Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 717, Task ID: 450001

Task ID:	450001
Risk Level:	7
Date Processed:	2016-04-08 16:37:32 (UTC)
Processing Time:	60.0 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\ToggleService32.exe"
Sample ID:	717
Type:	basic
Owner:	admin
Label:	ToggleService32.exe
Date Added:	2016-04-08 16:37:32 (UTC)
File Type:	PE32:win32
File Size:	10254 bytes
MD5:	1439e0552127dda0c66b7be1eadb723d
SHA256:	89e815c8779e61dda1e5f6aa0af737361ffc6296c25300e82a5c23dcc165f82a
Description:	None

Pattern Matching Results

3 Writes to a log file [Info]
6 PE: File has TLS callbacks
6 Writes to system32 folder
6 Modifies registry autorun entries
7 Injects thread into Windows process
2 PE: Nonstandard section
5 Installs service
4 Terminates process under Windows subfolder

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Anomaly:	PE: File contain TLS callbacks

Process/Thread Events

Creates process:	C:\windows\temp\ToggleService32.exe ["C:\windows\temp\ToggleService32.exe"]
Creates process:	\SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe 0xffffffff]
Creates process:	C:\Windows\System32\alg.exe [C:\Windows\System32\alg.exe]
Creates process:	C:\Windows\System32\msdtc.exe [C:\Windows\System32\msdtc.exe]
Creates process:	C:\Windows\system32\UIODetect.exe [C:\Windows\system32\UIODetect.exe]
Creates process:	C:\Windows\System32\svchost.exe [C:\Windows\System32\svchost.exe -k LocalServicePeerNet]
Creates process:	C:\Windows\System32\spoolsv.exe [C:\Windows\System32\spoolsv.exe]
Creates process:	C:\Windows\system32\vssvc.exe [C:\Windows\system32\vssvc.exe]
Creates process:	C:\Windows\System32\svchost.exe [C:\Windows\System32\svchost.exe -k WerSvcGroup]
Creates process:	C:\Windows\system32\svchost.exe [C:\Windows\system32\svchost.exe -k imgsvc]
Loads service:	ALG [C:\Windows\System32\alg.exe]
Loads service:	AppMgmt [C:\Windows\system32\svchost.exe -k netsvcs]
Loads service:	BITS [C:\Windows\System32\svchost.exe -k netsvcs]
Loads service:	TrkWks [C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted]
Loads service:	MSDTC [C:\Windows\System32\msdtc.exe]
Loads service:	DNSCache [C:\Windows\system32\svchost.exe -k NetworkService]
Loads service:	EventLog [C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted]
Loads service:	EAPHost [C:\Windows\System32\svchost.exe -k netsvcs]
Loads service:	UIODetect [C:\Windows\system32\UIODetect.exe]
Loads service:	SharedAccess [C:\Windows\System32\svchost.exe -k netsvcs]
Loads service:	PNRPSvc [C:\Windows\System32\svchost.exe -k LocalServicePeerNet]
Loads service:	PlugPlay [C:\Windows\system32\svchost.exe -k DcomLaunch]
Loads service:	Spooler [C:\Windows\System32\spoolsv.exe]
Loads service:	RpcSs [C:\Windows\system32\svchost.exe -k rpcss]
Loads service:	SecLogon [C:\Windows\system32\svchost.exe -k netsvcs]
Loads service:	SENS [C:\Windows\system32\svchost.exe -k netsvcs]
Loads service:	SysMain [C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted]
Loads service:	Schedule [C:\Windows\system32\svchost.exe -k netsvcs]
Loads service:	LmHosts [C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted]
Loads service:	VSS [C:\Windows\system32\vssvc.exe]
Loads service:	AudioSrv [C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted]
Loads service:	WERSvc [C:\Windows\System32\svchost.exe -k WerSvcGroup]
Loads service:	MpsSvc [C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork]
Loads service:	STISvc [C:\Windows\system32\svchost.exe -k imgsvc]
Loads service:	W32Time [C:\Windows\system32\svchost.exe -k LocalService]
Loads service:	WUAUServ [C:\Windows\system32\svchost.exe -k netsvcs]
Loads service:	WLANSvc [C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted]
Terminates process:	C:\Windows\System32\alg.exe
Terminates process:	C:\Windows\System32\UIODetect.exe

Terminates process: C:\Windows\System32\VSSVC.exe
Terminates process: C:\Windows\System32\svchost.exe
Creates remote thread: System
Creates remote thread: C:\Windows\System32\services.exe
Creates remote thread: C:\Windows\System32\svchost.exe
Creates remote thread: C:\Windows\System32\spoolsv.exe
Creates remote thread: C:\Windows\explorer.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \BaseNamedObjects\DBWinMutex
Creates mutex: \BaseNamedObjects\MSDTC_STATS_EVENT
Creates mutex: \BaseNamedObjects\{d2e3d0ea-5528-4255-b52b-c95244d6d08a}_S-1-5-19
Creates mutex: \BaseNamedObjects\WIATRACE_MUTEX
Creates event: \BaseNamedObjects\RouterPreInitEvent
Creates event: \BaseNamedObjects\WerSvcSystemPermissionsEvent
Creates event: \BaseNamedObjects\WiaServiceStarted

File System Events

Creates: C:\Windows\SysWOW64\output.txt
Creates: C:\Windows\System32\MsDtc\Trace\dtctrace.log
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.lkg
Creates: C:\ProgramData\Microsoft
Creates: C:\ProgramData\Microsoft\Crypto
Creates: C:\ProgramData\Microsoft\Crypto\RSA
Creates: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
Creates: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\759cc9695d0b4f46f1829631c1525324_de228479-9e18-473a-b3d7-31d4d2573dc2
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Creates: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Creates: C:\Windows\Debug\WIA
Opens: C:\Windows\Prefetch\TOGGLESERVICE32.EXE-2248A864.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\System32\conhost.exe
Opens: C:\Windows\System32\combase.dll
Opens: C:\Windows\System32\ole32.dll
Opens: C:\Windows\System32\uxtheme.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\System32\dwmapi.dll
Opens: C:\Windows\system32\uxtheme.dll.Config
Opens: C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f
Opens: C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f\comctl32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\System32\sechost.dll
Opens: C:\Windows\System32\rpcss.dll
Opens: C:\Windows\System32\cryptbase.dll
Opens: C:\Windows\System32\bcryptprimitives.dll
Opens: C:\Windows\System32\SHCore.dll
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\Temp\ToggleService32.exe
Opens: C:\Windows\SysWOW64\ntdll.dll
Opens: C:\Windows\SysWOW64\kernel32.dll
Opens: C:\Windows\SysWOW64\KernelBase.dll
Opens: C:\Windows\apppatch\sysmain.sdb
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\msvcrt.dll
Opens: C:\Windows\SysWOW64\bcryptprimitives.dll
Opens: C:\Windows\SysWOW64\cryptbase.dll
Opens: C:\Windows\SysWOW64\sspicli.dll
Opens: C:\Windows\SysWOW64\rpcrt4.dll
Opens: C:\Windows\SysWOW64\advapi32.dll
Opens: C:\Windows\SysWOW64\output.txt
Opens: C:\Windows\Prefetch\ALG.EXE-1D11534C.pf
Opens: C:\Windows\System32
Opens: C:\Windows\System32\mswsock.dll
Opens: C:\Windows\System32\clbcatq.dll
Opens: C:\Windows\System32\user32.dll
Opens: C:\Windows\System32\en-US\alg.exe.mui
Opens: C:\Windows\System32\cryptsp.dll
Opens: C:\Windows\System32\rsaenh.dll
Opens: C:\Windows\Prefetch\MSDTC.EXE-CC1DEC77.pf
Opens: C:\Windows\System32\msdtctm.dll
Opens: C:\Windows\System32\msdtcprx.dll
Opens: C:\Windows\System32\msdtclog.dll
Opens: C:\Windows\System32\mtxclu.dll
Opens: C:\Windows\System32\winmm.dll
Opens: C:\Windows\System32\clusapi.dll
Opens: C:\Windows\System32\bcrypt.dll
Opens: C:\Windows\System32\xolehlp.dll
Opens: C:\Windows\System32\dnsapi.dll
Opens: C:\Windows\System32\ktmw32.dll

Opens: C:\Windows\System32\resutils.dll
Opens: C:\Windows\System32\winmmbase.dll
Opens: C:\Windows\System32\cryptdll.dll
Opens: C:\Windows\System32\en-US\msdtc.exe.mui
Opens: C:\Windows\System32\comres.dll
Opens: C:\Windows\System32\msdtcVSp1res.dll
Opens: C:\Windows\System32\mtxoci.dll
Opens: C:\Windows\System32\MsDtc\Trace
Opens: C:\Windows\System32\sspicli.dll
Opens: C:\Windows\DtcInstall.log
Opens: C:\Windows\System32\ntmarta.dll
Opens: C:\Windows\System32\MsDtc
Opens: C:\Windows\System32\MsDtc\MSDTC.LOG
Opens: C:\Windows\System32\en-US\msdtcVSp1res.dll.mui
Opens: C:\Windows\System32\FirewallAPI.dll
Opens: C:\Windows\System32\UIODetect.exe
Opens: C:\Windows\Prefetch\UIODETECT.EXE-A794C8BB.pf
Opens: C:\Windows\System32\wtsapi32.dll
Opens: C:\Windows\System32\version.dll
Opens: C:\Windows\System32\winsta.dll
Opens: C:\Windows\System32\en-US\uiOdetect.exe.mui
Opens: C:\Windows\ServiceProfiles
Opens: C:\Windows\System32\svchost.exe
Opens: C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
Opens: C:
Opens: C:\$Extend
Opens: C:\ProgramData
Opens: C:\ProgramData\Microsoft
Opens: C:\ProgramData\Microsoft\Crypto
Opens: C:\ProgramData\Microsoft\Crypto\RSA
Opens: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
Opens: C:\Windows\Globalization
Opens: C:\Windows\Globalization\Sorting
Opens: C:\Windows\ServiceProfiles\LocalService
Opens: C:\Windows\ServiceProfiles\LocalService\AppData
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates\My
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking
Opens: C:\Windows\System32\en-US
Opens: C:\Windows\System32\ntdll.dll
Opens: C:\Windows\System32\kernel32.dll
Opens: C:\Windows\System32\KernelBase.dll
Opens: C:\Windows\System32\locale.nls
Opens: C:\Windows\System32\rpcrt4.dll
Opens: C:\Windows\System32\pnrpsvc.dll
Opens: C:\Windows\System32\msvcrt.dll
Opens: C:\Windows\System32\gpapi.dll
Opens: C:\Windows\System32\powrprof.dll
Opens: C:\Windows\System32\profapi.dll
Opens: C:\Windows\System32\crypt32.dll
Opens: C:\Windows\System32\msasn1.dll
Opens:
C:\PROGRAMDATA\MICROSOFT\CRYPTO\RSA\MACHINEKEYS\358129098041A0483A25B784E8E10913_DE228479-9E18-
473A-B3D7-31D4D2573DC2
Opens: C:\Windows\System32\en-US\crypt32.dll.mui
Opens: C:\Windows\System32\dpapi.dll
Opens: C:\Windows\System32\ncrypt.dll
Opens: C:\Windows\System32\ntasn1.dll
Opens: C:\Windows\System32\QAGENTRT.DLL
Opens: C:\Windows\System32\en-US\QAgentRT.dll.mui
Opens: C:\Windows\System32\en-US\dnsapi.dll.mui
Opens: C:\Windows\System32\fveui.dll
Opens: C:\Windows\System32\en-US\fveui.dll.mui
Opens: C:\Windows\System32\wuaueng.dll
Opens: C:\Windows\System32\en-US\wuaueng.dll.mui
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Opens: C:\Windows\System32\advapi32.dll
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Opens:
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.lkg
Opens: C:\Windows\System32\ws2_32.dll
Opens: C:\Windows\System32\nsi.dll
Opens: C:\Windows\System32\IPHLPAPI.DLL
Opens: C:\Windows\System32\winnsi.dll
Opens: C:\Windows\System32\dhcpcsvc6.dll
Opens: C:\Windows\System32\dhcpcsvc.dll
Opens: C:\Windows\System32\sqmapi.dll
Opens: C:\Windows\System32\gdi32.dll
Opens: C:\Windows\System32\en-US\svchost.exe.mui
Opens: C:\Windows\System32\oleaut32.dll
Opens: C:\Windows\System32\ssdpapi.dll
Opens:

