdb9886-80f3-4540-aa8b-b85192217ddf}[
  Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[providerguid]
  Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[eventmessagefile]
  Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[categorymessagefile]
  Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[resourcefilename]
  Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[parametermessagefile]
  Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[helpink]
  Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\eventlog\system\eventlog[categorycount]
  Queries value:
HKLM\system\currentcontrolset\services\netlogon\parameters[expecteddialupdelay]
  Queries value:
HKLM\system\currentcontrolset\services\fileinfo\instances\fileinfo[flags]
  Queries value:
HKLM\system\currentcontrolset\services\fileinfo\instances\fileinfo[altitude]
  Queries value:
HKLM\system\currentcontrolset\services\fileinfo\instances\fileinfo[flags]
  Queries value:
HKLM\system\currentcontrolset\services\fileinfo\instances\fileinfo[altitude]
  Queries value:
HKLM\system\currentcontrolset\control\wmi\security[b40325fe-7106-42ac-849e-8aa81df5cb01]
  Queries value:
HKLM\system\currentcontrolset\control\timezoneinformation[bias]
  Queries value:
HKLM\system\currentcontrolset\control\timezoneinformation[standardname]
  Queries value:
HKLM\system\currentcontrolset\control\timezoneinformation[standardbias]
  Queries value:
HKLM\system\currentcontrolset\control\timezoneinformation[standardstart]
  Queries value:
HKLM\system\currentcontrolset\control\timezoneinformation[daylightname]
  Queries value:
HKLM\system\currentcontrolset\control\timezoneinformation[daylightbias]
  Queries value:
HKLM\system\currentcontrolset\control\wmi\security[f4c19371-9e73-45ef-96de-2efb32299a79]
  Queries value:
HKLM\system\currentcontrolset\control\wmi\security[b696cfe-f69c-431b-81c4-68a83567a600]
  Queries value:
HKLM\system\currentcontrolset\control\wmi\security[37a3e5d6-9edb-46d7-baec-6b841d4e89e7]
  Queries value:
HKLM\system\currentcontrolset\control\wmi\security[d14e883c-c62a-450f-9a3d-ac55797cd8b2]
  Queries value:
HKLM\software\microsoft\wbem\cimom[configvalueessneedsloading]
  Queries value:
HKLM\system\currentcontrolset\control\nls\customlocale[root]
  Queries value:
HKLM\system\currentcontrolset\control\nls\extendedlocale[root]
  Queries value:
HKLM\software\microsoft\reliability\analysis\wmi[wminenable]
  Queries value:
HKLM\software\policies\microsoft\windows\ipsec\policy\local[activepolicy]
  Queries value:
HKLM\software\microsoft\windows\currentversion\superfetch\diskassessment[disknumber]
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e6307a09-292c-497e-aad6-498f68e2b619}[messagefilename]
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e6307a09-292c-497e-aad6-498f68e2b619}[categorymessagefile]
  Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\publishers\{e6307a09-292c-497e-aad6-498f68e2b619}[resourcefilename]
  Queries value:

```

[illegible]

Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-readyboost/analytic[maxsize]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-readyboost/analytic[maxsizeupper]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-readyboost/analytic[retention]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-readyboost/analytic[autobackuplogfiles]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-readyboost/analytic[file]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-readyboost/analytic[filterid]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-readyboost/analytic[isolation]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-readyboost/analytic[owningpublisher]
Queries value:
HKLM\software\microsoft\windows\currentversion\winevt\channels\microsoft-windows-readyboost/analytic[channelaccess]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[981f2d7e-b1f3-11d0-8dd7-00c04fc3358c]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-000000000000]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[981f2d7d-b1f3-11d0-8dd7-00c04fc3358c]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0006\linkage[upperbind]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[1h6wzb8fwvux1exfmpbqaa]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1409]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1609]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\1[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\2[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\3[1406]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4[1406]
Sets/Creates value: HKCU\software\microsoft\internet explorer\phishingfilter[shownservicedownballoon]
Sets/Creates value: HKCU\software\microsoft\internet explorer\recovery[clearbrowsinghistoryonexit]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline]
Sets/Creates value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpnameserver]
Sets/Creates value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpnameserver]
Sets/Creates value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpsubnetmaskopt]
Sets/Creates value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpdefaultgateway]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{7bf7ed91-f442-458a-abea-c661d1bd5efb}[wpaddecisionreason]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{7bf7ed91-f442-458a-abea-c661d1bd5efb}[wpaddecisiontime]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{7bf7ed91-f442-458a-abea-c661d1bd5efb}[wpaddecision]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{7bf7ed91-f442-458a-abea-c661d1bd5efb}[wpadnetworkname]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\82-da-ad-19-17-f7[wpaddecisionreason]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\82-da-ad-19-17-f7[wpaddecisiontime]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\wpad\82-da-ad-19-17-f7[wpaddecision]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[enablehttp1_1]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyhttp1.1]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpost]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpostredirect]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[warnonintranet]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[1406]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1409]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[1609]
Value changes: HKCU\software\microsoft\windows\currentversion\internet

```
settings\zones\4[1406]
  Value changes:      HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]
  Value changes:      HKLM\software\microsoft\windows
nt\currentversion\networklist\nla\cache\intranet[{128919e8-8a5e-41d1-ac17-c19ce8a73253}]
  Value changes:      HKLM\system\currentcontrolset\control\network\{4d36e972-e325-11ce-bfc1-08002be10318}\{128919e8-8a5e-41d1-ac17-c19ce8a73253}\connection[pnpinstanceid]
  Value changes:      HKCU\software\classes\local settings\muicache\27\52c64b7e[language]
  Value changes:      HKLM\system\currentcontrolset\control\wmi\autologger\readyboot[start]
  Value changes:
HKLM\system\currentcontrolset\services\rdyboost\parameters[readybootvolumeuniqueid]
  Value changes:      HKLM\system\currentcontrolset\control\session manager\memory
management\prefetchparameters[enableboottrace]
  Value changes:      HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Value changes:      HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Value changes:
HKLM\system\currentcontrolset\services\mpssvc\parameters\portkeywords\dhcp[collection]
  Value changes:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpinterfaceoptions]
  Value changes:      HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Value changes:      HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadlastnetwork]
  Value changes:      HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
  Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{q6523100-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
  Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[hrzr_pgyfrffvba]
  Value changes:      HKLM\system\currentcontrolset\services\rdyboost\parameters[bootplan]
  Value changes:
HKLM\system\currentcontrolset\services\rdyboost\parameters[readybootplanage]
  Value changes:
HKLM\system\currentcontrolset\services\rdyboost\parameters[lastbootplanusertime]
```