C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\5fe46d6f4fbbaedee4917a93b3902d78_de228479-9e18-473a-b3d7-31d4d2573dc2
Opens: C:\Windows\System32\p2psvc.dll
Opens: C:\Windows\System32\P2PGraph.dll
Opens: C:\Windows\System32\esent.dll
Opens: C:\Windows\System32\en-US\p2psvc.dll.mui
Opens: C:\Windows\System32\authz.dll
Opens: C:\Windows\System32\secur32.dll
Opens: C:\Windows\System32\slc.dll
Opens: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\d924c2fbb1b73c639740e02ee2ab504b_de228479-9e18-473a-b3d7-31d4d2573dc2
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9C99BD1474CEB9C1AB13129747684184429ED3A1
Opens: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\4601d02f1df7da88667245cbda62ad09_de228479-9e18-473a-b3d7-31d4d2573dc2
Opens: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\759cc9695d0b4f46f1829631c1525324_de228479-9e18-473a-b3d7-31d4d2573dc2
Opens: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\a2d04321c581b1a4e19de84f31738e31.sst
Opens: C:\Windows\System32\spoolsv.exe
Opens: C:\Windows\Prefetch\SPOOLSV.EXE-D1F6B8B6.pf
Opens: C:\Windows\System32\en-US\spoolsv.exe.mui
Opens: C:\Windows\System32\VSSVC.exe
Opens: C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
Opens: C:\Windows\System32\vssapi.dll
Opens: C:\Windows\System32\vsstrace.dll
Opens: C:\Windows\System32\virtdisk.dll
Opens: C:\Windows\System32\dsrole.dll
Opens: C:\Windows\System32\fltLib.dll
Opens: C:\Windows\System32\en-US\VSSVC.exe.mui
Opens: C:\Windows\System32\vss_ps.dll
Opens: C:\Windows\System32\en-US\vsstrace.dll.mui
Opens: C:\Windows\System32\samcli.dll
Opens: C:\Windows\System32\netutils.dll
Opens: C:\Windows\System32\samlib.dll
Opens: C:\Windows\System32\es.dll
Opens: C:\Windows\System32\propsys.dll
Opens: C:\Windows\System32\catsrvut.dll
Opens: C:\Windows\System32\mfcsubs.dll
Opens: C:\Windows\System32\sxs.dll
Opens: C:\Windows\System32\eventcls.dll
Opens: C:\Windows\System32\stdole2.tlb
Opens: C:\Windows\System32\msxml3.dll
Opens: C:\Windows\System32\shlwapi.dll
Opens: C:\Windows\System32\en-US\KernelBase.dll.mui
Opens: C:\Windows\System32\msxml3r.dll
Opens: C:\Windows\System32\setupapi.dll
Opens: C:\Windows\System32\cfgmgr32.dll
Opens: C:\Windows\System32\devobj.dll
Opens: C:\Windows\System32\en-US\setupapi.dll.mui
Opens: C:\Windows\System32\wintrust.dll
Opens: C:\Windows\Prefetch\SVCHOST.EXE-80F4A784.pf
Opens: C:\Windows\System32\wersvc.dll
Opens: C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
Opens: C:\Windows\debug
Opens: C:\Windows\debug\WIA
Opens: C:\Windows\System32\wiaservc.dll
Opens: C:\Windows\System32\wiatrace.dll
Opens: C:\Windows\System32\msv1_0.dll
Opens: C:\Windows\System32\sti.dll
Opens: C:\Windows\debug\WIA\wiatrace.log
Opens: C:\Windows\System32\LogFiles\Scm\e5918cb5-cb06-4d74-80c7-8dd0399361c4
Opens: C:\Windows\System32\LogFiles\Scm\26c02f2c-5d20-44dd-b03f-e87f8ff3ea9b
Opens: C:\Windows\System32\Drivers\nwifi.sys
Opens: C:\Windows\apppatch\drvmain.sdb
Opens: C:\Windows\System32\Drivers\ndisuio.sys
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Adobe-Flash-For-Windows-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Common-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Guest-Integration-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Management-Clients-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Management-Clients-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package-net~31bf3856ad364e35~amd64~en-

US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\LogFiles\Scm\2b28902f-a99d-4568-8c8b-fee05f3984cc
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Server-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Server-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Media-Foundation-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Media-Foundation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Virtualization-Client-Interop-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-AvCore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-AvCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-

Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Shell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-AvCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-ClientCore-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-ClientCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Shell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Shell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Backup-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Backup-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package-minkernel~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package-minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Branding-Professional-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Branding-Professional-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Branding-ProfessionalWMC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Branding-ProfessionalWMC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package-admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-base~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-drivers~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-ds~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-multimedia~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-net~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-windows~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-avcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-com~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mergedcomponents~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mergedcomponents~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-mincore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mincore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-minio~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-multimedia~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-printscan~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-Client-Features-Package-termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ua~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-windows~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package-windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Client-Wired-Network-Drivers-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-COM-MSMQ-package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-base~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-base~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-drivers~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-ds~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-minio~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-minkernel~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-net~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-vm~31bf3856ad364e35~amd64~en-

US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
vm~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CommonFoundation-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Com-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-DS-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Net-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Net-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-DS-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Net-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Net-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package-
admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\microsoft-windows-directoryservices-adam-snapins-package-
admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\microsoft-windows-directoryservices-adam-snapins-package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Editions-Professional-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Editions-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Editions-ProfessionalWMC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Editions-ProfessionalWMC-

Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-FCI-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-FCI-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Foundation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-
admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-com~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
drivers~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
enduser~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-minio~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
minkernel~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
multimedia~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
windows~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-HandwritingRecognizer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-ProfessionalWMC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-ProfessionalWMC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ICM-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ICM-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Identity-Foundation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Identity-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-2-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-2-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-Base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
Base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~en-
US~10.0.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-
Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package~31bf3856ad364e35~amd64~en-
US~10.0.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-
Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Killbits-Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Links-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Links-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Streaming-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Streaming-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Multilingual-Package-windows~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Multilingual-Package-windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-AutoNgenEnable.3.5~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-NgenAssemblyExclusionClient~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Misc~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-MOF-Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-MOF-Extended~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-Extended~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Typelibs~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-HttpActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-HttpNamespace~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-MsmqActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-PipeActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-TcpActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-TcpPortSharing~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WPF-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WPF-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-VCRedist-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx-Windows-Built-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx2-OC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx2-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package-redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx3-WCF-OC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx3-WCF-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx4-US-OC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx4-US-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx4-WCF-US-OC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-NetFx4-WCF-US-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-OfflineFiles-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ParentalControls-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ParentalControls-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerDist-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerDist-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerToPeer-Full-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerToPeer-Full-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Personalization-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PlayToManager-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PlayToManager-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PowerShell-V2-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PowerShell-V2-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Presentation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Presentation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-LocalPrinting-Home-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-PremiumTools-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-PremiumTools-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-XPSServices-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-XPSServices-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ProfessionalEdition~31bf3856ad364e35~amd64~~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ProfessionalWMCEdition~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-PsuedoTool-HashIDSpy-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RasCMAK-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RasCMAK-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RDC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RDC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Redhawk-v1.0-package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RemoteAssistance-Package-Client~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RemoteAssistance-Package-Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RemoteDesktop-UserModeRDPProtocol-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RemoteDesktop-UserModeRDPProtocol-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RemoteFX-RemoteClient-Setup-LanguagePack~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RemoteFX-RemoteClient-Setup-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RotMgr-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-RotMgr-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-base~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-shell~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SecureStartup-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SecureStartup-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-APPXLOB-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-OCUR-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-Professional-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-ProfessionalWMC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ServicingBaseline-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat

Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package-printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package-printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-SoundThemes-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Shell-Wallpaper-Common-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-avcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-base~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-com~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-drivers~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-ds~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-enduser~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-mergedcomponents~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-mergedcomponents~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-mincore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-mincore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minio~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minkernel~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-multimedia~31bf3856ad364e35~amd64~en-

US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-net~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-sdktools~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-sdktools~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-shell~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-sql~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-sql~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-ua~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-windows~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SnippingTool-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SnippingTool-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SNMP-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SNMP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SpeechRecognizer-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-StorageService-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-StorageService-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Store-Client-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Store-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SystemRestore-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-SystemRestore-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TabletPC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-TabletPC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Telnet-Client-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Telnet-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-CommandLineTools-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-CommandLineTools-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-WMIProvider-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-WMIProvider-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TextPrediction-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TextPrediction-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualXP-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WebcamExperience-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WebcamExperience-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsFoundation-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinMDE-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinMDE-Package-avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinOcr-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinOcr-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinSATMediaFiles-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package-
avcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-

00C04FC295EE}\Networking-MPSSVC-Rules-BusinessEdition-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\nt5.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\ntexe.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\ntpe.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\ntph.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\oem0.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows-Defender-AM-Default-Definitions-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows-Defender-Group-Policy-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows-Defender-Group-Policy-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows-Defender-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
Opens: C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Windows-Defender-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
Writes to: C:\Windows\SysWOW64\output.txt
Writes to: C:\Windows\System32\MsDtc\Trace\dtctrace.log
Writes to: C:\Windows\System32\MsDtc\MSDTC.LOG
Writes to: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.lkg
Writes to: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\759cc9695d0b4f46f1829631c1525324_de228479-9e18-473a-b3d7-31d4d2573dc2
Writes to: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Writes to: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Reads from: C:\Windows\SysWOW64\output.txt
Reads from: C:\Windows\Prefetch\SVCHOST.EXE-C871F054.pf
Reads from: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst
Reads from: C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\PeerNetworking\idstore.sst.new
Reads from: C:\Windows\Prefetch\SPOOLSV.EXE-D1F6B8B6.pf
Reads from: C:\Windows\Prefetch\VSSVC.EXE-B8AFC319.pf
Reads from: C:\Windows\Prefetch\SVCHOST.EXE-80F4A784.pf
Reads from: C:\Windows\Prefetch\SVCHOST.EXE-61AE5AB6.pf
Reads from: C:\Windows\System32\LogFiles\Scm\e5918cb5-cb06-4d74-80c7-8dd0399361c4
Reads from: C:\Windows\System32\LogFiles\Scm\26c02f2c-5d20-44dd-b03f-e87f8ff3ea9b
Reads from: C:\Windows\System32\LogFiles\Scm\2b28902f-a99d-4568-8c8b-fee05f3984cc

Windows Registry Events

Creates key: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%12/8
Creates key: HKCU\software\classes\local settings\muicache\13\52c64b7e
Creates key: HKCU\software\classes\local settings\muicache
Creates key: HKLM\software\classes
Creates key: HKLM\system\currentcontrolset\services\vss\diag\registry writer
Creates key: HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer
Creates key: HKLM\system\currentcontrolset\services\vss\diag\asr writer
Creates key: HKLM\system\currentcontrolset\services\vss\diag\shadow copy optimization writer
Creates key: HKLM\system\currentcontrolset\control\stillimage\trace
Creates key: HKLM\system
Creates key: HKLM\system\currentcontrolset
Creates key: HKLM\system\currentcontrolset\control
Creates key: HKLM\system\currentcontrolset\control\stillimage
Creates key: HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll
Creates key: HKLM\system\currentcontrolset\services\nativewifip\parameters
Creates key: HKLM\system\currentcontrolset\services\nativewifip\parameters\adapters
Creates key: HKLM\system\currentcontrolset\services\nativewifip
Creates key: HKLM\system\currentcontrolset\services\ndisuio
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\conhost.exe
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
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\muicached

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
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\
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 nt\currentversion\console\truetypefont
Opens key: HKLM\software\microsoft\windows nt\currentversion\console\fullscreen
Opens key: HKCU\console
Opens key: HKCU\console\
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKCU\console\%systemroot%_temp_toggleservice32.exe
Opens key: HKCU\console\%systemroot%\temp\toggleservice32.exe
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation
Opens key: HKLM\software\microsoft\ctf\compatibility\conhost.exe
Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
Opens key: HKLM\software\wow6432node\microsoft\rpc
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
Opens key: HKLM\system\currentcontrolset\control\mui\settings
Opens key: HKLM\software\microsoft\rpc
Opens key: HKCU\software\classes\
Opens key: HKLM\software\classes
Opens key: HKLM\software\microsoft\com3
Opens key: HKLM\software\microsoft\windowsruntime\clsid
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{d6015ec3-fa16-4813-9ca1-
da204574f5da}
Opens key: HKCR\activatableclasses\clsid
Opens key: HKCR\activatableclasses\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\treatas
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprocserver32
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler32
Opens key: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}\inprochandler
Opens key: HKCR\appid\alg.exe
Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKCR\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{f8ade1d3-49df-4b75-9005-

ef9508e6a337}
Opens key: HKCR\activatableclasses\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337}
Opens key: HKCR\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337}
Opens key: HKCR\wow6432node\clsid\{f8ade1d3-49df-4b75-9005-ef9508e6a337}
Opens key: HKCU\software\classes\activatableclasses\clsid
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{3ceb5509-c1cd-432f-9d8f-
65d1e286aa80}
Opens key: HKCR\activatableclasses\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
Opens key: HKCR\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
Opens key: HKCR\wow6432node\clsid\{3ceb5509-c1cd-432f-9d8f-65d1e286aa80}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{7b3181a0-c92f-4567-b0fa-
cd9a10ecd7d1}
Opens key: HKCR\activatableclasses\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}
Opens key: HKCR\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}
Opens key: HKCR\wow6432node\clsid\{7b3181a0-c92f-4567-b0fa-cd9a10ecd7d1}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{d8a68e5e-2b37-426c-a329-
c117c14c429e}
Opens key: HKCR\activatableclasses\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
Opens key: HKCR\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
Opens key: HKCR\wow6432node\clsid\{d8a68e5e-2b37-426c-a329-c117c14c429e}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{bbb36f15-408d-4056-8c27-
920843d40be5}
Opens key: HKCR\activatableclasses\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
Opens key: HKCR\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
Opens key: HKCR\wow6432node\clsid\{bbb36f15-408d-4056-8c27-920843d40be5}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{6f9942c9-c1b1-4ab5-93da-
6058991dc8f3}
Opens key: HKCR\activatableclasses\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
Opens key: HKCR\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
Opens key: HKCR\wow6432node\clsid\{6f9942c9-c1b1-4ab5-93da-6058991dc8f3}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{bc9b54ab-7883-4c13-909f-
033d03267990}
Opens key: HKCR\activatableclasses\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}
Opens key: HKCR\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}
Opens key: HKCR\wow6432node\clsid\{bc9b54ab-7883-4c13-909f-033d03267990}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{6e590d61-f6bc-4dad-ac21-
7dc40d304059}
Opens key: HKCR\activatableclasses\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}
Opens key: HKCR\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}
Opens key: HKCR\wow6432node\clsid\{6e590d61-f6bc-4dad-ac21-7dc40d304059}
Opens key: HKLM\software\microsoft\alg\isv
Opens key: HKLM\software\microsoft\msdtc\tracing
Opens key: HKLM\software\microsoft\msdtc\tracing\sources
Opens key: HKLM\software\microsoft\msdtc\tracing\output
Opens key: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\misc
Opens key: HKLM\software\microsoft\msdtc
Opens key: HKCR\cid.local
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\description
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\svcid
Opens key: HKCR\svcid.local
Opens key: HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\host
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\clsid
Opens key: HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\protocol
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\endpoint
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\customproperties
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\customproperties\log
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-
0b84583f2fe1\customproperties\log\size
Opens key: HKLM\software\microsoft\msdtc\mtxoci
Opens key: HKLM\software\microsoft\msdtc\security
Opens key: HKLM\software\microsoft\windows nt\currentversion\asr\restoresession
Opens key: HKCR\cid.local\15546232-d044-45d4-88a8-
0b84583f2fe1\customproperties\log\path
Opens key: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions
Opens key: HKLM\system\currentcontrolset\control\minint
Opens key: HKLM\system\currentcontrolset\control\timezoneinformation
Opens key: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules
Opens key: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions
Opens key: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\changed
Opens key: HKLM\software\microsoft\windows nt\currentversion
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\description
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\svcid
Opens key: HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\host
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\clsid
Opens key: HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\protocol
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\endpoint
Opens key: HKCU\control panel\international
Opens key: HKLM\software\microsoft\rpc\securityservice
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\saslprofiles

Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\customproperties
Opens key: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\customproperties\dac
Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders
Opens key: HKCR\cid.local\4969ae2c-2c9c-4949-bb44-ca30dbe31bbc
Opens key: HKCR\cid.local\4969ae2c-2c9c-4949-bb44-ca30dbe31bbc\description
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\description
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\svcid
Opens key: HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e
Opens key: HKLM\system\currentcontrolset\services\keyiso
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\host
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\clsid
Opens key: HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\protocol
Opens key: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\endpoint
Opens key: HKLM\system\currentcontrolset\services\eaphost
Opens key: HKLM\system\currentcontrolset\services\msdtc
Opens key: HKLM\system\currentcontrolset\services\msdtc\startoverride
Opens key: HKLM\system\currentcontrolset\services\eaphost\startoverride
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
Opens key: HKCR\activatableclasses\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32
Opens key: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler
Opens key: HKLM\system\currentcontrolset\services\ui0detect
Opens key: HKLM\system\currentcontrolset\services\ui0detect\startoverride
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\system\currentcontrolset\control\session manager\environment
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKU\.default\environment
Opens key: HKU\.default\volatile environment
Opens key: HKU\.default\volatile environment\0
Opens key: HKLM\system\currentcontrolset\control\windows
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ui0detect.exe
Opens key: HKCU\software\microsoft\windows nt\currentversion
Opens key: HKU\.default\software\microsoft\windows nt\currentversion
Opens key: HKU\.default\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\ui0detect.exe
Opens key: HKU\.default\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKU\.default\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKU\.default\software\policies\microsoft\control panel\desktop
Opens key: HKU\.default\control panel\desktop\languageconfiguration
Opens key: HKU\.default\control panel\desktop
Opens key: HKU\.default\control panel\desktop\muicached
Opens key: HKLM\system\currentcontrolset\services\sharedaccess
Opens key: HKLM\system\currentcontrolset\services\sharedaccess\startoverride
Opens key: HKLM\system\currentcontrolset\services\pnrpsvc
Opens key: HKLM\system\currentcontrolset\services\pnrpsvc\startoverride
Opens key: HKLM\system\currentcontrolset\services\p2pimsvc
Opens key: HKLM\system\currentcontrolset\services\alluserinstallagent
Opens key: HKLM\system\currentcontrolset\services\appidsvc
Opens key: HKLM\system\currentcontrolset\services\appinfo
Opens key: HKLM\system\currentcontrolset\services\appmgmt
Opens key: HKLM\system\currentcontrolset\services\axinstsv
Opens key: HKLM\system\currentcontrolset\services\bdesvc
Opens key: HKLM\system\currentcontrolset\services\bits
Opens key: HKLM\system\currentcontrolset\services\bthserv
Opens key: HKLM\system\currentcontrolset\services\cscservice
Opens key: HKLM\system\currentcontrolset\services\deviceassociationservice
Opens key: HKLM\system\currentcontrolset\services\dnscache
Opens key: HKLM\system\currentcontrolset\services\dot3svc
Opens key: HKLM\system\currentcontrolset\services\dsmsvc
Opens key: HKLM\system\currentcontrolset\services\efs
Opens key: HKLM\system\currentcontrolset\services\eventlog
Opens key: HKLM\system\currentcontrolset\services\fdphost
Opens key: HKLM\system\currentcontrolset\services\fdrespub
Opens key: HKLM\system\currentcontrolset\services\fhsvc
Opens key: HKLM\system\currentcontrolset\services\hidserv
Opens key: HKLM\system\currentcontrolset\services\hkmsvc
Opens key: HKLM\system\currentcontrolset\services\homegrouplistener
Opens key: HKLM\system\currentcontrolset\services\homegroupprovider
Opens key: HKLM\system\currentcontrolset\services\ktmrm
Opens key: HKLM\system\currentcontrolset\services\lltdsvc
Opens key: HKLM\system\currentcontrolset\services\mpssvc
Opens key: HKLM\system\currentcontrolset\services\msiscsi
Opens key: HKLM\system\currentcontrolset\services\napagent
Opens key: HKLM\system\currentcontrolset\services\ncasvc

Opens key: HKLM\system\currentcontrolset\services\ncdautosetup
Opens key: HKLM\system\currentcontrolset\services\netlogon
Opens key: HKLM\system\currentcontrolset\services\netman
Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing
Opens key: HKLM\system\currentcontrolset\services\p2psvc
Opens key: HKLM\system\currentcontrolset\services\peerdistsvc
Opens key: HKLM\system\currentcontrolset\services\pla
Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg
Opens key: HKLM\system\currentcontrolset\services\printnotify
Opens key: HKLM\system\currentcontrolset\services\qwave
Opens key: HKLM\system\currentcontrolset\services\rasauto
Opens key: HKLM\system\currentcontrolset\services\rasman
Opens key: HKLM\system\currentcontrolset\services\remoteaccess
Opens key: HKLM\system\currentcontrolset\services\remoteregistry
Opens key: HKLM\system\currentcontrolset\services\scardsvr
Opens key: HKLM\system\currentcontrolset\services\scpolicysvc
Opens key: HKLM\system\currentcontrolset\services\seclogon
Opens key: HKLM\system\currentcontrolset\services\sensrsvc
Opens key: HKLM\system\currentcontrolset\services\sstpsvc
Opens key: HKLM\system\currentcontrolset\services\stornsvc
Opens key: HKLM\system\currentcontrolset\services\svsvc
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice
Opens key: HKLM\system\currentcontrolset\services\tapisrv
Opens key: HKLM\system\currentcontrolset\services\threadorder
Opens key: HKLM\system\currentcontrolset\services\upnphost
Opens key: HKLM\system\currentcontrolset\services\vaultsvc
Opens key: HKLM\system\currentcontrolset\services\vmicheartbeat
Opens key: HKLM\system\currentcontrolset\services\vmickvpexchange
Opens key: HKLM\system\currentcontrolset\services\vmicrdv
Opens key: HKLM\system\currentcontrolset\services\vmicshutdown
Opens key: HKLM\system\currentcontrolset\services\vmictimesync
Opens key: HKLM\system\currentcontrolset\services\vmicvss
Opens key: HKLM\system\currentcontrolset\services\w32time
Opens key: HKLM\system\currentcontrolset\services\wbiosrvc
Opens key: HKLM\system\currentcontrolset\services\wcncsvc
Opens key: HKLM\system\currentcontrolset\services\wcspluginservice
Opens key: HKLM\system\currentcontrolset\services\wdisystemhost
Opens key: HKLM\system\currentcontrolset\services\webclient
Opens key: HKLM\system\currentcontrolset\services\wecsvc
Opens key: HKLM\system\currentcontrolset\services\wercplsupport
Opens key: HKLM\system\currentcontrolset\services\wersvc
Opens key: HKLM\system\currentcontrolset\services\wiarpc
Opens key: HKLM\system\currentcontrolset\services\winrm
Opens key: HKLM\system\currentcontrolset\services\wlansvc
Opens key: HKLM\system\currentcontrolset\services\wlidsvc
Opens key: HKLM\system\currentcontrolset\services\wpcsvc
Opens key: HKLM\system\currentcontrolset\services\wscsvc
Opens key: HKLM\system\currentcontrolset\services\wsservice
Opens key: HKLM\system\currentcontrolset\services\wudfsvc
Opens key: HKLM\system\currentcontrolset\services\wwansvc
Opens key: HKU\s-1-5-19
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19
Opens key: HKU\s-1-5-19\software\microsoft\windows\currentversion\explorer\user
shell folders
Opens key: HKU\s-1-5-19\environment
Opens key: HKU\s-1-5-19\volatile environment
Opens key: HKU\s-1-5-19\volatile environment\0
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\svchost.exe
Opens key: HKLM\system\currentcontrolset\control\session manager\quota system\s-1-
5-19
Opens key: HKU\s-1-5-19\software\microsoft\windows nt\currentversion
Opens key: HKU\s-1-5-19\software\microsoft\windows
nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\svchost.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\svchost
Opens key: HKLM\software\microsoft\windows
nt\currentversion\svchost\localservicepeernet
Opens key:
HKLM\software\microsoft\windows\currentversion\diagnostics\perftrack\traceprofile
Opens key: HKLM\system\currentcontrolset\services
Opens key: HKLM\system\currentcontrolset\services\p2pimsvc\parameters
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key: HKLM\software\policies\microsoft\windows\system
Opens key: HKLM\software\policies\microsoft\peernet
Opens key: HKLM\system\currentcontrolset\services\pnrpsvc\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2c69d9f1-3a1fc5ac
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2c69d9f1
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64

Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a04231f6-42eb-4732-b850-
25b8d56dd1d8}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\software\microsoft\sqmclient
Opens key: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp
Opens key: HKLM\software\policies\microsoft\peernet\pnrp\ipv6-linklocal
Opens key: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal
Opens key: HKU\
Opens key: HKLM\system\currentcontrolset\services\crypt32
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: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdlldecodeobjectex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1

Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.12
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.2
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.3
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.4
Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa schannel cryptographic provider
Opens key: HKLM\software\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7
Opens key: HKLM\system\currentcontrolset\control\mui\stringcachesettings
Opens key: HKCU\software\classes\local settings\muicache\13\52c64b7e
Opens key: HKCU\software\classes\local settings\muicache
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.2!7
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.76.6.1!7
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllencodepublickeyandparameters
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodepublickeyandparameters
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllencodeobjectex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.1.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.1
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.11
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.12
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.2
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.3
Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1\cryptdllencodeobjectex\1.2.840.113549.1.9.16.2.4
Opens key: HKLM\system\currentcontrolset\services\plugplay
Opens key: HKLM\system\currentcontrolset\services\plugplay\startoverride
Opens key: HKLM\system\currentcontrolset\services\spooler
Opens key: HKLM\system\currentcontrolset\services\spooler\startoverride
Opens key: HKLM\system\currentcontrolset\services\http
Opens key: HKLM\system\currentcontrolset\services\dcomlaunch
Opens key: HKLM\system\currentcontrolset\services\rpceptmapper
Opens key: HKLM\system\currentcontrolset\services\rpcss
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe\perfoptions
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\spoolsv.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\system\currentcontrolset\services\rpcss\startoverride
Opens key: HKLM\system\currentcontrolset\control\print
Opens key: HKCR\clsid
Opens key: HKLM\software\policies\microsoft\windows nt\printers
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238528
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238528
Opens key: HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238784
Opens key: HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784
Opens key: HKLM\system\currentcontrolset\services\seclogon\startoverride
Opens key: HKLM\system\currentcontrolset\services\sens

Opens key: HKLM\system\currentcontrolset\services\sens\startoverride
Opens key: HKLM\system\currentcontrolset\services\eventsystem
Opens key: HKLM\system\currentcontrolset\services\sysmain
Opens key: HKLM\system\currentcontrolset\services\sysmain\startoverride
Opens key: HKLM\system\currentcontrolset\services\fltmgr
Opens key: HKLM\system\currentcontrolset\services\fileinfo
Opens key: HKLM\system\currentcontrolset\services\schedule
Opens key: HKLM\system\currentcontrolset\services\schedule\startoverride
Opens key: HKLM\system\currentcontrolset\control\diagnostics\performance
Opens key: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger
Opens key: HKLM\system\currentcontrolset\services\lmhosts
Opens key: HKLM\system\currentcontrolset\services\lmhosts\startoverride
Opens key: HKLM\system\currentcontrolset\services\afd
Opens key: HKLM\system\currentcontrolset\services\tcpip
Opens key: HKLM\system\currentcontrolset\services\tdx
Opens key: HKLM\system\currentcontrolset\services\netbt
Opens key: HKLM\system\currentcontrolset\services\vss
Opens key: HKLM\system\currentcontrolset\services\vss\startoverride
Opens key: HKLM\system\currentcontrolset\services\lmhosts\linkage
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\vssvc.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\vssvc.exe
Opens key: HKLM\system\currentcontrolset\services\vss\vssaccesscontrol
Opens key: HKCR\appid\vssvc.exe
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}
Opens key: HKCR\activatableclasses\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\treatas
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprocserver32
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler32
Opens key: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}\inprochandler
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
Opens key: HKCR\activatableclasses\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
Opens key: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}
Opens key: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\treatas
Opens key: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprocserver32
Opens key: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprochandler32
Opens key: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}\inprochandler
Opens key: HKLM\system\currentcontrolset\services\vss\settings
Opens key: HKLM\system\currentcontrolset\services\vss\diag
Opens key: HKLM\system\currentcontrolset\services\vss\diag\registry writer
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
Opens key: HKCR\activatableclasses\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\treatas
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler32
Opens key: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprochandler
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
Opens key: HKCR\activatableclasses\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\treatas
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprocserver32
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler32
Opens key: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler
Opens key: HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
Opens key: HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\proxystubclsid32
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
Opens key: HKCR\activatableclasses\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\treatas
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler32
Opens key: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler
Opens key: HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}
Opens key: HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
Opens key: HKCR\interface\{00000100-0000-0000-c000-000000000046}
Opens key: HKCR\interface\{00000100-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}
Opens key: HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}
Opens key: HKCR\activatableclasses\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}
Opens key: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}
Opens key: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\treatas
Opens key: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32
Opens key: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprochandler32
Opens key: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprochandler
Opens key: HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}
Opens key: HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32
Opens key: HKLM\system\currentcontrolset\services\vss\diag\com+ regdb writer
Opens key: HKLM\system\currentcontrolset\services\vss\diag\asr writer
Opens key: HKLM\system\currentcontrolset\services\vss\diag\shadow copy optimization

writer
Opens key:
HKLM\software\policies\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key:
HKCU\\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key: HKLM\software\microsoft\windows\currentversion\mmdevices\audio\render\
Opens key: HKLM\software\microsoft\windows\currentversion\mmdevices\audio\capture\
Opens key: HKLM\system\currentcontrolset\services\audiosrv
Opens key: HKLM\system\currentcontrolset\services\audiosrv\startoverride
Opens key: HKLM\system\currentcontrolset\services\mmcss
Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder
Opens key: HKLM\system\currentcontrolset\services\wersvc\startoverride
Opens key: HKLM\software\microsoft\windows\currentversion\audio
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{6994ad04-93ef-11d0-
a3cc-00a0c9223196}
Opens key: HKLM\software\microsoft\windows nt\currentversion\svchost\wersvcgroup
Opens key: HKU\.default\control panel\international
Opens key: HKLM\system\currentcontrolset\services\wersvc\parameters
Opens key: HKLM\software\microsoft\windows\windows error reporting
Opens key: HKLM\system\currentcontrolset\services\mpssvc\startoverride
Opens key: HKLM\system\currentcontrolset\services\stisvc
Opens key: HKLM\system\currentcontrolset\services\stisvc\startoverride
Opens key: HKLM\software\microsoft\windows nt\currentversion\svchost\imgsvc
Opens key: HKLM\system\currentcontrolset\services\stisvc\parameters
Opens key: HKLM\system\currentcontrolset\control\stillimage\trace
Opens key: HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll
Opens key: HKCR\appid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{a1f4e726-8cf1-11d1-bf92-
0060081ed811}
Opens key: HKCR\activatableclasses\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
Opens key: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}
Opens key: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\treatas
Opens key: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprocserver32
Opens key: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprochandler32
Opens key: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}\inprochandler
Opens key: HKLM\system\currentcontrolset\control\stillimage\fakedevices
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{6bdd1fc6-810f-11d0-
bec7-08002be2092f}
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{b6c292bc-7c88-41ee-8b54-
8ec92617e599}
Opens key: HKCR\activatableclasses\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\treatas
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprocserver32
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler32
Opens key: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}\inprochandler
Opens key: HKLM\software\microsoft\windowsruntime\clsid\{a1e75357-881a-419e-83e2-
bb16db197c68}
Opens key: HKCR\activatableclasses\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
Opens key: HKCR\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
Opens key: HKCR\wow6432node\clsid\{a1e75357-881a-419e-83e2-bb16db197c68}
Opens key: HKLM\system\currentcontrolset\control\stillimage\mscdevicelist
Opens key: HKLM\system\currentcontrolset\control\stillimage
Opens key: HKLM\system\currentcontrolset\control\stillimage\events
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\connected
Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\connected\{ee1ddf29-1c65-4ea6-b5cc-
6c15f82b5905}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\disconnected
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\emailimage
Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\faximage
Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\printimage
Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton
Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-
783ce7a92f22}
Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-
759eb35cdf9a}
Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-
7105fd3b53b1}
Opens key:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{ee1ddf29-1c65-4ea6-b5cc-
6c15f82b5905}
Opens key: HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent
Opens key: HKLM\system\currentcontrolset\control\stillimage\serversettings
Opens key: HKLM\system\currentcontrolset\services\w32time\startoverride

Opens key: HKLM\system\currentcontrolset\services\dnscache\startoverride
Opens key: HKLM\system\currentcontrolset\services\wuauserv
Opens key: HKLM\system\currentcontrolset\services\wuauserv\startoverride
Opens key: HKLM\system\currentcontrolset\services\wlansvc\startoverride
Opens key: HKLM\system\currentcontrolset\services\wcmsvc
Opens key: HKLM\system\currentcontrolset\services\ndisuio
Opens key: HKLM\system\currentcontrolset\services\nativewifip
Opens key: HKLM\system\currentcontrolset\services\nativewifip\parameters
Opens key: HKLM\system\currentcontrolset\services\nativewifip\filterdriverparams
Opens key: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi
Opens key: HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&1&18
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000
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\linkage
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0010\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\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\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\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\linkage
Opens key: HKLM\system\currentcontrolset\services\nnetsecl\parameters
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}
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}\0001
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}\0003
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}\0008
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}\0011
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0012
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\properties
Opens key: HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0004\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0000\linkage
Opens key: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000
Opens key: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-08002be10318}\0003\linkage
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\nls\sorting\versions[]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[conhost]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value: HKCU\console[screencolors]
Queries value: HKCU\console[popupcolors]
Queries value: HKCU\console[insertmode]
Queries value: HKCU\console[quickedit]
Queries value: HKCU\console[codepage]
Queries value: HKCU\console[screenbuffersize]
Queries value: HKCU\console[windowsize]
Queries value: HKCU\console[windowposition]
Queries value: HKCU\console[fontsize]
Queries value: HKCU\console[fontfamily]

Queries value: HKCU\console[fontweight]
Queries value: HKCU\console[facename]
Queries value: HKCU\console[cursorsize]
Queries value: HKCU\console[historybuffersize]
Queries value: HKCU\console[numberofhistorybuffers]
Queries value: HKCU\console[historynodup]
Queries value: HKCU\console[colortable00]
Queries value: HKCU\console[colortable01]
Queries value: HKCU\console[colortable02]
Queries value: HKCU\console[colortable03]
Queries value: HKCU\console[colortable04]
Queries value: HKCU\console[colortable05]
Queries value: HKCU\console[colortable06]
Queries value: HKCU\console[colortable07]
Queries value: HKCU\console[colortable08]
Queries value: HKCU\console[colortable09]
Queries value: HKCU\console[colortable10]
Queries value: HKCU\console[colortable11]
Queries value: HKCU\console[colortable12]
Queries value: HKCU\console[colortable13]
Queries value: HKCU\console[colortable14]
Queries value: HKCU\console[colortable15]
Queries value: HKCU\console[loadconime]
Queries value: HKCU\console[extendededitkey]
Queries value: HKCU\console[extendededitkeycustom]
Queries value: HKCU\console[worddelimiters]
Queries value: HKCU\console[trimleadingzeros]
Queries value: HKCU\console[enablecolorselection]
Queries value: HKCU\console[scrollscale]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[toggleservice32.exe]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\software\microsoft\rpc[idletimerwindow]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value: HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages]
Queries value: HKLM\software\microsoft\com3[com+enabled]
Queries value: HKCR\clsid\{d6015ec3-fa16-4813-9ca1-da204574f5da}[]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[alg]
Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[msdtc]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_misc]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_cm]

Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_trace]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_svc]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_gateway]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_ui]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_contact]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_util]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_cluster]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_resource]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_tip]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_xa]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_log]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_mtxoci]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_etwtrace]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_proxy]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_ktmrm]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_vssbackup]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_perfmon]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_tm]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_lu]
Queries value: HKLM\software\microsoft\msdtc\tracing\sources[trace_wmi]
Queries value: HKLM\software\microsoft\msdtc\tracing\output[tracefilepath]
Queries value: HKLM\software\microsoft\msdtc\tracing\output[memorybuffersize]
Queries value: HKLM\software\microsoft\msdtc\tracing\output[debugoutenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\misc[disabletracing]
Queries value: HKLM\software\microsoft\msdtc[noparallellogflushnotification]
Queries value: HKLM\software\microsoft\msdtc[snapshotprefertransactionstimeoutduringbackup]
Queries value: HKLM\software\microsoft\msdtc[turnoffbadmsgevents]
Queries value: HKLM\software\microsoft\msdtc[disableterminationonheapcorruption]
Queries value: HKLM\software\microsoft\msdtc[sysprepinprogress]
Queries value: HKLM\software\microsoft\msdtc[maxrecoverytimepermbinminutes]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\description[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\svcid[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\host[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\clsid[]
Queries value: HKCR\svcid.local\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\protocol[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\endpoint[]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\customproperties\log\size[]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oraclexalibpath]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oraclesqllibpath]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oracleocilibpath]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oraclexalib]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oraclesqllib]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oracleocilib]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[mtxocicptimeout]
Queries value: HKLM\software\microsoft\msdtc\mtxoci[oracletracefilepath]
Queries value: HKLM\software\microsoft\msdtc\security[accountname]
Queries value: HKLM\software\microsoft\msdtc\security[networkdtcaccess]
Queries value: HKLM\software\microsoft\msdtc\security[networkdtcaccessadmin]
Queries value: HKLM\software\microsoft\msdtc\security[networkdtcaccessclients]
Queries value: HKLM\software\microsoft\msdtc\security[networkdtcaccesstransactions]
Queries value: HKLM\software\microsoft\msdtc\security[networkdtcaccesstip]
Queries value: HKLM\software\microsoft\msdtc[allowonlysecurerpccalls]
Queries value: HKLM\software\microsoft\msdtc\security[xatransactions]
Queries value: HKLM\software\microsoft\msdtc\security[lutransactions]
Queries value: HKCR\cid.local\15546232-d044-45d4-88a8-0b84583f2fe1\customproperties\log\path[]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[1b1d4ff4-f27b-4c99-8bd7-da8f1a74051a]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\loggingoptions[requestsessionup]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\loggingoptions[maxbuffers]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\loggingoptions[minbuffers]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\loggingoptions[buffersize]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\loggingoptions[maxfilesize]
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\timezoneinformation[daylightstart]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules[uniqueid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules[active]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules[level]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules[controlflags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules\transaction_transitions[uniqueid]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\tracing\msdtc\modules\transaction_transitions[active]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[level]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[controlflags]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[e80aa9fe-913d-4ede-
af58-73e332dcac8d]
Queries value: HKLM\software\microsoft\msdtc[dtcmaxsessions]
Queries value: HKLM\software\microsoft\msdtc[donotgoidle]
Queries value: HKLM\software\microsoft\msdtc[disabletippassthrucheck]
Queries value: HKLM\software\microsoft\msdtc[mincheckpointinterval]
Queries value: HKLM\software\microsoft\msdtc[maxcheckpointinterval]
Queries value: HKLM\software\microsoft\msdtc[waitforallxabranchprepares]
Queries value: HKLM\software\microsoft\msdtc\security[snapshotsecuritydisabled]
Queries value: HKLM\software\microsoft\msdtc[servertcpport]
Queries value: HKLM\software\microsoft\windows nt\currentversion[currentversion]
Queries value: HKLM\software\microsoft\msdtc[cmcancelrpcafter]
Queries value: HKLM\software\microsoft\msdtc[cmmaxnumberbindretries]
Queries value: HKLM\software\microsoft\msdtc[cmmaxidlepings]
Queries value: HKLM\software\microsoft\msdtc[cmpingfreqsecs]
Queries value: HKLM\software\microsoft\msdtc[cmverbose]
Queries value: HKLM\software\microsoft\msdtc[rpcqoscapabilities]
Queries value: HKLM\software\microsoft\msdtc[rpcqosidentity]
Queries value: HKLM\software\microsoft\msdtc[rpcauthnsvc]
Queries value: HKLM\software\microsoft\msdtc[numcccimhistoryentries]
Queries value: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\description[]
Queries value: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\svcid[]
Queries value: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\host[]
Queries value: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\clsid[]
Queries value: HKCR\svcid.local\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
Queries value: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\protocol[]
Queries value: HKCR\cid.local\4452c425-ad2f-4cde-b895-734b166ac4ac\endpoint[]
Queries value: HKCU\control panel\international[scurrencyoverride]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
Queries value: HKLM\software\microsoft\msdtc[notracking]
Queries value: HKLM\software\microsoft\rpc\securityservice[9]
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]
Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
Queries value: HKLM\software\microsoft\msdtc[shared_memory_mutex_timeout]
Queries value: HKCR\cid.local\4969ae2c-2c9c-4949-bb44-ca30dbe31bbc\description[]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\description[]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\svcid[]
Queries value: HKLM\system\currentcontrolset\services\keyiso[objectname]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\host[]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\clsid[]
Queries value: HKCR\svcid.local\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider[]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\protocol[]
Queries value: HKLM\system\currentcontrolset\services\eaphost[imagepath]
Queries value: HKLM\system\currentcontrolset\services\eaphost[wow64]
Queries value: HKLM\system\currentcontrolset\services\eaphost[objectname]
Queries value: HKLM\system\currentcontrolset\services\eaphost[requiredprivileges]
Queries value: HKCR\cid.local\4f8239c2-5d61-4676-ba28-72bcfe3172ab\endpoint[]
Queries value: HKLM\software\microsoft\msdtc[xatmminwarmrecoveryinterval]
Queries value: HKLM\software\microsoft\msdtc[xatmmaxwarmrecoveryinterval]
Queries value: HKLM\system\currentcontrolset\services\msdtc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\msdtc[type]
Queries value: HKLM\system\currentcontrolset\services\msdtc[start]
Queries value: HKLM\system\currentcontrolset\services\msdtc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\msdtc[tag]
Queries value: HKLM\system\currentcontrolset\services\msdtc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\msdtc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\msdtc[group]
Queries value: HKLM\system\currentcontrolset\services\msdtc[objectname]
Queries value: HKLM\software\microsoft\msdtc[transactionbridge]
Queries value: HKLM\software\microsoft\msdtc[logwarnenabled]
Queries value: HKLM\system\currentcontrolset\services\eaphost[type]
Queries value: HKLM\system\currentcontrolset\services\eaphost[start]
Queries value: HKLM\system\currentcontrolset\services\eaphost[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\eaphost[tag]
Queries value: HKLM\system\currentcontrolset\services\eaphost[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\eaphost[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\eaphost[group]
Queries value: HKLM\software\microsoft\msdtc[suppressduplicateduration]
Queries value: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[]
Queries value: HKCR\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[]
Queries value: HKCR\clsid\{304ce942-6e39-40d8-943a-

b913c40c9cd4}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value: HKLM\software\microsoft\msdtc[supportns]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[type]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[start]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[tag]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[group]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[objectname]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[wow64]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[requiredprivileges]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[public]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)]
Queries value: HKLM\software\microsoft\windows\currentversion[programw6432dir]
Queries value: HKLM\software\microsoft\windows\currentversion[commonw6432dir]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
18[profileimagepath]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
Queries value: HKLM\system\currentcontrolset\services\ui0detect[environment]
Queries value: HKLM\system\currentcontrolset\control\windows[nointeractiveservices]
Queries value: HKU\.default\control panel\desktop[preferreduilanguages]
Queries value: HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[ui0detect]
Queries value: HKLM\system\currentcontrolset\services\sharedaccess[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sharedaccess[type]
Queries value: HKLM\system\currentcontrolset\services\sharedaccess[start]
Queries value: HKLM\system\currentcontrolset\services\sharedaccess[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\sharedaccess[tag]
Queries value: HKLM\system\currentcontrolset\services\sharedaccess[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\sharedaccess[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\sharedaccess[group]
Queries value: HKLM\system\currentcontrolset\services\sharedaccess[objectname]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[type]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[start]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[group]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\alluserinstallagent[imagepath]
Queries value: HKLM\system\currentcontrolset\services\alluserinstallagent[wow64]
Queries value: HKLM\system\currentcontrolset\services\appidsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\appidsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\appinfo[imagepath]
Queries value: HKLM\system\currentcontrolset\services\appinfo[wow64]
Queries value: HKLM\system\currentcontrolset\services\appmgmt[imagepath]
Queries value: HKLM\system\currentcontrolset\services\appmgmt[wow64]
Queries value: HKLM\system\currentcontrolset\services\axinstsv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\axinstsv[wow64]
Queries value: HKLM\system\currentcontrolset\services\bdesvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\bdesvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\bits[imagepath]
Queries value: HKLM\system\currentcontrolset\services\bits[wow64]
Queries value: HKLM\system\currentcontrolset\services\bthserv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\bthserv[wow64]
Queries value: HKLM\system\currentcontrolset\services\cscservice[imagepath]
Queries value: HKLM\system\currentcontrolset\services\cscservice[wow64]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice[imagepath]
Queries value: HKLM\system\currentcontrolset\services\deviceassociationservice[wow64]
Queries value: HKLM\system\currentcontrolset\services\dnscache[imagepath]
Queries value: HKLM\system\currentcontrolset\services\dnscache[wow64]
Queries value: HKLM\system\currentcontrolset\services\dot3svc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\dot3svc[wow64]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\efs[imagepath]
Queries value: HKLM\system\currentcontrolset\services\efs[wow64]
Queries value: HKLM\system\currentcontrolset\services\eventlog[imagepath]
Queries value: HKLM\system\currentcontrolset\services\eventlog[wow64]
Queries value: HKLM\system\currentcontrolset\services\fdphost[imagepath]

Queries value: HKLM\system\currentcontrolset\services\fdphost[wow64]
Queries value: HKLM\system\currentcontrolset\services\fdrespub[imagepath]
Queries value: HKLM\system\currentcontrolset\services\fdrespub[wow64]
Queries value: HKLM\system\currentcontrolset\services\fhsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\fhsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\hidserv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\hidserv[wow64]
Queries value: HKLM\system\currentcontrolset\services\hkmsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\hkmsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\homegrouplistener[imagepath]
Queries value: HKLM\system\currentcontrolset\services\homegrouplistener[wow64]
Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[imagepath]
Queries value: HKLM\system\currentcontrolset\services\homegroupprovider[wow64]
Queries value: HKLM\system\currentcontrolset\services\ktmrm[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ktmrm[wow64]
Queries value: HKLM\system\currentcontrolset\services\lltdsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\lltdsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\mpssvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\mpssvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\msiscsi[imagepath]
Queries value: HKLM\system\currentcontrolset\services\msiscsi[wow64]
Queries value: HKLM\system\currentcontrolset\services\napagent[imagepath]
Queries value: HKLM\system\currentcontrolset\services\napagent[wow64]
Queries value: HKLM\system\currentcontrolset\services\ncasvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ncasvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\ncdautosetup[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ncdautosetup[wow64]
Queries value: HKLM\system\currentcontrolset\services\netlogon[imagepath]
Queries value: HKLM\system\currentcontrolset\services\netlogon[wow64]
Queries value: HKLM\system\currentcontrolset\services\netman[imagepath]
Queries value: HKLM\system\currentcontrolset\services\netman[wow64]
Queries value: HKLM\system\currentcontrolset\services\nettcpportsharing[imagepath]
Queries value: HKLM\system\currentcontrolset\services\nettcpportsharing[wow64]
Queries value: HKLM\system\currentcontrolset\services\p2psvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\p2psvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\peerdistsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\pla[imagepath]
Queries value: HKLM\system\currentcontrolset\services\pla[wow64]
Queries value: HKLM\system\currentcontrolset\services\pnrpautoreg[imagepath]
Queries value: HKLM\system\currentcontrolset\services\pnrpautoreg[wow64]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\printnotify[imagepath]
Queries value: HKLM\system\currentcontrolset\services\printnotify[wow64]
Queries value: HKLM\system\currentcontrolset\services\qwave[imagepath]
Queries value: HKLM\system\currentcontrolset\services\qwave[wow64]
Queries value: HKLM\system\currentcontrolset\services\rasauto[imagepath]
Queries value: HKLM\system\currentcontrolset\services\rasauto[wow64]
Queries value: HKLM\system\currentcontrolset\services\rasman[imagepath]
Queries value: HKLM\system\currentcontrolset\services\rasman[wow64]
Queries value: HKLM\system\currentcontrolset\services\remoteaccess[imagepath]
Queries value: HKLM\system\currentcontrolset\services\remoteaccess[wow64]
Queries value: HKLM\system\currentcontrolset\services\remoteregistry[imagepath]
Queries value: HKLM\system\currentcontrolset\services\remoteregistry[wow64]
Queries value: HKLM\system\currentcontrolset\services\scardsvr[imagepath]
Queries value: HKLM\system\currentcontrolset\services\scardsvr[wow64]
Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\scpolicysvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\seclogon[imagepath]
Queries value: HKLM\system\currentcontrolset\services\seclogon[wow64]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\sharedaccess[wow64]
Queries value: HKLM\system\currentcontrolset\services\sstpsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sstpsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\storsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\storsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\svsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\svsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[imagepath]
Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[wow64]
Queries value: HKLM\system\currentcontrolset\services\tapisrv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\tapisrv[wow64]
Queries value: HKLM\system\currentcontrolset\services\threadorder[imagepath]
Queries value: HKLM\system\currentcontrolset\services\threadorder[wow64]
Queries value: HKLM\system\currentcontrolset\services\upnphost[imagepath]
Queries value: HKLM\system\currentcontrolset\services\upnphost[wow64]
Queries value: HKLM\system\currentcontrolset\services\vaultsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\vaultsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\vmicheartbeat[imagepath]
Queries value: HKLM\system\currentcontrolset\services\vmicheartbeat[wow64]
Queries value: HKLM\system\currentcontrolset\services\vmickvpexchange[imagepath]
Queries value: HKLM\system\currentcontrolset\services\vmickvpexchange[wow64]
Queries value: HKLM\system\currentcontrolset\services\vmicrdv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\vmicrdv[wow64]
Queries value: HKLM\system\currentcontrolset\services\vmicshutdown[imagepath]
Queries value: HKLM\system\currentcontrolset\services\vmicshutdown[wow64]
Queries value: HKLM\system\currentcontrolset\services\vmictimesync[imagepath]
Queries value: HKLM\system\currentcontrolset\services\vmictimesync[wow64]
Queries value: HKLM\system\currentcontrolset\services\vmicvss[imagepath]

Queries value: HKLM\system\currentcontrolset\services\vmicvss[wow64]
Queries value: HKLM\system\currentcontrolset\services\w32time[imagepath]
Queries value: HKLM\system\currentcontrolset\services\w32time[wow64]
Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\wcncsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wcncsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[wow64]
Queries value: HKLM\system\currentcontrolset\services\wdisystemhost[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wdisystemhost[wow64]
Queries value: HKLM\system\currentcontrolset\services\webclient[imagepath]
Queries value: HKLM\system\currentcontrolset\services\webclient[wow64]
Queries value: HKLM\system\currentcontrolset\services\wecsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wecsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\wercplsupport[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wercplsupport[wow64]
Queries value: HKLM\system\currentcontrolset\services\wersvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wersvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\wiarpc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wiarpc[wow64]
Queries value: HKLM\system\currentcontrolset\services\winrm[imagepath]
Queries value: HKLM\system\currentcontrolset\services\winrm[wow64]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\wpcsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wpcsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wscsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\wsservice[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wsservice[wow64]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\wwansvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wwansvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\p2psvc[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\pnrpautoreg[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc[requiredprivileges]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19[profileimagepath]
Queries value: HKU\s-1-5-19\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKU\s-1-5-19\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[environment]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc[startprotected]
Queries value: HKLM\software\microsoft\windows nt\currentversion\svchost[localservicepeernet]
Queries value: HKLM\software\microsoft\windows\currentversion\diagnostics\perftrack\traceprofile[svchost]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedll]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicemain]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\policies\microsoft\windows\system[gpsvcdebuglevel]
Queries value: HKLM\software\policies\microsoft\peernet[disabled]
Queries value: HKLM\system\currentcontrolset\services\p2pimsvc\parameters[servicedllunloadonstop]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedll]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicemain]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[seedserver]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
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_entries64]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[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_entries64]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerid]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
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\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpv6domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpdomain]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[svchost]
Queries value: HKLM\software\microsoft\sqmclient[machineid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[seedserver]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[disablemulticastpublish]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[disablemulticastsearch]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[disabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-
linklocal\linklocal_ff00::%12/8[searchonly]

Queries value: HKLM\software\microsoft\windows nt\currentversion\peernet\pnrp\ipv6-linklocal\linklocal_ff00::%12/8[mincpalifetime]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa schannel cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa schannel cryptographic provider[image path]
Queries value: HKLM\software\policies\microsoft\cryptography[forcekeyprotection]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.47.1.1!7[name]
Queries value: HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.64.1.1!7[name]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.1!7[name]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.67.1.2!7[name]
Queries value: HKLM\software\microsoft\cryptography\oid\encodingtype 0\cryptdllfindoidinfo\1.3.6.1.4.1.311.76.6.1!7[name]
Queries value: HKLM\system\currentcontrolset\services\pnrpsvc\parameters[servicedllunloadonstop]
Queries value: HKLM\system\currentcontrolset\services\plugplay[imagepath]
Queries value: HKLM\system\currentcontrolset\services\plugplay[type]
Queries value: HKLM\system\currentcontrolset\services\plugplay[start]
Queries value: HKLM\system\currentcontrolset\services\plugplay[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\plugplay[tag]
Queries value: HKLM\system\currentcontrolset\services\plugplay[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\plugplay[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\plugplay[group]
Queries value: HKLM\system\currentcontrolset\services\plugplay[objectname]
Queries value: HKLM\system\currentcontrolset\services\plugplay[wow64]
Queries value: HKLM\system\currentcontrolset\services\spooler[imagepath]
Queries value: HKLM\system\currentcontrolset\services\spooler[type]
Queries value: HKLM\system\currentcontrolset\services\spooler[start]
Queries value: HKLM\system\currentcontrolset\services\spooler[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\spooler[tag]
Queries value: HKLM\system\currentcontrolset\services\spooler[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\spooler[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\spooler[group]
Queries value: HKLM\system\currentcontrolset\services\spooler[objectname]
Queries value: HKLM\system\currentcontrolset\services\http[objectname]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[objectname]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[objectname]
Queries value: HKLM\system\currentcontrolset\services\rpcss[objectname]
Queries value: HKLM\system\currentcontrolset\services\spooler[wow64]
Queries value: HKLM\system\currentcontrolset\services\spooler[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\spooler[environment]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[debugger]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[uselargepages]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[nodeoptions]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[disablewakecharge]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[mitigationoptions]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[disableheaplookaside]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[frontendheapdebugoptions]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[shutdownflags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[unloadeventtracedepth]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[tracingflags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[minimumstackcommitinbytes]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[breakoninitializeprocessfailure]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[keepactivationcontextsalive]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[trackactivationcontextreleases]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[maxdeadactivationcontexts]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[globalflag]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[cwdillegalindllsearch]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[debugprocessheaponly]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\spoolsv.exe[searchpathmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[spoolsv]
Queries value: HKLM\system\currentcontrolset\services\rpcss[imagepath]
Queries value: HKLM\system\currentcontrolset\services\rpcss[type]
Queries value: HKLM\system\currentcontrolset\services\rpcss[start]
Queries value: HKLM\system\currentcontrolset\services\rpcss[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\rpcss[tag]
Queries value: HKLM\system\currentcontrolset\services\rpcss[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\rpcss[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\rpcss[group]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[d2e1bab2-eb9b-4ba7-9123-19c01ddc4f78]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[c9bf4a9e-d547-4d11-8242-e03a18b5be01]
Queries value: HKLM\system\currentcontrolset\control\print[exceptionhandlerenabled]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[b1ad9b49-051a-4896-ae24-ebc9b8676e76]
Queries value: HKLM\system\currentcontrolset\control\print[threadnotifymax]
Queries value: HKLM\system\currentcontrolset\control\print[threadnotifyidlelife]
Queries value: HKLM\system\currentcontrolset\control\print[threadnotifysleep]
Queries value: HKLM\system\currentcontrolset\control\print[maxrpcsize]
Queries value: HKLM\system\currentcontrolset\control\print[maxrpccalls]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[71e8376c]
Queries value: HKLM\software\microsoft\sqmclient\windows[studyid]
Queries value: HKLM\software\microsoft\telemetryclient\samplestore\sqm[sampledout]
Queries value: HKLM\system\currentcontrolset\control\print[callexitprocessonshutdown]
Queries value: HKLM\system\currentcontrolset\services\seclogon[type]
Queries value: HKLM\system\currentcontrolset\services\seclogon[start]
Queries value: HKLM\system\currentcontrolset\services\seclogon[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\seclogon[tag]
Queries value: HKLM\system\currentcontrolset\services\seclogon[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\seclogon[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\seclogon[group]
Queries value: HKLM\system\currentcontrolset\services\seclogon[objectname]
Queries value: HKLM\system\currentcontrolset\services\seclogon[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\sens[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sens[type]
Queries value: HKLM\system\currentcontrolset\services\sens[start]
Queries value: HKLM\system\currentcontrolset\services\sens[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\sens[tag]
Queries value: HKLM\system\currentcontrolset\services\sens[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\sens[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\sens[group]
Queries value: HKLM\system\currentcontrolset\services\sens[objectname]
Queries value: HKLM\system\currentcontrolset\services\eventsystem[objectname]
Queries value: HKLM\system\currentcontrolset\services\sens[wow64]
Queries value: HKLM\system\currentcontrolset\services\sens[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\sysmain[imagepath]
Queries value: HKLM\system\currentcontrolset\services\sysmain[type]
Queries value: HKLM\system\currentcontrolset\services\sysmain[start]
Queries value: HKLM\system\currentcontrolset\services\sysmain[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\sysmain[tag]
Queries value: HKLM\system\currentcontrolset\services\sysmain[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\sysmain[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\sysmain[group]
Queries value: HKLM\system\currentcontrolset\services\sysmain[objectname]
Queries value: HKLM\system\currentcontrolset\services\fltmgr[objectname]
Queries value: HKLM\system\currentcontrolset\services\fileinfo[objectname]
Queries value: HKLM\system\currentcontrolset\services\sysmain[wow64]
Queries value: HKLM\system\currentcontrolset\services\sysmain[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\schedule[imagepath]
Queries value: HKLM\system\currentcontrolset\services\schedule[type]
Queries value: HKLM\system\currentcontrolset\services\schedule[start]
Queries value: HKLM\system\currentcontrolset\services\schedule[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\schedule[tag]
Queries value: HKLM\system\currentcontrolset\services\schedule[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\schedule[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\schedule[group]
Queries value: HKLM\system\currentcontrolset\services\schedule[objectname]
Queries value: HKLM\system\currentcontrolset\control\diagnostics\performance[disablediagnostictracing]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[start]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[flushthreshold]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[buffersize]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[minimumbuffers]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[flushtimer]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[maximumbuffers]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[filename]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel

context logger[enablekernelflags]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[stackwalkingfilter]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[clocktype]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[maxfilesize]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[logfilemode]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[disablerealtimepersistence]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[guid]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[filecounter]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[filemax]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[pooltagfilter]
Queries value: HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel
context logger[stackcaching]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[54dea73a-ed1f-42a4-
af71-3e63d056f174]
Queries value: HKLM\system\currentcontrolset\services\lmhosts[imagepath]
Queries value: HKLM\system\currentcontrolset\services\lmhosts[type]
Queries value: HKLM\system\currentcontrolset\services\lmhosts[start]
Queries value: HKLM\system\currentcontrolset\services\lmhosts[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\lmhosts[tag]
Queries value: HKLM\system\currentcontrolset\services\lmhosts[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\lmhosts[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\lmhosts[group]
Queries value: HKLM\system\currentcontrolset\services\lmhosts[objectname]
Queries value: HKLM\system\currentcontrolset\services\afd[objectname]
Queries value: HKLM\system\currentcontrolset\services\tcpip[objectname]
Queries value: HKLM\system\currentcontrolset\services\tdx[objectname]
Queries value: HKLM\system\currentcontrolset\services\netbt[objectname]
Queries value: HKLM\system\currentcontrolset\services\lmhosts[wow64]
Queries value: HKLM\system\currentcontrolset\services\lmhosts[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\vss[imagepath]
Queries value: HKLM\system\currentcontrolset\services\vss[type]
Queries value: HKLM\system\currentcontrolset\services\vss[start]
Queries value: HKLM\system\currentcontrolset\services\vss[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\vss[tag]
Queries value: HKLM\system\currentcontrolset\services\vss[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\vss[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\vss[group]
Queries value: HKLM\system\currentcontrolset\services\vss[objectname]
Queries value: HKLM\system\currentcontrolset\services\vss[wow64]
Queries value: HKLM\system\currentcontrolset\services\vss[environment]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[e14dcdd9-d1ec-4dc3-
8395-a606df8ef115]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[4d20df22-e177-4514-
a369-f1759feedeb3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[vssvc]
Queries value: HKLM\software\microsoft\com3[finalizeractivitybypass]
Queries value: HKCR\clsid\{e579ab5f-1cc4-44b4-bed9-de0991ff0623}[]
Queries value: HKCR\clsid\{0b5a2c52-3eb9-470a-96e2-6c6d4570e40f}[]
Queries value: HKLM\system\currentcontrolset\services\vss\settings[idletimeout]
Queries value: HKLM\system\setup[upgradeinprogress]
Queries value:
HKLM\system\currentcontrolset\services\vss\settings[activewriterstatetimeout]
Queries value: HKLM\system\currentcontrolset\services\vss\diag[]
Queries value: HKLM\system\currentcontrolset\services\vss\settings[torncomponentsmax]
Queries value: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}[]
Queries value: HKCR\clsid\{4e14fba2-2e22-11d1-9964-
00c04fbbb345}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{4e14fba2-2e22-11d1-9964-00c04fbbb345}\inprocserver32[]
Queries value: HKCR\clsid\{4e14fba2-2e22-11d1-9964-
00c04fbbb345}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}[]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKCR\interface\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\proxystubclsid32[]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}[]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
00c04fb926af}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32[]
Queries value: HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
00c04fb926af}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{609b954b-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
Queries value: HKCR\interface\{00000100-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKCR\interface\{609b9555-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
Queries value: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}[]
Queries value: HKCR\clsid\{7542e960-79c7-11d1-88f9-
0080c7d771bf}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{7542e960-79c7-11d1-88f9-0080c7d771bf}\inprocserver32[]
Queries value: HKCR\clsid\{7542e960-79c7-11d1-88f9-
0080c7d771bf}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{609b9557-4fb6-11d1-9971-00c04fbbb345}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\windows[displayversion]

Queries value: HKCU\control panel\desktop[paintdesktopversion]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[type]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[start]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[tag]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[group]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[objectname]
Queries value: HKLM\system\currentcontrolset\services\mmcss[objectname]
Queries value: HKLM\system\currentcontrolset\services\audioendpointbuilder[objectname]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[wow64]
Queries value: HKLM\system\currentcontrolset\services\audiosrv[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\wersvc[type]
Queries value: HKLM\system\currentcontrolset\services\wersvc[start]
Queries value: HKLM\system\currentcontrolset\services\wersvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wersvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wersvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wersvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wersvc[group]
Queries value: HKLM\system\currentcontrolset\services\wersvc[objectname]
Queries value:
HKLM\software\microsoft\windows\currentversion\audio[enablecapturemonitor]
Queries value: HKLM\system\currentcontrolset\services\wersvc[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\wersvc[environment]
Queries value: HKLM\software\microsoft\windows nt\currentversion\svchost[wersvcgroup]
Queries value: HKU\.default\control panel\international[scurrencyoverride]
Queries value: HKLM\system\currentcontrolset\services\wersvc\parameters[servicedll]
Queries value:
HKLM\system\currentcontrolset\services\wersvc\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\wersvc\parameters[servicemain]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[6851adeb-79da-4250-
a440-f1f52d28711d]
Queries value: HKLM\software\microsoft\windows\windows error reporting[servicetimeout]
Queries value:
HKLM\system\currentcontrolset\services\wersvc\parameters[servicedllunloadonstop]
Queries value: HKLM\system\currentcontrolset\services\mpssvc[type]
Queries value: HKLM\system\currentcontrolset\services\mpssvc[start]
Queries value: HKLM\system\currentcontrolset\services\mpssvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\mpssvc[tag]
Queries value: HKLM\system\currentcontrolset\services\mpssvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\mpssvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\mpssvc[group]
Queries value: HKLM\system\currentcontrolset\services\mpssvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\stisvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\stisvc[type]
Queries value: HKLM\system\currentcontrolset\services\stisvc[start]
Queries value: HKLM\system\currentcontrolset\services\stisvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\stisvc[tag]
Queries value: HKLM\system\currentcontrolset\services\stisvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\stisvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\stisvc[group]
Queries value: HKLM\system\currentcontrolset\services\stisvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\stisvc[wow64]
Queries value: HKLM\system\currentcontrolset\services\stisvc[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\stisvc[environment]
Queries value: HKLM\system\currentcontrolset\services\stisvc[startprotected]
Queries value: HKLM\software\microsoft\windows nt\currentversion\svchost[imgsvc]
Queries value: HKLM\system\currentcontrolset\services\stisvc\parameters[servicedll]
Queries value:
HKLM\system\currentcontrolset\services\stisvc\parameters[servicemanifest]
Queries value: HKLM\system\currentcontrolset\services\stisvc\parameters[servicemain]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace[suppressprocessoutput]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[maxfilesize]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace[defaulttraceflags]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[defaulttracemask]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace[defaulttracelevel]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace[defaultmaxtracearraysize]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace[defaultenableobjecttracking]
Queries value: HKLM\system\currentcontrolset\control\stillimage\trace[heapoptions]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[traceflags]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[tracemask]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[tracelevel]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[maxtracearraysize]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[enableobjecttracking]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\trace\wiaservc.dll[heapoptions]
Queries value: HKLM\software\microsoft\rpc\securityservice[10]
Queries value: HKCR\appid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[authenticationlevel]

Queries value: HKCR\appid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[accesspermission]
Queries value: HKCR\clsid\{a1f4e726-8cf1-11d1-bf92-0060081ed811}[]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
Queries value: HKCR\clsid\{b6c292bc-7c88-41ee-8b54-8ec92617e599}[]
Queries value: HKLM\system\currentcontrolset\control\stillimage[deviceid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected[defaulthandler]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\connected[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\connected\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\disconnected[defaulthandler]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\disconnected[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage[defaulthandler]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\emailimage[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\emailimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage[defaulthandler]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\faximage[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\faximage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage[defaulthandler]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\printimage[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\printimage\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton[defaulthandler]
Queries value: HKLM\system\currentcontrolset\control\stillimage\events\scanbutton[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-783ce7a92f22}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-783ce7a92f22}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-783ce7a92f22}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{5f4baad0-4d59-4fcd-b213-783ce7a92f22}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-

759eb35cdf9a}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{d13e3f25-1688-45a0-9743-759eb35cdf9a}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-7105fd3b53b1}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-7105fd3b53b1}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-7105fd3b53b1}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{eabbd70d-a25f-4e90-96a4-7105fd3b53b1}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[name]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[desc]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[icon]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\scanbutton\{ee1ddf29-1c65-4ea6-b5cc-6c15f82b5905}[cmdline]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent[defaulthandler]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\events\stiproxyevent[guid]
Queries value:
HKLM\system\currentcontrolset\control\stillimage\serversettings[shutdownifunuseddelay]
Queries value: HKLM\system\currentcontrolset\services\w32time[type]
Queries value: HKLM\system\currentcontrolset\services\w32time[start]
Queries value: HKLM\system\currentcontrolset\services\w32time[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\w32time[tag]
Queries value: HKLM\system\currentcontrolset\services\w32time[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\w32time[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\w32time[group]
Queries value: HKLM\system\currentcontrolset\services\w32time[objectname]
Queries value: HKLM\system\currentcontrolset\services\w32time[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\dnscache[type]
Queries value: HKLM\system\currentcontrolset\services\dnscache[start]
Queries value: HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\dnscache[tag]
Queries value: HKLM\system\currentcontrolset\services\dnscache[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\dnscache[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\dnscache[group]
Queries value: HKLM\system\currentcontrolset\services\dnscache[objectname]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[type]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[start]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[tag]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[group]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[objectname]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[type]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[start]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[tag]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[group]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\wcmsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\ndisuio[objectname]
Queries value: HKLM\system\currentcontrolset\services\nativewifip[objectname]
Queries value: HKLM\system\currentcontrolset\services\nativewifip[imagepath]
Queries value: HKLM\system\currentcontrolset\services\nativewifip[type]
Queries value: HKLM\system\currentcontrolset\services\nativewifip[pnpflags]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[d905ac1c-65e7-4242-99ea-fe66a8355df8]
Queries value:
HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filtertype]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filterruntype]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[filterclass]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[unbindonattach]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e974-e325-11ce-bfc1-

08002be10318}\{e475cf9a-60cd-4439-a75f-0079ce0e18a1}\ndi[unbindondetach]
Queries value: HKLM\system\currentcontrolset\services\ndisuio[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ndisuio[type]
Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_100e&subsys_001e8086&rev_02\3&267a616a&1&18[driver]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanbh\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanipv6\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005\linkage[upperbind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpnameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[netcfginstanceid]
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}\0008[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0009[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0010[characteristics]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0012[netcfginstanceid]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0011[characteristics]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0012[characteristics]
Queries value: HKLM\system\currentcontrolset\services\ndisuio[pnpflags]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[d086235d-48b9-4e49-
aded-5304bf8f636d]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[b3eee223-d0a9-40cd-
adfc-50f1888138ab]
Queries value: HKLM\system\currentcontrolset\services\ndisuio[legacypause]
Queries value: HKLM\system\currentcontrolset\services\ndisuio[ndisbootstart]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_l2tpminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000\linkage[upperbind]
Queries value: HKLM\system\currentcontrolset\services\wlansvc[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[driver]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003\linkage[upperbind]
Sets/Creates value:
HKLM\system\currentcontrolset\services\nativewifip\parameters[defaultfiltersettings]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip[ndismajorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip[ndisminorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip[drivermajorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\nativewifip[driverminorversion]
Sets/Creates value: HKLM\system\currentcontrolset\services\ndisuio[ndismajorversion]

Sets/Creates value:	HKLM\system\currentcontrolset\services\ndisuio[ndisminorversion]
Sets/Creates value:	HKLM\system\currentcontrolset\services\ndisuio[drivermajorversion]
Sets/Creates value:	HKLM\system\currentcontrolset\services\ndisuio[driverminorversion]
Value changes:	HKLM\system\currentcontrolset\control\wmi\autologger\circular kernel context logger[status]